Horizon 7 でのリモート デスクトップ機能の構成

Horizon 7 7.3.2 での変更点
VMware Horizon 7 7.3

vmware®

最新の技術ドキュメントは、VMware の Web サイト（https://docs.vmware.com/jp/）でご確認いただけます。 このドキュメントに関するご意見およびご感想は、docfeedback@vmware.com までお送りください。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

Horizon 7 でのリモート デスクトップ機能の構成

1

『Horizon 7 でのリモート デスクトップ機能の構成』では、仮想マシン デスクトップまたは RDS ホストに Horizon Agent とともにインストールされるリモート デスクトップ機能を構成する方法について説明します。デスクトップ プール、アプリケーション プール、マシン、およびユーザーの動作を制御するポリシーも構成できます。

対象読者

本書の情報は、仮想マシン デスクトップまたは RDS ホストでリモート デスクトップの機能またはポリシーを構成するすべてのユーザーを対象としています。本書に記載されている情報は、仮想マシンのテクノロジーとデータセンターの操作に精通した、Windows システム管理者向けに書かれています。

リモート デスクトップ機能の構成 2

Horizon Agent とともにインストールされる特定のリモート デスクトップ機能は、コア Horizon 7 リリースおよび Feature Pack アップデートのリリースで更新できます。これらの機能を設定すると、エンド ユーザーのリモート デスクトップ エクスペリエンスを強化できます。

これらの機能には、HTML Access、Unity Touch、フラッシュ URL リダイレクト、HTML5 マルチメディア リダイレクト、リアルタイム オーディオ ビデオ、Windows Media マルチメディア リダイレクト (MMR)、USB リダイレクト、スキャナ リダイレクト、シリアル ポート リダイレクト、URL コンテンツ リダイレクトが含まれます。

HTML Access の詳細については、『VMware Horizon HTML Access のインストールとセットアップ ガイド』ドキュメントを参照してください。USB リダイレクトの詳細については、4 章 リモート デスクトップおよびアプリケーションでの USB デバイスの使用を参照してください。URL コンテンツ リダイレクトの詳細については、3 章 URL コンテンツ リダイレクトの構成を参照してください。

この章には、次のトピックが含まれています。

- Unity Touch の構成
- マルチキャストまたはユニキャスト ストリーミング用の Flash URL リダイレクトの構成
- Flash リダイレクトの構成
- HTML5 マルチメディア リダイレクトの設定
- リアルタイム オーディオビデオの構成
- スキャナ リダイレクトの構成
- シリアル ポート リダイレクトの構成
- Windows Media マルチメディア リダイレクト (MMR) へのアクセスの管理
- クライアント ドライブ リダイレクトへのアクセスの管理
- Skype for Business の構成
- USB またはクライアント ドライブ リダイレクトでの BEAT サイド チャネルの有効化

Unity Touch の構成

Unity Touch を使用すれば、タブレットおよびスマートフォン ユーザーは Windows アプリケーションやファイルの参照、検索、およびオープンを簡単に行ったり、お気に入りのアプリケーションやファイルを選択したり、スタート メニューまたはタスクバーを使用せずに実行しているアプリケーションを切り替えることができます。Unity Touch サイドバーに表示されるデフォルトのお気に入りアプリケーションのリストを構成できます。

Horizon Agent がインストールされた後で、Horizon Agent 構成 ADMX テンプレート ファイル (`vdm_agent.admx`) の [Unity Touch を有効にする] グループ ポリシー設定を使用すると、Unity Touch 機能を無効または有効にできます。

iOS、Android、Chrome OS デバイス向けの VMware Horizon Client ドキュメントには、Unity Touch で提供されるエンド ユーザー機能についての詳細が記載されています。

Unity Touch のシステム要件

Horizon Client をインストールする Horizon Client ソフトウェアおよびモバイル デバイスは、Unity Touch をサポートするために特定のバージョン要件を満たす必要があります。

Horizon 7 デスクトップ

Unity Touch をサポートため、以下のソフトウェアは、エンド ユーザーがアクセスする仮想マシンにインストールする必要があります:

- View Agent 6.0 以降をインストールすることにより、Unity Touch 機能をインストールします。『Horizon 7 での仮想デスクトップのセットアップ』の「仮想マシンへの View Agent のインストール」を参照してください。
- オペレーティング システム：Windows 7（32 ビットまたは 64 ビット）、Windows 8（32 ビットまたは 64 ビット）、Windows 8.1（32 ビットまたは 64 ビット）、Windows Server 2008 R2 または Windows Server 2012 R2、Windows 10（32 ビットまたは 64 ビット）

Horizon Client ソフトウェア

Unity Touch は以下の Horizon Client バージョンでサポートされます:

- Horizon Client for iOS
- Horizon Client for Android
- Horizon Client for Chrome OS

Unity Touch で表示されるお気に入りアプリケーションの構成

Unity Touch 機能を使用すれば、タブレットおよびスマート フォン ユーザーは、Unity Touch スライドバーから Horizon 7 デスクトップ アプリケーションまたはファイルに素早く移動できます。エンド ユーザーはサイドバーにどのお気に入りアプリケーションが表示されるかを指定できますが、利便性のために管理者はお気に入りアプリケーションのデフォルト リストを構成できます。

フローティング割り当てデスクトップ プールを使用する場合、エンド ユーザーが指定するお気に入りのアプリケーションおよびお気に入りのファイルは、Active Directory でローミング ユーザー プロファイルを有効にしない限り、デスクトップから切断すると失われます。

お気に入りのアプリケーションのデフォルト リストは、エンド ユーザーが Unity Touch が有効になっているデスクトップに最初に接続したときに有効になります。ただし、ユーザーが自分のお気に入りのアプリケーション リストを構成すると、デフォルト リストは無視されます。ユーザーのお気に入りのアプリケーション リストは、ユーザーのローミング プロファイルに残り、フローティング プールまたは専用プールで別のマシンにユーザーが接続すると使用できるようになります。

お気に入りのアプリケーションのデフォルト リストを作成し、1 つ以上のアプリケーションが Horizon 7 デスクトップ オペレーティング システムにインストールされない場合やそれらのアプリケーションへのパスが [スタート] メニューに表示されない場合、アプリケーションはお気に入りのリストに表示されません。この動作を使用して、代わりのアプリケーションの異なるセットで複数の仮想マシン イメージに適用できるお気に入りのアプリケーションのマスター デフォルト リストを設定することができます。

たとえば、Microsoft Office と Microsoft Visio が 1 台の仮想マシンにインストールされ、Windows Powershell と VMware vSphere Client が 2 台目の仮想マシンにインストールされている場合、4 つのアプリケーションすべてを含む 1 つのリストを作成できます。インストールされたアプリケーションだけが、それぞれのデスクトップにデフォルトのお気に入りのアプリケーションとして表示されます。

異なる方法を使用して、お気に入りのアプリケーションのデフォルト リストを指定できます。

- デスクトップ プール内の仮想マシンの Windows レジストリに値を追加します
- Horizon Agent インストーラから管理インストール パッケージを作成し、仮想マシンにそのパッケージを配布します
- 仮想マシンのコマンド ラインから Horizon Agent インストーラを実行します

注: Unity Touch では、[スタート] メニューの [プログラム] フォルダにアプリケーションへのショートカットが置かれていると想定しています。ショートカットが [プログラム] フォルダの外に置かれている場合、プリフィクス **Programs** をショートカット パスに追加します。たとえば、`Windows Update.lnk` は `ProgramData\Microsoft\Windows\Start Menu` フォルダに格納されています。デフォルトのお気に入りのアプリケーションとしてこのショートカットをパブリッシュするには、プリフィックス **Programs** をショートカット パスに追加します。たとえば、`"Programs/Windows Update.lnk"` です。

前提条件

- Horizon Agent が仮想マシンにインストールされていることを確認します。
- 仮想マシンに対して管理者権限を持っていることを確認します。この手順では、レジストリ設定を編集する必要はありません。
- フローティング割り当てデスクトップ プールを使用する場合、Active Directory を使用してローミング ユーザー プロファイルを設定します。Microsoft によって提供されている手順に従ってください。

  フローティング割り当てデスクトップ プールのユーザーには、ログインするたびにお気に入りのアプリケーションおよびお気に入りのファイルのリストが表示されます。

手順

- （オプション） Windows レジストリに値を追加してお気に入りのアプリケーションのデフォルト リストを作成します。
  a `regedit` を開き、`HKLM\Software\VMware, Inc.\VMware Unity` レジストリ設定に移動します。

  64 ビット仮想マシンでは、`HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity` ディレクトリに移動します。

  b `FavAppList` と呼ばれる文字列値を作成します。

  c デフォルトのお気に入りのアプリケーションを指定します。

  以下のフォーマットを使用して、[スタート] メニューで使用されるアプリケーションへのショートカット パスを指定します。

  ```
  path-to-app-1|path-to-app-2|path-to-app-3|…
  ```

  例：

  ```
  Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere
  Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010
  Language Preferences.lnk
  ```

- （オプション）Horizon Agent インストーラから管理インストール パッケージを作成してお気に入りのアプリケーションのデフォルト リストを作成します。
  a コマンド ラインから、以下のフォーマットを使用して管理インストール パッケージを作成します。

  ```
  VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""a network share to store
  the admin install package"" UNITY_DEFAULT_APPS=""the list of default favorite apps that
  should be set in the registry"""
  ```

  例：

  ```
  VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-share
  \ViewFeaturePack\"" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of
  Access.lnk|Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows
  PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|Programs/Google
  Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft
  SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|Programs/Skype/Skype.lnk|Programs/
  WebEx/Productivity Tools/WebEx Settings.lnk|"""
  ```

  b 社内で導入されている標準の Microsoft Windows Installer (MSI) 展開ツールを使用して、ネットワーク共有からデスクトップ仮想マシンに管理インストール パッケージを配布します。

- （オプション） 仮想マシンにコマンド ラインで直接 Horizon Agent インストーラを実行してお気に入りのアプリケーションのデフォルト リストを作成します。

  次のフォーマットを使用します。

  ```
  VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /v"/qn UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the registry"""
  ```

  注: 上記のコマンドは、Horizon Agent のインストールと、お気に入りアプリケーションのデフォルト リストの指定を組み合わせたものです。このコマンドを実行する前に Horizon Agent をインストールする必要はありません。

次のステップ

仮想マシンでこのタスクを直接実行した場合（Windows レジストリを編集するか、コマンド ラインから Horizon Agent をインストールすることによって）、新たに構成した仮想マシンをデプロイする必要があります。スナップショットまたはテンプレートを作成してからデスクトップ プールを作成することも、既存のプールを再構成することもできます。または、Active Directory グループ ポリシを作成して新しい構成を導入することができます。

マルチキャストまたはユニキャスト ストリーミング用の Flash URL リダイレクトの構成

Adobe Media Server およびマルチキャストまたはユニキャストを使用して仮想デスクトップ インフラストラクチャ (VDI) 環境でライブ ビデオ イベントを配信できるようになりました。VDI 環境でマルチキャストまたはユニキャストのライブ ビデオ ストリームを配信するには、メディア ストリームを、リモート デスクトップをバイパスしてメディア ソースからエンド ポイントに直接送信する必要があります。Flash URL リダイレクト機能は、リモート デスクトップからクライアント エンドポイントに ShockWave Flash (SWF) ファイルをインターセプトおよびリダイレクトすることで、この機能をサポートします。

そして、Flash コンテンツは、クライアントのローカル Flash メディア プレーヤを使用して表示されます。

Adobe Media Server からクライアント エンドポイントに Flash コンテンツを直接ストリーミングするとデータセンタ ESXi ホストへの負荷が軽減され、データセンタを経由する余分なルーティングが不要になり、複数のクライアント エンドポイントに Flash コンテンツを同時にストリームするために必要となる帯域幅が削減されます。

Flash URL リダイレクト機能は、Web ページの管理者によって HTML Web ページ内に組み込まれた JavaScript を使用します。リモート デスクトップ ユーザーが Web ページ内に指定された URL リンクをクリックすると、JavaScript は SWF ファイルをインターセプトし、リモート デスクトップ セッションからクライアント エンドポイントにリダイレクトします。エンドポイントは次に、リモート デスクトップ セクションの外のローカル Flash Projector を開き、メディア ストリームをローカルで再生します。

Flash URL リダイレクトを構成するには、HTML Web ページおよびクライアント デバイスをセットアップする必要があります。

手順

1 Flash URL リダイレクトのシステム要件

Flash URL リダイレクトをサポートするには、Horizon 7 の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

2 Flash URL リダイレクト機能がインストールされていることの確認

この機能を使用する前に、Flash URL リダイレクト機能がインストールされ、仮想デスクトップで実行されていることを確認します。

3 マルチキャストまたはユニキャストのストリームを提供する Web ページの設定

Flash URL リダイレクトの実行を許可するには、マルチキャストまたはユニキャストのストリームにリンクを提供する MIME HTML (MHTML) Web ページに JavaScript コマンドを組み込む必要があります。ユーザーはビデオ ストリームにアクセスするために、リモート デスクトップのブラウザでこれらの Web ページを表示します。

4 Flash URL リダイレクト用にクライアント デバイスを設定

Flash URL リダイレクト機能は、リモート デスクトップからクライアント デバイスに SWF ファイルをリダイレクトします。これらのデバイスでマルチキャストまたはユニキャストのストリームから Flash ビデオの再生を許可するには、適切な Adobe Flash Player がクライアント デバイスにインストールされていることを確認する必要があります。クライアントは、メディア ソースに対する IP 接続性を持つ必要もあります。

5 Flash URL リダイレクトを無効または有効

Flash URL リダイレクトは、`VDM_FLASH_URL_REDIRECTION=1` プロパティを指定して Horizon Agent のサイレント インストールを実行すると有効になります。選択されたリモート デスクトップの Windows レジストリ キーの値を設定することで、それらの仮想マシンでの Flash URL リダイレクト機能を無効にするか、または再度有効にすることができます。

Flash URL リダイレクトのシステム要件

Flash URL リダイレクトをサポートするには、Horizon 7 の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

Horizon 7 デスクトップ

- Flash URL リダイレクトは、View Agent 6.0 以降のサイレント インストールでコマンド ラインに `VDM_FLASH_URL_REDIRECTION` プロパティを指定することによってインストールします。『Horizon 7 での仮想デスクトップのセットアップ』の「Horizon Agent のサイレント インストールのプロパティ」を参照してください。
- デスクトップは、64 ビットまたは 32 ビットの Windows 7 オペレーティング システムで実行する必要があります。

- サポートされているデスクトップ ブラウザには、Internet Explorer 8、9、および 10、Chrome 29.*x*、および Firefox 20.*x* が含まれます。

Flash メディア プレイヤーと ShockWave Flash (SWF)

Strobe Media Playback などの適切な Flash メディア プレイヤーを、お使いの Web サイトに統合する必要があります。マルチキャスト コンテンツをストリーミングするには、お使いの Web ページで `multicastplayer.swf` または `StrobeMediaPlayback.swf` を使用できます。ライブのユニキャスト コンテンツをストリーミングするには、`StrobeMediaPlayback.swf` を使用する必要があります。RTMP ストリーミングや HTTP ダイナミック ストリーミングなどの、サポートされる他の機能には、`StrobeMediaPlayback.swf` も使用できます。

Horizon Client ソフトウェア

次の Horizon Client リリースは、マルチキャストとユニキャストをサポートしています。

- Horizon Client 2.2 for Linux または以降のリリース
- Horizon Client 2.2 for Windows 以降のリリース

以下の Horizon Client リリースはマルチキャストのみをサポートしています (ユニキャストはサポートしていません)。

- Horizon Client 2.0 or 2.1 for Linux
- Horizon Client 5.4 for Windows

Horizon Client コンピュータまたはクライアント アクセス デバイス

- Flash URL リダイレクトは、x86 シン クライアント デバイスで Horizon Client for Linux を実行するすべてのオペレーティング システムでサポートされます。この機能は ARM プロセッサではサポートされません。
- Flash URL リダイレクトは、Horizon Client for Windows を実行するすべてのオペレーティング システムでサポートされます。詳細については、『VMware Horizon Client for Windows の使用』を参照してください。
- Windows クライアント デバイスでは、Internet Explorer 用の Adobe Flash Player 10.1 以降をインストールする必要があります。
- Linux シン クライアント デバイスでは、`libexpat.so.0` と `libflashplayer.so` ファイルをインストールする必要があります。Flash URL リダイレクト用にクライアント デバイスを設定を参照してください。

注: Flash URL リダイレクトを使用すれば、マルチキャストまたはユニキャストのストリームは、社内のファイアウォールの外にあるクライアント デバイスにリダイレクトされます。クライアントは、マルチキャストまたはユニキャストのストリーミングを開始する ShockWave Flash (SWF) ファイルをホストする Adobe Web サーバにアクセスする必要があります。必要に応じて、クライアント デバイスがこのサーバにアクセスすることを許可するために適切なポートを開くようにファイアウォールを構成します。

Flash URL リダイレクト機能がインストールされていることの確認

この機能を使用する前に、Flash URL リダイレクト機能がインストールされ、仮想デスクトップで実行されていることを確認します。

Flash URL リダイレクト機能は、マルチキャストまたはユニキャストのリダイレクトを使用するすべてのデスクトップにインストールしておく必要があります。Horizon Agent のインストール手順については、『Horizon 7 での仮想デスクトップのセットアップ』の「Horizon Agent のサイレント インストールのプロパティ」を参照してください。

手順

1 PCoIP を使用するリモート デスクトップ セッションを開始します。

2 タスク マネージャを開きます。

3 `ViewMPServer.exe` プロセスがデスクトップで動作していることを確認します。

マルチキャストまたはユニキャストのストリームを提供する Web ページの設定

Flash URL リダイレクトの実行を許可するには、マルチキャストまたはユニキャストのストリームにリンクを提供する MIME HTML (MHTML) Web ページに JavaScript コマンドを組み込む必要があります。ユーザーはビデオ ストリームにアクセスするために、リモート デスクトップのブラウザでこれらの Web ページを表示します。

また、Flash URL リダイレクトで問題が発生した場合にエンド ユーザーに対して表示される英語のエラー メッセージをカスタマイズできます。各国語のエラー メッセージをエンド ユーザーに対して表示する場合は、このオプションの手順を実行します。`var vmwareScriptErroMessage` 構成を各国語のテキスト文字列と一緒に MHTML Web ページに埋め込む必要があります。

前提条件

`swfobject.js` ライブラリが MHTML Web ページにインポートされていることを確認します。

手順

1 MHTML Web ページに `viewmp.js` JavaScript コマンドを組み込みます。

例：`<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`

2 （オプション） エンド ユーザーに送信される Flash URL リダイレクトのエラー メッセージをカスタマイズします。

例：`"var vmwareScriptErroMessage=`*`localized error message`*`"`

3 ShockWave Flash (SWF) ファイルが MHTML Web ページにインポートされる前に、`viewmp.js` JavaScript コマンドを埋め込んだことを確認し、オプションで Flash URL リダイレクトのエラー メッセージをカスタマイズします。

ユーザーがリモート デスクトップで Web ページを表示すると、`viewmp.js` JavaScript コマンドがリモート デスクトップで Flash URL リダイレクト機能を起動し、デスクトップからホスティングしているクライアント デバイスに SWF ファイルをリダイレクトします。

Flash URL リダイレクト用にクライアント デバイスを設定

Flash URL リダイレクト機能は、リモート デスクトップからクライアント デバイスに SWF ファイルをリダイレクトします。これらのデバイスでマルチキャストまたはユニキャストのストリームから Flash ビデオの再生を許可するには、適切な Adobe Flash Player がクライアント デバイスにインストールされていることを確認する必要があります。クライアントは、メディア ソースに対する IP 接続性を持つ必要もあります。

注: Flash URL リダイレクトを使用すれば、マルチキャストまたはユニキャストのストリームは、社内のファイアウォールの外にあるクライアント デバイスにリダイレクトされます。クライアントは、マルチキャストまたはユニキャストのストリーミングを開始する SWF ファイルをホストする Adobe Web サーバにアクセスする必要があります。必要に応じて、クライアント デバイスがこのサーバにアクセスすることを許可するために適切なポートを開くためにファイアウォールを構成します。

手順

- クライアント デバイスに Adobe Flash Player をインストールします。

オペレーティング システム	操作
Windows	Internet Explorer 用に Adobe Flash Player 10.1 以降をインストールします。
Linux	a `libexpat.so.0` ファイルをインストールするか、このファイルが既にインストールされていることを確認します。 ファイルが `/usr/lib` または `/usr/local/lib` ディレクトリにインストールされていることを確認します。 b `libflashplayer.so` ファイルをインストールするか、このファイルが既にインストールされていることを確認します。 このファイルが Linux オペレーティング システムの適切な Flash プラグイン ディレクトリにインストールされていることを確認します。 c `wget` プログラムをインストールするか、プログラム ファイルが既にインストールされていることを確認します。

Flash URL リダイレクトを無効または有効

Flash URL リダイレクトは、`VDM_FLASH_URL_REDIRECTION=1` プロパティを指定して Horizon Agent のサイレント インストールを実行すると有効になります。選択されたリモート デスクトップの Windows レジストリ キーの値を設定することで、それらの仮想マシンでの Flash URL リダイレクト機能を無効にするか、または再度有効にすることができます。

手順

1 仮想マシンで Windows レジストリ エディタを起動します。

2 Flash URL リダイレクトを制御する Windows レジストリ キーに移動します。

オプション	説明
Windows 7 64 ビット	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware ViewMP\enabled = value`
Windows 7 32 ビット	`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware ViewMP\enabled = value`

3 Flash URL リダイレクトを無効化または有効化する値を設定します。

オプション	値
無効	`0`
有効	`1`

デフォルトでは、値は 1 に設定されます。

Flash リダイレクトの構成

エンドユーザーが Internet Explorer 9、10 または 11 を使用している場合、Flash リダイレクトは Flash コンテンツをクライアント システムに送信します。これにより、ESXi ホストの負荷が軽減されます。クライアント システムは、Flash Player ActiveX バージョンを使用し、Flash コンテナ ウィンドウでメディア コンテンツを再生します。

この機能の名前は Flash URL リダイレクトと呼ばれる機能と似ていますが、次の表に示す大きな違いがあります。

表 2-1. Flash リダイレクト機能と Flash URL リダイレクトの比較

差異項目	Flash リダイレクト	Flash URL リダイレクト
この機能をサポートする Horizon Client のタイプ	Windows クライアントのみ	Windows クライアントおよび Linux クライアント
表示プロトコル	PCoIP および VMware Blast。	PCoIP
ブラウザ	Internet Explorer 9、10 または 11（リモート デスクトップ）	Horizon Client および Horizon Agent で現在サポートされているすべてのブラウザ
構成メカニズム	Horizon Agent グループ ポリシー設定を使用して、Flash リダイレクトを使用または使用しない Web サイトのリスト（ホワイトリストまたはブラックリスト）を指定します。	必要な JavaScript を埋め込むには、Web ページのソース コードを変更します。

機能制限

Flash リダイレクト機能には次の制限があります。

- Flash Player ウィンドウ内の URL リンクをクリックすると、リモート デスクトップ（エージェント側）ではなくクライアントのブラウザが開きます。
- 一部のブラウザ バージョンでは、Flash リダイレクトと連携しない Web サイトもあります。たとえば、Internet Explorer 11 を使用している場合、vimeo.com の Web サイトは機能しません。

- Flash と Java のスクリプトは期待どおりに動作しない可能性があります。
- Flash コンテンツの再生時に Horizon Client ウィンドウがフリーズする可能性があります。ただし、Windows レジストリ キーを設定してこの問題を回避できます。

  32 ビット クライアントでは `HKLM\Software\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer` 値を「FALSE」に設定し、64 ビット クライアントでは `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer` を「FALSE」に設定します。
- YouTube では Flash メディアがサポートされなくなりました。
- Flash リダイレクトは、redbox.com では動作しません。
- [Flash] コンテキスト メニュー（右クリックで有効化）は無効です。
- Horizon Client 4.1 が PCoIP でリモート デスクトップに接続すると、Flash リダイレクトが失敗します。Horizon Client がリモート デスクトップのネイティブのプレーヤーで Flash コンテンツを再生するか、または白色の画面が表示されます。

Flash リダイレクトのシステム要件

Horizon Agent と Horizon Client、エージェントとクライアント ソフトウェアをインストールするリモート デスクトップとクライアント システムは、Flash リダイレクト機能をサポートする特定の要件を満たす必要があります。

リモート デスクトップ

- Horizon Agent 7.0 以降の場合、Flash リダイレクト カスタム セットアップ オプションを選択されている仮想デスクトップにインストールする必要があります。Flash リダイレクト カスタム セットアップ オプションはデフォルトで選択されていません。『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントで、Horizon Agent のインストールに関するトピックを参照してください。
- 適切なグループ ポリシー設定が構成されている必要があります。Flash リダイレクトのインストールと構成を参照してください。
- Flash リダイレクトは、Windows 7、Windows 8、Windows 8.1、Windows 10 の仮想デスクトップでサポートされています。
- Internet Explorer 9、10、または 11 が、対応する Flash ActiveX プラグインとともにインストールされている必要があります。
- インストールした後に、VMware View FlashMMR Server アドオンを Internet Explorer で有効にする必要があります。

Horizon Client コンピュータまたはクライアント アクセス デバイス

- Horizon Client 4.0 以降がインストールされている必要があります。Flash リダイレクト オプションはデフォルトで有効です。『VMware Horizon Client for Windows のインストールとセットアップ ガイド』ドキュメントで、Horizon Client のインストールに関するトピックを参照してください。
- Flash リダイレクトは、Windows 7、Windows 8、Windows 8.1、および Windows 10 でサポートされています。

	■ Flash ActiveX プラグインがインストールされ、有効になっている必要があります
リモート セッションの表示プロトコル	■ PCoIP ■ VMware Blast（Horizon Agent 7.0 以降が必要）

Flash リダイレクトのインストールと構成

リモート デスクトップからローカル クライアント システムの Flash Player ウィンドウに Flash コンテンツをリダイレクトするには、Flash リダイレクト機能と Internet Explorer をリモート デスクトップとクライアント システムにインストールし、この機能を使用する Web サイトを指定する必要があります。

この機能を有効にして、この機能を使用する Web サイトを指定するには、グループ ポリシー設定を使用します。あるいは、リモート デスクトップの Windows レジストリ設定を使用して、Flash リダイレクトで使用する Web サイトのホワイト リストを設定することもできます。Windows レジストリ設定を使用した Flash リダイレクトの構成を参照してください。

前提条件

- クライアント システムに Horizon Client をインストールし、Flash リダイレクトが有効になっているリモート デスクトップに Horizon Agent をインストールします。必要なバージョン、セットアップ オプション、詳細なシステム要件については、Flash リダイレクトのシステム要件を参照してください。
- Active Directory サーバをホストするマシンに管理者ドメイン ユーザーとしてログインできることを確認します。
- MMC およびグループ ポリシー オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。
- Horizon Agent 設定 ADMX テンプレート ファイル (`vdm_agent.admx`) をリモート デスクトップの組織単位 (OU) に追加します。インストール手順については、Active Directory への ADMX テンプレート ファイルの追加を参照してください。
- Flash コンテンツのリダイレクトを許可する Web サイトのリスト（ホワイト リスト）または許可しない Web サイトのリスト（ブラック リスト）を編集します。
- Flash ActiveX がインストールされており適切に動作することを確認します。インストールを確認するには、Internet Explorer を実行して https://helpx.adobe.com/flash-player.html に移動します。

手順

1 必要であれば、NPAPI バージョンではなく、Flash Player の ActiveX バージョンをクライアント システムにインストールします。

Internet Explorer 10 および 11 の場合、Flash Player はデフォルトでインストールされています。Internet Explorer 9 の場合、必要に応じて https://get.adobe.com/flashplayer/にアクセスし、Flash Player をダウンロードしてインストールします。

2 リモート デスクトップで、次のインストール手順を実行します。

a Internet Explorer 9、10、または 11 をインストールします。

b 必要であれば、NPAPI バージョンではなく、Flash Player の ActiveX バージョンをインストールします。

Internet Explorer 10 および 11 の場合、Flash Player はデフォルトでインストールされています。Internet Explorer 9 の場合、必要に応じて https://get.adobe.com/flashplayer/にアクセスし、Flash Player をダウンロードしてインストールします。

3 リモート デスクトップで、Internet Explorer のメニュー バーから [ツール] - [アドオンの管理] を選択し、[VMware View FlashMMR サーバ] が表示されていて有効になっていることを確認します。

4 Active Directory サーバで、グループ ポリシー管理エディタを開き、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Agent の構成] - [VMware FlashMMR] フォルダの順に移動し、Flash リダイレクト ポリシーを設定します。

設定	説明
Flash マルチメディア リダイレクトを有効にする	リモート デスクトップ（エージェント側）で Flash リダイレクト (FlashMMR) を有効にするかどうかを指定します。この機能が有効になっている場合、Flash マルチメディア データが指定の URL から TCP チャネルを介してクライアントに転送され、クライアント システムでローカル Flash Player が起動します。この機能により、エージェント側の CPU およびネットワーク バンド幅の負荷が大幅に減少します。
FlashMMR を有効にする長方形の最小サイズ	Flash コンテンツが再生される長方形の幅と高さの最小値をピクセル単位で指定します。たとえば、**400,300** と指定すると、幅が 400 ピクセル、高さが 300 ピクセルになります。Flash コンテンツがこのポリシーで指定した値以上になっている場合にのみ Flash リダイレクトが使用されます。GPO が構成されていない場合、デフォルト値の **320,200** が使用されます。

5 Active Directory サーバで、グループ ポリシー管理エディタを開き、[ユーザーの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Agent の構成] - [VMware FlashMMR] フォルダの順に移動し、Flash リダイレクト ポリシーを設定します。

a Flash リダイレクトで使用するホスト URL のリストを定義するには、[FlashMMR URL リストの使用方法の定義] の設定を開き、[有効] を選択します。

b [FlashMMR URL リストの使用方法の定義] ドロップダウン メニューで、[ホワイト リストを有効にする] または [ブラック リストを有効にする] を選択し、[OK] をクリックします。

デフォルトでは、ホワイト リストが有効になります。

c Flash リダイレクトを使用または使用しないホスト URL のリストを追加するには、[FlashMMR を有効にするホストの URL リスト] の設定を開き、[有効] を選択します。

d [表示] をクリックして、ホワイト リストまたはブラック リストで編集した完全な URL を [値名] 列に入力します。

URL には `http://` または `https://` プリフィックスを含めます。正規表現を使用できます。たとえば、`https://*.google.com` や `http://www.cnn.com/*` を指定できます。

必要であれば、[値] 列で `requireIECompatibility=true` または `appMode=0`、あるいは両方を指定できます。カンマを使用して 2 つの文字列を区切ります。

デフォルトでは、Flash リダイレクトの実行中に外部インターフェイス サポートを有効にすると、パフォーマンスが低下する可能性があります。`appMode=0` を設定すると、パフォーマンスが向上し、ユーザーの操作性が向上する場合もあります。

e [OK] をクリックして URL リストを保存します。[OK] をもう一度クリックしてポリシー設定を保存します。

6 リモート デスクトップでコマンド プロンプトを開き、`%Program Files%\Common Files\VMware\Remote Experience` ディレクトリに移動します。

7 Internet Explorer にホワイト リストまたはブラック リストを追加するには、`cscript mergeflashmmrwhitelist.vbs` コマンドを実行します。

8 Internet Explorer を再起動します。

`requireIECompatibility=true` パラメータが設定されたサイトは、Internet Explorer の [互換表示] に追加されます。互換表示でサイトを確認するには、メニュー バーから [ツール] - [互換設定表示] を選択します。

これらのサイトは、Internet Explorer の信頼済みサイトのリストにも追加されます。信頼済みサイトを確認するには、Internet Explorer のメニュー バーから [ツール] - [インターネット オプション] の順に選択し、[セキュリティ] タブで [サイト] をクリックします。

Windows レジストリ設定を使用した Flash リダイレクトの構成

Active Directory サーバに対する管理者権限がないドメイン ユーザーは、代わりにリモート デスクトップで Windows レジストリ キーに適切な値を設定して、Flash リダイレクトを構成できます。

この手順は、Flash リダイレクトの設定にグループ ポリシーを使用する代わりに使用できます。

前提条件

- リストに指定された URL のみが Flash コンテンツをリダイレクトするように、Web サイトのホワイト リストを編集します。Windows レジストリの設定を使用して、ブラック リストを有効にすることはできません。ブラック リストを有効にするには、Flash リダイレクトのグループ ポリシー設定を使用します。
- リモート デスクトップに Horizon Agent 7.0 以降、Flash Player、Internet Explorer 9、10 または 11 がインストールされていることを確認します。Flash リダイレクトのシステム要件を参照してください。
- クライアント システムに Horizon Client 4.0 以降と Flash Player ActiveX バージョンがインストールされていることを確認します。

手順

1 Horizon Client を使用して、リモート デスクトップにアクセスします。

2 リモート デスクトップで Windows レジストリ エディタ (`regedit.exe`) を開き、`HKLM\Software\VMware, Inc.\VMware FlashMMR` フォルダに移動して、[FlashRedirection] を **`1`** に設定します。

注: この設定により、Flash リダイレクト機能が有効になります。この設定が無効になっている場合（`HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR` で 0 に設定されている場合）、ドメイン全体で Flash リダイレクトが無効になります。この機能は、ドメイン管理者が有効にする必要があります。

3 `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR` フォルダに移動します。

このフォルダが存在しない場合は作成します。

4 `VMware FlashMMR` フォルダで、[UrlWhiteList] というサブキーを作成します。

5 [UrlWhiteList] キーを右クリックして、[新規] - [文字列値] の順に選択し、Flash リダイレクトを使用する Web サイトの URL を名前に入力します。

正規表現を使用できます。たとえば、 **`https://*.google.com`** と指定します。[データ] の値は空白のままにします。

6 （オプション） 新しいレジストリ値のデータ フィールドで、**`requireIECompatibility=true`** または **`appMode=0`**、あるいはその両方を追加します。

カンマを使用して 2 つの文字列を区切ります。デフォルトでは、Flash リダイレクトの実行中に外部インターフェイス サポートを有効にすると、パフォーマンスが低下する可能性があります。**`appMode=0`** を設定するとパフォーマンスが向上し、**`appMode=1`** を設定するとユーザーの操作性が向上する場合もあります。

7 追加の URL を追加するには、前の手順を繰り返してレジストリ エディタを終了します。

8 リモート デスクトップでコマンド プロンプトを開き、`%Program Files%\Common Files\VMware\Remote Experience` ディレクトリに移動します。

9 Internet Explorer にホワイト リストを追加するには、`cscript mergeflashmmrwhitelist.vbs` コマンドを実行します。

10 Internet Explorer を再起動します。

`requireIECompatibility=true` パラメータ が設定されたサイトは、Internet Explorer の [互換表示] に追加されます。互換表示でサイトを確認するには、メニュー バーから [ツール] - [互換設定表示] を選択します。

これらのサイトは、Internet Explorer の信頼済みサイトのリストにも追加されます。信頼済みサイトを確認するには、Internet Explorer のメニュー バーから [ツール] - [インターネット オプション] の順に選択し、[セキュリティ] タブで [サイト] をクリックします。

HTML5 マルチメディア リダイレクトの設定

エンドユーザーが Chrome ブラウザを使用している場合、HTML5 マルチメディア リダイレクトは HTML5 マルチメディア コンテンツをクライアント システムに送信します。これにより、ESXi ホストの負荷が軽減されます。クライアント システムがマルチメディア コンテンツを再生するので、オーディオとビデオのユーザー エクスペリエンスが向上します。

HTML5 マルチメディア リダイレクトのシステム要件

Horizon Agent と Horizon Client、エージェントとクライアント ソフトウェアをインストールするリモート デスクトップとクライアント システムは、HTML5 マルチメディア リダイレクト機能をサポートする特定の要件を満たす必要があります。

リモート デスクトップ	■ HTML5 マルチメディア リダイレクト カスタム セットアップ オプションを選択して、仮想デスクトップに Horizon Agent 7.3 以降がインストールされている必要があります。デフォルトではこのオプションが選択されていません。『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントで、Horizon Agent のインストールに関するトピックを参照してください。 ■ HTML5 マルチメディア リダイレクト カスタム セットアップ オプションを選択して、公開デスクトップの RDS ホストに Horizon Agent 7.3 以降がインストールされている必要があります。デフォルトではこのオプションが選択されていません。『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』ドキュメントで、Horizon Agent のインストールに関するトピックを参照してください。 ■ Active Directory サーバで HTML5 マルチメディア リダイレクトのグループ ポリシー設定が使用されている必要があります。HTML5 マルチメディア リダイレクトのインストールと設定を参照してください。 ■ Chrome ブラウザがインストールされている必要があります。 ■ Chrome ブラウザに VMware Horizon HTML5 マルチメディア リダイレクト拡張機能がインストールされている必要があります。VMware Horizon HTML5 リダイレクト拡張機能の強制インストールを参照してください。
クライアント システム	■ HTML5 マルチメディア リダイレクト サポートのカスタム セットアップ オプションを選択して、Horizon Client 4.6 以降がインストールされている必要があります。このオプションはデフォルトで選択されています。『VMware Horizon Client for Windows のインストールとセットアップ ガイド』ドキュメントで、Horizon Client のインストールに関するトピックを参照してください。Windows 以外のクライアント システムはサポートされていません。
リモート セッションの表示プロトコル	■ PCoIP ■ VMware Blast

HTML5 マルチメディア リダイレクトのインストールと設定

リモート デスクトップからローカル クライアント システムに HTML5 マルチメディア コンテンツをリダイレクトするには、リモート デスクトップに HTML5 マルチメディア リダイレクト機能と Chrome ブラウザをインストールし、HTML5 マルチメディア リダイレクト機能を有効にして、この機能を使用する Web サイトを指定する必要があります。

HTML5 マルチメディア リダイレクトを有効にし、この機能を使用する Web サイトを指定するには、Active Directory サーバでグループ ポリシーを設定します。HTML5 マルチメディア コンテンツをリダイレクトする Web サイトの URL のリストを編集する必要があります。URL には、`http://` または `https://` プリフィックスが含まれます。一致したパターンを URL で使用できます。たとえば、YouTube 上のすべてのビデオをリダイレクトするには、`https://www.youtube.com/*` と指定します。Vimeo 上のすべてのビデオをリダイレクトするには、`https://www.vimeo.com/*` と指定します。詳細については、https://developer.chrome.com/extensions/match_patterns を参照してください。

前提条件

- クライアント システムに Horizon Client をインストールし、HTML5 マルチメディア リダイレクト機能が有効なリモート デスクトップに Horizon Agent をインストールします。必要なバージョン、セットアップ オプション、詳細なシステム要件については、HTML5 マルチメディア リダイレクトのシステム要件を参照してください。
- Active Directory サーバをホストするマシンに管理者ドメイン ユーザーとしてログインできることを確認します。
- MMC およびグループ ポリシー オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。
- 仮想デスクトップの場合には組織単位 (OU)、公開アプリケーションの場合には RDS ホストにリンクしている GPO に、Horizon Agent 設定の ADMX テンプレート ファイル (`vdm_agent.admx`) を追加します。インストール手順については、Active Directory への ADMX テンプレート ファイルの追加を参照してください。
- HTML5 マルチメディア コンテンツをリダイレクトする Web サイトの URL リストを編集します。

手順

1. リモート デスクトップに Chrome ブラウザをインストールします。
2. Active Directory サーバでグループ ポリシー管理エディタを開き、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Agent の構成] - [VMware HTML5 マルチメディア リダイレクト] フォルダに移動します。
3. [VMware HTML5 マルチメディア リダイレクトを有効にする] の設定を開き、[有効] を選択して [OK] をクリックします。
4. [VMware HTML5 マルチメディア リダイレクトの URL リストを有効にします] の設定を開き、[有効] をクリックします。
5. [表示] をクリックして、[値名] 列で編集した URL を入力します。

   指定した URL にのみ HTML5 マルチメディア コンテンツをリダイレクトできます。デフォルトでは、URL は追加されていません。[値] 列は空白のままにします。
6. [OK] をクリックして URL リストを保存します。さらに、[OK] をクリックしてポリシー設定を保存します。

次のステップ

リモート デスクトップの Chrome ブラウザに、VMware Horizon HTML5 リダイレクト拡張機能を強制的にインストールします。VMware Horizon HTML5 リダイレクト拡張機能の強制インストールを参照してください。

VMware Horizon HTML5 リダイレクト拡張機能の強制インストール

HTML5 マルチメディア リダイレクト機能を使用するには、リモート デスクトップに VMware Horizon HTML5 リダイレクトの拡張機能を強制的にインストールする必要があります。拡張機能を強制インストールするには、Active Directory サーバで Google Chrome グループ ポリシー設定を使用します。

Chrome グループ ポリシー設定をリモート デスクトップに適用するには、Active Directory サーバの GPO に ADMX テンプレート ファイルを追加する必要があります。仮想デスクトップの場合には、GPO が仮想デスクトップを含む組織単位 (OU) にリンクする必要があります。公開デスクトップの場合には、RDS ホストを含む OU に GPO をリンクする必要があります。

前提条件

- HTML5 マルチメディア リダイレクト機能を設定します。HTML5 マルチメディア リダイレクトのインストールと設定を参照してください。
- Active Directory サーバをホストするマシンに管理者ドメイン ユーザーとしてログインできることを確認します。
- MMC およびグループ ポリシー オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。

手順

1 Google Chrome `policy_templates.zip` ファイルを https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip からダウンロードします。

2 `policy_templates.zip` ファイルを展開して、`chrome.admx` ファイルと `chrome.adml` ファイルを Active Directory サーバにコピーします。

   `\windows\admx` フォルダの `chrome.admx` ファイルと `chrome.adml` ファイルは、`policy_templates.zip` ファイルの `\windows\admx\`*`language`* フォルダにあります。

   a `chrome.admx` ファイルを Active Directory サーバの `%systemroot%\PolicyDefinitions` フォルダにコピーします。

   b Active Directory サーバの `%systemroot%\PolicyDefinitions` で、適切な言語のサブフォルダに `chrome.adml` 言語リソース ファイルをコピーします。

   たとえば、`chrome.adml` ファイルの `en_us` バージョンを Active Directory サーバの `%systemroot%\PolicyDefinitions\en_us` サブフォルダにコピーします。

3 Active Directory サーバでグループ ポリシー管理エディタを開き、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [Google Chrome] - [拡張機能] フォルダの順に移動します。

4 [強制的にインストールされたアプリと拡張機能のリストを設定] ポリシー設定を開き、[有効] をクリックします。

5 [表示] をクリックして、[値] 列に **`ljmaegmnepbgjekghdfkgegbckolmcok;https://clients2.google.com/service/update2/crx`** を入力します。

6 [OK] をクリックして、拡張機能の ID/更新 URL を保存し、[OK] をクリックしてポリシー設定を保存します。

7 リモート デスクトップに HTML5 マルチメディア リダイレクト拡張機能がインストールされていることを確認します。

a リモート デスクトップに接続し、Chrome を開始します。

b Chrome のアドレス バーに **chrome://extensions** を入力します。

[VMware Horizon HTML5 リダイレクト拡張機能] が [拡張機能] リストに表示されます。

リアルタイム オーディオビデオの構成

リアルタイム オーディオ ビデオを利用すると、Horizon 7 ユーザーは Skype、Webex、Google Hangouts や他のオンライン会議アプリケーションをリモート デスクトップで実行できます。リアルタイム オーディオ ビデオを使用すれば、クライアント システムにローカルで接続される webcam およびオーディオ デバイスは、リモート デスクトップにリダイレクトされます。この機能は、USB リダイレクトを使用して達成できるよりも大幅に低いバンド幅でビデオおよびオーディオ データをデスクトップにリダイレクトします。

リアルタイム オーディオ ビデオは、標準的な会議アプリケーションおよびブラウザベースのビデオ アプリケーションと互換性があり、標準的な webcam、オーディオ USB デバイス、およびアナログ オーディオ入力をサポートします。

この機能は、VMware Virtual Webcam および VMware Virtual Microphone をデスクトップ オペレーティング システムにインストールします。VMware Virtual Web カメラは、ブラウザ ベースのビデオ アプリケーションや他のサードパーティ製の会議ソフトウェアとの高度な互換性を備えたカーネル モードの Web カメラドライバを使用します。

会議アプリケーションやビデオ アプリケーションが起動すると、VMware 仮想デバイスを表示および使用します。これらの VMware 仮想デバイスは、クライアントでローカル接続されたデバイスからのオーディオ ビデオ リダイレクトを処理します。VMware Virtual Web カメラおよび VMware Virtual Microphone は、デスクトップ オペレーティング システムのデバイス マネージャに表示されます。

オーディオおよび Web カメラデバイス用のドライバは、リダイレクトを有効にするために Horizon Client システムにインストールする必要があります。

リアルタイム オーディオ ビデオの構成の選択

リアルタイム オーディオ ビデオと共に Horizon Agent をインストール後、この機能はさらに構成しなくとも Horizon 7 デスクトップで動作します。Web カメラ フレーム レートおよび画像解像度のデフォルト値は、ほとんどの標準デバイスおよびアプリケーションで推奨されます。

グループ ポリシ設定を構成して、これらのデフォルト値を変更して、特定のアプリケーション、Web カメラ、または環境に適応することができます。ポリシーを設定して機能をすべて無効または有効にすることもできます。ADMX テンプレート ファイルにより、Active Directory または個々のデスクトップにリアルタイム オーディオ ビデオ グループ ポリシー設定をインストールできます。リアルタイム オーディオ ビデオ グループ ポリシ設定の構成を参照してください。

クライアント コンピュータに内蔵または接続されている複数の Web カメラおよびオーディオ入力デバイスがある場合、デスクトップにリダイレクトされる優先される Web カメラおよびオーディオ入力デバイスを構成できます。優先される Web カメラとマイクロフォンを選択を参照してください。

注: 優先されるオーディオ デバイスを選択できますが、他のオーディオ構成オプションは使用できません。

Web カメラ画像およびオーディオ入力がリモート デスクトップにリダイレクトされると、ユーザーはローカル コンピュータの Web カメラおよびオーディオ デバイスにアクセスできません。逆に言えば、これらのデバイスがローカル コンピュータで使用中であれば、リモート デスクトップでそれらにアクセスできません。

サポートされるアプリケーションについては、VMware ナレッジベースの記事『Guidelines for Using Real-Time Audio-Video with 3rd-Party Applications on Horizon View Desktops (リアルタイム オーディオ-ビデオを Horizon View デスクトップのサードパーティ アプリケーションで使用するためのガイドライン)』(http://kb.vmware.com/kb/2053754) を参照してください。

リアルタイム オーディオ ビデオのシステム要件

リアルタイム オーディオビデオは、標準的な webcam、USB オーディオ、およびアナログ オーディオ デバイス、そして Skype、WebEx、および Google Hangouts などの標準的な会議アプリケーションで動作します。リアルタイム オーディオビデオをサポートするには、Horizon 環境が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

リモート デスクトップ	View Agent 6.0 以降または Horizon Agent 7.0 以降をインストールすることにより、リアルタイム オーディオビデオ機能をインストールします。公開されたデスクトップとアプリケーションでこの機能を使用するには、Horizon Agent 7.0.2 以降をインストールする必要があります。Horizon Agent のインストールについては、各セットアップ ガイドを参照してください。
Horizon Client ソフトウェア	Horizon Client 2.2 for Windows 以降のリリース Horizon Client 2.2 for Linux 以降のリリース。Horizon Client for Linux 3.1 以前の場合、この機能はサードパーティ ベンダーによって提供される Horizon Client for Linux のバージョンでのみ使用できます。Horizon Client for Linux 3.2 以降の場合、この機能は VMware から入手できるクライアントのバージョンでも入手できます。 Horizon Client 2.3 for Mac 以降のリリース Horizon Client 4.0 for iOS 以降のリリース。 Horizon Client 4.0 for Android 以降のリリース。
Horizon Client コンピュータまたはクライアント アクセス デバイス	■ Horizon Client for Windows を実行するすべてのオペレーティング システム。 ■ x86 デバイスで Horizon Client for Linux を実行するすべてのオペレーティング システム。この機能は ARM プロセッサではサポートされません。 ■ Mac OS X Mountain Lion (10.8) 以降。それよりも前のすべての Mac OS X オペレーティング システムでは無効になっています。

- Horizon Client for iOS を実行するすべてのオペレーティング システム。
- Horizon Client for Android を実行するすべてのオペレーティング システム。
- サポートされているクライアント オペレーティング システムについては、『Horizon Client のインストール』と該当するシステムまたはデバイスのセットアップ ドキュメントを参照してください。
- webcam およびオーディオ デバイス ドライバをインストールする必要があり、webcam およびオーディオ デバイスがクライアント コンピュータで操作可能である必要があります。
- リアルタイム オーディオビデオをサポートするために、エージェントがインストールされているリモート デスクトップ オペレーティング システムにデバイス ドライバをインストールする必要はありません。

表示プロトコル

- PCoIP
- VMware Blast（Horizon Agent 7.0 以降が必要）

リアルタイム オーディオ ビデオが USB リダイレクトの代わりに使用されることを確認

リアルタイム オーディオ ビデオは、会議アプリケーションでの使用のために、Web カメラおよびオーディオ入力のリダイレクトをサポートします。Horizon Agent でインストールできる USB リダイレクト機能は Web カメラのリダイレクトをサポートしません。オーディオ入力デバイスを USB リダイレクト経由でリダイレクトすると、オーディオ ストリームはリアルタイム オーディオビデオ セッション中にビデオと適切に同期せず、ネットワーク帯域幅の要求を抑制する利点が失われます。Web カメラおよびオーディオ入力デバイスが USB リダイレクトではなくリアルタイム オーディオ ビデオ経由でデスクトップにリダイレクトされるように対策を講じることができます。

デスクトップが USB リダイレクトで構成されている場合、エンド ユーザーは Windows クライアント メニュー バーの [USB デバイスの接続] オプションを選択するか、または Mac クライアントの [デスクトップ > USB] メニューを選択することで、ローカルに接続されている USB デバイスに接続および表示できます。Linux クライアントはデフォルトでオーディオおよびビデオ デバイスの USB リダイレクトをブロックし、エンド ユーザーに USB デバイス オプションを提供しません。

エンド ユーザーが [USB デバイスの接続] または [デスクトップ > USB] リストから USB デバイスを選択すると、そのデバイスはビデオまたはオーディオ会議に使用できなくなります。たとえば、ユーザーが Skype 電話をかけている場合、ビデオ画像が表示されない、またはオーディオ ストリームが低下する可能性があります。エンド ユーザーが会議セッション中にデバイスを選択すると、Web カメラまたはオーディオのリダイレクトは中断されます。

これらのデバイスをエンド ユーザーに表示せず、中断の危険性を防ぐには、USB リダイレクト グループ ポリシー設定を構成し、Web カメラやオーディオ入力デバイスを VMware Horizon Client で表示できないようにします。

特に、Horizon Agent に対し USB リダイレクト フィルタ規則を作成し、`audio-in` および `video` デバイス ファミリ名を無効に指定します。グループ ポリシーの設定と USB リダイレクトに対するフィルタ規則の指定の詳細は、USB リダイレクトを制御するポリシーの使用を参照してください。

注意: USB デバイス ファミリを無効にする USB リダイレクトのフィルタ規則を設定しない場合、エンド ユーザーに、VMware Horizon Client メニュー バーの [USB デバイスの接続] または [デスクトップ > USB] リストから Web カメラやオーディオ デバイスを選択できないことを通知してください。

優先される Web カメラとマイクロフォンを選択

クライアント コンピュータに複数の Web カメラおよびマイクロフォンがある場合、リアルタイム オーディオ ビデオがデスクトップにリダイレクトする優先 Web カメラおよびデフォルトのマイクロフォンを構成できます。これらのデバイスは、ローカル クライアント コンピュータに内蔵または接続できます。

Horizon Client for Windows 4.2 以降がインストールされている Windows クライアント コンピュータでは、Horizon Client の [設定] ダイアログ ボックスのリアルタイム オーディオビデオ設定を構成して、優先される Web カメラとマイクロフォンを選択できます。Horizon Client の以前のバージョンでは、優先する Web カメラを選択するにはレジストリ設定を変更し、デフォルトのマイクロフォンを選択するには、Windows オペレーティング システムの [サウンド] コントロールを使用する必要がありました。

Mac クライアント コンピュータでは、Mac のデフォルトのシステムを使用して、優先する Web カメラまたはマイクロフォンを指定できます。

Linux クライアント コンピュータでは、構成ファイルを編集して、優先する Web カメラを指定できます。デフォルトのマイクロフォンを選択するために、クライアント コンピュータの Linux オペレーティング システムで [サウンド] コントロールを構成できます。

リアルタイム オーディオ ビデオは、優先される Web カメラ が使用できればそれをリダイレクトします。使用できない場合、リアルタイム オーディオ ビデオはシステムによって列挙される最初の Web カメラを使用します。

Windows クライアント システムでの優先する Web カメラまたはマイクロフォンの選択

リアルタイム オーディオ ビデオ機能で、ローカル クライアント システムに複数の Web カメラまたはマイクロフォンが接続されている場合、リモート デスクトップまたはアプリケーションで使用されるデバイスは 1 つだけです。Horizon Client でリアルタイム オーディオ ビデオ機能を構成して、優先的に使用する Web カメラまたはマイクロフォンを指定できます。

優先する Web カメラまたはマイクロフォンが使用できる場合は、リモート デスクトップやアプリケーションで使用され、使用できない場合は他の Web カメラまたはマイクロフォンが使用されます。

リアルタイム オーディオビデオ機能を使用すれば、ビデオ デバイス、オーディオ入力デバイス、およびオーディオ出力デバイスは USB リダイレクトを使用せずに動作し、必要となるネットワーク バンド幅の量は大幅に削減されます。アナログ オーディオ入力デバイスもサポートされます。

注: USB Web カメラやマイクロフォンを使用している場合は、Horizon Client の [USB デバイスを接続] メニューから接続しないでください。これを行うと USB リダイレクトからデバイスがルーティングされるので、デバイスはリアルタイム オーディオビデオ機能を使用できません。

前提条件

- USB Web カメラや USB マイクロフォンまたは他のタイプのマイクロフォンがインストールされ、ローカル クライアント システムで動作できる状態であることを確認します。
- リモート デスクトップやアプリケーション用に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用していることを確認します。
- サーバに接続します。

手順

1 [設定] ダイアログ ボックスを開いて、左ペインで [リアルタイム オーディオビデオ] を選択します。

デスクトップやアプリケーション画面の右上隅にある [設定]（歯車）アイコンをクリックするか、デスクトップやアプリケーションのアイコンを右クリックして [設定] をクリックし、[設定] ダイアログ ボックスを開くことができます。

2 [優先する Web カメラ] ドロップダウン メニューから優先する Web カメラを、[優先するマイクロフォン] ドロップダウン メニューから優先するマイクロフォンを選択します。

ドロップダウン メニューには、クライアント システムで利用可能な Web カメラとマイクロフォンが表示されます。

3 [OK] または [適用] をクリックして、変更を保存します。

リモート デスクトップやアプリケーションを次回起動するときに、優先するように選択した Web カメラとマイクロフォンが、リモート デスクトップやアプリケーションにリダイレクトされます。

Mac クライアント システムでのデフォルトのマイクロフォンの選択

クライアント システムに複数のマイクロフォンがある場合、リモート デスクトップで使用されるのは 1 つだけです。クライアント システムの [システム環境設定] を使用して、リモート デスクトップ用のデフォルトのマイクロフォンを指定できます。

リアルタイム オーディオ ビデオ機能を使用すれば、オーディオ入力デバイスおよびオーディオ出力デバイスは USB リダイレクトを使用せずに動作し、必要となるネットワーク バンド幅の量は大幅に削減されます。アナログ オーディオ入力デバイスもサポートされます。

この手順では、クライアント システムのユーザー インターフェイスからマイクロフォンを選択する方法について説明します。管理者は、Mac のデフォルト システムを使用して優先するマイクロフォンを構成することもできます。Mac クライアント システムで優先する Web カメラまたはマイクロフォンの構成を参照してください。

重要: USB マイクロフォンを使用している場合は、Horizon Client の [接続] - [USB] メニューから接続しないでください。このメニューから接続すると、デバイスは USB リダイレクトによってルーティングされるので、デバイスはリアルタイム オーディオ ビデオ機能を使用できなくなります。

前提条件

- USB マイクロフォンまたは他のタイプのマイクロフォンがインストールされ、クライアント システムで動作できる状態であることを確認します。

- リモート デスクトップ用に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用していることを確認します。

手順

1 クライアント システムで [Apple メニュー] - [システム環境設定] の順に選択して、[サウンド] をクリックします。

2 [サウンド環境設定] の [入力] ペインを開きます。

3 使用するマイクロフォンを選択します。

次回、リモート デスクトップに接続して呼び出しを開始すると、クライアント システムで選択したデフォルトのマイクロフォンがデスクトップで使用されます。

Mac クライアント上でのリアルタイム オーディオビデオの構成

リアルタイム オーディオビデオ設定は、Mac のデフォルト システムを使用して、コマンド ラインで構成できます。デフォルト システムでは、ターミナル（`/Applications/Utilities/Terminal.app`）を使用することで、Mac ユーザーのデフォルト設定の読み取り、書き込み、および削除を行うことができます。

Mac のデフォルト設定は、ドメインに属します。ドメインは通常、個々のアプリケーションに対応します。リアルタイム オーディオビデオ機能のドメインは com.vmware.rtav です。

リアルタイム オーディオビデオを構成するための構文

次のコマンドを使用して、リアルタイム オーディオビデオ機能を構成できます。

表 2-2. リアルタイム オーディオビデオ構成のコマンド構文

コマンド	説明
`defaults write com.vmware.rtav scrWCamId "`*webcam-userid*`"`	リモート デスクトップで優先して使用する Web カメラを設定します。この値を設定しない場合、Web カメラはシステム列挙によって自動的に選択されます。クライアント システムに接続されている（または組み込まれている）任意の Web カメラを指定できます。
`defaults write com.vmware.rtav srcAudioInId "`*audio-device-userid*`"`	リモート デスクトップで優先して使用するマイクロフォン（オーディオ入力デバイス）を設定します。この値を設定しない場合、リモート デスクトップでは、クライアント システムで設定されているデフォルトの録音デバイスが使用されます。クライアント システムに接続されている（または組み込まれている）任意のマイクロフォンを指定できます。
`defaults write com.vmware.rtav srcWCamFrameWidth` *pixels*	画像の幅を設定します。この値には、ハードコードされた値である 320 ピクセルがデフォルトとして設定されています。画像の幅は、どのようなピクセル値にも変更できます。
`defaults write com.vmware.rtav srcWCamFrameHeight` *pixels*	画像の高さを設定します。この値には、ハードコードされた値である 240 ピクセルがデフォルトとして設定されています。画像の高さは、任意のピクセル値に変更できます。
`defaults write com.vmware.rtav srcWCamFrameRate` *fps*	フレーム レートを設定します。この値には、15 fps がデフォルトとして設定されています。フレーム レートは、どのような値にも変更できます。
`defaults write com.vmware.rtav LogLevel "`*level*`"`	リアルタイム オーディオビデオ ログ ファイル (`~/Library/Logs/VMware/vmware-RTAV-`*pid*`.log`) のログ レベルを設定します。ログ レベルをトレースまたはデバッグに設定できます。

コマンド	説明
`defaults write com.vmware.rtav IsDisabled` *value*	リアルタイム オーディオビデオを有効にするか無効にするかを決定します。リアルタイム オーディオビデオはデフォルトで有効に設定されています(この値は適用されていません)。リアルタイム オーディオビデオをクライアント上で無効にするには、値を true に設定します。
`defaults read com.vmware.rtav`	リアルタイム オーディオビデオの構成設定を表示します。
`defaults delete com.vmware.rtav` *setting*	リアルタイム オーディオビデオの構成設定を削除します。以下に例を示します。`defaults delete com.vmware.rtav srcWCamFrameWidth`

注: フレーム レートを 1 fps から最大 25 fps まで、解像度を最大 1920x1080 まで調整できます。デバイスまたは環境によっては、高速フレーム レートでの高解像度がサポートされないことがあります。

Mac クライアント システムで優先する Web カメラまたはマイクロフォンの構成

リアルタイム オーディオ ビデオ機能を使用し、クライアント システムに複数の Web カメラとマイクロフォンがある場合、リモート デスクトップで使用できるのは 1 台の Web カメラと 1 台のマイクロフォンだけです。Mac のデフォルト システムを使用して、優先する Web カメラとマイクロフォンをコマンド ラインで指定します。

リアルタイム オーディオ ビデオ機能を使用すると、Web カメラ、オーディオ入力デバイス、オーディオ出力デバイスは、USB リダイレクトなしで動作し、必要なネットワーク バンド幅の量が大幅に軽減します。アナログ オーディオ入力デバイスもサポートされます。

ほとんどの環境では、優先マイクロフォンまたは Web カメラを設定する必要はありません。優先マイクロフォンを設定しない場合、リモート デスクトップでは、クライアント システムの [システム環境設定] で設定されたデフォルトのオーディオ デバイスが使用されます。Mac クライアント システムでのデフォルトのマイクロフォンの選択を参照してください。優先 Web カメラを構成しない場合、リモート デスクトップでは、列挙された順に従って Web カメラが選択されます。

前提条件

- 優先 USB Web カメラを構成する場合は、その Web カメラがクライアント システムにインストールされ、動作できる状態であることを確認します。
- 優先 USB マイクロフォンまたは他のタイプのマイクロフォンを構成する場合は、そのマイクロフォンがクライアント システムにインストールされ、動作できる状態であることを確認します。
- リモート デスクトップ用に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用していることを確認します。

手順

1 Mac クライアント システムで Web カメラまたはマイクロフォン アプリケーションを起動し、リアルタイム オーディオビデオのログ ファイルにカメラ デバイスまたはオーディオ デバイスを列挙します。

   a Web カメラまたはオーディオ デバイスを取り付けます。

   b [アプリケーション] フォルダで [VMware Horizon Client] をダブルクリックして、Horizon Client を起動します。

   c 呼び出しを開始し、その後呼び出しを停止します。

2 リアルタイム オーディオ ビデオ ログ ファイル内で、Web カメラまたはマイクロフォンのログ エントリを見つけます。

a リアルタイム オーディオ ビデオ ログ ファイルをテキスト エディタで開きます。

リアルタイム オーディオ ビデオ ログ ファイルには ~/Library/Logs/VMware/vmware-RTAV-*pid*.log という名前が付けられています。*pid* は現在のセッションの処理 ID です。

b リアルタイム オーディオ ビデオ ログ ファイルで、接続された Web カメラまたはマイクロフォンを特定するエントリを探します。

次の例では、リアルタイム オーディオ ビデオ ログ ファイルで Web カメラのエントリがどのように表示されるかを示します。

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() - 1
Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=FaceTime HD Camera (Built-in)   UserId=FaceTime HD Camera (Built-in)#0xfa20000005ac8509
SystemId=0xfa20000005ac8509
```

次の例では、リアルタイム オーディオ ビデオ ログ ファイルでマイクロフォンのエントリがどのように表示されるかを示します。

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int
AVCaptureEnumerateAudioDevices(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() - 2
Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() -
Index=255   Name=Built-in Microphone   UserId=Built-in
Microphone#AppleHDAEngineInput:1B,0,1,0:1   SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() -
Index=255   Name=Built-in Input   UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

3 リアルタイム オーディオ ビデオ ログ ファイルで、優先する Web カメラまたはマイクロフォンを見つけて、そのユーザー ID をメモします。

ログ ファイルでは、ユーザー ID が文字列 UserId= の後に表示されます。たとえば、内蔵フェイス タイム カメラのユーザー ID は FaceTime HD Camera（組み込み）で、内蔵マイクロフォンのユーザー ID は Built-in Microphone です。

4 ターミナル（/Applications/Utilities/Terminal.app）で defaults write コマンドを使用して、優先する Web カメラまたはマイクロフォンを設定します。

オプション	アクション
優先する Web カメラを設定する	**defaults write com.vmware.rtav srcWCamId "*webcam-userid*"**」と入力します。ここで、*webcam-userid* は、リアルタイム オーディオ ビデオ ログ ファイルで取得した、優先する Web カメラのユーザー ID です。例： `defaults write com.vmware.rtav srcWCamId "HD Webcam C525"`
優先するマイクロフォンを設定する	**defaults write com.vmware.rtav srcAudioInId "*audio-device-userid*"**」と入力します。ここで、*audio-device-userid* は、リアルタイム オーディオ ビデオ ログ ファイルで取得した、優先するマイクロフォンのユーザー ID です。例： `defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"`

5 （オプション） defaults read コマンドを使用して、リアルタイム オーディオ ビデオ機能への変更を確認します。

例：**defaults read com.vmware.rtav**

このコマンドにより、リアルタイム オーディオ ビデオ設定のすべてが表示されます。

次回、リモート デスクトップに接続して新しい呼び出しを開始すると、構成した優先 Web カメラまたはマイクロフォンが使用されます（利用可能な場合）。優先 Web カメラまたはマイクロフォンが利用できない場合、リモート デスクトップは別の利用可能な Web カメラまたはマイクロフォンを使用できます。

Linux クライアント システムでのデフォルトのマイクロフォンの選択

クライアント システムに複数のマイクロフォンがある場合、1 つだけが Horizon 7 デスクトップで使用されます。デフォルトで使用するマイクロフォンを指定するために、クライアント システムの [サウンド] コントロールを使用できます。

リアルタイム オーディオ ビデオ機能を使用すれば、オーディオ入力デバイスおよびオーディオ出力デバイスは USB リダイレクトを使用せずに動作し、必要となるネットワーク バンド幅の量は大幅に削減されます。アナログ オーディオ入力デバイスもサポートされます。

この手順では、クライアント システムのユーザー インターフェイスからデフォルトのマイクロフォンを選択する方法について説明します。管理者が構成ファイルを編集して、優先するマイクロフォンを構成することもできます。Linux クライアント システムで優先する Web カメラまたはマイクロフォンの選択を参照してください。

前提条件

- USB マイクロフォンまたは他のタイプのマイクロフォンがインストールされ、クライアント システムで動作できる状態であることを確認します。
- リモート デスクトップ用に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用していることを確認します。

手順

1 Ubuntu グラフィカル ユーザー インターフェイスで、[システム] - [プリファレンス] - [サウンド] の順に選択します。

または、画面の上にあるツール バーの右側の [サウンド] アイコンをクリックします。

2 [Sound Preferences] ダイアログ ボックスの [入力] タブをクリックします。

3 優先するデバイスを選択して [閉じる] をクリックします。

Linux クライアント システムで優先する Web カメラまたはマイクロフォンの選択

リアルタイム オーディオ ビデオ機能があり、クライアント システムに複数の Web カメラとマイクロフォンがある場合、1 台の Web カメラと 1 台のマイクロフォンだけを Horizon 7 デスクトップで使用できます。優先する Web カメラとマイクロフォンを指定するには、構成ファイルを編集します。

優先する Web カメラまたはマイクロフォンは、使用できる場合はリモート デスクトップで使用され、使用できない場合は他の Web カメラまたはマイクロフォンが使用されます。

リアルタイム オーディオ ビデオ機能を使用すれば、Web カメラ、オーディオ入力デバイスおよびオーディオ出力デバイスは、USB リダイレクトを使用せずに動作し、必要となるネットワーク バンド幅量は大幅に削減されます。アナログ オーディオ入力デバイスもサポートされます。

`/etc/vmware/config` ファイルにプロパティを設定し、優先するデバイスを指定するには、特定のフィールドの値を確定する必要があります。これらのフィールドの値については、ログ ファイルを検索できます。

- Web カメラについては、`rtav.srcWCamId` プロパティを Web カメラの `UserId` フィールドの値に設定し、`rtav.srcWCamName` プロパティを Web カメラの `Name` フィールドの値に設定します。

  `rtav.srcWCamName` プロパティには、`rtav.srcWCamId` プロパティよりも高い優先度が設定されています。両方のプロパティでは、同じ Web カメラが指定されるはずです。これらのプロパティが異なる Web カメラを指定する場合、`rtav.srcWCamName` が存在する場合、このプロパティによって指定される Web カメラが使用されます。このプロパティが存在しない場合、`rtav.srcWCamId` によって指定される Web カメラが使用されます。両方の Web カメラが見つからない場合、デフォルトの Web カメラが使用されます。

- オーディオ デバイスの場合、`rtav.srcAudioInId` プロパティを Pulse Audio `device.description` フィールドの値に設定します。

前提条件

優先する Web カメラ、優先するマイクロフォン、または両方のいずれを構成するかに応じて、所定の準備作業を実行します。

- USB webcam がインストールされ、クライアント システムで動作できる状態であることを確認します。
- USB マイクロフォンまたは他のタイプのマイクロフォンがインストールされ、クライアント システムで動作できる状態であることを確認します。
- リモート デスクトップ用に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用していることを確認します。

手順

1 クライアントを起動し、Web カメラまたはマイクロフォンのアプリケーションを開始して、カメラ デバイスまたはオーディオ デバイスの一覧がクライアント ログに出力されるようにします。

   a 使用する Web カメラまたはオーディオ デバイスを接続します。

   b `vmware-view` コマンドを使用して Horizon Client を起動します。

   c 呼び出しを開始し、その後呼び出しを停止します。

   このプロセスでログ ファイルが作成されます。

2 Web カメラまたはマイクロフォンというログのエントリを探します。

a テキスト エディタでデバッグ ログ ファイルを開きます。

リアルタイム オーディオ ビデオのログ メッセージが出力されるログ ファイルは、/tmp/vmware-*<username>*/vmware-RTAV-*<pid>*.log に保存されています。クライアント ログは、/tmp/vmware-*<username>*/vmware-view-*<pid>*.log に保存されています。

b ログ ファイルを検索して、接続されている Web カメラおよびマイクロフォンを参照しているログ ファイルのエントリを探します。

Web カメラを抽出する例を以下に示します。

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:0819)
UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.5
SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=Microsoft® LifeCam HD-6000 for Notebooks   UserId=Microsoft® LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6   SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) -
enumeration data unavailable
```

オーディオ デバイスとそれぞれの現在のオーディオ レベルを抽出する例を以下に示します。

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB Headset Analog Mono')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of Microsoft
LifeChat LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
```

選択したデバイスのいずれかのソース オーディオ レベルが PulseAudio 基準を満たしていない場合 (ソースが 100% (0dB) に設定されていない場合)、または選択したソース デバイスがミュートになっている場合は、以下の警告が表示されます。

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0:  67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

3 デバイスの記述をコピーし、それを利用して /etc/vmware/config ファイルに正しくプロパティを設定します。

Web カメラの例では、Microsoft® LifeCam HD-6000 for Notebooks と Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6 をコピーして、優先される Web カメラとして Microsoft の Web カメラを指定し、次のようにプロパティを設定します。

```
rtav.srcWCamName = “Microsoft® LifeCam HD-6000 for Notebooks”
rtav.srcWCamId = “Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/
usb1/1-3/1-3.6”
```

この例では、rtav.srcWCamId プロパティを "Microsoft" に設定することもできます。rtav.srcWCamId プロパティは、部分および完全一致の両方をサポートします。rtav.srcWCamName プロパティは、完全一致のみをサポートします。
オーディオ デバイスの場合には、たとえば Logitech ヘッドセットを優先オーディオ デバイスとして指定するために Logitech USB Headset Analog Mono をコピーし、プロパティを次のように設定します。

```
rtav.srcAudioInId="Logitech USB Headset Analog Mono"
```

4 変更を保存し、/etc/vmware/config 構成ファイルを閉じます。

5 デスクトップ セッションをログオフして、新しいセッションを開始します。

リアルタイム オーディオ ビデオ グループ ポリシ設定の構成

Horizon 7 デスクトップでのリアルタイム オーディオ ビデオ (RTAV) の動作を制御するグループ ポリシ設定を構成できます。これらの設定は、仮想 webcam の最大フレーム レートおよび画像の解像度を決定します。これらの設定によって、1 人のユーザーが消費できる最大バンド幅を管理できます。追加設定は RTAV 機能を無効または有効にします。

これらのポリシ設定を構成する必要はありません。リアルタイム オーディオ ビデオは、クライアント システムの webcam に設定されるフレーム レートおよび画像の解像度で動作します。デフォルト設定がほとんどの webcam およびオーディオ アプリケーションで推奨されます。

リアルタイム オーディオ ビデオ中に使用するバンド幅の例については、リアルタイム オーディオ ビデオの帯域幅を参照してください。

これらのポリシ設定は、物理デバイスが接続されているクライアント システムではなく、Horizon 7 デスクトップに影響します。これらの設定をデスクトップで構成するには、Active Directory に RTAV グループ ポリシー管理テンプレート (ADMX) ファイルを追加します。

クライアント システムでの設定については、VMware ナレッジベースの記事、『Setting Frame Rates and Resolution for Real-Time Audio-Video on Horizon View Clients (Horizon View Client でのリアルタイム オーディオ-ビデオのフレームレートと解像度の設定)』(http://kb.vmware.com/kb/2053644) を参照してください。

Active Directory への RTAV ADMX テンプレートの追加と設定の構成

RTAV ADMX ファイル (`vdm_agent_rtav.admx`) のポリシー設定を Active Directory のグループ ポリシー オブジェクト (GPO) に追加し、グループ ポリシー オブジェクト エディタで設定を構成することができます。

前提条件

- RTAV のセットアップ オプションが仮想マシン デスクトップと RDS ホストにインストールされていることを確認します。この設定オプションはデフォルトでインストールされますが、インストール中に選択を解除することができます。この設定は RTAV がインストールされなければ効果がありません。Horizon Agent のインストールについては、各セットアップ ガイドを参照してください。
- Active Directory GPO が RTAV グループ ポリシ設定で作成されることを確認します。GPO は、仮想マシン デスクトップまたは RDS ホストを含む OU にリンクする必要があります。Active Directory グループ ポリシーの例を参照してください。
- Active Directory サーバで、Microsoft MMC およびグループ ポリシー オブジェクト エディタ スナップインが使用できることを確認します。
- RTAV グループ ポリシ設定をよく理解してください。リアルタイム オーディオ ビデオ グループ ポリシ設定 を参照してください。

手順

1 Horizon 7 GPO Bundle `.zip` ファイルを https://my.vmware.com/web/vmware/downloads の VMware ダウンロード サイトからダウンロードします。

[Desktop & End-User Computing（デスクトップおよびエンドユーザー コンピューティング)] で VMware Horizon 7 のダウンロードを選択します。これには GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` で、*x.x.x* はバージョン、*yyyyyyy* はビルド番号を表します。Horizon 7 のグループ ポリシー設定用の ADMX ファイルはすべて、このファイルで提供されています。

2 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` ファイルを解凍して、ADMX ファイルを Active Directory サーバにコピーします。

a `vdm_agent_rtav.admx` ファイルと `en-US` フォルダを Active Directory サーバの `C:\Windows\PolicyDefinitions` フォルダにコピーします。

b （オプション） 言語リソース ファイル (`vdm_agent_rtav.adml`) を Active Directory サーバの `C:\Windows\PolicyDefinitions\` 内の適切なサブフォルダにコピーします。

3 Active Directory サーバで、グループ ポリシー管理エディタを開き、エディタでテンプレート ファイルへのパスを入力します。

設定は、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Agent の構成] - [View の RTAV 構成] フォルダに格納されています。

次のステップ

グループ ポリシー設定を構成します。

リアルタイム オーディオ ビデオ グループ ポリシ設定

リアルタイム オーディオ ビデオ (RTAV) グループ ポリシー設定により、仮想 Web カメラの最大フレーム レートおよび画像の最大解像度を制御できます。追加設定により RTAV 機能を無効または有効にできます。このポリシー設定はリモート デスクトップに影響し、物理デバイスが接続されたクライアント システムには影響しません。

RTAV グループ ポリシー設定を構成しない場合、RTAV はクライアント システムに設定されている値を使用します。クライアント システムでは、デフォルトの Web カメラフレーム レートは 1 秒あたり 15 フレームです。デフォルトの Web カメラ画像の解像度は 320x240 ピクセルです。

解像度グループ ポリシー設定で、使用できる最大値を決定します。クライアント システムで設定されるフレーム レートと解像度は絶対値です。たとえば、RTAV 設定の画像の最大解像度を 640x480 ピクセルに構成すると、Web カメラではクライアントで設定された最大 640x480 ピクセルまでの解像度を表示します。クライアントの画像解像度を 640x480 ピクセルよりも高い値に設定すると、クライアント解像度は 640x480 ピクセルが上限となります。

構成によっては、1 秒あたり 25 フレームで 1920x1080 の解像度の最大グループ ポリシー設定を達成できない場合があります。指定された解像度に対して構成で達成できる最大フレーム レートは、使用する Web カメラ、クライアント システム ハードウェア、Horizon Agent 仮想ハードウェア、利用可能な帯域幅によって異なります。

解像度グループ ポリシー設定は、ユーザーによって解像度の値が設定されていない場合に使用されるデフォルト値を決定します。

グループ ポリシー設定	説明
`Disable RTAV`	この設定を有効にすると、リアルタイム オーディオ ビデオ機能が無効になります。 この設定が構成されていない場合、または無効になっている場合は、リアルタイム オーディオ ビデオが有効になります。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [RTAV 構成を表示] フォルダにあります。
`Max frames per second`	Web カメラがフレームをキャプチャできる、1 秒あたりの最大レートを決定します。この設定を使用して、低帯域幅ネットワーク環境での Web カメラ フレーム レートを制限できます。 最小値は 1 秒あたり 1 フレームです。最大値は 1 秒あたり 25 フレームです。 この設定が構成されていない場合、または無効になっている場合は、最大フレーム レートは設定されません。リアルタイム オーディオ ビデオはクライアント システムで Web カメラに選択されたフレーム レートを使用します。 デフォルトでは、クライアント Web カメラのフレーム レートは 1 秒あたり 15 フレームです。クライアント システムで設定が構成されておらず、[1 秒あたりの最大フレーム] 設定が構成されていない場合、または無効になっている場合は、Web カメラは 1 秒あたり 15 フレームをキャプチャします。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [RTAV 構成を表示] - [RTAV Web カメラ設定を表示] フォルダにあります。

グループ ポリシー設定	説明
Resolution – Max image width in pixels	Web カメラによってキャプチャされる画像フレームのピクセル単位での最大幅を決定します。画像の最大幅を低く設定することで、キャプチャされるフレームの解像度を下げ、低帯域幅ネットワーク環境でのイメージングの使用環境を改善することができます。 この設定が構成されていない場合、または無効になっている場合は、画像の最大幅は設定されません。RTAV はクライアント システムで設定された画像の幅を使用します。クライアント システムのデフォルトの Web カメラ画像の幅は 320 ピクセルです。 Web カメラ画像の上限は 1920x1080 ピクセルです。この設定を 1920 ピクセルよりも大きい値で構成した場合、有効となる画像の最大幅は 1920 ピクセルです。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [RTAV 構成を表示] - [RTAV Web カメラ設定を表示] フォルダにあります。
Resolution – Max image height in pixels	Web カメラによってキャプチャされる画像フレームのピクセル単位での最大の高さを決定します。画像の最大の高さを低く設定することで、キャプチャされるフレームの解像度を下げ、低帯域幅ネットワーク環境でのイメージングの使用環境を改善することができます。 この設定が構成されていない場合、または無効になっている場合は、画像の最大の高さは設定されません。RTAV はクライアント システムで設定された画像の高さを使用します。クライアント システムのデフォルトの Web カメラ画像の高さは 240 ピクセルです。 Web カメラ画像の上限は 1920x1080 ピクセルです。この設定を 1080 ピクセルよりも大きい値で構成した場合、有効となる画像の最大の高さは 1080 ピクセルです。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [RTAV 構成を表示] - [RTAV Web カメラ設定を表示] フォルダにあります。
Resolution – Default image resolution width in pixels	Web カメラによってキャプチャされる画像フレームのピクセル単位でのデフォルトの解像度の幅を決定します。この設定は解像度の値がユーザーによって定義されていない場合に使用されます。 この設定が構成されていない場合、または無効になっている場合は、デフォルト イメージの幅は 320 ピクセルになります。 このポリシー設定によって構成された値は、View Agent 6.0 以降および Horizon Client 3.0 以降の両方が使用されている場合にのみ有効になります。View Agent または Horizon Client のバージョンが古い場合はこのポリシー設定が無効となり、デフォルト イメージの幅は 320 ピクセルになります。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [RTAV 構成を表示] - [RTAV Web カメラ設定を表示] フォルダにあります。
Resolution – Default image resolution height in pixels	Web カメラによってキャプチャされる画像フレームのピクセル単位でのデフォルトの解像度の高さを決定します。この設定は解像度の値がユーザーによって定義されていない場合に使用されます。 この設定が構成されていない場合、または無効になっている場合には、デフォルト イメージの高さは 240 ピクセルになります。 このポリシー設定によって構成された値は、View Agent 6.0 以降および Horizon Client 3.0 以降の両方が使用されている場合にのみ有効になります。View Agent または Horizon Client のバージョンが古い場合はこのポリシー設定が無効となり、デフォルト イメージの高さは 240 ピクセルになります。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [RTAV 構成を表示] - [RTAV Web カメラ設定を表示] フォルダにあります。

リアルタイム オーディオ ビデオの帯域幅

リアルタイム オーディオ ビデオの帯域幅は、Web カメラの画像解像度およびフレーム レート、キャプチャされている画像やオーディオ データによって異なります。

表 2-3. Horizon Client から Horizon Agent へのリアルタイム オーディオ ビデオ データの送信の帯域幅の結果のサンプルに示すサンプルのテストは、リアルタイム オーディオ ビデオが標準的な Web カメラとオーディオ入力デバイスを含む View 環境で使用する帯域幅を測定します。このテストは Horizon Client から Horizon Agent へのビデオおよびオーディオ データの両方を送信する帯域幅を測定します。Horizon Client からデスクトップ セッションを実行するのに必要な帯域幅の合計は、この数字よりも大きくなる可能性があります。これらのテストでは、Web カメラはイメージを各画像解像度に対し毎秒 15 フレームでキャプチャします。

表 2-3. Horizon Client から Horizon Agent へのリアルタイム オーディオ ビデオ データの送信の帯域幅の結果のサンプル

画像解像度（幅 x 高さ）	使用されている帯域幅 (Kbps)
160 x 120	225
320 x 240	320
640 x 480	600

スキャナ リダイレクトの構成

スキャナ リダイレクトを使用することで、Horizon 7 ユーザーはクライアント コンピュータにローカルに接続されたスキャナやイメージング デバイスを使用して、リモート デスクトップおよびアプリケーション内の情報をスキャンできます。スキャナ リダイレクトは Horizon 6.0.2 以降のリリースで使用できます。

スキャナ リダイレクトは、TWAIN および WIA 形式と互換性がある標準のスキャナやイメージング デバイスをサポートしています。

スキャナ リダイレクトのセットアップ オプションを使用して Horizon Agent をインストールすると、後から構成しなくても、リモート デスクトップおよびアプリケーションでスキャナ リダイレクトが機能します。リモート デスクトップまたはアプリケーションにスキャナ固有のドライバを構成する必要はありません。

グループ ポリシー設定を構成してデフォルト値を変更し、特定のスキャニングおよびイメージング アプリケーションまたは環境に適応することができます。ポリシーを設定して機能をすべて無効または有効にすることもできます。ADMX テンプレート ファイルを使用すると、スキャナ リダイレクト グループ ポリシー設定を Active Directory または個別のデスクトップにインストールできます。スキャナ リダイレクトのグループ ポリシー設定の構成を参照してください。

スキャニング データがリモート デスクトップまたはアプリケーションにリダイレクトされると、ユーザーはローカル コンピュータのスキャナやイメージング デバイスにアクセスできません。逆に言えば、デバイスがローカル コンピュータで使用中であれば、リモート デスクトップでそのデバイスにアクセスできません。

スキャナ リダイレクトのシステム要件

スキャナ リダイレクトをサポートするには、Horizon 7 の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

Horizon 7 リモート デスクトップまたはアプリケーション	この機能は、単一ユーザーの仮想マシンに展開された RDS デスクトップ、RDS アプリケーション、および VDI デスクトップでサポートされています。

	親またはテンプレート仮想マシンまたは RDS ホストに View Agent 6.0.2 以降をインストールして、スキャナ リダイレクト セットアップ オプションを選択する必要があります。 Windows デスクトップおよび Windows Server ゲスト OS では、Horizon Agent スキャナ リダイレクト セットアップ オプションがデフォルトでオフになっています。 単一ユーザーの仮想マシンおよび（記載されている場合は） RDS ホストでは、次のゲスト OS がサポートされます。 ■ 32 ビットまたは 64 ビットの Windows 7 ■ 32 ビットまたは 64 ビットの Windows 8。*x* ■ 32 ビットまたは 64 ビットの Windows 10 ■ デスクトップまたは RDS ホストとして構成されている Windows Server 2008 R2 ■ デスクトップまたは RDS ホストとして構成されている Windows Server 2012 R2 **重要:** デスクトップとして構成されているか RDS ホストとして構成されているかに関係なく、Windows Server ゲスト OS にはデスクトップ エクスペリエンス機能をインストールしておく必要があります。 Horizon Agent がインストールされているデスクトップ オペレーティング システムにスキャナ デバイス ドライバをインストールする必要はありません。
Horizon Client ソフトウェア	Horizon Client 3.2 for Windows 以降のリリース
Horizon Client コンピュータまたはクライアント アクセス デバイス	サポートされるオペレーティング システムは次のとおりです。 ■ 32 ビットまたは 64 ビットの Windows 7 ■ 32 ビットまたは 64 ビットの Windows 8。*x* ■ 32 ビットまたは 64 ビットの Windows 10 スキャナ デバイス ドライバをインストールする必要があり、スキャナがクライアント コンピュータで操作可能である必要があります。
スキャン デバイスの標準	TWAIN または WIA
Horizon 7 用の表示プロトコル	PCoIP スキャナ リダイレクトは、RDP デスクトップ セッションでサポートされません。

スキャナ リダイレクトのユーザー操作

スキャナ リダイレクトを使用すると、クライアント コンピュータに接続されている物理スキャナとイメージング デバイスを、リモート デスクトップおよびアプリケーションでスキャン操作を実行する仮想デバイスとして操作できます。

ユーザーは、ローカル接続されたクライアント コンピュータ上のスキャナを使用する場合とよく似た方法で仮想スキャナを操作できます。

- Horizon Agent でスキャナ リダイレクト オプションをインストールした後、スキャナ ツール トレイ アイコン () がデスクトップに追加されます。RDS アプリケーションでは、ツール トレイ アイコンはローカル クライアント コンピュータにリダイレクトされます。

  スキャナ ツール トレイ アイコンを使用する必要はありません。スキャンのリダイレクトは何も構成しなくても機能します。アイコンを使用すると、複数のデバイスがクライアント コンピュータに接続されている場合に使用するデバイスの変更など、オプションの構成を実行できます。

- スキャナ アイコンをクリックすると、[VMware Horizon のスキャナ リダイレクト] メニューが表示されます。クライアント コンピュータに互換性のないスキャナが接続されている場合、メニュー リストにスキャナは表示されません。

- デフォルトでは、スキャン デバイスが自動選択されます。TWAIN スキャナと WIA スキャナは個別に選択されます。TWAIN スキャナと WIA スキャナは同時に 1 つずつ選択できます。

- ローカル接続されたスキャナが複数構成されている場合は、デフォルトで選択されているスキャナとは別のスキャナを選択できます。

- WIA スキャナは、リモート デスクトップの [デバイス マネージャ] メニューの [イメージング デバイス] に表示されます。WIA スキャナの名前は [VMware Virtual WIA スキャナ] です。

- [VMware Horizon のスキャナ リダイレクト] メニューで [環境設定] オプションをクリックすると、スキャナ リダイレクト メニューでの Web カメラの非表示やデフォルト スキャナの選択方法の決定などのオプションを選択できます。

  また、Active Directory でスキャナ リダイレクト グループ ポリシー設定を構成して、この機能をコントロールすることもできます。スキャナ リダイレクトのグループ ポリシー設定を参照してください。

- TWAIN スキャナを操作する場合は、[VMware Horizon の TWAIN スキャナ リダイレクト] メニューに、イメージの領域を選択したり、カラー、白黒、またはグレースケールでスキャンしたり、その他の一般的な機能を選択したりするための追加のオプションが表示されます。

- デフォルトではウィンドウを表示しない TWAIN スキャン ソフトウェアの TWAIN ユーザー インターフェイス ウィンドウを表示するには、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスの [[スキャナ設定] ダイアログを常に表示] オプションを選択します。

ただし、ほとんどの TWAIN スキャン ソフトウェアはデフォルトで TWAIN ユーザー インターフェイス ウィンドウを表示します。このソフトウェアでは、[[スキャナ設定] ダイアログを常に表示] オプションを選択しているかどうかに関係なく、このウィンドウは常に表示されます。

注: 異なるファームでホストされている 2 つの RDS アプリケーションを実行している場合、クライアント コンピュータには 2 つのスキャナ リダイレクト ツール トレイ アイコンが表示されます。通常、クライアント コンピュータには 1 つのスキャナのみが接続されています。この場合は、両方のアイコンが同じデバイスを操作するため、どちらのアイコンを選択してもかまいません。状況によっては、ローカル接続されたスキャナが 2 つあり、異なるファームで稼動する 2 つの RDS アプリケーションを実行している場合があります。その場合は、各アイコンを開いて、どちらのスキャナ リダイレクト メニューがどちらの RDS アプリケーションをコントロールするかを確認する必要があります。

エンド ユーザーがリダイレクトされるスキャナを操作する手順については、『Windows 版 VMware Horizon Client の使用』を参照してください。

スキャナ リダイレクトのグループ ポリシー設定の構成

Horizon 7 デスクトップとアプリケーションでのスキャナ リダイレクトの動作を制御するグループ ポリシー設定を構成できます。これらのポリシー設定を使用すると、ユーザーのデスクトップおよびアプリケーションの VMware Horizon スキャナ リダイレクトの [環境設定] ダイアログ ボックスで使用可能なオプションを、Active Directory から集中管理できます。

これらのポリシ設定を構成する必要はありません。スキャナ リダイレクトは、リモート デスクトップやクライアント システムのスキャナ デバイス用に構成されたデフォルトの設定で機能します。

これらのポリシー設定はユーザーのリモート デスクトップとアプリケーションには影響しますが、物理スキャナが接続されたクライアント システムには影響しません。これらの設定をデスクトップとアプリケーションで構成するには、Active Directory にスキャナ リダイレクト グループ ポリシー管理テンプレート (ADMX) ファイルを追加します。

Active Directory へのスキャナ リダイレクト ADMX テンプレートの追加

スキャナ リダイレクト ADMX テンプレート ファイル、(`vdm_agent_scanner.admx`) のポリシー設定を Active Directory のグループ ポリシー オブジェクト (GPO) に追加し、グループ ポリシー オブジェクト エディタで設定を構成することができます。

前提条件

- スキャナ リダイレクトのセットアップ オプションが仮想マシン デスクトップまたは RDS ホストにインストールされていることを確認します。スキャナ リダイレクトがインストールされていないと、グループ ポリシー設定は有効になりません。Horizon Agent のインストールについては、各セットアップ ガイドを参照してください。
- スキャナ リダイレクトのグループ ポリシー設定用に Active Directory GPO が作成されていることを確認します。GPO は、仮想デスクトップまたは RDS ホストを含む OU にリンクする必要があります。Active Directory グループ ポリシーの例を参照してください。
- MMC およびグループ ポリシー オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。

- スキャナ リダイレクトのグループ ポリシー設定について理解しておきます。スキャナ リダイレクトのグループ ポリシー設定を参照してください。

手順

1 Horizon 7 GPO Bundle `.zip` ファイルを https://my.vmware.com/web/vmware/downloads の VMware ダウンロード サイトからダウンロードします。

[Desktop & End-User Computing（デスクトップおよびエンドユーザー コンピューティング）] で VMware Horizon 7 のダウンロードを選択します。これには GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` で、*x.x.x* はバージョン、*yyyyyyy* はビルド番号を表します。Horizon 7 のグループ ポリシー設定用の ADMX ファイルはすべて、このファイルで提供されています。

2 `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` ファイルを解凍して、ADMX ファイルを Active Directory サーバにコピーします。

a `vdm_agent_scanner.admx` ファイルと `en-US` フォルダを Active Directory サーバの `C:\Windows\PolicyDefinitions` フォルダにコピーします。

b （オプション） 言語リソース ファイル (`vdm_agent_scanner.adml`) を Active Directory サーバの `C:\Windows\PolicyDefinitions\` 内の適切なサブフォルダにコピーします。

3 Active Directory サーバで、グループ ポリシー管理エディタを開き、エディタでテンプレート ファイルへのパスを入力します。

設定は、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Agent の構成] - [スキャナ リダイレクト] フォルダに格納されています。

ほとんどの設定は、[ユーザー構成] フォルダにも追加されます。このフォルダは、[ユーザー構成] - [ポリシー] - [管理用テンプレート] - [VMware View Agent の構成] - [スキャナ リダイレクト] フォルダ内にあります。

次のステップ

グループ ポリシー設定を構成します。

スキャナ リダイレクトのグループ ポリシー設定

スキャナ リダイレクトのグループ ポリシーの設定は、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスでユーザーのデスクトップおよびアプリケーションに対して使用できるオプションを制御します。

スキャナ リダイレクト ADMX テンプレート ファイルには、コンピュータの構成とユーザーの構成の両方のポリシーが含まれます。ユーザーの構成ポリシーを使用すると、VDI デスクトップ、RDS デスクトップ、RDS アプリケーションのユーザーに対してさまざまな構成を設定できます。ユーザーのデスクトップ セッションやアプリケーションが同じ RDS ホスト上で実行されている場合であっても、さまざまなユーザーの構成ポリシーを適用できます。設定はすべて、グループ ポリシー管理エディタの [VMware Horizon Agent の構成] - [スキャナ リダイレクト] フォルダにあります。

グループ ポリシー設定	コンピュータ	ユーザー	説明
Disable functionality	X		スキャナ リダイレクト機能を無効にします。 この設定を有効にすると、スキャナはリダイレクトできなくなり、ユーザーのデスクトップおよびアプリケーションのスキャナ メニューに表示されません。 この設定を無効にすると、または構成しないと、スキャナ リダイレクトは動作し、スキャナ メニューにスキャナが表示されます。
Lock config	X		スキャナ リダイレクトのユーザー インターフェイスをロックし、ユーザーがデスクトップおよびアプリケーションで構成オプションを変更できないようにします。 この設定を有効にすると、ユーザーはデスクトップおよびアプリケーションのトレイ メニューから使用できるオプションを構成できません。ユーザーは [VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスを表示することはできますが、オプションが非アクティブになっていて、変更できません。 この設定を無効にすると、または構成しないと、ユーザーは [VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスでオプションを構成できます。
Compression		X	リモート デスクトップまたはアプリケーションへのイメージ転送時のイメージ圧縮率を設定します。 以下の圧縮モードから選択できます。 ■ [無効化]。イメージの圧縮を無効にします。 ■ [ロスレス]。イメージの品質が低下しないロスレス (zlib) 圧縮を使用します。 ■ [JPEG]。品質の低下がある JPEG 圧縮を使用します。[JPEG 圧縮品質] フィールドでイメージ品質のレベルを指定します。JPEG 圧縮品質に指定できる値は 0 ～ 100 です。 この設定を有効にすると、このポリシーが適用されるすべてのユーザーに対して選択した圧縮モードが設定されます。ただし、ユーザーは [VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスで [圧縮] オプションを変更することで、ポリシー設定をオーバーライドできます。 このポリシー設定を無効にすると、または構成しないと、[JPEG] 圧縮モードが使用されます。
Hide Webcam	X	X	[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスのスキャナ選択メニューに、Web カメラが表示されないようにします。 デフォルトでは、Web カメラをデスクトップおよびアプリケーションにリダイレクトできます。ユーザーは Web カメラを選択し、仮想スキャナとして使用してイメージをキャプチャできます。 この設定をコンピュータの構成ポリシーとして有効にすると、Web カメラは影響を受けるコンピュータのすべてのユーザーに対して表示されなくなります。ユーザーは、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスの [Web カメラを非表示] オプションを変更できません。 この設定をユーザーの構成ポリシーとして有効にすると、Web カメラは影響を受けるすべてのユーザーに対して表示されなくなります。ただし、ユーザーは、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスの [Web カメラを非表示] オプションを変更できます。 この設定をコンピュータの構成およびユーザーの構成の両方で有効にすると、影響を受けるコンピュータのすべてのユーザーについて、コンピュータの構成における [Web カメラを非表示] 設定によって、ユーザーの構成における対応するポリシー設定がオーバーライドされます。 どちらかのポリシー構成でこの設定を無効にするか、または構成しないと、[Web カメラを非表示] 設定は、対応するポリシー設定（ユーザーの構成またはコンピュータの構成）または [VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスにおけるユーザーの選択によって決まります。

グループ ポリシー設定	コンピュータ	ユーザー	説明
Default Scanner	X	X	スキャナの自動選択を集中管理できるようにします。 スキャナの自動選択オプションは、TWAIN スキャナと WIA スキャナで個別に選択します。以下の自動選択オプションから選択できます。 ■ [なし]。スキャナを自動的に選択しません。 ■ [自動選択]。ローカル接続されているスキャナを自動的に選択します。 ■ [前回使用]。最後に使用されたスキャナを自動的に選択します。 ■ [指定]。[指定したスキャナ] テキスト ボックスに入力したスキャナ名を選択します。 この設定をコンピュータの構成ポリシーとして有効にすると、影響を受けるコンピュータのすべてのユーザーについて、この設定によりスキャナの自動選択モードが決まります。ユーザーは、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスの [デフォルト スキャナ] オプションを変更できません。 この設定をユーザーの構成ポリシーとして有効にすると、影響を受けるすべてのユーザーについて、この設定によりスキャナの自動選択モードが決まります。ただし、ユーザーは、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスの [デフォルト スキャナ] オプションを変更できます。 この設定をコンピュータの構成およびユーザーの構成の両方で有効にすると、影響を受けるコンピュータのすべてのユーザーについて、コンピュータの構成におけるスキャナの自動選択モードによって、ユーザーの構成における対応するポリシー設定がオーバーライドされます。 どちらかのポリシー構成でこの設定を無効にするか、または構成しないと、スキャナの自動選択モードは、対応するポリシー設定（ユーザーの構成またはコンピュータの構成）または [VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスにおけるユーザーの選択によって決まります。

シリアル ポート リダイレクトの構成

シリアル ポート リダイレクトを使用すると、ユーザーは内蔵の RS232 ポートまたは USB シリアル アダプタなどの、ローカルに接続されたシリアル（COM）ポートをリダイレクトできます。プリンタ、バーコード リーダー、およびその他のシリアル デバイスをこれらのポートに接続して、リモート デスクトップで使用できます。

シリアル ポート リダイレクトは Horizon Client for Windows 3.4 以降のリリースを搭載した Horizon 6 バージョン 6.1.1 以降のリリースで使用できます。

Horizon Agent をインストールし、シリアル ポート リダイレクトの機能を設定すると、この機能はそれ以上の構成なしにリモート デスクトップ上で動作できます。たとえば、リモート デスクトップ上に COM ポートがすでに存在する場合を除いて、ローカル クライアント システム上の COM1 はリモート デスクトップ上で COM1 としてリダイレクトされ、COM2 は COM2 としてリダイレクトされます。COM ポートがすでに存在する場合は、COM ポートがマップされ、競合は回避されます。たとえば、COM1 と COM2 がリモート デスクトップにすでに存在する場合、デフォルトでクライアントの COM1 は COM3 にマップされます。COM ポートを構成したり、デバイス ドライバをリモート デスクトップにインストールする必要はありません。

リダイレクトされた COM ポートをアクティブにするには、ユーザーはデスクトップ セッション中にシリアル ポート ツール トレイ アイコンのメニューから、 [[接続]] オプションを選択します。また、ユーザーはリモート デスクトップへのログイン時に COM ポート デバイスが必ず自動的に接続するよう設定することも可能です。シリアル ポート リダイレクトのユーザー操作を参照してください。

デフォルトの構成を変更するには、グループ ポリシー設定を構成できます。たとえば、設定をロックして、COM ポート マッピングまたはプロパティをユーザーが変更できないようにすることができます。ポリシーを設定して機能をすべて無効または有効にすることもできます。ADMX テンプレート ファイルを使用すると、ポート リダイレクト グループ ポリシー設定を Active Directory または個別のデスクトップにインストールできます。シリアル ポート リダイレクトのグループ ポリシー設定の構成を参照してください。

リダイレクトされた COM ポートが開いておりリモート デスクトップで使用されている場合、ローカル コンピュータでこのポートにアクセスできません。逆に、COM ポートがローカル コンピュータで使用中であれば、リモート デスクトップでこのポートにアクセスできません。

シリアル ポート リダイレクトのシステム要件

この機能を使用すると、エンド ユーザーは、内蔵の RS232 ポートまたは USB シリアル アダプタなど、ローカルに接続されたシリアル (COM) ポートをリモート デスクトップにリダイレクトできます。シリアル ポート リダイレクトをサポートするには、Horizon 環境が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

リモート デスクトップ

親またはテンプレート仮想マシン上のリモート デスクトップには、View Agent 6.1.1 以降または Horizon Agent 7.0 以降をインストールし、シリアル ポート リダイレクト設定オプションを設定する必要があります。デフォルトではこの設定オプションは選択解除されています。

次のゲスト OS はシングルセッションの仮想マシンでサポートされています。

- 32 ビットまたは 64 ビットの Windows 7
- 32 ビットまたは 64 ビットの Windows 8.x
- 32 ビットまたは 64 ビットの Windows 10
- デスクトップとして構成されている Windows Server 2008 R2
- デスクトップとして構成されている Windows Server 2012 R2
- デスクトップとして構成されている Windows Server 2016

この機能は Windows Server RDS ホスト向けには現在サポートされていません。

エージェントがインストールされているデスクトップ オペレーティング システムにシリアル ポート デバイス ドライバをインストールする必要はありません。

Horizon Client コンピュータまたはクライアント アクセス デバイス

- シリアル ポート リダイレクトは、Windows 7、Windows 8.x クライアント システム、および Windows 10 でサポートされています。
- 必要なシリアル ポート デバイス ドライバをすべてインストールする必要があり、シリアル ポートがクライアント コンピュータ上で操作可能である必要があります。エージェントがインストールされているリモート デスクトップのオペレーティング システムにデバイス ドライバをインストールする必要はありません。

表示プロトコル

- PCoIP

- VMware Blast（Horizon Agent 7.0 以降が必要）

VMware Horizon シリアル ポート リダイレクトは、RDP デスクトップ セッションでサポートされません。

シリアル ポート リダイレクトのユーザー操作

ユーザーは、クライアント コンピュータに接続された物理 COM ポート デバイスを操作でき、シリアル ポートの仮想化を使用して、デバイスをリモート デスクトップに接続できます。デバイスはここでサード パーティ アプリケーションにアクセスできます。

- Horizon Agent を使用してシリアル ポート リダイレクト オプションをインストールした後、シリアル ポート ツール トレイ アイコン（  ）がリモート デスクトップに追加されます。公開されたアプリケーションの場合、アイコンはローカル クライアント コンピュータにリダイレクトされます。

  このアイコンは、必要なバージョンの Horizon Agent と Horizon Client for Windows を使用し、PCoIP を介して接続している場合に表示されます。Mac、Linux、またはモバイル クライアントからリモート デスクトップに接続する場合、アイコンは表示されません。

  アイコンを使用して、マップされた COM ポートの接続、切断、カスタマイズを行うためのオプションを構成できます。

- シリアル ポート アイコンをクリックすると、[VMware Horizon のシリアル COM リダイレクト] メニューが表示されます。
- デフォルトではローカルに接続された COM ポートは、リモート デスクトップ上の対応する COM ポートにマップされます。たとえば、[COM1 は COM3 にマップされます]。マップされたポートはデフォルトでは接続されません。
- マップされた COM ポートを使用するには、[VMware Horizon のシリアル COM リダイレクト]メニューで手動で[接続]オプションを選択するか、以前のデスクトップ セッション時、またはグループ ポリシー設定の構成で、[自動接続]オプションを選択しておく必要があります。[自動接続]は、リモート デスクトップ セッション開始時に、マップされたポートを自動で接続するよう構成します。
- [接続]オプションを選択すると、リダイレクトされたポートはアクティブになります。リモート デスクトップ上のゲスト オペレーティング システムの [デバイス マネージャ] で、リダイレクトされたポートは [VMware Horizon のシリアル ポート リダイレクタ (COM*n*)] として表示されます。

  COM ポートが接続されると、サードパーティ アプリケーションでポートを開くことができ、これによってクライアント マシンに接続された COM ポート デバイスとデータを交換できます。アプリケーションでポートが開いているときは、[VMware Horizon のシリアル COM リダイレクト] メニューのポートは切断できません。

  COM ポートを切断する前に、アプリケーションでポートを閉じるか、アプリケーションを閉じる必要があります。その後、[切断]オプションを選択してポートを切断し、物理 COM ポートをクライアント マシンで使用できるようにできます。

- [VMware Horizon のシリアル COM リダイレクト] メニューで、 リダイレクトされたポートを右クリックすると、[Port Properties] コマンドを選択できます。

[COM プロパティ] ダイアログ ボックスでは、リモート デスクトップ セッションの開始時にポートを自動的に接続したり、データ セット準備完了（DSR）信号を無視したり、ポートを永続ポートにするように設定できます。また、[カスタム ポート名] ドロップダウン リストでポートを選択して、クライアントのローカル ポートがリモート デスクトップ上の異なる COM ポートにマッピングされるように設定できます。

リモート デスクトップ ポートは重複して表示されることがあります。たとえば、[COM1（重複）] のように見えることがあります。この場合、仮想マシンは ESXi ホスト上の仮想ハードウェアの COM ポートで構成されます。仮想マシン上で重複するポートにマップされている場合でも、リダイレクトされたポートを使用できます。仮想マシンは ESXi ホストを介して、またはクライアント システムから、シリアル データを受信します。

- ゲスト オペレーティング システムの [デバイス マネージャ] で、[プロパティ] - [ポートの設定]タブを使用して、リダイレクトされた COM ポートの設定を構成できます。たとえば、デフォルトのボーレートとデータビットを設定できます。ただしアプリケーションがポートの設定を指定した場合、[デバイス マネージャ] で構成した設定は無視されます。

エンド ユーザーがリダイレクトされるシリアル COM ポートを操作する手順については、『VMware Horizon Client for Windows の使用』を参照してください。

シリアル ポート リダイレクトの構成に関するガイドライン

グループ ポリシーの設定を使用してシリアル ポート リダイレクトを構成し、リダイレクトされた COM ポートをユーザーがどの程度カスタマイズできるかを制御できます。選択肢は社内のユーザーのロールとサードパーティ アプリケーションによって異なります。

グループ ポリシー設定の詳細については、シリアル ポート リダイレクトのグループ ポリシー設定を参照してください。

- ユーザーが同じサードパーティ アプリケーションと COM ポート デバイスを使用している場合は、リダイレクトされたポートが同じように構成されていることを確認します。たとえば、POS（販売時点情報管理）デバイスを使用する銀行や小売店では、すべての COM ポート デバイスがクライアント エンドポイントの同じポートに接続され、すべてのポートがリモート デスクトップ上の同じリダイレクトされた COM ポートにマップされていることを確認してください。

  クライアント ポートをリダイレクトされたポートへマップするには、[PortSettings] ポリシー設定を設定します。各デスクトップ セッションの開始時に、[PortSettings] の [自動接続]の項目を選択し、リダイレクトされたポートが接続されていることを確認してください。ユーザーがポート マッピングを変更したり、ポートの構成をカスタマイズできないようにするには、[構成のロック] ポリシー設定を有効にします。このシナリオでは、ユーザーは手動で接続や切断を行う必要がなく、ユーザーが誤ってリダイレクトされた COM ポートがサードパーティ アプリケーションにアクセスできないようにしてしまうことを防ぎます。

- ユーザーが各種のサードパーティ アプリケーションを使用するナレッジ ワーカーで、クライアント マシンでローカルに COM ポートを使用する可能性がある場合、ユーザーがリダイレクトされた COM ポートから接続および切断を行えるようにする必要があります。

  デフォルトのポート マッピングが間違っている場合は、[PortSettings] ポリシー設定を設定できます。ユーザーの要件に応じて、[自動接続] の項目を設定する場合としない場合があります。[構成のロック] ポリシー設定は有効にしません。

- サードパーティ アプリケーションがリモート デスクトップにマップされている COM ポートを開くことを確認します。

- デバイスに使用中のボーレートがサードパーティ アプリケーションが使用しようとしているボーレートと一致することを確認します。
- クライアント システムからリモート デスクトップへ最大 5 個の COM ポートをリダイレクトできます。

シリアル ポート リダイレクトのグループ ポリシー設定の構成

リモート デスクトップでのシリアル ポート リダイレクトの動作を制御するグループ ポリシー設定を構成できます。これらのポリシー設定を使用して、ユーザのデスクトップの [[VMware Horizon のシリアル COM リダイレクト]] メニューで使用できるオプションを、一元的に Active Directory から制御できます。

これらのポリシ設定を構成する必要はありません。シリアル ポート リダイレクトは、リモート デスクトップやクライアント システム上のリダイレクトされた COM ポート用に構成されたデフォルトの設定で機能します。

このポリシー設定はユーザーのリモート デスクトップに影響し、物理 COM ポート デバイスが接続されたクライアント システムには影響しません。これらの設定をデスクトップで構成するには、Active Directory にシリアル ポート リダイレクト グループ ポリシー管理テンプレート (ADMX) ファイルを追加します。

Active Directory へのシリアル ポート リダイレクト ADMX テンプレートの追加

シリアル COM（シリアル ポート リダイレクト）ADMX ファイル (`vdm_agent_serialport.admx`) のポリシーを Active Directory のグループ ポリシー オブジェクト (GPO) に追加し、グループ ポリシー オブジェクト エディタで設定することができます。

前提条件

- デスクトップにシリアル ポート リダイレクト設定オプションがインストールされていることを確認します。シリアル ポート リダイレクトがインストールされていないと、グループ ポリシー設定は有効になりません。Horizon Agent のインストールの詳細については、各セットアップ ガイドを参照してください。
- シリアル ポート リダイレクトのグループ ポリシー設定用に Active Directory GPO が作成されていることを確認します。GPO は、デスクトップを含む OU にリンクする必要があります。Active Directory グループ ポリシーの例を参照してください。
- MMC およびグループ ポリシー オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。
- シリアル ポート リダイレクトのグループ ポリシー設定について理解しておきます。シリアル ポート リダイレクトのグループ ポリシー設定を参照してください。

手順

1 Horizon 7 GPO Bundle `.zip` ファイルを https://my.vmware.com/web/vmware/downloads の VMware ダウンロード サイトからダウンロードします。

[Desktop & End-User Computing（デスクトップおよびエンドユーザー コンピューティング）] で VMware Horizon 7 のダウンロードを選択します。これには GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` で、*x.x.x* はバージョン、*yyyyyyy* はビルド番号を表します。Horizon 7 のグループ ポリシー設定用の ADMX ファイルはすべて、このファイルで提供されています。

2 VMware-Horizon-Extras-Bundle-*x.x.x*-*yyyyyyy*.zip ファイルを解凍して、ADMX ファイルを Active Directory サーバにコピーします。

   a vdm_agent_serialport.admx ファイルと en-US フォルダを Active Directory サーバの C:\Windows\PolicyDefinitions フォルダにコピーします。

   b （オプション） 言語リソース ファイル (vdm_agent_serialport.adml) を Active Directory サーバの C:\Windows\PolicyDefinitions\ 内の適切なサブフォルダにコピーします。

3 Active Directory サーバで、グループ ポリシー管理エディタを開き、エディタでテンプレート ファイルへのパスを入力します。

   設定は、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware View Agent の構成] - [シリアル COM] フォルダに格納されています。

   ほとんどの設定は、[ユーザー構成] フォルダにも追加されます。このフォルダは、[ユーザー構成] - [ポリシー] - [管理用テンプレート] - [VMware View Agent の構成] - [シリアル COM] 内にあります。

次のステップ

グループ ポリシー設定を構成します。

シリアル ポート リダイレクトのグループ ポリシー設定

シリアル ポート リダイレクトのグループ ポリシー設定は、リダイレクトされた COM ポートの構成を制御します。これにはリモート デスクトップの [VMware Horizon のシリアル COM リダイレクト]メニューで使用できるオプションが含まれます。

シリアル ポート リダイレクト ADMX ファイルには、コンピュータの構成とユーザーの構成の両方のポリシーが含まれます。ユーザーの構成ポリシーによって、VDI デスクトップの指定されたユーザに異なる構成を設定できます。コンピュータの構成で構成されたポリシー設定は、ユーザーの構成で構成された対応する設定よりも優先されます。

グループ ポリシー設定	コンピュータ	ユーザー	説明
PortSettings1 PortSettings2 PortSettings3 PortSettings4 PortSettings5	X	X	ポート設定は、クライアント システム上の COM ポートと、リモート デスクトップ上のリダイレクトされた COM ポートの間のマッピングを決定し、リダイレクトされた COM ポートに影響する他の設定を決定します。リダイレクトされた 各 COM ポートを個別に構成します。 5 個のポート設定ポリシーを利用でき、最大 5 個の COM ポートをクライアントからリモート デスクトップにマッピングできます。構成する各 COM ポートのポート設定ポリシーを 1 つ選択します。ポート設定ポリシーを有効にすると、リダイレクトされた COM ポートに影響する以下の項目を設定できます。 ■ [ソース ポート番号]の設定は、クライアント システムに接続される物理 COM ポートの数を指定します。 ■ [ターゲット仮想ポート番号]の設定は、リモート デスクトップ上のリダイレクトされた仮想 COM ポートの数を指定します。 ■ [自動接続]の設定は各デスクトップ セッションの開始時に、COM ポートをリダイレクトされた COM ポートに自動的に接続します。 ■ [IgnoreDSR] の設定では、リダイレクトされた COM ポート デバイスは [データセットの準備完了 (DSR)] 信号を無視します。 ■ [ポートを閉じる前に停止（ミリ秒)]の設定は、ユーザーがリダイレクトされたポートを閉じた後と、ポートが実際に閉じる前に待機する時間（ミリ秒）を指定します。特定の USB シリアル アダプタでは、転送されたデータが確実に保持するために、この遅延を必要とします。この設定はトラブルシューティングを目的としています。 ■ [Serial2USBModeChangeEnabled] の設定は、GlobalSat BU353 GPS アダプタを含め、Prolific チップセットを使用する USB シリアル アダプタに該当する問題を解決します。Prolific チップセット アダプタ用のこの設定を有効にしない場合、接続したデバイスはデータを転送できますが、データを受信することはできません。 ■ [待機マスクのエラーの無効化]の設定は、COM ポート マスクのエラー値を無効にします。このトラブルシューティング設定は特定のアプリケーション向けに必要です。詳細については、http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx の `WaitCommEvent` 機能に関する Microsoft の文書を参照してください。 ■ [HandleBtDisappear] の設定は BlueTooth COM ポートの動作をサポートします。この設定はトラブルシューティングを目的としています。 ■ [UsbToComTroubleShooting] の設定は USB シリアル ポート アダプタに該当する一部の問題を解決します。この設定はトラブルシューティングを目的としています。 ■ [永久] 設定を使用すると、クライアントの切断後も、リモート セッションでリダイレクトされた COM ポートのステータスを維持できます。 特定の COM ポートのポート設定ポリシーを有効にすると、ユーザーはリダイレクトされたポートを接続/切断できますが、リモート デスクトップ上のポートのプロパティを構成することはできません。たとえば、ユーザーはデスクトップへのログイン時にポートが自動的にリダイレクトされるように設定することはできません。また、DSR 信号は無視できませせん。これらのプロパティはグループ ポリシー設定によって制御されます。 **注:** リダイレクトされた COM ポートは物理 COM ポートがローカルでクライアント システムに接続されている場合のみ接続されアクティブになります。クライアントに存在しない COM ポートをマップする場合、リダイレクトされたポートは非アクティブの表示になり、リモート デスクトップ上のツール トレイ メニューでは使用できません。 ポート設定ポリシーが無効になっているか構成されていない場合、リダイレクトされた COM ポートはユーザーがリモート デスクトップ上で構成した設定を使用します。[VMware Horizon のシリアル COM リダイレクト] メニュー オプションはアクティブでユーザーが使用できます。

グループ ポリシー設定	コンピュータ	ユーザー	説明
			これらの設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [シリアル COM] - [PortSettings] フォルダにあります。
Local settings priority	X	X	リモート デスクトップ上で構成された設定を優先します。 このポリシーを有効にすると、ユーザーがリモート デスクトップで構成するシリアル ポート リダイレクト設定が、グループ ポリシー設定よりも優先されます。グループ ポリシー設定は、設定がリモート デスクトップで構成されていない場合のみ有効になります。 この設定が無効になっているか構成されていない場合は、リモート デスクトップ上で構成された設定よりも、グループ ポリシー設定が優先されます。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [シリアル COM] フォルダにあります。
Disable functionality	X		シリアル ポート リダイレクト機能を無効にします。 この設定を有効にすると、COM ポートはリモート デスクトップにリダイレクトされません。リモート デスクトップ上のシリアル ポート ツール トレイ アイコンも表示されません。 この設定が無効になっている場合、シリアル ポート リダイレクトは機能し、シリアル ポート ツール トレイ アイコンが表示され、[VMware Horizon のシリアル COM リダイレクト] メニューに COM ポートが表示されます。 この設定が構成されていない場合、リモート デスクトップへのローカルの設定によって、シリアル ポート リダイレクトが無効か有効かが決まります。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [シリアル COM] フォルダにあります。
Lock configuration	X	X	シリアル ポート リダイレクトのユーザー インターフェイスをロックし、ユーザーがリモート デスクトップの構成オプションを変更するのを防止します。 この設定を有効にすると、ユーザーはデスクトップのツール トレイ メニューから使用できるオプションを構成できません。ユーザーは [VMware Horizon のシリアル COM リダイレクト] メニューを表示できますが、オプションは非アクティブで変更はできません。 この設定が無効になっている場合、ユーザーは [VMware Horizon のシリアル COM リダイレクト] メニューのオプションを設定できます。 この設定が構成されていない場合、リモート デスクトップのローカル プログラムの設定によって、ユーザーが COM ポート リダイレクト設定を構成できるかどうかが決まります。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [シリアル COM] フォルダにあります。
Bandwidth limit	X		データ転送速度の限界を、リダイレクトされたシリアル ポートとクライアント システムの間の 1 秒あたりのキロバイト数で設定します。 この設定を有効にすると、リダイレクトされたシリアル ポートとクライアントの間の最大データ転送速度を決定する[バンド幅制限（キロバイト/秒)] ボックスの値を設定できます。値「0」はバンド幅制限を無効にします。 この設定が無効になっている場合、バンド幅制限は設定されていません。 この設定が構成されていない場合、リモート デスクトップのローカル プログラムの設定によって、バンド幅制限が設定されるかどうか決定します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [シリアル COM] フォルダにあります。

USB シリアル アダプタの構成

シリアル ポート リダイレクト機能によって、Prolific チップセットを使用する USB シリアル アダプタを、リモート デスクトップにリダイレクトするように構成することができます。

Prolific チップセット アダプタでデータの適切な転送を確実に行うには、Active Directory または個別のデスクトップ仮想マシンのシリアル ポート リダイレクト グループ ポリシー設定を有効にします。

Prolific チップセット アダプタの問題を解決するようグループ ポリシー設定を構成しない場合、接続されたデバイスはデータを転送できますが、データを受信することはできません。

クライアント システムのポリシー設定またはレジストリ キーは構成する必要はありません。

前提条件

- デスクトップにシリアル ポート リダイレクト設定オプションがインストールされていることを確認します。シリアル ポート リダイレクトがインストールされていないと、グループ ポリシー設定は有効になりません。Horizon Agent のインストールの詳細については、各セットアップ ガイドを参照してください。
- シリアル ポート リダイレクト ADMX テンプレート ファイルが Active Directory またはデスクトップ仮想マシンに追加されていることを確認します。
- [PortSettings] グループ ポリシー設定の [Serial2USBModeChangeEnabled] の項目について理解しておきます。シリアル ポート リダイレクトのグループ ポリシー設定を参照してください。

手順

1 Active Directory または仮想マシン上で、[グループ ポリシー オブジェクト エディタ] を開きます。

2 [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [従来の管理テンプレート] - [VMware View Agent の構成] - [シリアル COM] フォルダの順に移動します。

3 [PortSettings] フォルダを選択します。

4 [PortSettings] グループ ポリシー設定を選択し有効にします。

5 COM ポートをマップするための、ソースおよびターゲットの COM ポート番号を指定します。

6 [Serial2USBModeChangeEnabled] チェックボックスを選択します。

7 必要に応じて [PortSettings] ポリシー設定の他の項目を構成します。

8 [OK] をクリックし、グループ ポリシー オブジェクト エディタを閉じます。

ユーザーが次のデスクトップ セッションを開始すると、USB シリアル アダプタはリモート デスクトップにリダイレクトでき、データを正常に受信できます。

Windows Media マルチメディア リダイレクト (MMR) へのアクセスの管理

Horizon 7 は、単一ユーザーのマシンで実行される VDI デスクトップと、 RDS デスクトップ向けの Windows Media MMR 機能を提供します。

MMR は、マルチメディア ストリームをクライアント コンピュータに直接提供します。MMR を使用すると、クライアント システムでマルチメディア ストリームが処理（デコード）されます。クライアント システムはメディア コンテンツを再生し、それによって ESXi ホストの要求を開放します。

MMR データはアプリケーション ベースの暗号化なしにネットワーク経由で送信されますが、リダイレクトされるコンテンツによっては、機密データが含まれていることもあります。このデータがネットワークで盗まれないようにするには、安全なネットワークで MMR だけを使用してください。

安全なトンネルが有効になっている場合、クライアントと View Secure Gateway の間の MMR 接続は保護されますが、View Secure Gateway からデスクトップ マシンへの接続は暗号化されません。安全なトンネルが無効になっている場合、クライアントからデスクトップ マシンへの MMR 接続は暗号化されません。

Horizon 7 でのマルチメディア リダイレクトの有効化

以下の手順によって、MMR がアクセス可能であるのは、ローカル マルチメディア デコーディングを処理するための十分なリソースを持ち、セキュア ネットワークの Horizon 7 に接続されている Horizon Client システムのみであることを確認できます。

デフォルトでは、View Administrator のグローバル ポリシーで、[マルチメディア リダイレクト (MMR)] は [拒否] に設定されています。

MMR を使用するには、この値を明示的に [許可] に設定する必要があります。

MMR へのアクセスを制御するには、個別のデスクトップ プール、または特定のユーザーに対してグローバルに [マルチメディア リダイレクト (MMR)] ポリシーを有効または無効にします。

Horizon Administrator でグローバル ポリシーを設定する手順については、 Horizon 7 ポリシーを参照してください。

Windows Media MMR のシステム要件

Windows Media マルチメディア リダイレクト (MMR) をサポートするには、Horizon 7 の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。Windows Media MMR は、Horizon 6.0.2 以降のリリースで提供されます。

Horizon 7 リモート デスクトップ

- この機能は、単一ユーザーの仮想マシンに展開された仮想マシン デスクトップと、RDS デスクトップでサポートされます。

  RDS デスクトップでこの機能をサポートするには、View Agent 6.1.1 以降が必要です。

  単一ユーザーのマシンでこの機能をサポートするには、View Agent 6.0.2 以降が必要です。

- 次のゲスト OS がサポートされています。
  - 64 ビットまたは 32 ビットの Windows 10。Windows Media Player がサポートされます。デフォルトの TV および動画プレーヤはサポートされません。

- Windows Server 2016 は、技術プレビュー機能です。Windows Media Player がサポートされます。デフォルトの TV および動画プレーヤはサポートされません。
- 64 ビットまたは 32 ビット Windows 7 SP1 Enterprise または Ultimate（単一ユーザーのマシン）Windows 7 Professional はサポートされません。
- 64 ビットまたは 32 ビットの Windows 8/8.1 Professional または Enterprise（単一ユーザーのマシン）
- RDS ホストとして構成されている Windows Server 2008 R2
- RDS ホストとして構成されている Windows Server 2012 および 2012 R2

- [3D レンダリング] はデスクトップ プールで有効または無効にできます。
- ユーザーは Windows Media Player 12 以降または Internet Explorer 8 以降でビデオを再生する必要があります。

  Internet Explorer を使用するには、保護モードを無効にする必要があります。[インターネット オプション] ダイアログ ボックスで、[セキュリティ] タブをクリックし、[保護モードを有効にする] をオフにします。

Horizon Client ソフトウェア

単一ユーザーのマシンで Windows Media MMR をサポートするには、Horizon Client 3.2 for Windows 以降のリリースが必要です。

Horizon Client コンピュータまたはクライアント アクセス デバイス

- クライアントは、64 ビットまたは 32 ビットの Windows 7、Windows 8/8.1、または Windows 10 オペレーティング システムで実行する必要があります。

サポートされるメディア フォーマット

Windows Media Player でサポートされるメディア フォーマットがサポートされます。たとえば、M4V、MOV、MP4、WMP、MPEG-4 Part 2、WMV 7/8/9、WMA、AVI、ACE、MP3、WAV などです。

注: DRM で保護されたコンテンツは、Windows Media MMR 経由でリダイレクトされません。

Horizon ポリシー

Horizon Administrator で、[マルチメディア リダイレクト (MMR)] ポリシーを [許可] に設定します。デフォルト値は [拒否] です。

バックエンド ファイアウォール

お使いの Horizon 7 で DMZ ベースのセキュリティ サーバと社内ネットワークの間にバックエンド ファイアウォールが置かれている場合は、バックエンド ファイアウォールがお使いのデスクトップのポート 9427 へのトラフィックを許可していることを確認します。

ネットワーク遅延に基づく Windows Media MMR の使用の決定

デフォルトでは、Windows Media MMR は、Windows 8 以降上で実行されている単一ユーザーのデスクトップ、あるいは Windows Server 2012 か 2012 R2 以降で実行されている RDS デスクトップのネットワーク状態に適応します。Horizon Client とリモート デスクトップの間のネットワーク遅延が 29 ミリ秒以下の場合、ビデオは Windows Media MMR を使用してリダイレクトされます。 ネットワーク遅延が 30 ミリ秒以上の場合、ビデオはリダイレクトされません。 代わりに、ビデオは ESXi ホストでレンダリングされ、PCoIP を介してクライアントに送信されます。

この機能は Windows 8 以降の単一ユーザー デスクトップと、Windows Server 2012 または 2012 R2 以降 の RDS デスクトップに適用されます。ユーザーはサポートされているクライアント システム、Windows 7、または Windows 8/8.1 を実行できます。

この機能は Windows 7 単一ユーザー デスクトップまたは Windows Server 2008 R2 RDS デスクトップには適用されません。これらのゲスト オペレーティング システムで、Windows Media MMR はネットワーク遅延と関わりなく常にマルチメディア リダイレクトを実行します。

デスクトップ上で `RedirectionPolicy` レジストリ設定を構成して、ネットワーク遅延に関係なく Windows Media MMR がマルチメディア リダイレクトを実行するように強制することで、この機能を上書きできます。

手順

1 リモート デスクトップで Windows レジストリ エディタを起動します。

2 リダイレクト ポリシーを制御する Windows レジストリ キーに移動します。

リモート デスクトップで構成するレジストリ キーは、Windows Media Player のバージョンが何ビット版かによって異なります。

オプション	説明
64 ビット版 Windows Media Player	■ 64 ビット版デスクトップの場合、レジストリ キー：`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr` を使用します。
32 ビット版 Windows Media Player	■ 32 ビット版デスクトップの場合、レジストリ キー：`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr` を使用します。 ■ 64 ビット版デスクトップの場合、レジストリ キー：`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware tsmmr` を使用します。

3 `RedirectionPolicy` の値を `always` に設定します。

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

4 Windows Media Player をデスクトップで再起動して、更新した値を有効にします。

クライアント ドライブ リダイレクトへのアクセスの管理

クライアント ドライブのリダイレクトを有効にして Horizon Client と Horizon Agent を展開すると、フォルダやファイルが暗号化され、ネットワーク上を転送されます。

クライアントと View Secure Gateway 間のクライアント ドライブ リダイレクト接続と、View Secure Gateway からデスクトップ マシンへの接続の安全性は確保されています。VMware Blast を有効にすると、ファイルとフォルダが暗号化され、仮想チャネル経由で転送されます。

クライアント ドライブ リダイレクトをサポートするには、ポート 9427 での TCP 接続が必要です。Horizon 7 環境で、DMZ ベースのセキュリティ サーバと社内ネットワークの間にバックエンド ファイアウォールを配置している場合、バックエンド ファイアウォールがリモート デスクトップのポート 9427 へのトラフィックを許可している必要があります。VMware Blast が有効になっている場合、クライアント ドライブのリダイレクトは仮想チャネル経由でデータを転送するため、TCP ポート 9427 を開く必要ありません。

Horizon Agent インストーラの [クライアント ドライブのリダイレクト] カスタム セットアップ オプションがデフォルトで選択されています。ベスト プラクティスとして、[クライアント ドライブのリダイレクト] カスタム セットアップ オプションは、ユーザーがこの機能を必要とするリモート デスクトップでのみ有効にします。

バージョン 3.5 より前の Horizon Client または バージョン 6.2 より前の Horizon Agent の場合、クライアント ドライブのリダイレクトでフォルダとファイルが暗号化されずに、ネットワーク上を転送されます。リダイレクトされるコンテンツによっては、これらのフォルダまたはファイルに秘密データが含まれている可能性があります。安全なトンネルを有効にすると、Horizon Client と View Secure Gateway のクライアント ドライブ リダイレクト接続は保護されますが、View Secure Gateway からデスクトップ マシンへの接続は暗号化されません。安全なトンネルを無効にすると、Horizon Client からデスクトップ マシンへのクライアント ドライブ リダイレクト接続は暗号化されません。以前のリリースのクライアントおよびエージェントの場合には、このようなデータがネットワーク上で監視されないように、保護されたネットワークに対してのみクライアント ドライブのリダイレクトを使用してください。

グループ ポリシーを使用したクライアント ドライブ リダイレクトの無効化

Active Directory サーバで、リモート デスクトップのグループ ポリシー設定を使用すると、クライアント ドライブのリダイレクトを無効にすることができます。

このグループ ポリシー設定により、クライアント ドライブのリダイレクト機能を有効にするローカル レジストリとスマート ポリシー 設定がオーバーライドされます。

前提条件

- Active Directory サーバをホストするマシンに管理者ドメイン ユーザーとしてログインできることを確認します。
- MMC およびグループ ポリシー オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。
- 仮想デスクトップの場合には、組織単位 (OU)、公開デスクトップの場合には RDS ホストにリンクしている GPO に、リモート デスクトップ サービスの ADMX テンプレート ファイル (`vmware_rdsh_server.admx`) を追加します。インストール手順については、Active Directory への ADMX テンプレート ファイルの追加を参照してください。

手順

1 Active Directory サーバで、グループ ポリシー管理エディタを開き、[コンピュータの構成\ポリシー\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] に移動します。

2 [ドライブ リダイレクトを許可しない] グループ ポリシー設定を開いて [有効] を選択し、[OK] をクリックします。

レジストリ設定を使用したクライアント ドライブ リダイレクトの構成

Windows レジストリ キー設定を使用して、リモート デスクトップでのクライアント ドライブ リダイレクトの動作を制御できます。この機能には Horizon Agent 7.0 以降および Horizon Client 4.0 以降が必要です。

リモート デスクトップでのクライアント ドライブ リダイレクトの動作を制御する Windows レジストリ設定は、次のパスにあります。

```
HKLM\Software\VMware, Inc.\VMware TSDR
```

リモート デスクトップで Windows レジストリ エディタを使用して、ローカル レジストリ設定を編集できます。

注: スマート ポリシー で設定されたクライアント ドライブ リダイレクト ポリシーは、ローカル レジストリ設定よりも優先されます。

クライアント ドライブ リダイレクトの無効化

クライアント ドライブ リダイレクトを無効にするには、`disabled` という新しい文字列値を作成し、その値を `true` に設定します。

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

デフォルトでは、この値は `false`（有効）になっています。

共有フォルダへの書き込みアクセスの防止

リモート デスクトップと共有されるすべてのフォルダへの書き込みアクセスを防止するには、`permissions` という新しい文字列値を作成し、その値を `rw` 以外の `r` で始まる任意の文字列に設定します。

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

デフォルトでは、この値は `rw`（すべての共有フォルダが読み取り可能で書き込み可能）になっています。

特定のフォルダの共有

特定のフォルダをリモート デスクトップと共有するには、`default shares` という新しいキーを作成し、リモート デスクトップと共有する各フォルダに対して新しいサブキーを作成します。各サブキーで、`name` という新しい文字列値を作成し、その値を共有するフォルダのパスに設定します。次の例では、フォルダ `C:\ebooks` と `C:\spreadsheets` を共有しています。

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

`name` を `*all` に設定すると、すべてのクライアント ドライブがリモート デスクトップと共有されます。`*all` 設定は、Windows クライアント システムでのみサポートされています。

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

クライアントの他のフォルダ（default shares キーで指定されていないフォルダ）が共有されることを防止するには、ForcedByAdmin という文字列値を作成し、その値を true に設定します。

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

値が true の場合、Horizon Client でユーザーがリモート デスクトップに接続したときに [共有] ダイアログ ボックスは表示されません。デフォルトでは、この値は false（クライアントの他のフォルダを共有可能） になっています。

次の例では、フォルダ C:\ebooks と C:\spreadsheets を共有して両方のフォルダを読み取り専用にし、クライアントの他のフォルダが共有されることを防止しています。

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

注: セキュリティ機能または共有制御として、ForcedByAdmin 機能を使用しないでください。ユーザーは、既存の共有へのリンクを作成することにより、ForcedByAdmin=true 設定をする必要がありません。既存の共有は、default shares キーで指定されていないフォルダを指定します。

Unified Access Gateway 環境でのクライアント ドライブ リダイレクトの使用

Horizon 7 環境で、セキュリティ サーバではなく Unified Access Gateway アプライアンスが使用され、ユーザーが PCoIP 表示プロトコルでクライアント ドライブ リダイレクトを使用し、Horizon Client と Horizon Agent マシンが別のネットワーク上にある場合、Unified Access Gateway アプライアンスで UDP トンネル サーバを有効にする必要があります。

UDP トンネル サーバを有効にするには、Unified Access Gateway 管理ユーザー インターフェイスで [UDP トンネル サーバが有効] を [はい] に設定します。

UDP トンネル サーバを有効にしないと、ユーザーは PCoIP 表示プロトコルでクライアント ドライブ リダイレクト機能を使用できません。クライアント ドライブ リダイレクトは、UDP トンネル サーバが有効かどうかに関係なく、VMware Blast 表示プロトコルで動作します。

詳細については、『Unified Access Gateway』ドキュメントを参照してください。

Skype for Business の構成

仮想インフラストラクチャに影響を及ぼしたり、ネットワークを過負荷状態にすることなく、仮想デスクトップ内の Skype for Business で最適な音声通話とビデオ通話を行うことができます。

Skype の音声通話またはビデオ通話中は、仮想デスクトップではなくクライアント マシンですべてのメディア処理が実行されます。

VMware Horizon Virtualization Pack for Skype for Business

Skype for Business を使用するには、クライアント マシンに VMware Horizon Virtualization Pack for Skype for Business が必要です。

デフォルトの構成を変更するには、グループ ポリシー設定を構成できます。VMware Virtualization Pack for Skype for Business ポリシー設定を参照してください。

Horizon Agent のインストール時に、Horizon 管理者が VMware Horizon Virtualization Pack for Skype for Business を仮想デスクトップにインストールする必要があります。Horizon Client for Windows のインストール方法については、『VMware Horizon Client for Windows の使用』ドキュメントを参照してください。

VMware Horizon Virtualization Pack for Skype for Business には、次のソフトウェア モジュールが含まれています。

- Horizon メディア プロキシ。仮想デスクトップ内にインストールされます。
- Horizon Media Provider。クライアント エンドポイントにインストールされます。

Skype for Business の機能

Skype for Business には次の機能があります。

- E911 呼び出し
- コールパークと応答
- 外部の会議に匿名で参加する
- 通話をモバイル デバイスにリダイレクトする
- 通話統計
- スマート カード認証
- ポイントツーポイントの音声通話
- ポイントツーポイントのビデオ通話
- ダイアル パッドでの PSTN 通話
- 通話の転送、ミュート、再開
- HID コマンド
- 仲介サーバ経由での PSTN 通話
- リモート接続と Edge サーバからの呼び出し
- 保留中の音楽再生
- カスタム着信音
- ボイスメールの統合
- USB フォン
- 公開アプリケーションのサポート
- オーディオとビデオの前方誤り訂正 (FEC)
- マルチパーティのオーディオ/ビデオ会議
- 「今すぐミーティング」会議

- ホワイトボード機能と画面共有

システム要件

この機能は次の構成をサポートします。

表 2-4. Skype for Business System の要件

システム	要件
Microsoft サーバ	Lync Server 2013、Skype for Business Server 2015、Office365
Microsoft クライアント	最新の Skype for Business 2015 クライアント 15.0.4933.100 以降を使用することを強く推奨します。 Office 365 Plus に含まれている Skype for Business 2016: 16.0.7571.2072 以降 Office 2016 に含まれている Skype for Business 2016: 16.0.4561.1000 以降
仮想デスクトップのオペレーティング システム	■ Windows 7 SP1 ■ Windows 8.1 ■ Windows 10 パーシステントおよび非パーシステント デスクトップ ■ Windows 2008 R2 SP1 デスクトップ ■ Windows 2012 R2 デスクトップ ■ Windows 2008 R2 SP1 RDSH デスクトップ ■ Windows 2012 R2 RDSH デスクトップ ■ 公開アプリケーションのサポート
クライアント マシンのオペレーティング システム	■ Windows 7 SP1 ■ Windows 8.1 ■ Windows 10 ■ WES7 ■ Windows 10 IoT ■ Ubuntu 14.04（32 ビット） ■ Ubuntu 14.04（64 ビット） ■ Ubuntu 16.04（64 ビット） ■ RHEL 6.9（32 ビット） ■ RHEL 6.9（64 ビット） ■ RHEL 7.3（64 ビット） ■ CentOS 6.x（32 ビット） ■ CentOS 6.x（64 ビット） ■ SLED 12 SP2（64 ビット）
展開	VDI のみ（オンプレミスとクラウド）、永続および非永続デスクトップ
表示プロトコル	VMware Blast および PCoIP
ネットワーク ポート	Skype for Business ネイティブ クライアントで使用されているポートと同じ。クライアント ポートの詳細については、https://technet.microsoft.com/en-us/library/gg398833.aspx を参照してください。
マイクロフォンと Web カメラ	Skype for Business で動作確認されている機器。Web カメラの一覧については、https://technet.microsoft.com/en-us/office/dn947482.aspx を参照してください。

システム	要件
オーディオおよびビデオ codec	Skype for Business ネイティブ クライアントで使用されている オーディオおよびビデオ codec と同じ。https://technet.microsoft.com/en-us/library/gg425841.aspx?f=255&MSPPError=-2147217396 を参照してください。
メディア機能パック	Windows 10 N および KN バージョンの場合には、リモート デスクトップにインストールする必要があります。メディア機能は、https://www.microsoft.com/en-us/download/details.aspx?id=48231 からインストールできます。

制限

Skype for Business には次の制限があります。

- IPv6 はサポートされません。IPv4 のみの展開がサポートされます。
- 応答グループ呼び出しまたは X（自宅、職場など）経由での通話はサポートされていません。
- ギャラリー ビューは現在サポートされていません。
- 通話を記録することはできません。
- Horizon Client にネストされた Horizon Agent など、ダブル ホップ シナリオはサポートされていません。
- クライアント マシンの Lync または Skype for Business クライアントと、リモート デスクトップで最適化された Skype for Business クライアントを同時に使用することはできません。
- Skype 2015 クライアントから Lync 2013 サーバに接続した場合、Lync 2013 クライアントのユーザー インターフェイスを使用できません。管理者は、サーバで Skype クライアントのユーザー インターフェイスを設定できます。https://social.technet.microsoft.com/wiki/contents/articles/30282.switch-between-skype-for-business-and-lync-client-ui.aspx を参照してください。
- ビデオのプレビュー ウィンドウで、リストにないカメラでプレビューする場合には、その機器を選択してダイアログを閉じ、再度開いてプレビューしてください。
- プライベート ネットワークに接続しているときに、リモート デスクトップに Skype for Business をインストールすると、インストーラがこのネットワークのプロファイルにファイアウォール ルール（受信および送信）を追加します。ドメイン ネットワークからリモート デスクトップにログインして Skype for Business を使用すると、ファイアウォール例外が発生します。この問題を解決するには、すべてのネットワーク プロファイルのファイアウォール ルールで、Skype for Business クライアントにファイアウォール例外を手動で追加してください。
- リモート デスクトップのオペレーティング システムで音量を調節しても、実行中の Skype 通話の音量レベルが変わりません。音量を変更するには、クライアント マシンで Skype 通話の音量を調整してください。

Skype for Business のトラブルシューティングのためのログ収集

Skype for Business のトラブルシューティングを行うには、Horizon Agent と Windows の Horizon Client からログを収集します。

手順

1 メディア プロキシ ログを含む Horizon ログを収集するには、Horizon Agent がインストールされている仮想マシンに Horizon Agent からログインします。

2 コマンド プロンプトを開いて、C:\Program Files\VMware\VMware View\Agent\DCT\support.bat を実行します。

3 メディア プロバイダ ログを含む Horizon ログを収集するには、Horizon Client がインストールされている仮想マシンに Horizon Client からログインします。

4 コマンド プロンプトを開いて、次のコマンドを実行します。

- 32 ビット：C:\Program Files\VMware\VMware Horizon View Client\DCT\support.bat
- 64 ビット：C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat

圧縮ログ ファイルを含む vdm-sdct フォルダがデスクトップに表示され、このフォルダに VMware Horizon Virtualization Pack for Skype for Business のログを含むこれらのディレクトリが収納されます。

- クライアント デバイス：%TEMP%\vmware-<username>\VMWMediaProvider
- 仮想デスクトップ：
  - %TEMP%\vmware-<username>\VMWMediaProviderProxy
  - %TEMP%\vmware-<username>\VMWMediaProviderProxyLocal
  - %TEMP%\vmware-<username>\MMAPlugin

デフォルトのログ レベルは 7 で、このレベルではログ レベル サイズとクラッシュ ダンプが小さくなります。ログ レベルを最大の 8 にすると、ログ レベルが最大になり、完全なクラッシュ ダンプが生成されます。すべての設定は DWORD で行います。

- クライアント：HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProvider/DebugLogging/LoggingPriority = 8
- エージェント：HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProviderProxy/DebugLogging/LoggingPriority = 8
- エージェント：HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProviderProxyLocal/DebugLogging/LoggingPriority = 8

USB またはクライアント ドライブ リダイレクトでの BEAT サイド チャネルの有効化

VMware Blast 表示プロトコルでは、USB リダイレクトとクライアント ドライブ リダイレクト機能を使用し、VMware 仮想チャネル (VVC) や TCP サイド チャネルではなく、Blast Extreme Adaptive Transport (BEAT) 接続を介してサイド チャネル トラフィックを送信できます。

BEAT サイド チャネルを使用すると、USB リダイレクトとクライアント ドライブ リダイレクトのネットワーク ポート要件を統合できます。BEAT サイド チャネルでは、コアの VMware Blast セッション トラフィック（マウス、キーボード、ディスプレイ）が 1 つの UDP ポートを共有するため、ネットワークで VMware Blast セッション トラフィックを許可する場合、追加の UDP ポートを開く必要はありません。これに対し、TCP サイド チャネルの場合には、セッション トラフィックで TCP ポートを共有しないため、別の TCP ポートを開くことが必要です。

この機能は、Horizon Client for Windows のみでサポートされます。今回のリリースでは、Windows 以外のクライアントはサポートされません。

手順

1 クライアント ドライブ リダイレクト機能に BEAT サイド チャネルを有効にするには、次の手順を実行します。

   a エージェント マシンで Windows レジストリ エディタ (`regedit.exe`) を起動します。

   b `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware TSDR` に移動し、`sideChannelType` キーを `beat` に設定します。

2 USB リダイレクト機能に BEAT サイド チャネルを有効にするには、次の手順を実行します。

   a エージェント マシンで Windows レジストリ エディタ (`regedit.exe`) を起動します。

   b `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration` に移動し、`UsbVirtualChannelEnabled` キーを `true` に設定します。

   c `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware UsbRedirection` に移動して、`vchanSideChannelEnabled` キーを `true` に設定し、`sideChannelType` キーを `beat` に設定します。

   d クライアント マシンで Windows レジストリ エディタ (`regedit.exe`) を起動します。

   e `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Client` に移動し、`EnableUsbVirtualChannelOnClient` キーを `true` に設定します。

URL コンテンツ リダイレクトの構成 3

URL コンテンツ リダイレクト機能を使用すると、特定の URL を構成して、クライアント マシンで開くか、あるいはリモート デスクトップまたはアプリケーションで開くようにすることができます。ユーザーが Internet Explorer のアドレス バーまたはアプリケーションで入力する URL をリダイレクトできます。

この章には、次のトピックが含まれています。

URL コンテンツ リダイレクトについて

URL コンテンツ リダイレクト機能は、リモート デスクトップまたはアプリケーションからクライアント、およびクライアントからリモート デスクトップまたはアプリケーションへのリダイレクトをサポートします。

リモート デスクトップまたはアプリケーションからクライアントへのリダイレクトは、エージェントからクライアントへのリダイレクトと呼ばれます。クライアントからリモート デスクトップまたはアプリケーションへのリダイレクトは、クライアントからエージェントへのリダイレクトと呼ばれます。

エージェントからクライアントへのリダイレクト

エージェントからクライアントへのリダイレクトでは、Horizon Agent は URL を Horizon Client に送信し、クライアント マシンで URL に指定されたプロトコルのデフォルト アプリケーションを開きます。

クライアントからエージェントへのリダイレクト

クライアントからエージェントへのリダイレクトでは、Horizon Client は、ユーザーが指定したリモート デスクトップまたはアプリケーションを開いて URL を処理します。URL がリモート デスクトップにリダイレクトされた場合、リンクはデスクトップ上でそのプロトコルのデフォルト ブラウザで開きます。URL がリモート アプリケーションにリダイレクトされた場合、リンクは指定されたアプリケーションによって開かれます。デスクトップまたはアプリケーション プールを使用する権限をエンド ユーザーが持っている必要があります。

一部の URL をリモート デスクトップまたはアプリケーションからクライアントにリダイレクトし、それ以外の URL をクライアントからリモート デスクトップまたはアプリケーションにリダイレクトできます。HTTP、HTTPS、mailto、および callto など、リダイレクトに必要なプロトコルをいくつでもリダイレクトできます。

URL コンテンツ リダイレクトの要件

URL コンテンツ リダイレクト機能を使用するには、クライアント マシン、リモート デスクトップ マシン、および RDS ホストが特定の要件を満たしている必要があります。

Windows クライアント	Horizon Client 4.0 for Windows 以降 クライアントからエージェントへのリダイレクトを使用するには、Horizon Client for Windows をインストールするときに、URL コンテンツ リダイレクト機能を有効にする必要があります。エージェントからクライアントへのリダイレクトを使用する場合、Horizon Client for Windows で URL コンテンツ リダイレクト機能を有効にする必要はありません。
Mac クライアント	Horizon Client 4.2 for Mac 以降 Horizon Client 4.2 または 4.3 for Mac では、URL コンテンツ リダイレクトは技術プレビュー機能であり、エージェントからクライアントへのリダイレクトのみがサポートされます。Horizon Client 4.4 for Mac 以降では、URL コンテンツ リダイレクトは正式にサポートされ、エージェントからクライアント、クライアントからエージェントへのリダイレクトの両方がサポートされます。
デスクトップ仮想マシンと RDS ホスト	デスクトップとアプリケーションを提供するリモート デスクトップ マシンと RDS ホストにある Horizon Agent 7.0 以降。 Horizon Agent のインストール時に URL コンテンツ リダイレクト機能を有効にする必要があります。
Web ブラウザ	Internet Explorer 9、10 および 11
表示プロトコル	VMware Blast および PCoIP

Cloud Pod アーキテクチャ 環境での URL コンテンツ リダイレクトの使用

Cloud Pod アーキテクチャ 環境を利用している場合、ローカル URL コンテンツ リダイレクト設定に加えて、グローバル URL コンテンツ リダイレクト設定を構成できます。

ローカル ポッドのみに表示されるローカル URL コンテンツ リダイレクト設定とは異なり、グローバル URL コンテンツ リダイレクト設定はポッド フェデレーション全体で表示されます。グローバル URL コンテンツ リダイレクト設定を使用すると、クライアントの URL リンクをグローバル デスクトップ資格やグローバル アプリケーション資格などのグローバル リソースにリダイレクトできます。

ユーザーが Horizon Client を使用して、ポッドフェデレーション内の接続サーバ インスタンスにログインする場合、接続サーバ インスタンスは、そのユーザーに割り当てられているローカルおよびグローバルの URL コンテンツ リダイレクト設定をすべて検索します。ユーザーがクライアント マシン上の URL をクリックするたびに、ローカル設定とグローバル設定がマージされて使用されます。

Cloud Pod アーキテクチャ 環境の構成と管理の詳細については、『Horizon 7 での Cloud Pod アーキテクチャの管理』を参照してください。

URL コンテンツ リダイレクト機能ありでの Horizon Agent のインストール

リモート デスクトップまたはアプリケーションからクライアントへの（エージェントからクライアントへのリダイレクト）、またはクライアントからリモート デスクトップまたはアプリケーション（クライアントからエージェントへのリダイレクト）への URL コンテンツ リダイレクトを使用するには、Horizon Agent をインストールするときに、URL コンテンツ リダイレクト機能を有効にする必要があります。

インストーラ ファイルをダブルクリックするのではなく、コマンド プロンプト ウィンドウで次のコマンドを実行し、Horizon Agent のインストールを開始します。

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

指示に従ってインストールを完了します。

URL コンテンツ リダイレクト機能がインストールされていることを確認するには、`vmware-url-protocol-launch-helper.exe` と `vmware-url-filtering-plugin.dll` ファイルが `%PROGRAMFILES%\VMware\VMware View\Agent\bin\UrlRedirection` ディレクトリにあることを確認します。また、Internet Explorer のアドオンとして VMware Horizon View URL Filtering Plugin が有効になっていることを確認します。

エージェントからクライアントへのリダイレクトの構成

エージェントからクライアントへのリダイレクトでは、Horizon Agent は URL を Horizon Client に送信し、URL に指定されたプロトコルのデフォルト アプリケーションが開きます。

エージェントからクライアントへのリダイレクトを有効にするには、次の構成タスクを実行します。

- Horizon Agent で URL コンテンツ リダイレクト機能を有効にします。URL コンテンツ リダイレクト機能ありでの Horizon Agent のインストールを参照してください。
- URL コンテンツ リダイレクト グループ ポリシー設定をリモート デスクトップとアプリケーションに適用します。GPO への URL コンテンツ リダイレクト ADMX テンプレートの追加を参照してください。
- グループ ポリシー設定を構成して、Horizon Agent での URL のリダイレクト方法をプロトコルごとに示します。URL コンテンツ リダイレクトのグループ ポリシー設定を参照してください。

GPO への URL コンテンツ リダイレクト ADMX テンプレートの追加

URL コンテンツ リダイレクト ADMX テンプレート ファイル (`urlRedirection.admx`) には、URL リンクをクライアントで開く（エージェントからクライアントへのリダイレクト）か、リモート デスクトップまたはアプリケーションで開く（クライアントからエージェントへのリダイレクト）かどうかを制御できる設定が含まれています。

URL コンテンツ リダイレクト グループ ポリシー設定をリモート デスクトップおよびアプリケーションに適用するには、Active Directory サーバの GPO に ADMX テンプレート ファイルを追加します。リモート デスクトップやアプリケーションでクリックされる URL リンクに関するルールについては、仮想デスクトップおよび RDS ホストを含む組織単位 (OU) に GPO がリンクされる必要があります。

また、ユーザーの Windows クライアント コンピュータが含まれる OU にリンクされている GPO にグループ ポリシー設定を適用することもできますが、クライアントからエージェントへのリダイレクトを構成するときに推奨されるのは、`vdmutil` コマンドライン ユーティリティを使用する方法です。macOS は GPO をサポートしていないため、Mac クライアントを使用している場合には、`vmdutil` を使用する必要があります。

前提条件

- Horizon Agent のインストール時に URL コンテンツ リダイレクト機能が含まれていることを確認します。URL コンテンツ リダイレクト機能ありでの Horizon Agent のインストールを参照してください。
- URL コンテンツ リダイレクトのグループ ポリシー設定用に Active Directory GPO が作成されていることを確認します。
- MMC およびグループ ポリシー管理エディタ スナップインが Active Directory サーバで使用できることを確認します。

手順

1 Horizon 7 GPO Bundle `.zip` ファイルを https://my.vmware.com/web/vmware/downloads の VMware ダウンロード サイトからダウンロードします。

[Desktop & End-User Computing（デスクトップおよびエンドユーザー コンピューティング）] で VMware Horizon 7 のダウンロードを選択します。これには GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` で、*x.x.x* はバージョン、*yyyyyyy* はビルド番号を表します。Horizon 7 のグループ ポリシー設定用の ADMX ファイルはすべて、このファイルで提供されています。

2 `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` ファイルを解凍して、URL コンテンツ リダイレクト ADMX ファイルを Active Directory サーバにコピーします。

a `urlRedirection.admx` ファイルを `C:\Windows\PolicyDefinitions` フォルダにコピーします。

b 言語リソース ファイル `urlRedirection.adml` を `C:\Windows\PolicyDefinitions` 内の適切なサブフォルダにコピーします。

たとえば、EN（英語）の場合、`urlRedirection.adml` ファイルを `C:\Windows\PolicyDefinitions\en-US` フォルダにコピーします。

3 Active Directory サーバで、[グループ ポリシー管理エディタ] を開きます。

URL コンテンツ リダイレクト グループ設定は、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [VMware Horizon URL リダイレクト] にインストールされます。

次のステップ

グループ ポリシー設定を構成します。

URL コンテンツ リダイレクトのグループ ポリシー設定

URL コンテンツ リダイレクト テンプレート ファイルには、エージェントからクライアントへのリダイレトとクライアントからエージェントへのリダイレクトのルールを作成するためのグループ ポリシー設定が含まれています。このテンプレート ファイルには、コンピュータの構成設定のみが含まれます。設定はすべて、グループ ポリシー管理エディタの [VMware Horizon URL リダイレクト] フォルダにあります。

次の表に、URL コンテンツ リダイレクト テンプレート ファイルのグループ ポリシー設定の説明を記載します。

表 3-1. URL コンテンツ リダイレクトのグループ ポリシー設定

設定	プロパティ
`IE Policy: Prevent users from changing URL Redirection plugin loading behavior`	ユーザーが URL コンテンツ リダイレクト機能を無効にできるかどうかを決定します。 デフォルトでは、この設定は構成されていません。
`IE Policy: Automatically enable URL Redirection plugin`	新しくインストールされた Internet Explorer プラグインを自動的に有効にするかどうかを決定します。 デフォルトでは、この設定は構成されていません。
`Url Redirection Enabled`	URL コンテンツ リダイレクト機能を有効にするかどうかを決定します。この機能をクライアントまたはエージェントにインストールしている場合でも、この設定を使用して URL コンテンツ リダイレクト機能を無効にできます。 デフォルトでは、この設定は構成されていません。

設定	プロパティ
`Url Redirection Protocol 'http'`	HTTP プロトコルを使用するすべての URL について、リダイレクトする URL を指定します。この設定には次のオプションがあります。 ■ [brokerHostname] - URL をリモート デスクトップまたはアプリケーションにリダイレクトするときに使用する接続サーバ ホストの IP アドレスまたは完全修飾名。 ■ [remoteItem] - [agentRules] で指定された URL を処理できるリモート デスクトップまたはアプリケーション プールの表示名。 ■ [clientRules] - クライアントにリダイレクトする必要がある URL。たとえば、[clientRules] を **`.*.mycompany.com`** に設定している場合、`mycompany.com` というテキストを含むすべての URL は、Windows ベースのクライアントにリダイレクトされ、クライアントのデフォルト ブラウザで開かれます。 ■ [agentRules] - [remoteItem] で指定されるリモート デスクトップまたはアプリケーションにリダイレクトする必要がある URL。たとえば、[agentRules] を **`.*.mycompany.com`** に設定すると、「mycompany.com」というテキストが含まれるすべての URL がリモート デスクトップまたはアプリケーションにリダイレクトされます。 エージェント ルールを作成するときは、[brokerHostname]オプションを使用して接続サーバ ホストの IP アドレスまたは完全修飾ドメイン名を指定し、[remoteItem] オプションを使用してデスクトップまたはアプリケーション プールの表示名を指定する必要があります。 **注:** クライアント ルールを構成する場合には、`vdmutil` コマンドライン ユーティリティを使用することをお勧めします。 デフォルトでは、この設定は有効になっています。
`Url Redirection Protocol '[...]'`	HTTP 以外のプロトコル（HTTPS、mailto、および callto など）にこの設定を使用します。 このオプションは、`Url Redirection Protocol 'http'` の場合と同じです。 その他のプロトコルを構成する必要がない場合は、URL コンテンツ リダイレクト テンプレート ファイルを Active Directory に追加する前に、このエントリを削除またはコメント アウトできます。 ベスト プラクティスとして、HTTP および HTTPS プロトコルに対して同じリダイレクト設定を構成します。この方法では、ユーザーが `mycompany.com` などの部分的な URL を Internet Explorer に入力し、そのサイトが自動的に HTTP から HTTPS にリダイレクトされると、URL コンテンツ リダイレクト機能が期待どおりに動作します。この例では、HTTPS のルールを設定していても、HTTP に対して同じリダイレクト設定を設定していない場合、ユーザーが入力する部分的な URL はリダイレクトされません。 デフォルトでは、この設定は構成されていません。

クライアントからエージェントへのリダイレクトについて、デフォルトのハンドラがないプロトコルを設定する場合、このプロトコルを指定する URL がリダイレクトされるようにするには、このプロトコルのグループ ポリシー設定後に Horizon Client を一度開始する必要があります。

URL コンテンツ リダイレクト ルールを作成する構文

クライアントまたはリモートのデスクトップまたはアプリケーションで開く URL を指定する場合には、正規表現を使用できます。複数のエントリを区切るにはセミコロンを使用します。エントリ間にスペースは使用できません。

次の表は、いくつかのエントリの例について説明します。

エントリ	説明
`.*`	すべての URL がリダイレクトされるように指定します。 この設定をエージェント ルール（[agentRules] オプション）に使用すると、すべての URL が指定されたリモート デスクトップまたはアプリケーションで開きます。 この設定を（[clientRules] オプション）クライアント ルールに使用すると、すべての URL がクライアントにリダイレクトされます。
`.*.acme.com;.*.example.com`	`.acme.com` や `example.com` というテキストを含むすべての URL がリダイレクトされるように指定します。
[スペースまたは空白]	URL をリダイレクトしないように指定します。たとえば、[clientRules] オプションを空白のままにすると、どの URL もクライアントにリダイレクトされないように指定されます。

エージェントからクライアントへのリダイレクト グループ ポリシーの例

リソースを節約するため、またはセキュリティ レイヤーを追加するために、エージェントからクライアントへのリダイレクトを使用する場合があります。たとえば、従業員がリモート デスクトップやアプリケーションでの作業中に動画を視聴したい場合であれば、それらの URL をクライアント マシンにリダイレクトすることで、データセンターに負荷がかかることはなくなります。あるいは、社内ネットワークの外で働く従業員のセキュリティを強化する目的で、社内ネットワークの外部にアクセスするすべての URL を従業員自身のクライアント マシンで開くようにしたいとします。

その場合は、たとえば、ルールを構成して、会社に関係のないコンテンツや社内ネットワークへのアクセスではない URL はすべて、クライアント マシンにリダイレクトして開くようにします。このような状況では、次の設定を正規表現を含めて使用します。

- [agentRules] の場合：`.*.mycompany.com`

  このルールは、`mycompany.com` というテキストを含む URL をリダイレクトして、指定されたリモート デスクトップまたはアプリケーション（エージェント）で開きます。

- [clientRules] の場合：`.*`

  このルールは、すべての URL をクライアントにリダイレクトし、デフォルトのクライアント ブラウザで開きます。

URL コンテンツ リダイレクト機能は、次のプロセスを使用してクライアントとエージェントのルールを適用します。

1 ユーザーがリモート アプリケーションまたはデスクトップでリンクをクリックすると、クライアント ルールが最初にチェックされます。

2 URL がクライアント ルールと一致すると、エージェント ルールが次にチェックされます。

3 エージェント ルールとクライアント ルールが競合する場合、リンクはローカルで開かれます。この場合、URL はエージェント マシンで開かれます。

4 競合がなければ、URL はクライアントにリダイレクトされます。

この例では、**mycompany.com** が含まれる URL はすべての URL のサブセットであるため、クライアント ルールとエージェント ルール間で競合が存在します。この競合のため、**mycompany.com** を含む URL はローカルで開かれます。リモート デスクトップで URL に **mycompany.com** が含まれるリンクをクリックすると、この URL はそのリモート デスクトップで開きます。クライアント システムから URL の **mycompany.com** のリンクをクリックすると、URL はクライアントで開きます。

クライアントからエージェントへのリダイレクトの構成

クライアントからエージェントへのリダイレクトでは、Horizon Client はリモート デスクトップまたはアプリケーションを開き、ユーザーがクライアントでクリックする URL リンクを処理します。リモート デスクトップが開くと、URL に指定されたプロトコルのデフォルト アプリケーションが URL を処理します。リモート アプリケーションが開かれている場合、アプリケーションは URL を処理します。

クライアントからエージェントへのリダイレクトを使用するには、次の設定タスクを実行します。

- Horizon Agent で URL コンテンツ リダイレクト機能を有効にします。URL コンテンツ リダイレクト機能ありでの Horizon Agent のインストールを参照してください。
- (Windows クライアントのみ) Horizon Client for Windows で URL コンテンツ リダイレクト機能を有効にします。URL コンテンツ リダイレクト機能ありでの Horizon Client for Windows のインストールを参照してください。
- `vdmutil` コマンドライン ユーティリティを使用して、Horizon Client での URL のリダイレクト方法をプロトコルごとに示す URL コンテンツ リダイレクト設定を作成します。ローカル URL コンテンツ リダイレクト設定の作成またはグローバル URL コンテンツ リダイレクト設定の作成を参照してください。
- `vdmutil` コマンドライン ユーティリティを使用して、URL コンテンツのリダイレクト設定を Active Directory ユーザーまたはグループに割り当てます。ユーザーまたはグループへの URL コンテンツ リダイレクト設定の割り当てを参照してください。
- URL コンテンツ リダイレクト設定を確認します。URL コンテンツ リダイレクト設定のテストを参照してください。

注: グループ ポリシー設定を使用してクライアントからエージェントへのリダイレクト ルールを設定できますが、`vdmutil` コマンドライン ユーティリティを使用することをお勧めします。グループ ポリシー設定の使用方法については、グループ ポリシー設定を使用したクライアントからエージェントへのリダイレクトの設定を参照してください。Mac クライアントの場合には、`vdmutil` を使用してクライアントからエージェントへのリダイレクトを設定する必要があります。macOS では GPO がサポートされていないため、Mac クライアントを使用している場合には、グループ ポリシー設定でクライアントからエージェントへのリダイレクトを設定することはできません。

URL コンテンツ リダイレクト機能ありでの Horizon Client for Windows のインストール

Windows クライアントからリモート デスクトップやアプリケーションへの URL コンテンツ リダイレクト (クライアントからエージェントへのリダイレクト) を使用するには、Horizon Client for Windows を URL コンテンツ リダイレクト機能ありでインストールする必要があります。

URL コンテンツ リダイレクト機能を有効にするには、コマンドラインから Horizon Client for Windows インストーラを使用する必要があります。インストーラ ファイルをダブルクリックするのではなく、コマンド プロンプト ウィンドウで次のコマンドを実行し、インストールを開始します。

```
VMware-Horizon-Client-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

この機能がインストールされていることを確認するには、`vmware-url-protocol-launch-helper.exe` と `vmware-url-filtering-plugin.dll` ファイルが `%PROGRAMFILES%\VMware\VMware Horizon View Client` ディレクトリにあることを確認します。また、Internet Explorer のアドオンとして VMware Horizon View URL Filtering Plugin がインストールされていることを確認します。

注: Horizon Client 4.4 for Mac は、クライアントからエージェントへのリダイレクトをデフォルトでサポートします。追加のインストール手順は不要です。Horizon Client 4.2 および 4.3 for Mac は、クライアントからエージェントへのリダイレクトをデフォルトでサポートしません。

vdmutil コマンドライン ユーティリティの使用

`vdmutil` コマンドライン インターフェイスを使用して、クライアントからエージェントへリダイレクトする URL コンテンツ リダイレクト設定を作成、割り当て、および管理できます。

注: Mac クライアントにクライアントからエージェントへのリダイレクトを設定するには、`vdmutil` コマンドを使用する必要があります。macOS では GPO がサポートされていないため、Mac クライアントを使用している場合は、GPO を使用してクライアントからエージェントへのリダイレクトを設定することはできません。

コマンドの使用方法

`vdmutil` コマンドの構文は、Windows のコマンド プロンプトの操作を制御します。

```
vdmutil command_option [additional_optionargument] ...
```

使用できる追加のオプションは、コマンド オプションによって異なります。

デフォルトの場合、`vdmutil` コマンドの実行可能ファイルのパスは `C:\Program Files\VMware\VMware View\Server\tools\bin` です。コマンド ラインにパスを入力するのを避けるには、PATH 環境変数にパスを追加します。

コマンド認証

管理者ロールを持つユーザーとして `vdmutil` コマンドを実行する必要があります。

Horizon Administrator を使用して管理者ロールをユーザーに割り当てることができます。詳細については、『View 管理』を参照してください。

`vdmutil` コマンドには、認証に使用するユーザー名、ドメイン、およびパスワードを指定するオプションがあります。これらの認証オプションは、`--help` および `--verbose` を除くすべての `vdmutil` コマンド オプションを指定して使用する必要があります。

表 3-2. vdmutil コマンド認証オプション

オプション	説明
--authAs	接続サーバ インスタンスを認証する Horizon 管理者ユーザーの名前。**domain\username** またはユーザー プリンシパル名 (UPN) 形式を使用しないでください。
--authDomain	--authAs オプションで指定された Horizon 管理者ユーザーの完全修飾ドメイン名。
--authPassword	--authAs オプションで指定された Horizon 管理者ユーザーのパスワード。パスワードの代わりに **"*"** を入力すると、vdmutil コマンドでパスワードが要求され、慎重に扱う必要があるパスワードがコマンドラインのコマンド履歴に残りません。

たとえば、次の vdmutil コマンドは、mydomain¥johndoe というユーザーをログインさせます。

```
vdmutil --listURLSetting --authAs johndoe --authDomain mydomain --authPassword secret
```

コマンド出力

vdmutil コマンドは、操作が成功すると 0 を返し、失敗すると操作の失敗に固有の 0 以外のコードを返します。vdmutil コマンドは標準エラー出力にエラー メッセージを書き込みます。操作で出力が生成されたり、--verbose オプションを使用して詳細なログ記録が有効になっていると、vdmutil コマンドは標準出力に米国英語で出力を書き込みます。

URL コンテンツ リダイレクトのオプション

次の vdmutil コマンド オプションを使用して、URL コンテンツのリダイレクト設定を作成、割り当て、および管理できます。どのオプションも 2 つのダッシュ (--) の後に指定する必要があります。

表 3-3. URL コンテンツ リダイレクトの vdmutil コマンド オプション

オプション	説明
--addGroupURLSetting	グループを特定の URL コンテンツリダイレクト設定に割り当てます。
--addUserURLSetting	ユーザーを特定の URL コンテンツリダイレクト設定に割り当てます。
--createURLSetting	URL コンテンツ リダイレクト設定を作成します。
--deleteURLSetting	URL コンテンツ リダイレクト設定を削除します。
--disableURLSetting	URL コンテンツ リダイレクト設定を無効にします。
--enableURLSetting	--disableURLSetting オプションで無効にされた URL コンテンツ リダイレクト設定を有効にします。
--listURLSetting	接続サーバ インスタンスのすべての URL コンテンツ リダイレクト設定を一覧表示します。
--readURLSetting	URL コンテンツ リダイレクト設定に関する情報を表示します。
--removeGroupURLSetting	URL コンテンツ リダイレクト設定からグループ割り当てを削除します。
--removeUserURLSetting	URL コンテンツ リダイレクト設定からユーザー割り当てを削除します。
--updateURLSetting	既存の URL コンテンツ リダイレクト設定を更新します。

vdmutil --help と入力して、すべての vdmutil オプションの構文情報を表示できます。特定のオプションの詳細な構文情報を表示するには、**vdmutil --*option* --help** と入力します。

ローカル URL コンテンツ リダイレクト設定の作成

ローカル URL コンテンツ リダイレクト設定を作成し、特定の URL をリダイレクトして、リモート デスクトップまたはアプリケーションで開くことができます。ローカル URL コンテンツ リダイレクト設定は、ローカル ポッドでのみ表示されます。

HTTP、HTTPS、mailto、および callto など、リダイレクトに必要なプロトコルをいくつでも設定できます。

ベスト プラクティスとして、HTTP および HTTPS プロトコルに対して同じリダイレクト設定を構成します。この方法では、ユーザーが mycompany.com などの部分的な URL を Internet Explorer に入力し、そのサイトが自動的に HTTP から HTTPS にリダイレクトされると、URL コンテンツ リダイレクト機能が期待どおりに動作します。この例では、HTTPS のルールを設定していても、HTTP に対して同じリダイレクト設定を設定していない場合、ユーザーが入力する部分的な URL はリダイレクトされません。

ポッド フェデレーション全体で表示されるグローバル URL コンテンツ リダイレクト設定を作成するには、グローバル URL コンテンツ リダイレクト設定の作成を参照してください。

前提条件

vdmutil コマンドライン インターフェイスのオプションと要件について理解し、vdmutil コマンドを実行するための適切な権限があることを確認します。vdmutil コマンドライン ユーティリティの使用を参照してください。

手順

1 接続サーバ インスタンスにログインします。

2 --createURLSetting オプションを指定して vdmutil コマンドを実行し、URL コンテンツ リダイレクト設定を作成します。

```
vdmutil --createURLSetting --urlSettingName value --urlRedirectionScope LOCAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop value]
[--agentURLPattern value]
```

オプション	説明
--urlSettingName	URL コンテンツ リダイレクト設定の一意の名前。名前には 1 文字から 64 文字が使用できます。
--urlRedirectionScope	URL コンテンツ リダイレクト設定の範囲。設定を ローカル ポッドのみに表示するには LOCAL を指定します。
--description	URL コンテンツ リダイレクト設定の説明。説明には 1 文字から 1024 文字が使用できます。
--urlScheme	http、https、mailto、または callto など URL コンテンツ リダイレクト設定が適用されるプロトコル。
--entitledApplication	たとえば iexplore-2012 など、指定された URL を開くために使用されるローカル アプリケーション プールの名前を表示します。このオプションを使用して、ローカル RDS デスクトップ プールの表示名も指定できます。

オプション	説明
--entitledDesktop	たとえば xx など、指定された URL を開くために使用されるローカル デスクトップ プールの名前を表示します。RDS デスクトップ プールでは、--entitledApplication オプションを使用します。
--agentURLPattern	リモート デスクトップまたはアプリケーションで開く必要がある URL を指定する引用符で囲まれた文字列。プロトコルのプリフィックスを含める必要があります。ワイルドカードを使用して、複数の URL に一致する URL パターンを指定できます。 たとえば、**"http://google.*"** と入力すると、**google** というテキストが含まれるすべての URL が指定したリモート デスクトップまたはアプリケーション プールにリダイレクトされます。**.*** （ドットとアスタリスク）を入力すると、すべての URL がリモート デスクトップまたはアプリケーションにリダイレクトされます。

3 （オプション） 作成した URL コンテンツ リダイレクト設定にプロトコル、URL、およびローカル リソースを追加するには、--updateURLSetting オプションを指定して vdmutil コマンドを実行します。

```
vdmutil --updateURLSetting --urlSettingName value --urlRedirectionScope LOCAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop value]
[--agentURLPattern value]
```

これらのオプションは、--createURLSetting オプションを指定した vdmutil コマンドと同じです。

例： ローカル URL コンテンツ リダイレクト設定の作成

次の例では、url-filtering という名前のローカル URL コンテンツ リダイレクト設定を作成しています。この設定は、http://google.* というテキストを含むすべてのクライアント URL を iexplore2012 という名前のアプリケーション プールにリダイレクトします。

```
VdmUtil --createURLSetting --urlSettingName url-filtering --urlScheme http
--entitledApplication iexplore2012 --agentURLPattern "http://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

次の例は、url-filtering 設定を更新して、https://google.* というテキストを含むすべてのクライアント URL を iexplore2012 という名前のアプリケーション プールにリダイレクトします。

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme https
--entitledApplication iexplore2012 --agentURLPattern "https://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

次の例は、url-filtering 設定を更新して、mailto://.*.mycompany.com というテキストを含むすべてのクライアント URL を Outlook2008 という名前のアプリケーション プールにリダイレクトします。

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme mailto
--entitledApplication Outlook2008 --agentURLPattern "mailto://.*.mycompany.com"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

次のステップ

ユーザーまたはグループに URL コンテンツ リダイレクト設定を割り当てます。ユーザーまたはグループへの URL コンテンツ リダイレクト設定の割り当てを参照してください。

グローバル URL コンテンツ リダイレクト設定の作成

Cloud Pod アーキテクチャ 環境がある場合は、グローバル URL コンテンツリダイレクト設定を作成し、特定の URL をリダイレクトして、ポッド フェデレーションの任意のポッドにあるリモート デスクトップまたはアプリケーションで開くようにできます。

グローバル URL コンテンツ リダイレクト設定は、ポッド フェデレーション全体で表示されます。グローバル URL コンテンツ リダイレクト設定を作成すると、URL をグローバル デスクトップ資格やグローバル アプリケーション資格などのグローバル リソースにリダイレクトできます。

HTTP、HTTPS、mailto、および callto など、リダイレクトに必要なプロトコルをいくつでも設定できます。

ベスト プラクティスとして、HTTP および HTTPS プロトコルに対して同じリダイレクト設定を構成します。この方法では、ユーザーが `mycompany.com` などの部分的な URL を Internet Explorer に入力し、そのサイトが自動的に HTTP から HTTPS にリダイレクトされると、URL コンテンツ リダイレクト機能が期待どおりに動作します。この例では、HTTPS のルールを設定していても、HTTP に対して同じリダイレクト設定を設定していない場合、ユーザーが入力する部分的な URL はリダイレクトされません。

Cloud Pod アーキテクチャ 環境の構成と管理の詳細については、『Horizon 7 での Cloud Pod アーキテクチャの管理』を参照してください。

ローカル URL コンテンツ リダイレクト設定を作成するには、ローカル URL コンテンツ リダイレクト設定の作成を参照してください。

前提条件

`vdmutil` コマンドライン インターフェイスのオプションと要件について理解し、`vdmutil` コマンドを実行するための適切な権限があることを確認します。vdmutil コマンドライン ユーティリティの使用を参照してください。

手順

1 ポッド フェデレーションの任意の接続サーバ インスタンスにログインします。

2 `--createURLSetting` オプションを指定して `vdmutil` コマンドを実行し、URL コンテンツ リダイレクト設定を作成します。

```
vdmutil --createURLSetting --urlSettingName value --urlRedirectionScope GLOBAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

オプション	説明
--urlSettingName	URL コンテンツ リダイレクト設定の一意の名前。名前には 1 文字から 64 文字が使用できます。
--urlRedirectionScope	URL コンテンツ リダイレクト設定の範囲。GLOBAL を指定すると、ポッド フェデレーション全体で設定が表示されます。
--description	URL コンテンツ リダイレクト設定の説明。説明には 1 文字から 1024 文字が使用できます。
--urlScheme	http、https、mailto、または callto など URL コンテンツ リダイレクト設定が適用されるプロトコル。
--entitledApplication	指定された URL を開くために使用されるグローバル アプリケーション資格の名前を表示します。

オプション	説明
--entitledDesktop	たとえば GE-1 など、指定された URL を開くために使用されるグローバル デスクトップ資格の名前を表示します。
--agentURLPattern	リモート デスクトップまたはアプリケーションで開く必要がある URL を指定する引用符で囲まれた文字列。プロトコルのプリフィックスを含める必要があります。ワイルドカードを使用して、複数の URL に一致する URL パターンを指定できます。 たとえば、"http://google.*" と入力すると、google というテキストが含まれるすべての URL がリモート デスクトップまたはアプリケーションにリダイレクトされます。.*（ドットとアスタリスク）を入力すると、すべての URL がリモート デスクトップまたはアプリケーションにリダイレクトされます。

3 （オプション） 作成した URL コンテンツ リダイレクト設定にプロトコル、URL、およびグローバル リソースを追加するには、--updateURLSetting オプションを指定して vdmutil コマンドを実行します。

```
vdmutil --updateURLSetting --urlSettingName value --urlRedirectionScope GLOBAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

これらのオプションは、--createURLSetting オプションを指定した vdmutil コマンドと同じです。

例： グローバル URL コンテンツ リダイレクト設定の構成

次の例では、Operations-Setting という名前のグローバル URL コンテンツ リダイレクト設定を作成しています。この設定は、http://google.* というテキストを含むすべてのクライアント URL を GAE1 という名前のグローバル アプリケーション資格にリダイレクトするようにしています。

```
vdmutil --createURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme http --entitledApplication GAE1 --agentURLPattern "http://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

次の例は、Operations-Setting 設定を更新して、https://google.* というテキストを含むすべての URL を GAE1 という名前のグローバル アプリケーション資格にリダイレクトするようにしています。

```
vdmutil --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme https --entitledApplication GAE1 --agentURLPattern "https://google.*" -authAs johndoe
--authDomain mydomain --authPassword secret
```

次の例は、Operations-Setting 設定を更新して、"mailto://.*.mycompany.com" というテキストを含むすべての URL を GA2 という名前のグローバル アプリケーション資格にリダイレクトするようにしています。

```
vdmutil --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme mailto --entitledApplication GAE2 --agentURLPattern "mailto://.*.mycompany.com"
--authAs johndoe --authDomain mydomain --authPassword secret
```

次のステップ

ユーザーまたはグループに URL コンテンツ リダイレクト設定を割り当てます。ユーザーまたはグループへの URL コンテンツ リダイレクト設定の割り当てを参照してください。

ユーザーまたはグループへの URL コンテンツ リダイレクト設定の割り当て

URL コンテンツ リダイレクト設定を作成したら、Active Directory のユーザーやグループにその設定を割り当てることができます。

前提条件

vdmutil コマンドライン インターフェイスのオプションと要件について理解し、vdmutil コマンドを実行するための適切な権限があることを確認します。vdmutil コマンドライン ユーティリティの使用を参照してください。

手順

- URL コンテンツ リダイレクト設定をユーザーに割り当てるには、--addUserURLSetting オプションを指定して、vdmutil コマンドを実行します。

```
vdmutil --addUserURLSetting --urlSettingName value --userName value
```

オプション	説明
--urlSettingName	割り当てる URL コンテンツ リダイレクト設定の名前。
--userName	ドメイン\ユーザー名の形式での Active Directory ユーザーの名前。

- URL コンテンツ リダイレクト設定をグループに割り当てるには、--addGroupURLSetting オプションを指定して、vdmutil コマンドを実行します。

```
vdmutil --addGroupURLSetting --urlSettingName value --groupName value
```

オプション	説明
--urlSettingName	割り当てる URL コンテンツ リダイレクト設定の名前。
--groupName	ドメイン\グループの形式での Active Directory グループの名前。

例： URL コンテンツ リダイレクト設定の割り当て

次の例では、url-filtering という URL コンテンツのリダイレクト設定を、mydomain\janedoe という名前のユーザーに割り当てています。

```
vdmutil --addUserURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --userName mydomain\janedoe
```

次の例では、url-filtering という URL コンテンツのリダイレクト設定を、mydomain\usergroup という名前のグループに割り当てています。

```
vdmutil --addGoupURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --groupName mydomain\usergroup
```

次のステップ

URL コンテンツ リダイレクト設定を確認します。URL コンテンツ リダイレクト設定のテストを参照してください。

URL コンテンツ リダイレクト設定のテスト

URL コンテンツ リダイレクト設定を作成して割り当てたら、いくつかの手順を実行して、設定が適切に機能していることを確認します。

前提条件

vdmutil コマンドライン インターフェイスのオプションと要件について理解し、vdmutil コマンドを実行するための適切な権限があることを確認します。vdmutil コマンドライン ユーティリティの使用を参照してください。

手順

1 接続サーバ インスタンスにログインします。

2 --readURLSetting オプションを指定して vdmutil コマンドを実行します。

例：

```
vdmutil --readURLSetting --urlSettingName url-filtering --authAs johndoe
--authDomain mydomain --authPassword secret
```

このコマンドは、URL コンテンツ リダイレクト設定に関する詳細情報を表示します。たとえば、url-filtering 設定の次のコマンド出力では、google.* というテキストを含む HTTP および HTTPS URL は、クライアントから iexplore2012 という名前のローカル アプリケーション プールにリダイレクトされることを示しています。

```
URL Redirection setting url-filtering
   Description                                    : null
   Enabled                                        : true
   Scope of URL Redirection Setting               : LOCAL
   URL Scheme And Local Resource handler pairs
      URL Scheme                                  : http
      Handler type                                : APPLICATION
      Handler Resource name                       : iexplore2012
      URL Scheme                                  : https
      Handler type                                : APPLICATION
      Handler Resource name                       : iexplore2012
   AgentPatterns
        https://google.*
        http://google.*
   ClientPatterns
      No client patterns configured
```

3 Windows クライアント マシンで、Horizon Client を開いて、接続サーバ インスタンスに接続し、設定で構成されている URL パターンに一致する URL をクリックし、URL が予想どおりにリダイレクトされていることを確認します。

4 同じ Windows クライアント マシンで、レジストリ エディタ (regedit) を開いて、\Computer \HKEY_CURRENT_USER\Software\Vmware.Inc.\VMware VDM\URLRedirection\ のパスにあるレジストリ キーを確認します。

設定で指定された各プロトコルのキーが表示されます。プロトコルをクリックすると、そのプロトコルに関連付けられているルールを表示できます。たとえば、agentRules はリダイレクトされている URL を示し、brokerHostName は URL のリダイレクト時に使用される接続サーバ インスタンスの IP アドレスや完全修飾ホスト名を示し、remoteItem はリダイレクトされた URL を処理するデスクトップまたはアプリケーションプールの表示名を示します。

URL コンテンツ リダイレクトの設定の管理

vdmutil コマンドを使用して URL コンテンツ リダイレクトの設定を管理できます。

すべてのコマンドで --authAs、--authDomain、および --authPassword オプションを指定する必要があります。詳細については、vdmutil コマンドライン ユーティリティの使用を参照してください。

設定を表示する

--listURLSetting オプションを指定して vdmutil コマンドを実行し、構成されているすべての URL コンテンツ リダイレクト設定の名前を一覧表示します。

```
vdmutil --listURLSetting
```

--readURLSetting を指定して vdmutil コマンドを実行し、特定の URL コンテンツ リダイレクト設定の詳細情報を表示します。

```
vdmutil --readURLSetting --urlSettingName value
```

設定を削除する

--deleteURLSetting オプションを指定して vdmutil コマンドを実行し、URL コンテンツ リダイレクト設定を削除します。

```
vdmutil --deleteURLSetting --urlSettingName value
```

設定を有効および無効にする

--disableURLSetting オプションを指定して vdmutil コマンドを実行し、URL コンテンツ リダイレクト設定を無効にします。

```
vdmutil --disableURLSetting --urlSettingName value
```

--enableURLSetting オプションを指定して vdmutil を実行し、無効になっていた URL コンテンツ リダイレクト設定を有効にします。

```
vdmutil --enableURLSetting --urlSettingName value
```

設定からユーザーまたはグループを削除する

--removeUserURLSetting オプションを指定して vdmutil コマンドを実行し、URL コンテンツ リダイレクト設定からユーザーを削除します。

```
vdmutil --removeUserURLSetting --urlSettingName value --userName value
```

--removeGroupURLSetting オプションを指定して vdmutil コマンドを実行し、URL コンテンツ リダイレクト設定からグループを削除します。

```
vdmutil --removeGroupURLSetting --urlSettingName value --userGroup value
```

ユーザーまたはグループ名を指定するときには、ドメイン\ユーザー名またはドメイン\グループ名の形式を使用します。

グループ ポリシー設定を使用したクライアントからエージェントへのリダイレクトの設定

URL コンテンツ リダイレクト ADMX テンプレート ファイル (urlRedirection.admx) には、クライアントからリモート デスクトップまたはアプリケーションに URL をリダイレクトする（クライアントからエージェントへのリダイレクト）ルールを作成するためのグループ ポリシー設定が含まれています。

注: クライアントからエージェントへのリダイレクトを設定する場合には、vdmutil コマンドライン インターフェイスを使用することをお勧めします。macOS では GPO がサポートされていないため、Mac クライアントを使用している場合は、GPO を使用してクライアントからエージェントへのリダイレクトを設定することはできません。

クライアントからエージェントへリダイレクトするルールを作成するには、[remoteItem] オプションを使用してリモート デスクトップまたはアプリケーション プールの表示名を指定し、[agentRules] オプションを使用してリモート デスクトップまたはアプリケーションにリダイレクトする必要がある URL を指定します。また、URL をリモート デスクトップまたはアプリケーションにリダイレクトするときに使用する接続サーバ ホストの IP アドレスまたは完全修飾ドメイン名を指定するには、[brokerHostname] オプションも使用する必要があります。

たとえば、セキュリティ上の目的で、社内ネットワークにアクセスするすべての HTTP URL をリモート デスクトップまたはアプリケーションで開くようにしたいとします。この場合、[agentRules] オプションを **.*.mycompany.com** に設定できます。

URL コンテンツ リダイレクト テンプレート ファイルのインストール方法については、GPO への URL コンテンツ リダイレクト ADMX テンプレートの追加を参照してください。

URL コンテンツ リダイレクトの制限事項

URL コンテンツ リダイレクト機能の動作によって、予期しないいくつかの結果が生じる場合があります。

- URL から開かれるページがロケールに基づく各国対応ページの場合、開くロケール ページは、リンクのソースによって決定されます。たとえば、リモート デスクトップ（エージェント ソース）が日本のデータセンターに存在し、ユーザーのコンピュータが米国に存在する場合、URL がエージェントからクライアント マシンにリダイレクトされると、米国のクライアントで開くページは日本語のページになります。
- ユーザーが Web ページからお気に入りを作成すると、リダイレクト後のお気に入りが作成されます。たとえば、ユーザーがクライアント マシンでリンクをクリックし、URL がリモート デスクトップ（エージェント）にリダ

イレクトされ、ユーザーがそのページのお気に入りを作成すると、お気に入りはエージェントで作成されます。ユーザーが次にブラウザをクライアント マシンで開いたときに、ユーザーは、クライアント マシンにお気に入りがあるものと考えますが、実際には、リモート デスクトップ（エージェント ソース）にお気に入りが保存されています。

- ユーザーがダウンロードしたファイルは、URL を開くために使用されたブラウザがあるマシンにダウンロードされます。たとえば、ユーザーがクライアント マシンでリンクをクリックするときに、その URL はリモート デスクトップにリダイレクトされます。そのリンクがファイルをダウンロードするためのリンクであったり、ユーザーがファイルをダウンロードするための Web ページ リンクであったりする場合、クライアント マシンではなく、リモート デスクトップにファイルがダウンロードされます。
- Horizon Agent と Horizon Client を同じマシンにインストールする場合、URL コンテンツ リダイレクトを Horizon Agent または Horizon Client で有効にできますが、両方では有効にできません。このマシンでは、クライアントからエージェントへのリダイレクトまたはエージェントからクライアントへのリダイレクトのいずれかを設定できますが、両方を設定することはできません。

サポートされない URL コンテンツ リダイレクト機能

URL コンテンツ リダイレクト機能は、特定の状況では機能しません。

短縮 URL

`https://goo.gl/abc` などの短縮 URL は、フィルタリング規則に基づいてリダイレクトできますが、フィルタリング メカニズムでは、元の短縮されていない URL が確認されません。

たとえば、`acme.com` が含まれる URL をリダイレクトするルールがある場合、元の URL が `http://www.acme.com/some-really-long-path` で、元の URL の短縮 URL が `https://goo.gl/xyz` だとすると、元の URL はリダイレクトされますが、短縮 URL はリダイレクトされません。

URL を短縮するために頻繁に使用される Web サイトの URL をブロックまたはリダイレクトするルールを作成して、この制限を回避できます。

埋め込み HTML ページ

たとえば、ユーザーが URL リダイレクト ルールと一致しない URL に移動する場合、埋め込み HTML ページは URL リダイレクトをバイパスします。ページに埋め込み HTML ページが含まれていて (iFrame またはインライン フレーム)、そのページにリダイレクト ルールに一致しない URL がある場合、URL リダイレクト ルールは機能しません。ルールは、最上位の URL でのみ動作します。

Internet Explorer プラグインが無効な場合

URL コンテンツ リダイレクトは、Internet Explorer プラグインが無効な状況、たとえば、ユーザーが Internet Explorer で InPrivate ブラウズに切り替えている状況では機能しません。プライベート ブラウズを使用すると、Web ページや Web ページからダウンロードされたファイルは、コンピュータで閲覧やダウンロード履歴に記録されません。URL リダイレクト機能では特定の Internet Explorer プラグインを有効にする必要がありますが、プライベート ブラウズによってこれらのプラグインが無効になるために、この制限事項が発生します。

ユーザーがプラグインを無効にできないようにする GPO 設定を使用して、この制限を回避できます。これに該当する設定は、[ユーザーによるアドオンの有効化および無効化を許可しない] と [新しくインストールされたアドオンを自動的に有効にする] です。グループ ポリシー管理エディタでは、これらの設定は、[コンピュータの構成] - [管理用テンプレート] - [Windows コンポーネント] - [Internet Explorer] にあります。

Internet Explorer でこの制限を回避するには、InPrivate モードを無効にする GPO 設定を使用します。この設定は、[InPrivate ブラウズを無効にする] という名前です。グループ ポリシー管理エディタでは、これらの設定は、[コンピュータの構成] - [管理用テンプレート] - [Windows コンポーネント] - [Internet Explorer] - [プライバシー] にあります。

これらの回避策は、ベスト プラクティスであり、プライベート ブラウズ以外の状況によって発生する可能性があるリダイレクトの問題を防止できます。

Windows 10 のユニバーサル アプリケーションがプロトコルのデフォルトのハンドラである場合

リンクで指定されている Windows 10 のユニバーサル アプリケーションがプロトコルのデフォルトのハンドラである場合、URL リダイレクトが動作しません。ユニバーサル Windows プラットフォームに組み込まれ、PC、タブレット、およびスマートフォンにダウンロードできるユニバーサル アプリケーションとしては、Microsoft Edge ブラウザ、メール、マップ、フォト、Grove ミュージックなどがあります。

デフォルト ハンドラがこれらのいずれかのアプリケーションとなっているリンクをクリックすると、URL はリダイレクトされません。たとえば、ユーザーがアプリケーションのメールのリンクをクリックし、デフォルトのメール アプリケーションがユニバーサル アプリケーションのメールであった場合、リンクで指定された URL はリダイレクトされません。

リダイレクトする URL のプロトコルのデフォルト ハンドラを別のアプリケーションに設定して、この制限を回避できます。たとえば、Edge がデフォルト ブラウザの場合は、Internet Explorer をデフォルト ブラウザにします。

セキュア ブートが有効なマシンの場合

セキュア ブートが有効であるマシンでは、URL コンテンツ リダイレクト機能が無効のままになります。これらのマシンから URL をリダイレクトすることはできません。これらのマシンに URL をリダイレクトすることはできます。

リモート デスクトップおよびアプリケーションでの USB デバイスの使用

4

管理者は、サム フラッシュ ドライブ、カメラ、VoIP (Voice over IP) デバイス、プリンタなどの USB デバイスをリモート デスクトップから使用できるように構成できます。この機能は USB リダイレクトと呼ばれ、Blast Extreme、PCoIP、または Microsoft RDP 表示プロトコルの使用をサポートします。リモート デスクトップでは、最大 128 個の USB デバイスに対応できます。

RDS デスクトップおよびアプリケーションで使用する場合、ローカルで接続された USB サム フラッシュ ドライブとハード ディスクをリダイレクトすることもできます。他のタイプのストレージ デバイスを含め、他のタイプの USB デバイスは RDS デスクトップおよびアプリケーションでサポートされていません。

単一ユーザー マシンに展開されているデスクトップ プールでこの機能を使用すると、ローカル クライアント システムに接続されているほとんどの USB デバイスをリモート デスクトップで使用できるようになります。リモート デスクトップから iPad に接続して管理することもできます。たとえば、リモート デスクトップにインストールした iTunes と iPad を同期できます。Windows や Mac コンピュータなどの一部のクライアント デバイスでは、USB デバイスが Horizon Client のメニューに一覧表示されます。デバイスの接続や接続解除にもこのメニューを使用します。

ほとんどの場合、クライアント システムとリモート デスクトップまたはアプリケーションの USB デバイスを同時に使用することはできません。ごく一部のタイプの USB デバイスのみ、リモート デスクトップとローカル コンピュータ間で共有できます。そのようなデバイスには、スマート カード リーダーと、キーボードやポインティング デバイスなどのヒューマン インターフェイス デバイスがあります。

管理者はエンド ユーザーに接続を許可する USB デバイスのタイプを指定できます。一部のクライアント システム上のビデオ入力デバイスとストレージ デバイスなど複数タイプのデバイスが含まれる複合デバイスについては、管理者はデバイスを分離し、あるデバイス (たとえば、ビデオ入力デバイス) は許可し、その他のデバイス (たとえば、ストレージ デバイス) は許可しないようにできます。

USB リダイレクト機能は、一部のクライアントのタイプだけで使用できます。この機能が特定のタイプのクライアントでサポートされるかどうかを確認するには、デスクトップまたはモバイル クライアント デバイスのそれぞれのタイプに関する「VMware Horizon Client の使用」に含まれる機能サポート マトリックスを参照してください。「https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html」をご覧ください。

重要: USB リダイレクト機能を展開すると、USB デバイスに影響を及ぼす可能性のあるセキュリティ上の脆弱性から組織を保護する措置を講じることができます。保護された Horizon 7 環境での USB デバイスの展開を参照してください。

この章には、次のトピックが含まれています。

USB デバイス タイプに関する制限事項

リモート デスクトップにおけるデバイスの動作を Horizon 7 が明示的に阻止することはありませんが、ネットワークの遅延やバンド幅などの要因で、デバイスのパフォーマンスには差があります。デフォルトでは、使用されないように一部のデバイスがフィルタリングまたはブロックされます。

Horizon 6.0.1 を Horizon Client 3.1 以降と一緒に使用すると、Windows、Linux、および Mac クライアントのクライアント マシンで USB 3.0 デバイスを USB 3.0 ポートに接続できます。USB 3.0 デバイスは、単一ストリームのみでサポートされます。複数のストリームのサポートはこのリリースで実装されていないため、USB デバイスのパフォーマンスは強化されません。常に高いスループットを出さないと適切に動作しない一部の USB 3.0 デバイスの場合、ネットワークの待機時間によって VDI セッションで動作しない可能性があります。

以前の View のリリースでは、超高速 USB 3.0 デバイスはサポートされていませんが、USB 3.0 デバイスは多くの場合、クライアント マシンの USB 2.0 ポートに接続すると動作します。ただし、クライアント システムのマザーボードの USB チップセットのタイプによっては、動作しないことがあります。

次のタイプのデバイスは、シングル ユーザー マシンに展開されているリモート デスクトップへの USB リダイレクトに適さない可能性があります。

- Web カメラは、そのバンド幅要件（通常 60Mbps を超えるバンド幅を使用する）上の理由で、USB リダイレクトではサポートされません。Web カメラではリアルタイム オーディオ ビデオ機能を使用できます。
- USB オーディオ デバイスのリダイレクトは、ネットワークの状態に依存し、信頼できません。一部のデバイスでは、アイドル状態のときでさえ、高いデータ スループットが必要です。リアルタイム オーディオ ビデオ機能があれば、オーディオ入出力デバイスはこの機能を使用して問題なく動作します。それらのデバイス用に USB リダイレクトを使用する必要はありません。
- USB CD/DVD の焼き付けはサポートされていません。
- 一部の USB デバイスは、ネットワークの遅延や信頼性次第でパフォーマンスが大幅に変化します。特に、WAN 経由の場合、この変化が顕著です。たとえば、USB ストレージ デバイスの 1 回の読み取り要求では、クライアントとリモート デスクトップ間のラウンドトリップを 3 回必要とします。ファイル全体の読み取りは複数の USB 読み取り操作が必要になることもあり、遅延が大きくなるほど、ラウンドトリップにかかる時間が長くなります。

ファイル構造は、ファイル形式次第でかなり大きくなることがあります。大容量 USB ディスク ドライブは、デスクトップに表示されるまでに数分かかる場合があります。USB デバイスを FAT ではなく NTFS でフォーマットすると、最初の接続時間が短縮されます。信頼性の低いネットワーク リンクは再試行を引き起こし、パフォーマンスをさらに低下させます。

同様に、USB CD/DVD リーダー、スキャナ、署名付きタブレットなどのタッチ デバイスは、WAN などの速度の遅いネットワーク上では機能しません。

- USB スキャナのリダイレクトはネットワークの状態に左右されるため、スキャンの完了には通常より時間がかかることがあります。

RDS ホストで公開されているデスクトップまたはアプリケーションに、次の種類のデバイスをリダイレクトできます。

- USB サム フラッシュ ドライブ
- USB ハード ディスク

Horizon 7 バージョン 7.0.2 から、公開されたデスクトップやアプリケーションに署名パッド、ディクテーション用フット ペダル、さらにいくつかの Wacom タブレットをリダイレクトできるようになりました。Horizon 7 バージョン 7.0.2 では、これらのデバイスはデフォルトで無効になっています。これらのデバイスを有効にするには、Windows レジストリ キーの設定 (`ExcludeAllDevices` と `IncludeFamily`) を `HKLM\Software\Policies\VMware, Inc\VMware VDM\Agent\USB` から削除します。Horizon 7 バージョン 7.0.3 以降では、これらのデバイスはデフォルトで有効になっています。

公開されたデスクトップやアプリケーションに、他のタイプの USB デバイス、セキュリティ ストレージ ドライブや USB CD-ROM などの他のタイプの USB ストレージ デバイスをリダイレクトすることはできません。

USB リダイレクトの設定の概要

エンド ユーザーが USB フラッシュ ドライブ、カメラ、ヘッドセットなどのリムーバブル デバイスに接続できるように展開を設定するには、リモート デスクトップまたは RDS ホストとクライアント デバイスの両方に特定のコンポーネントをインストールし、View Administrator で USB デバイスのグローバル設定が有効になっていることを確認する必要があります。

このチェックリストには、企業で USB リダイレクトを設定するための必須タスクとオプション タスクの両方が含まれます。

USB リダイレクト機能は、Windows クライアント、Mac クライアント、パートナー提供の Linux クライアントなど、一部のクライアント タイプのみで使用できます。この機能が特定タイプのクライアントでサポートされるかどうかを確認するには、特定タイプのクライアント デバイスに関する「VMware Horizon Client の使用」に含まれる機能サポート一覧を参照してください。「https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html」をご覧ください。

重要: USB リダイレクト機能を展開すると、USB デバイスに影響を及ぼす可能性のあるセキュリティ上の脆弱性から組織を保護する措置を講じることができます。たとえば、グループ ポリシー設定を使用して、一部のリモート デスクトップおよびユーザーに対して USB リダイレクトを無効にしたり、リダイレクトできる USB デバイスのタイプを制限したりすることができます。保護された Horizon 7 環境での USB デバイスの展開を参照してください。

1 リモート デスクトップ ソースまたは RDS ホストで Horizon Agent インストール ウィザードを実行するときは、必ず USB リダイレクト コンポーネントを含めてください。

   デフォルトでは、このコンポーネントが選択されていません。このコンポーネントを選択してインストールする必要があります。

2 クライアント システムで VMware Horizon Client インストール ウィザードを実行する際は、必ず USB リダイレクト コンポーネントを含めてください。

   デフォルトでは、このコンポーネントは含まれています。

3 View Administrator で、リモート デスクトップまたはアプリケーションから USB デバイスへのアクセスが有効になっていることを確認します。

   View Administrator で、[ポリシー] - [グローバル ポリシー] に移動し、[USB アクセス] が [許可] になっていることを確認します。

4 (オプション) リダイレクトを許可するデバイスのタイプを指定する Horizon Agent グループ ポリシーを構成します。

   USB リダイレクトを制御するポリシーの使用を参照してください。

5 (オプション) クライアント デバイスで、同様の設定を構成します。

   Horizon Client がリモート デスクトップまたはアプリケーションに接続するとき、またはエンド ユーザーが USB デバイスを接続するときに、デバイスが自動的に接続されるかどうかも構成できます。クライアント デバイスで USB 設定を構成する方法は、デバイスのタイプによって異なります。たとえば、Windows クライアント エンドポイントの場合はグループ ポリシーを構成できますが、Mac エンドポイントの場合はコマンドライン コマンドを使用します。手順については、特定タイプのクライアント デバイスの『VMware Horizon Client の使用』を参照してください。

6 エンド ユーザーにリモート デスクトップまたはアプリケーションに接続し、USB デバイスをローカル クライアント システムに接続するように指示します。

   USB デバイスのドライバがまだリモート デスクトップまたは RDS ホストにインストールされていない場合、物理 Windows コンピュータ上と同じように、ゲスト OS は USB デバイスを検出して適切なドライバを探します。

ネットワーク トラフィックと USB リダイレクト

USB リダイレクトは表示プロトコルとは別に動作し、USB トラフィックは通常 TCP ポート 32111 を使用します。クライアント システムとリモート デスクトップまたはアプリケーションとの間のネットワーク トラフィックは、クライアント システムが企業ネットワーク内部にあるかどうか、および管理者がセキュリティの設定をどのように選択したかにより、さまざまな経路をとる可能性があります。

クライアント システムが企業ネットワーク内部にある場合、クライアントとリモート デスクトップまたはアプリケーションとの間に直接接続が確立されるように、USB トラフィックは TCP ポート 32111 を使用します。

クライアント システムが会社のネットワークの外部にある場合、DMZ の Unified Access Gateway アプライアンスやセキュリティ サーバを経由してクライアントに接続できます。DMZ の Unified Access Gateway アプライアンスとセキュリティ サーバは、会社のファイアウォールの内側にある接続サーバ インスタンスと通信を行い、公衆網に接するインターネットから接続サーバ インスタンスを遮断し、セキュリティ レイヤーを追加します。

Unified Access Gateway アプライアンス（推奨方法）では、USB トラフィックを処理するため、ファイアウォールで他のポートを開く必要はありません。セキュリティ サーバでは、USB トラフィックを処理するため、ファイアウォールで TCP ポート 32111 を開く必要があります。セキュリティ サーバのポート要件については、『View アーキテクチャの計画』ドキュメントの「DMZ ベースのセキュリティ サーバのファイアウォール ルール」を参照してください。

Session Enhancement SDK 機能経由で USB を使用すると、TCP ポート 32111 を開く必要がありません。Session Enhancement SDK 機能経由での USB の有効化を参照してください。

注: ゼロ クライアントを使用している場合、TCP ポート 32111 ではなく、PCoIP 仮想チャネル経由で USB トラフィックがリダイレクトされます。TCP/UDP ポート 4172 を使用する PCoIP Secure Gateway でデータがカプセル化され、暗号化されます。ゼロ クライアントのみを使用している場合、TCP ポート 32111 を開く必要はありません。

Session Enhancement SDK 機能経由での USB の有効化

Session Enhancement SDK 機能経由で USB を使用すると、USB トラフィック用に TCP ポート 32111 を開く必要はありません。この機能は、RDS ホストの仮想デスクトップと公開デスクトップの両方でサポートされます。

Session Enhancement SDK 機能経由で USB を有効にするには、リモート デスクトップで Windows レジストリ エディタ (`regedit.exe`) を開いて `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration` に移動し、`UsbVirtualChannelEnabled` キーを `true` に設定します。

この機能を有効にすると、USB トラフィックは表示プロトコルの TCP または Blast Extreme Adaptive Transport (BEAT) 接続を使用するか、専用の TCP または BEAT 接続を使用します。USB トラフィックが使用する接続は構成によって異なります。

たとえば、VMware Blast 表示プロトコルの場合、USB トラフィックは VMware 仮想チャネル (VVC)、BEAT サイド チャネルまたは TCP サイド チャネルを使用します。PCoIP 表示プロトコルの場合、USB トラフィックは TCP サイド チャネルのみを使用します。

デフォルトでは、TCP サイド チャネルは TCP ポート 9427 を使用します。VVC と BEAT サイド チャネルは、VMware Blast 表示プロトコルと同じポートを使用します。

USB トラフィックが VVC を使用するように設定されている場合、Windows エージェントのパフォーマンス モニターに表示される USB カウンターは有効になります。

VMware Blast の USB トラフィックに BEAT サイド チャネルを使用する方法については、USB またはクライアント ドライブ リダイレクトでの BEAT サイド チャネルの有効化を参照してください。

USB デバイスへの自動接続

一部のクライアント システムでは、管理者、エンド ユーザー、またはその両方が、リモート デスクトップへの USB デバイスの自動接続を構成できます。自動接続は、ユーザーが USB デバイスをクライアント システムに差し込んだとき、またはクライアントがリモート デスクトップに接続したときに確立することができます。

スマート フォンやタブレットなどの一部のデバイスでは、アップグレード中にデバイスが再起動されて接続が切れるため、自動接続が必要となります。これらのデバイスがリモート デスクトップに自動的に再接続するように設定されていない場合、アップグレード中、デバイスの再起動後に、代わりにローカル クライアント システムに接続します。

管理者がクライアントに設定する、またはエンド ユーザーが Horizon Client メニュー項目を使用して設定する自動 USB 接続の構成プロパティは、デバイスが USB リダイレクトから除外されるように構成されている場合を除いて、すべての USB デバイスに適用されます。たとえば、一部のクライアントのバージョンでは、Web カメラとマイクロフォンはリアルタイム オーディオビデオ機能を使用する方が良好に動作するため、デフォルトで USB リダイレクトから除外されています。場合によっては、USB デバイスがデフォルトでリダイレクトから除外されておらず、管理者が明示的にデバイスをリダイレクトから除外する必要があります。たとえば、次のタイプの USB デバイスは USB リダイレクトには適しておらず、リモート デスクトップに自動的に接続してはなりません。

- USB イーサネット デバイス。USB イーサネット デバイスをリダイレクトすると、そのデバイスが唯一のイーサネット デバイスの場合、クライアント システムのネットワーク接続が切断されます。
- タッチ画面デバイス。タッチ画面デバイスをリダイレクトすると、リモート デスクトップはタッチ入力を受け付けますが、キーボード入力は受け付けません。

リモート デスクトップを USB デバイスに自動接続するように設定している場合、タッチ画面デバイスやネットワーク デバイスなどの特定のデバイスを除外するようにポリシーを構成することができます。詳細については、USB デバイスのフィルタ ポリシー設定の構成 を参照してください。

Windows クライアントでは、除外されたデバイスを除くすべてのデバイスに自動的に接続する設定を使用する代わりに、Horizon Client がスマート フォンやタブレットなどの特定のデバイスもしくは特定の複数デバイスのみをリモート デスクトップに再接続するように設定する構成ファイルをクライアントで編集することができます。手順については、『Windows 版 VMware Horizon Client の使用』を参照してください。

保護された Horizon 7 環境での USB デバイスの展開

USB デバイスは BadUSB と呼ばれるセキュリティ脅威に対して脆弱である可能性があり、一部の USB デバイスではファームウェアがハイジャックされたり、マルウェアに置き換えられたりする場合があります。たとえば、ネットワーク トラフィックをリダイレクトしたり、キーボードをエミュレートしてキーストロークを取得したりするデバイスを作成できます。このようなセキュリティ上の脆弱性から Horizon 7 の展開が保護されるように USB リダイレクト機能を構成できます。

USB リダイレクトを無効にすることで、すべての USB デバイスがユーザーの Horizon 7 デスクトップやアプリケーションにリダイレクトされないようにできます。あるいは、特定の USB デバイスのリダイレクト機能を無効にすることで、ユーザーが自分のデスクトップやアプリケーションで特定のデバイスにしかアクセスできないようにすることができます。

組織のセキュリティ要件に従って、このような設定を施すかどうかを決定してください。これらの設定は必須ではありません。Horizon 7 の展開で、USB リダイレクトをインストールし、すべての USB デバイスでその機能を有効なままにしておくこともできます。少なくとも、組織がこのセキュリティ上の脆弱性に晒される可能性をどの程度まで限定する必要があるかについて、慎重に検討してください。

すべてのタイプのデバイスに対する USB リダイレクトの無効化

一部の非常にセキュリティ要件が厳しい環境では、ユーザーがクライアント デバイスに接続した可能性のあるすべての USB デバイスがリモート デスクトップおよびアプリケーションにリダイレクトされるのを回避する必要があります。すべてのデスクトップ プール、特定のデスクトップ プール、またはデスクトップ プール内の特定のユーザーの USB リダイレクトを無効にすることができます。

状況に応じて、次に示す方法の中から任意のものを使用してください。

- Horizon Agent をデスクトップ イメージまたは RDS ホストでインストールする場合、[USB リダイレクト] セットアップ オプションを選択解除してください（このオプションはデフォルトで選択されていません）。この手法では、デスクトップ イメージまたは RDS ホストから展開されるすべてのリモート デスクトップおよびアプリケーションで、USB デバイスへのアクセスが回避されます。
- Horizon Administrator で、特定のプールに対する [USB アクセス] ポリシーを編集して、アクセスを拒否または許可します。この手法では、デスクトップ イメージを変更する必要はなく、特定のデスクトップおよびアプリケーション プールで USB デバイスへのアクセスを制御できます。

  RDS デスクトップおよびアプリケーション プールには、グローバル [USB アクセス] ポリシーのみを使用できます。個々の RDS デスクトップまたはアプリケーション プールに対してこのポリシーを設定することはできません。
- View Administrator で、デスクトップまたはアプリケーション プール レベルでポリシーを設定した後、[ユーザー上書き] 設定を選択し、ユーザーを選択することで、プール内の特定のユーザーに対するポリシーを上書きできます。
- 必要に応じて、Horizon Agent 側またはクライアント側で `Exclude All Devices` ポリシーを **`true`** に設定します。
- スマート ポリシーを使用して、[USB リダイレクト] Horizon ポリシー設定を無効にするポリシーを作成します。この手法により、特定の条件が満たされる場合に特定のリモート デスクトップでの USB リダイレクトを無効化できます。たとえば、ユーザーが企業のネットワーク以外からリモート デスクトップに接続している場合は USB リダイレクトを無効にするポリシーを設定できます。

`Exclude All Devices` ポリシーを **`true`** に設定すると、Horizon Client はどの USB デバイスもリダイレクトされないようにします。その他のポリシー設定を使用して、特定のデバイスまたはデバイス ファミリがリダイレクトされるように変更できます。このポリシーを **`false`** に設定すると、Horizon Client は、その他のポリシー設定でブロックされているものを除き、すべての USB デバイスがリダイレクトされるようにします。このポリシーは、Horizon Agent と Horizon Client の両方に設定できます。次の表は、Horizon Agent と Horizon Client に設定できる `Exclude All Devices` ポリシーを組み合わせて、クライアント コンピュータに効果的なポリシーを作成する方法を示しています。デフォルトでは、ブロックされていない限り、すべての USB デバイスがリダイレクトされるようになっています。

表 4-1. Exclude All Devices（すべてのデバイスを除外する）ポリシーの組み合わせた場合の効果

Horizon Agent での Exclude All Devices（すべてのデバイスを除外する）ポリシー	Horizon Client での Exclude All Devices（すべてのデバイスを除外する）ポリシー	組み合わせた場合の効果的な Exclude All Devices（すべてのデバイスを除外する）ポリシー
false または未定義（すべての USB デバイスを含む）	**false** または未定義（すべての USB デバイスを含む）	すべての USB デバイスを含む
false（すべての USB デバイスを含む）	**true**（すべての USB デバイスを除外する）	すべての USB デバイスを除外する
true（すべての USB デバイスを除外する）	いずれか、または未定義	すべての USB デバイスを除外する

`Disable Remote Configuration Download` ポリシーを **true** に設定すると、Horizon Agent での `Exclude All Devices` の値が Horizon Client に渡されませんが、Horizon Agent と Horizon Client は `Exclude All Devices` のローカル値を適用します。

これらのポリシーは、Horizon Agent の構成 ADMX テンプレート ファイル (`vdm_agent.admx`) に含まれています。

特定のデバイスに対する USB リダイレクトの無効化

ユーザーの中には、ローカル側で接続された特定の USB デバイスをリダイレクトして、リモート デスクトップまたはアプリケーションでそれらのデバイスがタスクを実行できるようにする必要のあるユーザーもいます。たとえば、医師は Dictaphone USB デバイスを使用して、患者の医療情報を記録しなければならない場合があります。このような場合、すべての USB デバイスへのアクセスを無効にすることはできません。グループ ポリシー設定を使用して、特定のデバイスに対して USB リダイレクトを有効または無効にすることができます。

特定のデバイスに対して USB リダイレクトを有効にする前に、会社内のクライアント マシンに接続される物理デバイスを信用できることを確認してください。サプライ チェーンを信用できることを確認します。可能であれば、USB デバイスの加工および流通過程の管理体制を追跡します。

また、従業員に不明な発行元からのデバイスを接続しないように周知します。可能な場合は、環境内のデバイスを署名付きファームウェア更新のみ、つまり FIPS 140-2 レベル 3 認定のもののみに限定し、現場で更新可能なすべての種類のファームウェアをサポートしないようにします。このようなタイプの USB デバイスは発行元を特定するのが困難であり、デバイスの要件によっては検出不可能である可能性があります。このような選択肢は実用的ではないかもしれませんが、検討する価値はあります。

各 USB デバイスにはコンピュータにそれ自体を認識させるためのベンダー ID と製品 ID が付けられています。Horizon Agent 構成のグループ ポリシー設定を構成することで、既知のデバイス タイプを含めるポリシーを設定できます。この手法により、不明なデバイスが環境内で使用されるリスクをなくすことができます。

たとえば、既知のデバイス ベンダー ID および製品 ID である `vid/pid=0123/abcd` を除くすべてのデバイスがリモート デスクトップまたはアプリケーションにリダイレクトされるのを回避できます。

```
ExcludeAllDevices   Enabled

IncludeVidPid       o:vid-0123_pid-abcd
```

注: この例の構成では保護することはできますが、感染したデバイスによって何らかの vid/pid が報告される可能性があるため、攻撃の可能性は依然としてあります。

デフォルトで、Horizon 7 は特定のデバイス ファミリがリモート デスクトップまたはアプリケーションにリダイレクトされるのをブロックします。たとえば、HID（ヒューマン インターフェイス デバイス）やキーボードなどはゲスト内への表示がブロックされます。出回っている一部の BadUSB コードは USB キーボード デバイスをターゲットにしています。

特定のデバイス ファミリがリモート デスクトップまたはアプリケーションにリダイレクトされるのを回避できます。たとえば、すべてのビデオ、オーディオ、および大規模ストレージ デバイスをブロックできます。

```
ExcludeDeviceFamily   o:video;audio;storage
```

反対に、ホワイトリストを作成し、すべてのデバイスがリダイレクトされないようにしても特定のデバイス ファミリのみは使用できるようにすることもできます。たとえば、ストレージ デバイスを除くすべてのデバイスをブロックできます。

```
ExcludeAllDevices     Enabled

IncludeDeviceFamily   o:storage
```

リモート ユーザーがデスクトップまたはアプリケーションにログインして、それを感染させる場合、別のリスクが発生する可能性があります。会社のファイアウォールの外側から行われたすべての Horizon 7 接続への USB アクセスを回避できます。USB デバイスは内的には使用できますが、外的には使用できなくなります。

TCP ポート 32111 をブロックして USB デバイスへの外部アクセスを無効にすると、タイム ゾーン同期が動作しなくなります。これは、タイム ゾーン同期でもポート 32111 が使用されているためです。ゼロ クライアントの場合、USB トラフィックは UDP ポート 4172 の仮想チャネル内に組み込まれます。ポート 4172 は USB リダイレクトの他にディスプレイ プロトコルにも使用されるため、ポート 4172 をブロックすることはできません。必要な場合は、ゼロ クライアントに対して USB リダイレクトを無効に設定できます。詳細については、ゼロ クライアント製品パンフレットを参照するか、ゼロ クライアント ベンダーにお問い合わせください。

特定のデバイス ファミリまたは特定のデバイスをブロックするポリシーを設定すると、BadUSB マルウェアによって感染させられるリスクを軽減できる可能性があります。これらのポリシーによってすべてのリスクが軽減されるわけではありませんが、全体的なセキュリティ戦略の一部として有効に機能する可能性があります。

ログ ファイルを使用してのトラブルシューティングと USB デバイス ID の確認

USB に有用なログ ファイルは、クライアント システムとリモート デスクトップの両方のオペレーティング システムまたは RDS ホストにあります。トラブルシューティングを行うには、両方の場所にあるログ ファイルを使用します。特定のデバイスの製品 ID を見つけるには、クライアント側のログを使用します。

USB デバイスの分割またはフィルタリングを構成しようとしている場合、または特定のデバイスが Horizon Client メニューに表示されない理由を判断しようとしている場合は、クライアント側のログを確認します。クライアント ログは USB アービトレータ（USB 仲裁デバイス）および Horizon View USB サービスのために生成されます。Windows および Linux クライアントでのログ記録はデフォルトで有効になっています。Mac クライアントでは、ログ記録はデフォルトで無効になっています。Mac クライアントでログ記録を有効にするには、『VMware Horizon Client for Mac の使用』を参照してください。

USB デバイスの分割およびフィルタリングのポリシーを構成する場合、設定する一部の値で USB デバイス用の VID（ベンダー ID）および PID（製品 ID）が必要になります。VID および PID を見つけるには、**vid** および **pid** と組み合わされた製品名をインターネット検索できます。あるいは、Horizon Client の実行中に、USB デバイスをローカル システムに接続してクライアント側のログを調べることができます。次の表は、ログ ファイルのデフォルトの場所を示しています。

表 4-2. ログ ファイルの場所

クライアントまたはエージェント	ログ ファイルのパス
Windows クライアント	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log
Horizon Agent	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt
Mac クライアント	/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log /Library/Logs/VMware/vmware-usbarbitrator-xxxx.log
Linux クライアント	（デフォルトの場所）/tmp/vmware-root/vmware-view-usbd-*.log

デバイスがリモート デスクトップまたはアプリケーションにリダイレクトされた後に、デバイスに関する問題が発生する場合は、クライアント側とエージェント側両方のログを調べてください。

USB リダイレクトを制御するポリシーの使用

リモート デスクトップまたはアプリケーション (Horizon Agent) と Horizon Client の両方に USB ポリシーを構成できます。これらのポリシーは、クライアント デバイスで複合 USB デバイスを個別のコンポーネントに分割してリダイレクト可能にするかどうかを指定します。デバイスを分割して、クライアントがリダイレクト可能とする USB デバイスのタイプを制限し、Horizon Agent で特定の USB デバイスがクライアント コンピュータから転送されないように防止します。

Horizon Agent または Horizon Client の以前のバージョンをインストールしている場合は、USB リダイレクト ポリシーの機能の一部を使用できません。表 4-3. USB ポリシー設定の互換性 は、Horizon Agent と Horizon Client の組み合わせに応じて Horizon 7 が適用するポリシーについて示しています。

表 4-3. USB ポリシー設定の互換性

Horizon Agent のバージョン	Horizon Client のバージョン	USB ポリシー設定の USB リダイレクトへの影響
5.1 以降	5.1 以降	USB ポリシー設定は、Horizon Agent と Horizon Client の両方に適用されます。Horizon Agent USB ポリシー設定を使用して、USB デバイスがデスクトップに転送されないようブロックできます。Horizon Agent では、デバイス分割およびフィルタリング ポリシーの設定を Horizon Client に送信可能です。Horizon Client USB ポリシー設定を使用して、USB デバイスがクライアント コンピュータからデスクトップにリダイレクトされないよう防止できます。 **注:** View Agent 6.1 以降と Horizon Client 3.3 以降では、これらの USB リダイレクト ポリシー設定が単一ユーザー マシンで実行されるリモート デスクトップに加えて、RDS デスクトップとアプリケーションにも適用されます。
5.1 以降	5.0.x 以前	USB ポリシー設定は、Horizon Agent にのみ適用されます。Horizon Agent USB ポリシー設定を使用して、USB デバイスがデスクトップに転送されないようブロックできます。Horizon Client USB ポリシー設定を使用して、クライアント コンピュータからデスクトップにリダイレクト可能なデバイスの選択を制御することはできません。Horizon Client では、デバイス分割およびフィルタリング ポリシーの設定を Horizon Agent から受信できません。Horizon Client による USB リダイレクトの既存のレジストリ設定は有効なままです。
5.0.x 以前	5.1 以降	USB ポリシー設定は、Horizon Client にのみ適用されます。Horizon Client USB ポリシー設定を使用して、USB デバイスがクライアント コンピュータからデスクトップにリダイレクトされないよう防止できます。Horizon Agent USB ポリシー設定を使用して、USB デバイスがデスクトップに転送されないようブロックすることはできません。Horizon Agent では、デバイス分割およびフィルタリング ポリシーの設定を Horizon Client に送信できません。
5.0.x 以前	5.0.x 以前	USB ポリシー設定は適用されません。Horizon Client による USB リダイレクトの既存のレジストリ設定は有効なままです。

Horizon Client をアップグレードする場合、`HardwareIdFilters` など USB リダイレクトに関する既存のレジストリ設定は、Horizon Client 用に USB ポリシーを定義するまで、すべて有効なままです。

クライアントサイドの USB ポリシーをサポートしていないクライアント デバイスでは、Horizon Agent に USB ポリシーを使用してクライアントからデスクトップまたはアプリケーションへの転送を許可する USB デバイスを制御できます。

複合 USB デバイスのデバイス分割ポリシー設定の構成

複合 USB デバイスは、ビデオ入力デバイスとストレージ デバイス、もしくはマイクロフォンとマウス デバイスなど、2 つ以上のデバイスの組み合わせで構成されます。1 つ以上のコンポーネントをリダイレクトに利用できるようにする必要がある場合は、複合デバイスをコンポーネント インターフェイスに分割し、特定のインターフェイスをリダイレクト対象から除外し、残りのインターフェイスをリダイレクトに含めることができます。

複合デバイスを自動的に分割するポリシーを設定できます。特定のデバイスで自動デバイス分割が機能しない場合や、使用しているアプリケーションで必要な結果が自動分割で得られない場合には、複合デバイスを手動で分割できます。

自動デバイス分割

自動デバイス分割を有効にすると、Horizon 7 は現在適用されているフィルタ ルールに従って複合デバイス内の機能もしくはデバイスを分割しようとします。たとえば、マウス デバイスをクライアントでしか使えない状態に保つために口述マイクロフォンを自動分割しても他のデバイスはリモート デスクトップに転送するというケースが考えられます。

次の表は、Horizon Client が複合 USB デバイスを自動分割するかどうかを決定する `Allow Auto Device Splitting` の設定値を示しています。デフォルトでは、自動分割は無効になっています。

表 4-4. Disable Auto Device Splitting（自動デバイス分割を無効にする）ポリシーを組み合わせた場合の効果

Horizon Agent での自動デバイス分割を許可するポリシー	Horizon Client での自動デバイス分割を許可するポリシー	組み合わせた場合の効果的な自動デバイス分割を許可するポリシー
`Allow – Default Client Setting`	**`false`**（自動分割が無効）	自動分割が無効
`Allow – Default Client Setting`	**`true`**（自動分割が有効）	自動分割が有効
`Allow – Default Client Setting`	未定義	自動分割が有効
`Allow – Override Client Setting`	いずれか、または未定義	自動分割が有効
未定義	未定義	自動分割が無効

注: これらのポリシーは、Horizon Agent 構成 ADMX テンプレート ファイルに含まれています。ADMX テンプレート ファイルの名前は (`vdm_agent.admx`)。

デフォルトでは、Horizon 7 の自動分割は無効であり、複合 USB デバイスのオーディオ出力、キーボード、マウス、スマート カードのコンポーネントはすべてリダイレクト対象から除外されます。

Horizon 7 では、デバイス分割ポリシー設定を適用してから、フィルタ ポリシー設定をすべて適用します。自動分割を有効にしたときに、ベンダー/プロダクト ID を指定し、分割対象から複合 USB デバイスを明示的に除外しない場合は、Horizon 7 が複合 USB デバイスの各インターフェイスを調べ、フィルタ ポリシー設定に従って、除外するインターフェイスか、含めるインターフェイスかを判断します。自動デバイス分割を無効にしたときに、分割する複合 USB デバイスのベンダー/プロダクト ID を明示的に指定しない場合、Horizon 7 はデバイス全体にフィルタ ポリシー設定を適用します。

自動分割を有効にすると、`Exclude Vid/Pid Device From Split` ポリシーを使用して、分割対象から除外する複合 USB デバイスを指定できます。

手動デバイス分割

`Split Vid/Pid Device` ポリシーを使用して、分割したい複合 USB デバイスのベンダーおよびプロダクト ID を指定できます。リダイレクト対象から除外したい複合 USB デバイスのコンポーネントについては、そのインターフェイスも指定できます。このようにして除外したコンポーネントに対しては、どのフィルタ ポリシー設定も Horizon 7 で適用されません。

重要: `Split Vid/Pid Device` ポリシーを使用する場合、明示的に除外しなかったコンポーネントは、Horizon 7 で自動的に含まれることはありません。これらのコンポーネントを含めるには、`Include Vid/Pid Device` などのフィルタ ポリシーを指定する必要があります。

表 4-5. Horizon Agent でのデバイス分割ポリシー設定の分割修飾子 では、Horizon Client に同等のデバイス分割ポリシー設定が存在する場合に、Horizon Client で Horizon Agent デバイス分割ポリシー設定を処理する方法を指定する修飾子を示しています。これらの修飾子は、すべてのデバイス分割ポリシー設定に適用されます。

表 4-5. Horizon Agent でのデバイス分割ポリシー設定の分割修飾子

修飾子	説明
m（マージ）	Horizon Client は、Horizon Client デバイス分割ポリシー設定に加えて、Horizon Agent デバイス分割ポリシー設定を適用します。
o（上書き）	Horizon Client は、Horizon Client デバイス分割ポリシー設定の代わりに、Horizon Agent デバイス分割ポリシー設定を使用します。

表 4-6. デバイス分割ポリシー設定への分割修飾子の適用例 では、別の分割修飾子を指定したときに、Horizon Client で `Exclude Device From Split by Vendor/Product ID` の設定を処理する方法の例を示しています。

表 4-6. デバイス分割ポリシー設定への分割修飾子の適用例

Horizon Agent でのベンダー/製品 ID によりデバイスを分割から除外するポリシー	Horizon Client でのベンダー/製品 ID によりデバイスを分割から除外するポリシー	Horizon Client で使用される効果的なベンダー/製品 ID によりデバイスを分割から除外するポリシー
m:vid-XXXX_pid-XXXX	**vid-YYYY_pid-YYYY**	**vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY**
o:vid-XXXX_pid-XXXX	**vid-YYYY_pid-YYYY**	**vid-XXXX_pid-XXXX**
m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY	**vid-YYYY_pid-YYYY**	**vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY**
o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY	**vid-YYYY_pid-YYYY**	**vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY**

Horizon Agent は、デバイス分割ポリシー設定を接続先で適用しません。

Horizon Client は、次の優先順序で、デバイス分割ポリシー設定を評価します。

- `Exclude Vid/Pid Device From Split`
- `Split Vid/Pid Device`

分割対象からデバイスを除外するデバイス分割ポリシー設定は、デバイスを分割するためのどのポリシー設定よりも優先されます。分割対象から除外するインターフェイスまたはデバイスを定義すると、Horizon Client は、一致するコンポーネント デバイスをリダイレクトに利用可能なデバイスから除外します。

複合 USB デバイスを分割するためのポリシーの設定例

自動分割後に、特定のベンダーおよび製品 ID のデバイスをリダイレクト対象から除外するデスクトップの分割ポリシーを設定し、そのポリシーをクライアント コンピュータに渡します。

- Horizon Agent の場合、`Allow Auto Device Splitting` ポリシーを `Allow – Override Client Setting` に設定します。
- Horizon Agent の場合、`Exclude VidPid From Split` ポリシーを **o:vid-*xxx*_pid-*yyyy*** に設定します（*xxx* と *yyyy* は該当する ID）。

デスクトップの自動デバイス分割を許可し、クライアント コンピュータで特定のデバイスを分割するポリシーを指定します。

- Horizon Agent の場合、`Allow Auto Device Splitting` ポリシーを `Allow – Override Client Setting` に設定します。
- クライアント デバイスの場合、`Include Vid/Pid Device` フィルタ ポリシーを、分割したい特定のデバイスを含めるように設定します（例：**`vid-0781_pid-554c`**）。
- クライアント デバイスの場合、`Split Vid/Pid Device` ポリシーを、指定した複合 USB デバイスを分割してインターフェイス 00 とインターフェイス 01 をリダイレクト対象から除外するように設定します（例：**`vid-0781_pid-554c(exintf:00;exintf:01)`**）。

USB デバイスのフィルタ ポリシー設定の構成

Horizon Agent および Horizon Client に対して構成するフィルタ ポリシー設定では、クライアント コンピュータからリモート デスクトップまたはアプリケーションまでリダイレクト可能な USB デバイスが指定されます。USB デバイス フィルタリングは、多くの場合、企業がリモート デスクトップ上の大容量ストレージ デバイスの使用を無効にしたり、クライアント デバイスをリモート デスクトップに接続する USB イーサネット アダプタのような、特定タイプのデバイスが転送されないようにブロックするために使用されます。

デスクトップまたはアプリケーションに接続すると、Horizon Client は Horizon Agent の USB ポリシー設定をダウンロードし、Horizon Client USB ポリシー設定とともにそれらの設定を使用して、クライアント コンピュータからのリダイレクトを許可する USB デバイスを決定します。

Horizon 7 では、デバイス分割ポリシー設定をすべて適用してから、フィルタ ポリシー設定を適用します。複合 USB デバイスを分割した場合、Horizon 7 では各デバイスのインターフェイスが調べられ、フィルタ ポリシー設定に従って、含めるものと含めないものが判断されます。複合 USB デバイスを分割しなかった場合、Horizon 7 でフィルタ ポリシー設定がデバイス全体に適用されます。

デバイス分割ポリシーは Horizon Agent の構成 ADMX テンプレート ファイル (`vdm_agent.admx`) に含まれます。

エージェント適用型 USB 設定の操作

次の表に、Horizon Client に同等のフィルタ ポリシー設定が存在する場合に、Horizon Client でエージェント適用型設定の Horizon Agent フィルタ ポリシー設定を処理する方法を指定する修飾子を示します。

表 4-7. エージェント適用型設定のフィルタ修飾子

修飾子	説明
`m`（マージ）	Horizon Client により、Horizon Client フィルタ ポリシー設定に加えて、Horizon Agent フィルタ ポリシー設定が適用されます。ブール (true/false) 設定の場合、クライアント ポリシーが設定されていなければエージェントの設定が使用されます。クライアント ポリシーが設定されている場合、`Exclude All Devices` 設定の場合を除き、エージェントの設定は無視されます。`Exclude All Devices` ポリシーがエージェント側に設定されている場合、このポリシーはクライアント設定よりも優先されます。
`o`（上書き）	Horizon Client は Horizon Client フィルタ ポリシー設定ではなく、Horizon Agent フィルタ ポリシー設定を使用します。

たとえば、エージェント側で次のポリシー設定を行うと、クライアント側のすべての包含ルールに優先し、デバイス VID-0911_PID-149a にのみ包含ルールが適用されます。

```
IncludeVidPid: o:VID-0911_PID-149a
```

アスタリスクをワイルドカードとして使用することもできます（例：**o:vid-0911_pid-******）。

重要: **o** または **m** 修飾子なしでエージェント側の構成を行うと、構成ルールは無効と見なされ、無視されます。

クライアント解釈型 USB 設定の操作

次の表に、クライアント解釈型設定の Horizon Agent フィルタ ポリシー設定を、Horizon Client で処理する方法を指定する修飾子を示します。

表 4-8. クライアント解釈型設定のフィルタ修飾子

修飾子	説明
`Default`（レジストリ設定では **d**）	Horizon Client フィルタ ポリシー設定が存在しない場合、Horizon Client は Horizon Agent フィルタ ポリシー設定を使用します。 Horizon Client フィルタ ポリシー設定が存在する場合、Horizon Client はそのポリシー設定を適用し、Horizon Agent フィルタ ポリシー設定は無視します。
`Override`（レジストリ設定では **o**）	Horizon Client では、同等の Horizon Client フィルタ ポリシー設定ではなく、Horizon Agent フィルタ ポリシー設定が使用されます。

Horizon Agent は、クライアント解釈型設定のフィルタ ポリシー設定を接続先で適用しません。

次の表に、別のフィルタ修飾子を指定したときに、Horizon Client で `Allow Smart Cards` の設定を処理する方法の例を示します。

表 4-9. クライアント解釈型設定へのフィルタ修飾子の適用例

Horizon Agent での Allow Smart Cards（スマート カードを許可する）設定	Horizon Client での Allow Smart Cards（スマート カードを許可する）設定	Horizon Client で使用される効果的な Allow Smart Cards（スマート カードを許可する）ポリシー設定
`Disable – Default Client Setting`（レジストリ設定では **d:false**）	**true**（許可する）	**true**（許可する）
`Disable – Override Client Setting`（レジストリ設定では **o:false**）	**true**（許可する）	**false**（無効にする）

`Disable Remote Configuration Download` ポリシーを **true** に設定すると、Horizon Client は、Horizon Agent から送信されるフィルタ ポリシー設定をすべて無視します。

Horizon Agent は、別のフィルタ ポリシー設定を使用するよう Horizon Client を構成しても、または Horizon Client において Horizon Agent からのフィルタ ポリシー設定のダウンロードを無効にしても、エージェント適用型設定にあるフィルタ ポリシー設定を常に接続先で適用します。Horizon Client では、Horizon Agent がデバイスの転送をブロックしていることをレポートしません。

設定の優先

Horizon Client では、優先順位に従って、フィルタ ポリシー設定が評価されます。一致デバイスがリダイレクトされないようにするフィルタ ポリシー設定は、デバイスを含む同等のフィルタ ポリシー設定よりも優先されます。デバイスを除外するフィルタ ポリシー設定が Horizon Client にない場合は、`Exclude All Devices` ポリシーを **`true`** に設定していない限り、Horizon Client ではデバイスのリダイレクトが許可されます。しかし、デバイスを除外するように Horizon Agent でフィルタ ポリシー設定を構成した場合、デスクトップまたはアプリケーションはデバイスをそれにリダイレクトしようとする試みをすべてブロックします。

Horizon Client は、Horizon Client 設定と Horizon Agent 設定に加え、Horizon Agent 設定に適用する修飾子の値を考慮し、優先順位に従いフィルタ ポリシー設定を評価します。次のリストに優先順位（項目 1 が最優先）を示します。

1 `Exclude Path`

2 `Include Path`

3 `Exclude Vid/Pid Device`

4 `Include Vid/Pid Device`

5 `Exclude Device Family`

6 `Include Device Family`

7 `Allow Audio Input Devices`、`Allow Audio Output Devices`、`Allow HIDBootable`、`Allow HID (Non Bootable and Not Mouse Keyboard)`、`Allow Keyboard and Mouse Devices`、`Allow Smart Cards`、`Allow Video Devices`

8 すべての USB デバイスを除外するか含めるかが判断される、組み合わせた場合の効果的な `Exclude All Devices` ポリシー

`Exclude Path` および `Include Path` フィルタ ポリシー設定は、Horizon Client に対してのみ設定できます。別のデバイス ファミリ向けの `Allow` フィルタ ポリシー設定は、優先順位が同じです。

ベンダーおよびプロダクト ID の値に基づいてデバイスを除外するポリシー設定を構成すると、デバイスが属するファミリの `Allow` ポリシー設定を構成していたとしても、Horizon Client によりベンダーとプロダクト ID の値がこのポリシー設定と一致するデバイスは除外されます。

ポリシー設定の優先順位により、ポリシー設定間の競合が解決されます。スマート カードのリダイレクトを可能にするために `Allow Smart Cards` を構成した場合、それよりも優先順位の高い除外ポリシー設定を構成すると、このポリシーは上書きされます。たとえば、パス、ベンダー、プロダクト ID の値が一致するスマート カード デバイスを除外するよう `Exclude Vid/Pid Device` ポリシー設定を構成する場合が考えられます。また、`Exclude Device Family` デバイス ファミリ全体も除外する `smart-card` ポリシー設定を構成する場合も同様です。

何らかの Horizon Agent フィルタ ポリシー設定を構成すると、Horizon Agent はリモート デスクトップまたはアプリケーション上で次の優先順位（項目 1 が最優先）に従って、フィルタ ポリシー設定を評価して適用します。

1 `Exclude Vid/Pid Device`

2 `Include Vid/Pid Device`

3 `Exclude Device Family`

4 `Include Device Family`

5 すべての USB デバイスを除外するか含めるかが設定されている、エージェント適用型の `Exclude All Devices` ポリシー

Horizon Agent は、この限定的なフィルタ ポリシー設定のセットを接続先で適用します。

Horizon Agent のフィルタ ポリシー設定を定義することで、管理されていないクライアント コンピュータのフィルタリング ポリシーを作成できます。また、この機能により、Horizon Client のフィルタ ポリシー設定でリダイレクトが許可されている場合でも、クライアント コンピュータから転送されないようデバイスをブロックすることもできます。

たとえば、Horizon Client がデバイスのリダイレクトを可能にするのを許可するポリシーを構成する場合、デバイスを除外するよう Horizon Agent のポリシーを構成すれば、Horizon Agent はデバイスをブロックします。

USB デバイスをフィルタリングするためのポリシーの設定例

これらの例で使用されるベンダー ID とプロダクト ID は、単なる例です。特定デバイスに対するベンダー ID とプロダクト ID の決定については、ログ ファイルを使用してのトラブルシューティングと USB デバイス ID の確認を参照してください。

- クライアントで特定のデバイスがリダイレクトされないようにする

```
Exclude Vid/Pid Device:     Vid-0341_Pid-1a11
```

- すべてのストレージ デバイスがこのデスクトップまたはアプリケーション プールにリダイレクトされないようにブロックします。次のエージェント側設定を使用します。

```
Exclude Device Family:      o:storage
```

- デスクトップ プールのすべてのユーザーに対してオーディオおよびビデオ デバイスをブロックし、これらのデバイスがリアルタイム オーディオビデオ機能で常時利用可能になるようにする次のエージェント側設定を使用します。

```
Exclude Device Family:      o:video;audio
```

  ベンダーおよびプロダクト ID を使用して特定のデバイスを除外することもできることに注意してください。

- クライアントで 1 つの特定のデバイスを除くすべてのデバイスがリダイレクトされないようにブロックする

```
Exclude All Devices:        true
Include Vid/Pid Device:     Vid-0123_Pid-abcd
```

- エンド ユーザーに問題が起こるため、特定の企業で製造されたすべてのデバイスを除外する次のエージェント側設定を使用します。

```
Exclude Vid/Pid Device:     o:Vid-0341_Pid-*
```

- クライアントで 2 つの特定のデバイスを含め、その他すべてを除外する

```
Exclude All Devices:        true
Include Vid/Pid Device:     Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
```

USB デバイス ファミリ

Horizon Client、または View Agent または Horizon Agent の USB フィルタリング規則を作成する場合にファミリを指定できます。

注: 一部のデバイスはデバイス ファミリを報告しません。

表 4-10. USB デバイス ファミリ

デバイス ファミリ名	説明
audio	すべてのオーディオ入力またはオーディオ出力デバイス。
audio-in	マイクロフォンなどのオーディオ入力デバイス。
audio-out	ラウドスピーカーおよびヘッドホンなどのオーディオ出力デバイス。
bluetooth	Bluetooth に接続されたデバイス。
comm	モデムおよび有線ネットワーク アダプタなどの通信デバイス。
hid	キーボードおよびポインティング デバイスを除くヒューマン インターフェイス デバイス。
hid-bootable	キーボードおよびポインティング デバイスを除く、起動時に使用できるヒューマン インターフェイス デバイス。
imaging	スキャナなどの画像デバイス。
keyboard	キーボード デバイス。
mouse	マウスなどのポインティング デバイス。
other	ファミリが指定されていません。
pda	携帯情報端末。
physical	カフィードバック ジョイスティックなどのカフィードバック デバイス。
printer	印刷デバイス。
security	指紋読み取りなどのセキュリティ デバイス。
smart-card	スマート カード デバイス。
storage	フラッシュ ドライブおよび外部ハードディスク ドライブなどの大容量ストレージ デバイス。
unknown	ファミリが不明です。
vendor	ベンダ固有の機能のあるデバイス。
video	ビデオ入力デバイス。
wireless	無線ネットワーク アダプタ。
wusb	無線 USB デバイス。

Horizon Agent の構成 ADMX テンプレートの USB 設定

Horizon Agent と Horizon Client の両方で USB ポリシー設定を定義できます。接続時に、Horizon Client は USB ポリシー設定を Horizon Agent からダウンロードし、それらを Horizon Client USB ポリシー設定と一緒に使用して、クライアント コンピュータからのリダイレクトに利用できるようにするデバイスを指定します。

Horizon Agent の構成 ADMX テンプレート ファイルには、Horizon Agent の認証および環境コンポーネントに関連するポリシー設定（USB リダイレクトなど）が含まれています。ADMX テンプレート ファイルには名前が付けられています (`vdm_agent.admx`)。設定はコンピュータ レベルで適用されます。Horizon Agent は、コンピュータ レベルで GPO から設定を優先的に読み取ります。GPO からの読み取りがない場合は、`HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB` のレジストリから設定を読み取ります。

USB デバイス分割を構成するための設定

次の表で、Horizon Agent の構成 ADMX テンプレート ファイル内にある、複合 USB デバイスの分割に関する各ポリシー設定について説明します。グループ ポリシー管理エディタで、[VMware Horizon Agent の構成] - [View の USB 構成] - [クライアントがダウンロード可能な設定のみ] フォルダの順に移動すると、これらの設定を確認できます。Horizon Agent は、これらの設定を適用しません。Horizon Agent は、設定を Horizon Client に渡し、マージ (`m`) またはオーバーライド (`o`) のどちらの修飾子を指定したかに応じて、解釈と適用が行われます。Horizon Client は設定を使用して、複合 USB デバイスをコンポーネント デバイスに分割するかどうか、そしてコンポーネント デバイスをリダイレクトに利用可能なデバイスから除外するかどうかを決定します。複合 USB デバイスの分割ポリシーの Horizon での適用方法については、複合 USB デバイスのデバイス分割ポリシー設定の構成を参照してください。

表 4-11. Horizon Agent の構成テンプレート：デバイス分割設定

設定	プロパティ
Allow Auto Device Splitting プロパティ： AllowAutoDeviceSplitting	複合 USB デバイスの自動分割を許可します。 デフォルト値は未定義で、**false** と同じです。
Exclude Vid/Pid Device from Split プロパティ： SplitExcludeVidPid	ベンダーおよびプロダクト ID で指定された複合 USB デバイスは、分割対象から除外します。設定の形式：{m|o}:vid-*xxx1*_pid-*yyy2*[;vid-*xxx2*_pid-*yyy2*]... ID 番号は 16 進数で指定する必要があります。ID の個々の数字の位置にワイルドカード文字（*****）を使用できます。 例：**o:vid-0781_pid-55**** デフォルト値は定義されていません。
Split Vid/Pid Device プロパティ： SplitVidPid	ベンダーおよびプロダクト ID で指定した複合 USB デバイスのコンポーネントを、別のデバイスとして扱います。設定の形式： {m|o}:vid-*xxxx*_pid-*yyyy*(exintf:*zz*[;exintf:*ww*]) または {m|o}:vid-*xxxx*_pid-*yyyy*(exintf:*zz*[;exintf:*ww*]) exintf というキーワードを使用すれば、インターフェイス番号を指定することで、コンポーネントをリダイレクトから除外することができます。ID 番号は 16 進数で指定し、インターフェイス番号は先行ゼロをすべて含む 10 進数で指定する必要があります。ID の個々の数字の位置にワイルドカード文字（*****）を使用できます。 例：**o:vid-0781_pid-554c(exintf:01;exintf:02)** **注:** 明示的に除外しなかったコンポーネントが、Horizon 7 に自動的に含まれることはありません。これらのコンポーネントを含めるには、Include Vid/Pid Device などのフィルタ ポリシーを指定する必要があります。 デフォルト値は定義されていません。

Horizon Agent 適用型 USB 設定

次の表で、Horizon Agent の構成 ADMX テンプレート ファイルにある、USB 用の各エージェント適用型ポリシー設定について説明します。グループ ポリシー管理エディタで、[VMware Horizon Agent の構成] - [View の USB 構成] フォルダの順に移動すると、これらの設定を確認できます。Horizon Agent は設定を使用して、USB デバイスがホスト マシンに転送できるかどうかを判断します。Horizon Agent はまた、設定を Horizon Client に渡し、マージ (m) またはオーバーライド (o) のどちらの修飾子を指定したかに応じて、解釈と適用が行われます。Horizon Client は設定を使用して、USB デバイスがリダイレクトに利用可能かどうかを決定します。Horizon Agent は、エージェント適用型ポリシー設定を常に適用するため、Horizon Client に設定したポリシーとは逆の結果になることがあります。USB デバイスをフィルタリングするためのポリシーを Horizon 7 で適用する方法については、USB デバイスのフィルタ ポリシー設定の構成を参照してください。

表 4-12. Horizon Agent の構成テンプレート：エージェント適用型設定

設定	プロパティ
Exclude All Devices プロパティ： ExcludeAllDevices	転送対象からすべての USB デバイスを除外します。**true** に設定すると、その他のポリシー設定を使用して、特定のデバイスまたはデバイス ファミリが転送されるようにすることができます。**false** に設定すると、その他のポリシー設定を使用して、特定のデバイスまたはデバイス ファミリが転送されるのを防止できます **true** に設定し、Horizon Client に渡すようにすると、この設定は Horizon Client での設定を常にオーバーライドします。この設定では、マージ（m）または上書き（o）の修飾子は使用できません。 デフォルト値は未定義で、**false** と同じです。
Exclude Device Family プロパティ： ExcludeFamily	転送対象からデバイス ファミリを除外します。設定の形式：{m|o}:*family_name_1*[;*family_name_2*]... 例：**o:bluetooth;smart-card** 自動デバイス分割を有効にした場合、Horizon 7 はコンポジット USB デバイスの各インターフェイスのデバイス ファミリを調べ、除外するインターフェイスを決定します。自動デバイス分割を無効にした場合、Horizon 7 はコンポジット USB デバイス全体のデバイス ファミリを調べます。 デフォルト値は定義されていません。
Exclude Vid/Pid Device プロパティ： ExcludeVidPid	指定したベンダーとプロダクト ID のデバイスを、転送対象から除外します。設定の形式：{m|o}:vid-*xxx1*_pid-*yyy1*[;vid-*xxx2*_pid-*yyy2*]... ID 番号は 16 進数で指定する必要があります。ID の個々の数字の位置にワイルドカード文字（*）を使用できます。 例：**m:vid-0781_pid-****;vid-0561_pid-554c** デフォルト値は定義されていません。
Include Device Family プロパティ： IncludeFamily	デバイス ファミリを転送対象に含めます。設定の形式：{m|o}:*family_name_1*[;*family_name_2*]... 例：**m:storage** デフォルト値は定義されていません。
Include Vid/Pid Device プロパティ： IncludeVidPid	指定したベンダーとプロダクト ID のデバイスを、転送対象に含めます。設定の形式：{m|o}:vid-*xxx1*_pid-*yyy1*[;vid-*xxx2*_pid-*yyy2*]... ID 番号は 16 進数で指定する必要があります。ID の個々の数字の位置にワイルドカード文字（*）を使用できます。 例：**o:vid-0561_pid-554c** デフォルト値は定義されていません。

クライアント解釈型 USB 設定

次の表で、Horizon Agent の構成 ADMX テンプレート ファイル内にある各クライアント解釈型ポリシー設定について説明します。グループ ポリシー管理エディタで、[VMware Horizon Agent の構成] - [View の USB 構成] - [クライアントがダウンロード可能な設定のみ] フォルダの順に移動すると、これらの設定を確認できます。Horizon Agent は、これらの設定を適用しません。Horizon Agent は、Horizon Client に設定を渡し、解釈と適用が行われます。Horizon Client は設定を使用して、USB デバイスがリダイレクトに利用可能かどうかを決定します。

表 4-13. Horizon Agent の構成テンプレート：クライアント解釈型設定

設定	プロパティ
Allow Audio Input Devices プロパティ： AllowAudioIn	オーディオ入力デバイスの転送を許可します。 デフォルト値は定義されていませんが、これは **true** が設定されている場合に相当します。
Allow Audio Output Devices プロパティ： AllowAudioOut	オーディオ出力デバイスの転送を許可します。 デフォルト値は未定義で、**false** と同じです。
Allow HID-Bootable プロパティ： AllowHIDBootable	キーボードとマウス以外で、起動時に利用可能な入力デバイス（別名 HID 起動可能なデバイス）の転送を許可します。 デフォルト値は定義されていませんが、これは **true** が設定されている場合に相当します。
Allow Other Input Devices	HID 起動可能なデバイスやポインティング デバイス付きキーボード以外の入力デバイスの転送を許可します。 デフォルト値は定義されていません。
Allow Keyboard and Mouse Devices プロパティ： AllowKeyboardMouse	マウス、トラックボール、タッチ パッドなどのポインティング デバイス付きキーボードの転送を許可します。 デフォルト値は未定義で、**false** と同じです。
Allow Smart Cards プロパティ： AllowSmartcard	スマート カード デバイスの転送を許可します。 デフォルト値は未定義で、**false** と同じです。
Allow Video Devices プロパティ： AllowVideo	ビデオ デバイスの転送を許可します。 デフォルト値は定義されていませんが、これは **true** が設定されている場合に相当します。

USB リダイレクトに関する問題のトラブルシューティング

Horizon Client で USB リダイレクトに関する各種の問題が発生することがあります。

問題

Horizon Client の USB リダイレクトで、ローカル デバイスをリモート デスクトップで使用可能にできなかったり、Horizon Client で一部のデバイスがリダイレクトに使用できるように表示されなかったりします。

原因

USB リダイレクトが正常に機能しない場合、または予想どおりに機能しない場合、可能性のある原因は次のとおりです。

- デバイスが複合 USB デバイスであり、含まれるデバイスの 1 つがデフォルトでブロックされています。たとえばマウスを含む読み上げデバイスはデフォルトでブロックされています。これはマウス デバイスがデフォルトでブロックされているためです。この問題を回避するには、『Horizon 7 でのリモート デスクトップ機能の構成』の「複合 USB デバイスのデバイス分割ポリシー設定の構成」を参照してください。
- USB リダイレクトは、リモート デスクトップおよびアプリケーションが展開されている Windows Server 2008 RDS ホストではサポートされません。View Agent 6.1 以降では、Windows Server 2012 RDS ホストで USB リダイレクトがサポートされますが、サポート対象は USB ストレージ デバイスのみです。USB リダイレクトは、単一ユーザー デスクトップとして使用されいる Windows Server 2008 R2 および Windows Server 2012 R2 システムでサポートされます。

- RDS デスクトップおよびアプリケーションでは、USB フラッシュ ドライブとハード ディスクのみがサポートされます。その他のタイプの USB デバイスや、セキュリティ ストレージ ドライブや USB CD-ROM などのその他のタイプの USB ストレージ デバイスを RDS デスクトップやアプリケーションにリダイレクトすることはできません。
- Web カメラはリダイレクトの対象としてサポートされていません。
- USB オーディオ デバイスのリダイレクトは、ネットワークの状態に依存し、信頼できません。一部のデバイスでは、アイドル状態のときでさえ、高いデータ スループットが必要です。
- ブート デバイスでは USB リダイレクトがサポートされていません。USB デバイスからブートする Windows システムで Horizon Client を実行しており、このデバイスをリモート デスクトップにリダイレクトした場合、ローカル オペレーティング システムが応答しなかったり使用できなかったりすることがあります。http://kb.vmware.com/kb/1021409 を参照してください。
- Horizon Client for Windows では、デフォルトで、キーボード、マウス、スマート カード、オーディオ出力デバイスをリダイレクト対象として選択できません。http://kb.vmware.com/kb/1011600 を参照してください。
- RDP は、コンソール セッションの USB HID またはスマート カード リーダのリダイレクトをサポートしていません。http://kb.vmware.com/kb/1011600 を参照してください。
- Windows Mobile デバイス センターにより、RDP セッションの USB デバイスのリダイレクトが妨げられることがあります。http://kb.vmware.com/kb/1019205 を参照してください。
- 一部の USB HID では、マウス ポインタの位置を更新するように、仮想マシンを構成する必要があります。http://kb.vmware.com/kb/1022076 を参照してください。
- 一部のオーディオ デバイスでは、ポリシー設定またはレジストリ設定を変更する必要がある場合があります。http://kb.vmware.com/kb/1023868 を参照してください。
- ネットワークのレイテンシーが原因で、デバイスの相互作用が低速になったり、アプリケーションがフリーズしているように見えることがあります。これはアプリケーションがローカル デバイスと相互作用するように設計されているからです。非常に大容量の USB ディスク ドライブは、Windows エクスプローラに表示されるまでに数分かかることがあります。
- FAT32 ファイル システムでフォーマットされた USB フラッシュ カードはロードが遅くなります。http://kb.vmware.com/kb/1022836 を参照してください。
- リモート デスクトップまたはアプリケーションに接続する前に、ローカル システムでプロセスまたはサービスがデバイスを開いていた。
- リダイレクトされた USB デバイスは、デスクトップまたはアプリケーションにそのデバイスが使用可能であることが表示されている場合でも、デスクトップまたはアプリケーション セッションを再接続すると、動作が停止します。
- Horizon Administrator で USB リダイレクトが無効になっている。
- ゲスト上で、USB リダイレクト ドライバが存在しないか、無効になっている。

解決方法

- PCoIP が使用可能な場合は、RDP の代わりにプロトコルとして使用します。

- 一時的な切断後に、リダイレクトされたデバイスが使用できないままであるか、動作を停止した場合、デバイスを取り外し、再度接続して、リダイレクトを再試行してください。
- Horizon Administrator で、[ポリシー] - [グローバル ポリシー] の順に移動して、[View ポリシー] で USB アクセスが [許可] に設定されていることを確認します。
- ゲストのログでクラス `ws_vhub` のエントリの有無、クライアントのログでクラス `vmware-view-usbd` のエントリの有無を調べます。

  ユーザーが管理者でない場合、または USB リダイレクト ドライバがインストールされていないか、機能していない場合には、これらのクラスのエントリがログに書き込まれます。これらのログ ファイルの場所については、『Horizon 7 でのリモート デスクトップ機能の構成』の「ログ ファイルを使用してのトラブルシューティングと USB デバイス ID の確認」を参照してください。
- ゲスト上でデバイス マネージャを開き、[ユニバーサル シリアル バス コントローラ] を展開して、VMware View 仮想 USB ホスト コントローラのドライバおよび VMware View 仮想 USB ハブのドライバが表示されない場合はそれらを再インストールし、無効になっている場合は再度有効にします。

デスクトップ プールとアプリケーション プールのポリシーの構成 5

デスクトップ プール、アプリケーション プール、マシン、およびユーザーの動作を制御するポリシーを構成できます。Horizon Administrator を使用して、クライアント セッションのポリシーを設定できます。Active Directory グループ ポリシー設定を使用して、シングルユーザー マシン、RDS ホスト、PCoIP、または VMware Blast に影響を及ぼす、Horizon Agent の動作、Windows 用 Horizon Client の動作、および各種機能の動作を制御できます。

この章には、次のトピックが含まれています。

Horizon Administrator でのポリシーの設定

Horizon Administrator を使用して、クライアント セッションのポリシーを設定できます。

これらのポリシーを設定して、特定のユーザー、特定のデスクトップ プール、またはすべてのクライアント セッション ユーザーに適用できます。特定のユーザーとデスクトップ プールに適用するポリシーは、ユーザー レベルのポリシーおよびデスクトップ プール レベルのポリシーと呼ばれます。すべてのセッションとユーザーに適用するポリシーはグローバル ポリシーと呼ばれます。

ユーザー レベルのポリシーでは、対応するデスクトップ プール レベルのポリシー設定から設定が継承されます。同様に、デスクトップ プール レベルのポリシーでは、対応するグローバル ポリシー設定から設定が継承されます。デスクトップ プール レベルのポリシー設定は、対応するグローバル ポリシー設定より優先されます。ユーザー レベルのポリシー設定は、対応するグローバル ポリシー設定およびデスクトップ プール レベルのポリシー設定より優先されます。

低いレベルのポリシー設定は、対応する高いレベルの設定より、制限を厳しくすることも緩くすることもできます。たとえば、グローバル ポリシーを [拒否] に設定し、対応するデスクトップ プール レベルのポリシーを [許可] に設定することも、この逆に設定することもできます。

注: RDS デスクトップおよびアプリケーション プールでは、グローバル ポリシーのみを使用できます。RDS デスクトップおよびアプリケーション プールに対して、ユーザー レベル ポリシーまたはプール レベル ポリシーを設定することはできません。

グローバル ポリシー設定の構成

すべてのクライアント セッション ユーザーの動作を制御するグローバル ポリシーを構成できます。

前提条件

ポリシーの説明を理解しておきます。 Horizon 7 ポリシーを参照してください。

手順

1 Horizon Administrator で、[ポリシー] - [グローバル ポリシー] の順に選択します。

2 [View ポリシー] ペインで [ポリシーを編集] をクリックします。

3 [OK] をクリックして変更を保存します。

デスクトップ プールのポリシーの構成

特定のデスクトップ プールに影響を与えるデスクトップ レベルのポリシーを構成できます。デスクトップ レベルのポリシー設定は、対応するグローバル ポリシー設定より優先されます。

前提条件

ポリシーの説明を理解しておきます。 Horizon 7 ポリシーを参照してください。

手順

1 Horizon Administrator で、[カタログ] - [デスクトップ プール] の順に選択します。

2 デスクトップ プールの ID をダブルクリックし、[ポリシー] タブをクリックします。

[ポリシー] タブには、現在のポリシー設定が表示されます。設定が対応するグローバル ポリシーから継承されている場合は、[デスクトップ プール ポリシー] 列に [継承] と表示されます。

3 [View ポリシー] ペインで [ポリシーを編集] をクリックします。

4 [OK] をクリックして変更を保存します。

ユーザーのポリシーの構成

特定のユーザーに影響を与えるユーザー レベルのポリシーを構成できます。ユーザー レベルのポリシー設定は、常に、対応するグローバルおよびデスクトップ プール レベルのポリシー設定より優先されます。

前提条件

ポリシーの説明を理解しておきます。 Horizon 7 ポリシーを参照してください。

手順

1 Horizon Administrator で、[カタログ] - [デスクトップ プール] の順に選択します。

2 デスクトップ プールの ID をダブルクリックし、[ポリシー] タブをクリックします。

[ポリシー] タブには、現在のポリシー設定が表示されます。設定が対応するグローバル ポリシーから継承されている場合は、[デスクトップ プール ポリシー] 列に [継承] と表示されます。

3 [ユーザーによる上書き] をクリックし、[ユーザーの追加] をクリックします。

4 ユーザーを見つけるには、[追加] をクリックし、ユーザーの名前または説明を入力して、[検索] をクリックします。

5 リストから 1 名以上のユーザーを選択し、[OK] をクリックし、[次へ] をクリックします。

Add Individual Policy（個別のポリシーの追加） ダイアログ ボックスが表示されます。

6 Horizon ポリシーを構成し、[終了] をクリックして変更を保存します。

Horizon 7 ポリシー

すべてのクライアント セッションに影響を与えるように Horizon 7 ポリシーを構成することも、特定のデスクトップ プールまたはユーザーに影響を与えるように View ポリシーを適用することもできます。

表 5-1. Horizon ポリシー 各 Horizon 7 ポリシー設定について説明します。

表 5-1. Horizon ポリシー

ポリシー	説明
マルチメディア リダイレクト (MMR)	クライアント システムで MMR を有効にするかどうかを指定します。 MMR は Windows Media Foundation のフィルタであり、マルチメディア データをリモート デスクトップ上の特定のコーデックから TCP ソケット経由で直接クライアント システムに転送します。その後、データはクライアント システム上で直接デコードされ、そこで再生されます。 デフォルト値は [拒否] です。 クライアント システムにローカル マルチメディアのデコードを処理する十分なリソースがない場合、設定を [拒否] のままにします。 マルチメディア リダイレクト (MMR) データは、アプリケーション ベースの暗号化なしでネットワークを介して送信され、リダイレクトされる内容によっては機密データが含まれる場合があります。このデータがネットワークで盗まれないようにするには、安全なネットワークで MMR だけを使用してください。
USB Access（USB アクセス）	リモート デスクトップがクライアント システムに接続されている USB デバイスを使用できるかどうかを指定します。 デフォルト値は [許可] です。セキュリティ上の理由のため、外部デバイスを使用できないようにするには、設定を [拒否] に変更します。
PCoIP ハードウェアのアクセラレーション	PCoIP 表示プロトコルのハードウェアのアクセラレーションを有効にするかどうか、および PCoIP ユーザー セッションに割り当てられるアクセラレーションの優先度を指定します。 この設定は、リモート デスクトップをホストする物理コンピュータ上に PCoIP ハードウェアのアクセラレーション デバイスが存在する場合にのみ有効です。 デフォルト値は [許可] で、優先度が [中] です。

スマート ポリシー の使用

スマート ポリシー を使用して、特定のリモート デスクトップでの USB リダイレクト、仮想印刷、クリップボード リダイレクト、クライアント ドライブ リダイレクト、および PCoIP 表示プロトコル機能の動作を制御できます。また、スマート ポリシー を使用して、公開アプリケーションの動作を制御するポリシーを作成できます。

スマート ポリシー により、特定の条件が満たされる場合にのみ有効になるポリシーを作成できます。たとえば、ユーザーが企業のネットワーク以外からリモート デスクトップに接続している場合はクライアント ドライブ リダイレクト機能を無効にするポリシーを設定できます。

スマート ポリシー の要件

スマート ポリシー を使用するには、Horizon 7 環境が特定の要件を満たす必要があります。

- スマート ポリシー で管理するリモート デスクトップに、Horizon Agent 7.0 以降と VMware User Environment Manager 9.0 以降をインストールする必要があります。
- スマート ポリシー で管理するリモート デスクトップに接続するには、ユーザーが Horizon Client 4.0 以降を使用する必要があります。

User Environment Manager のインストール

スマート ポリシーを使用して、リモート デスクトップ機能の動作を制御するには、User Environment Manager 9.0 以降をリモート デスクトップにインストールする必要があります。

User Environment Manager インストーラは、VMware ダウンロード ページからダウンロードできます。User Environment Manager を使用して管理する各リモート デスクトップに VMware UEM FlexEngine クライアント コンポーネントをインストールする必要があります。User Environment Manager 環境を管理する任意のデスクトップに User Environment Manager 管理コンソール コンポーネントをインストールできます。

リンククローン プールの場合、リンク クローンの基本イメージとして使用する親仮想マシンに User Environment Manager をインストールします。RDS デスクトップ プールの場合、RDS デスクトップ セッションを提供する RDS ホストに User Environment Manager をインストールします。

User Environment Manager のシステム要件および完全なインストール手順については、『User Environment Manager 管理者ガイド』ドキュメントを参照してください。

User Environment Manager の構成

リモート デスクトップ機能のスマート ポリシーを作成するには、User Environment Manager を構成してから使用する必要があります。

User Environment Manager を構成するには、『User Environment Manager 管理者ガイド』の構成手順に従います。次の構成手順は、上記ドキュメントの情報を補足します。

- VMware UEM FlexEngine クライアント コンポーネントをリモート デスクトップに構成するとき、FlexEngine のログオン スクリプトとログオフ スクリプトを作成します。ログオン スクリプトには **–HorizonViewMultiSession –r** パラメータを使用し、ログオフ スクリプトには **–HorizonViewMultiSession –s** パラメータを使用します。

  注: リモート デスクトップの他のアプリケーションの起動にログオン スクリプトを使用しないでください。追加のログオン スクリプトにより、リモート デスクトップのログオンが最大 10 分間遅延する可能性があります。

- リモート デスクトップのユーザー グループ ポリシー設定 **Run logon scripts synchronously** を有効にします。この設定は **ユーザーの構成\ポリシー\管理用テンプレート\システム\スクリプト** フォルダにあります。
- リモート デスクトップのコンピュータ グループ ポリシー設定 **Always wait for the network at computer startup and logon** を有効にします。この設定は **コンピュータの構成\管理用テンプレート\システム\ログオン** フォルダにあります。
- Windows 8.1 リモート デスクトップの場合、コンピュータ グループ ポリシー設定 **Configure Logon Script Delay** を無効にします。この設定は **コンピュータの構成\管理用テンプレート\システム\グループ ポリシー** フォルダにあります。
- ユーザーがデスクトップ セッションに再接続すると Horizon のスマート ポリシー設定が更新されるようにするには、User Environment Manager 管理コンソールを使用してトリガされるタスクを作成します。トリガを [セッションの再接続]、アクションを [ユーザー環境の更新] に設定し、更新に [Horizon スマート ポリシー] を選択します。

  注: トリガされるタスクの作成が、ユーザーのリモート デスクトップへのログイン中に行われた場合、デスクトップからログオフして、トリガされるタスクを有効にする必要があります。

Horizon スマート ポリシー設定

User Environment Manager で Horizon スマート ポリシーを作成して、リモート デスクトップ機能の動作を制御します。

表 5-2. Horizon スマート ポリシー設定では、User Environment Manager で Horizon スマート ポリシーを定義する場合に選択できる設定について説明します。

表 5-2. Horizon スマート ポリシー設定

設定	説明
USB リダイレクト	リモート デスクトップで USB リダイレクトを有効にするかどうかを指定します。USB リダイレクト機能により、ユーザーはリモート デスクトップから小型のフラッシュ ドライブ、カメラ、プリンタなどのローカルで接続された USB デバイスを使用できます。
印刷	リモート デスクトップで仮想印刷を有効にするかどうかを指定します。仮想印刷機能により、ユーザーはリモート デスクトップからクライアント コンピュータに接続された仮想プリンタまたは USB プリンタに印刷できます。
クリップボード	クリップボード リダイレクトを許可する方向を決定します。次のいずれかの値を選択できます。 ■ [無効化]。クリップボード リダイレクトは両方の方向で無効になります。 ■ [すべて許可]。クリップボード リダイレクトが有効になります。ユーザーは、クライアント システムからリモート デスクトップ、およびリモート デスクトップからクライアント システムにコピーして貼り付けることができます。 ■ [クライアントからエージェントへのコピーを許可]。ユーザーは、クライアント システムからリモート デスクトップにのみコピーして貼り付けることができます。 ■ [エージェントからクライアントへのコピーを許可]。ユーザーは、リモート デスクトップからクライアント システムにのみコピーして貼り付けることができます。
クライアント ドライブ リダイレクト	リモート デスクトップでクライアント ドライブ リダイレクトを有効にするかどうかと、共有ドライブおよびフォルダを書き込み可能にするかどうかを指定します。次のいずれかの値を選択できます。 ■ [無効化]。リモート デスクトップでクライアント ドライブ リダイレクトが無効になります。 ■ [すべて許可]。クライアント ドライブおよびフォルダは、リモート デスクトップと共有され、読み取り/書き込み可能になります。 ■ [読み取り専用]。クライアント ドライブおよびフォルダは、リモート デスクトップと共有され、読み取り可能になりますが、書き込みはできません。 この設定を構成しない場合、共有ドライブおよびフォルダが書き込み可能になるかどうかは、ローカル レジストリ設定によって決まります。詳細については、レジストリ設定を使用したクライアント ドライブ リダイレクトの構成を参照してください。
帯域幅プロファイル	リモート デスクトップの PCoIP および Blast セッションの帯域幅プロファイルを構成します。[LAN] などの事前定義帯域幅プロファイルを選択できます。事前定義帯域幅プロファイルを選択すると、エージェントはリンク容量よりも高い速度で送信を試行できなくなります。デフォルトのプロファイルを選択した場合、最大帯域幅は毎秒 90,000 kbps になります。 詳細については、帯域幅プロファイル リファレンスを参照してください。
HTML Access ファイル転送	クライアントとエージェント間の HTML ファイルの転送を決定します。

通常、User Environment Manager で構成するリモート デスクトップ機能の Horizon スマート ポリシー設定は、対応するレジストリ キーおよびグループ ポリシー設定よりも優先されます。

帯域幅プロファイル リファレンス

スマート ポリシーでは、帯域幅プロファイルのポリシー設定を使用して、リモート デスクトップ上の PCoIP または Blast セッションの帯域幅プロファイルを構成できます。

表 5-3. 帯域幅プロファイル

帯域幅プロファイル	最大セッション帯域幅 (Kbps)	最小セッション帯域幅 (Kbps)	BTL の有効化	最高初期イメージ品質	最低イメージ品質	最大 FPS	最大オーディオ帯域幅 (Kbps)	イメージ品質のパフォーマンス
高速 LAN	900,000	100	はい	100	50	60	1600	50
LAN	900,000	100	はい	90	50	30	1600	50
専用 WAN	900,000	100	いいえ	80	40	30	500	50
ブロードバンド WAN	5,000	100	いいえ	70	40	20	500	50
低速 WAN	2,000	100	いいえ	70	30	15	200	25
超低速接続	1,000	100	いいえ	70	30	5	90	0

Horizon スマート ポリシー定義への条件の追加

User Environment Manager で Horizon スマート ポリシーを定義する場合、ポリシーを有効にするための必要条件を追加できます。たとえば、ユーザーが企業のネットワーク以外からリモート デスクトップに接続した場合にのみクライアント ドライブのリダイレクト機能を無効にする条件を追加できます。

同じリモート デスクトップ機能に対して複数の条件を追加できます。たとえば、ユーザーが HR グループのメンバーである場合にローカル印刷を有効にする条件や、リモート デスクトップが Win7 プールにある場合にローカル印刷を有効にする条件を追加できます。

User Environment Manager 管理コンソールで条件を追加および編集する方法の詳細については、『User Environment Manager 管理者ガイド』を参照してください。

Horizon Client プロパティ条件の使用

ユーザーがリモート デスクトップに接続するか、再接続すると、Horizon Client がクライアント コンピュータに関する情報を収集し、接続サーバがその情報をリモート デスクトップに送信します。Horizon Client プロパティ条件を Horizon ポリシー定義に追加し、リモート デスクトップが受信する情報に基づいて、ポリシーが有効になるタイミングを制御できます。

注: Horizon Client プロパティ条件は、ユーザーが PCoIP 表示プロトコルまたは VMware Blast 表示プロトコルを使用してリモート デスクトップを起動した場合にのみ有効になります。ユーザーが RDP 表示プロトコルを使用してリモート デスクトップを起動した場合、Horizon Client プロパティ条件は無効になります。

表 5-4. Horizon Client プロパティ条件の事前定義プロパティ では、Horizon Client プロパティ条件を使用するときに [プロパティ] ドロップダウン メニューから選択できる事前定義プロパティについて説明します。各事前定義プロパティは、`ViewClient_` レジストリ キーに対応します。

表 5-4. Horizon Client プロパティ条件の事前定義プロパティ

プロパティ	対応するレジストリ キー	説明
[クライアントの場所]	ViewClient_Broker_GatewayLocation	ユーザーのクライアント システムの場所を指定します。有効な値は以下のとおりです。 ■ Internal - ユーザーが企業のネットワークの内からリモート デスクトップに接続した場合にのみポリシーが有効になります。 ■ External - ユーザーが企業のネットワーク以外からリモート デスクトップに接続した場合にのみポリシーが有効になります。 接続サーバまたはセキュリティ サーバ ホストのゲートウェイの場所の設定については、『View 管理』ドキュメントを参照してください。 Access Point アプライアンスのゲートウェイの場所の設定については、『Unified Access Gateway の導入および設定』ドキュメントを参照してください。
[起動タグ]	ViewClient_Launch_Matched_Tags	1 つ以上のタグを指定します。複数のタグはカンマまたはセミコロンで区切ります。リモート デスクトップまたはアプリケーションを起動できるようにしたタグが指定のタグのいずれかと一致した場合にのみ、ポリシーが有効になります。 タグを接続サーバ インスタンスおよびデスクトップ プールに割り当てる方法については、各セットアップ ガイドを参照してください。
[プール名]	ViewClient_Launch_ID	デスクトップまたはアプリケーション プールの ID を指定します。リモート デスクトップまたはアプリケーションの起動時にユーザーが選択したデスクトップまたはアプリケーション プールの ID が、指定のデスクトップ プールまたはアプリケーションの ID と一致した場合にのみ、ポリシーが有効になります。たとえば、ユーザーが Win7 プールを選択していて、このプロパティが Win7 に設定されている場合、ポリシーが有効になります。 **注:** 同じ RDS ホスト セッションで複数のアプリケーション ツールを起動した場合、この値は、Horizon Client から起動した最初のアプリケーションの ID になります。

[プロパティ] ドロップダウン メニューはテキスト ボックスでもあるため、そのテキスト ボックスに ViewClient_ レジストリ キーを手動で入力できます。レジストリ キーを入力する場合、ViewClient_ プリフィックスを含めないでください。ViewClient_Broker_URL を指定するには、「Broker_URL」と入力します。

リモート デスクトップで Windows レジストリ エディタ (regedit.exe) を使用して、ViewClient_ レジストリ キーを表示できます。Horizon Client は、クライアント コンピュータ情報を、単一ユーザー マシンにデプロイされたリモート デスクトップのシステム レジストリ パス HKEY_CURRENT_USER\Volatile Environment に書き込みます。RDS セッションにデプロイされたリモート デスクトップの場合、Horizon Client は、クライアント コンピュータ情報をシステム レジストリ パス HKEY_CURRENT_USER\Volatile Environment*x* に書き込みます。この *x* は RDS ホストでのセッション ID です。

その他の条件の使用

User Environment Manager 管理コンソールには、多数の条件が用意されています。次の条件は、リモート デスクトップ機能のポリシーを作成する場合に特に便利です。

グループ メンバー	この条件を使用して、ユーザーが特定のグループのメンバーである場合にのみ有効になるようにポリシーを構成できます。
リモート表示プロトコル	この条件を使用して、ユーザーが特定の表示プロトコルを選択した場合にのみ有効になるようにポリシーを構成できます。条件設定には、RDP、PCoIP、および Blast が含まれます。
IP アドレス	この条件を使用して、ユーザーが企業のネットワークの内部または外部から接続した場合にのみ有効になるようにポリシーを構成できます。条件設定を使用して、内部 IP アドレス範囲または外部 IP アドレス範囲を指定します。 **注:** また、Horizon Client プロパティ条件の [クライアントの場所] プロパティを使用することもできます。

使用可能なすべての条件の詳細については、『User Environment Manager 管理者ガイド』ドキュメントを参照してください。

User Environment Manager の Horizon スマート ポリシーの作成

User Environment Manager 管理コンソールを使用して、User Environment Manager の Horizon スマート ポリシーを作成します。Horizon スマート ポリシーを定義するときに、スマート ポリシーを有効にするために必要な条件を追加できます。

前提条件

- User Environment Manager をインストールして構成します。 User Environment Manager のインストールおよび User Environment Manager の構成を参照してください。
- Horizon スマート ポリシー設定について理解しておきます。Horizon スマート ポリシー設定を参照してください。
- Horizon スマート ポリシー定義を追加できる条件について理解しておきます。Horizon スマート ポリシー定義への条件の追加を参照してください。

User Environment Manager 管理コンソールの使用方法の詳細については、『User Environment Manager 管理者ガイド』ドキュメントを参照してください。

手順

1 User Environment Manager 管理コンソールで、[ユーザー環境] タブを選択し、ツリー ビューで [Horizon スマート ポリシー] をクリックします。

  既存の Horizon スマート ポリシー定義がある場合には、[Horizon スマート ポリシー] ペインに表示されます。

2 [Horizon スマート ポリシー] を右クリックし、[Horizon スマート ポリシー定義の作成] を選択して新しいスマート ポリシーを作成します。

[Horizon スマート ポリシー] ダイアログ ボックスが表示されます。

3 [設定] タブを選択し、スマート ポリシー設定を定義します。

a [全般設定] セクションで、[名前] テキスト ボックスにスマート ポリシーの名前を入力します。

たとえば、スマート ポリシーがクライアント ドライブ リダイレクト機能に影響する場合、CDR などのスマート ポリシー名を付けます。

b [Horizon スマート ポリシー設定] セクションで、スマート ポリシーに含めるリモート デスクトップ機能と設定を選択します。

複数のリモート デスクトップ機能を選択できます。

4 （オプション） スマート ポリシーに条件を追加するには、[条件] タブを選択して [追加] をクリックし、条件を選択します。

1 つのスマート ポリシー定義に複数の条件を追加できます。

5 [保存] をクリックしてスマート ポリシーを保存します。

User Environment Manager は、ユーザーがリモート デスクトップに接続または再接続するたびに Horizon スマート ポリシーを処理します。

User Environment Manager は複数のスマート ポリシーをスマート ポリシー名のアルファベット順に処理します。Horizon スマート ポリシーは、[Horizon スマート ポリシー] ペインにアルファベット順に表示されます。スマート ポリシーが競合する場合、最後に処理されたスマート ポリシーが優先されます。たとえば、Sue というユーザーの USB リダイレクトを有効にする Sue というスマート ポリシーがあり、Win7 というデスクトップ プールの USB リダイレクトを無効にする Pool という別のスマート ポリシーがある場合、Sue が Win7 デスクトップ プールのリモート デスクトップに接続したときに USB リダイレクト機能が有効になります。

Active Directory グループ ポリシーの使用

Microsoft Windows グループ ポリシーを使用して、リモート デスクトップの最適化とセキュリティ保護、Horizon 7 コンポーネントの動作の制御、ロケーションベースの印刷の設定を行うことができます。

グループ ポリシーは、Active Directory 環境でのコンピュータとリモート ユーザーの一元化された管理および構成を提供する、Microsoft Windows オペレーティング システムの機能です。

グループ ポリシー設定は、グループ ポリシー オブジェクト (GPO) と呼ばれるエンティティに格納されます。GPO は Active Directory オブジェクトに関連付けられます。Horizon 7 環境のさまざまな領域を制御するために、ドメイン全体にわたるレベルで GPO を Horizon 7 コンポーネントに適用できます。適用後、GPO 設定は指定されたコンポーネントのローカル Windows レジストリに格納されます。

Microsoft Windows グループ ポリシー オブジェクト エディタを使用して、グループ ポリシー設定を管理します。グループ ポリシー オブジェクト エディタは Microsoft 管理コンソール（MMC）スナップインです。MMC は Microsoft グループ ポリシー管理コンソール（GPMC）に含まれています。GPMC のインストールと使用については、Microsoft TechNet Web サイトを参照してください。

リモート デスクトップの OU の作成

Active Directory にリモート デスクトップ固有の組織単位 (OU) を作成します。

リモート デスクトップと同じドメイン内の他の Windows サーバまたはワークステーションにグループ ポリシー設定が適用されないようにするには、Horizon 7 グループ ポリシーの GPO を作成し、それをリモート デスクトップが含まれる OU にリンクします。

OU および GPO の作成については、Microsoft TechNet Web サイトの Microsoft Active Directory のマニュアルを参照してください。

リモート デスクトップのループバック処理の有効化

デフォルトでは、ユーザーのポリシー設定は、Active Directory 内のユーザー オブジェクトに適用される一連の GPO から取得されます。ただし、Horizon 7 環境では、ユーザーがログインするコンピュータに基づいて GPO をユーザーに適用します。

ループバック処理を有効にすると、Active Directory 内の場所には関係なく、一貫した一連のポリシーが、特定のコンピュータにログインするすべてのユーザーに適用されます。

ループバック処理を有効にする方法については、Microsoft Active Directory のマニュアルを参照してください。

注: ループバック処理は、Horizon 7 で GPO を処理する方法の一つにすぎません。別の方法を実装する必要がある場合もあります。

Horizon 7 グループ ポリシー管理用テンプレート ファイルの使用

Horizon 7 には、コンポーネント固有のグループ ポリシー管理用 ADMX テンプレート ファイルがいくつか含まれています。ADMX テンプレート ファイル内のポリシー設定を Active Directory 内の新しい GPO または既存の GPO に追加することによって、リモート デスクトップとアプリケーションを最適化し、セキュリティ保護することができます。

Horizon 7 のグループ ポリシー設定を提供する ADMX ファイルはすべて、`VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` という `.zip` バンドル ファイル内にあります。*x.x.x* はバージョン、*yyyyyyy* はビルド番号です。このファイルは、https://my.vmware.com/web/vmware/downloads の VMware ダウンロード サイトからダウンロードできます。[Desktop & End-User Computing (デスクトップおよびエンドユーザー コンピューティング)] で VMware Horizon 7 のダウンロードを選択します。これには `.zip` バンドル ファイルが含まれます。

Horizon 7 ADMX テンプレート ファイルには、コンピュータの設定とユーザーの設定の両方のグループ ポリシーが含まれます。

- コンピュータの構成ポリシーは、だれがデスクトップに接続するかにはかかわらず、すべてのリモート デスクトップに適用されるポリシーを設定します。
- ユーザーの構成ポリシーは、ユーザーが接続するリモート デスクトップやアプリケーションにはかかわらず、すべてのユーザーに適用されるポリシーを構成します。ユーザーの構成ポリシーは、対応するコンピュータの構成ポリシーより優先されます。

Microsoft Windows は、デスクトップの起動時とユーザーのログイン時にポリシーを適用します。

Horizon 7 ADMX テンプレート ファイル

Horizon 7 ADMX テンプレート ファイルでは、Horizon 7 コンポーネントを制御および最適化できるグループ ポリシー設定が提供されます。

表 5-5. Horizon ADMX テンプレート ファイル

テンプレート名	テンプレート ファイル	説明
VMware View Agent の構成	vdm_agent.admx	Horizon Agent の認証および環境コンポーネントに関するポリシー設定が含まれています。
VMware Horizon Client の設定	vdm_client.admx	Horizon Client for Windows に関するポリシー設定が含まれています。 接続サーバ ホスト ドメインの外部から接続するクライアントは、Horizon Client に適用されるポリシーの影響を受けません。 『VMware Horizon Client for Windows のインストールとセットアップ ガイド』ドキュメントを参照してください。
VMware Horizon URL リダイレクト	urlRedirection.admx	URL コンテンツ リダイレクト機能に関するポリシー設定が含まれています。このテンプレートをリモート デスクトップ プールまたはアプリケーション プールの GPO に追加すると、リモート デスクトップまたはアプリケーション内でクリックされた特定の URL リンクを Windows ベースのクライアントにリダイレクトし、クライアント側のブラウザで開くことができます。 このテンプレートをクライアント側の GPO に追加すると、ユーザーが Windows ベースのクライアント システムで特定の URL リンクをクリックしたときに、リモート デスクトップまたはアプリケーションで URL を開くことができます。 3 章 URL コンテンツ リダイレクトの構成および『VMware Horizon Client for Windows のインストールとセットアップ ガイド』ドキュメントを参照してください。
VMware View Server の構成	vdm_server.admx	接続サーバに関するポリシー設定が含まれています。 『View 管理』を参照してください。
VMware View の一般的な設定	vdm_common.admx	すべての Horizon コンポーネントに共通のポリシー設定が含まれています。 『View 管理』を参照してください。
PCoIP セッション変数	pcoip.admx	PCoIP 表示プロトコルに関するポリシー設定が含まれています。
PCoIP クライアントのセッション変数	pcoip.client.admx	Horizon Client for Windows に影響を与える PCoIP 表示プロトコルに関するポリシー設定が含まれています。 『VMware Horizon Client for Windows のインストールとセットアップ ガイド』ドキュメントを参照してください。
個人設定管理	ViewPM.admx	Horizon Persona Management に関するポリシー設定が含まれています。 『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントを参照してください。

テンプレート名	テンプレート ファイル	説明
リモート デスクトップ サービス	vmware_rdsh_server.admx	リモート デスクトップ サービスに関するポリシー設定が含まれています。 リモート デスクトップ サービス グループ ポリシーの使用を参照してください。
View の RTAV 構成	vdm_agent_rtav.admx	リアルタイム オーディオ ビデオ機能で使用される Web カメラに関するポリシー設定が含まれています。 リアルタイム オーディオ ビデオ グループ ポリシ設定 を参照してください。
スキャナ リダイレクト	vdm_agent_scanner.admx	公開されたデスクトップおよびアプリケーションで使用するためにリダイレクトされるスキャン デバイスに関するポリシー設定が含まれています。 スキャナ リダイレクトのグループ ポリシー設定を参照してください。
シリアル COM	vdm_agent_serialport.admx	仮想デスクトップで使用するためにリダイレクトされるシリアル（COM）ポートに関するポリシー設定が含まれています。 シリアル ポート リダイレクトのグループ ポリシー設定を参照してください。
VMware Horizon プリンタ リダイレクト	vdm_agent_printing.admx	リダイレクトされたプリンタのフィルタリングに関するポリシー設定が含まれます。 仮想印刷でプリンタのフィルタリングを参照してください。

Active Directory への ADMX テンプレート ファイルの追加

Horizon 7 ADMX ファイルの特定のリモート デスクトップ機能のポリシー設定を、Active Directory のグループ ポリシー オブジェクト (GPO) に追加できます。

前提条件

- ポリシーを適用しているリモート デスクトップ機能のセットアップ オプションが、仮想マシン デスクトップと RDS ホストにインストールされていることを確認します。リモート デスクトップ機能がインストールされていないと、グループ ポリシー設定は有効になりません。Horizon Agent のインストールについては、各セットアップ ガイドを参照してください。
- グループポリシー設定を適用するリモート デスクトップ機能に GPO を作成し、仮想デスクトップ マシンまたは RDS ホストを含む組織単位 (OU) に GPO をリンクします。
- Active Directory に追加する ADMX テンプレート ファイルの名前を確認します。 Horizon 7 ADMX テンプレート ファイルを参照してください。
- Active Directory サーバでグループ ポリシー管理機能が使用できることを確認します。

手順

1 Horizon 7 GPO Bundle `.zip` ファイルを https://my.vmware.com/web/vmware/downloads の VMware ダウンロード サイトからダウンロードします。

[Desktop & End-User Computing（デスクトップおよびエンドユーザー コンピューティング）] で VMware Horizon 7 のダウンロードを選択します。これには GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` で、*x.x.x* はバージョン、*yyyyyyy* はビルド番号を表します。Horizon 7 のグループ ポリシー設定用の ADMX ファイルはすべて、このファイルで提供されています。

2 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` ファイルを解凍して、ADMX ファイルを Active Directory サーバにコピーします。

a `.admx` ファイルと `en-US` フォルダを Active Directory サーバの `%systemroot%\PolicyDefinitions` フォルダにコピーします。

b 言語リソース (`.adml`) を Active Directory サーバの `%systemroot%\PolicyDefinitions\` 内の適切なサブフォルダにコピーします。

3 Active Directory サーバで、グループ ポリシー管理エディタを開き、インストール後にエディタに表示される場所となるテンプレート ファイルのパスを入力します。

次のステップ

グループ ポリシー設定を構成します。

VMware View Agent 構成 ADMX テンプレートの設定

VMware View Agent 構成 ADMX テンプレート ファイル (`vdm_agent.admx`) には、Horizon Agent の認証および環境コンポーネントに関するポリシー設定が含まれています。

ADMX ファイルは、`VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` という `.zip` バンドル ファイル内にあり、VMware ダウンロードサイト（https://my.vmware.com/web/vmware/downloads）からダウンロードできます。[Desktop & End-User Computing（デスクトップおよびエンドユーザー コンピューティング）] で VMware Horizon 7 のダウンロードを選択します。これには `.zip` バンドル ファイルが含まれます。

次の表で、USB デバイスで使用されているポリシー設定以外に、VMware View Agent の構成 ADMX テンプレート ファイル内にあるポリシー設定について説明します。テンプレートには、コンピュータの構成とユーザーの構成の両方の設定が含まれています。ユーザーの構成設定は、対応するコンピュータの構成設定より優先されます。

表 5-6. VMware View Agent 構成テンプレートの設定

設定	コンピュータ	ユーザー	プロパティ
AllowDirectRDP	X		Horizon Client デバイス以外のクライアントが RDP を使用してリモート デスクトップに直接接続できるかどうかを指定します。この設定が無効になっていると、エージェントでは、Horizon Client 経由での Horizon によって管理される接続のみが許可されます。 Horizon Clientfor Mac からリモート デスクトップに接続する場合は、AllowDirectRDP の設定を無効にしないでください。この設定を無効にすると、Access is denied(アクセスが拒否されました) エラーが発生して接続に失敗します。 デフォルトの設定の場合、ユーザーは、リモート デスクトップ セッションにログイン中に RDP を使用して仮想マシンに接続できます。RDP 接続によってリモート デスクトップ セッションが終了し、ユーザーの保存されていないデータや設定は失われます。ユーザーは、外部の RDP 接続が閉じられるまで、デスクトップにログインできません。この状況を回避するには、AllowDirectRDP 設定を無効にします。 **重要:** Windows リモート デスクトップ サービスが各デスクトップのゲスト OS で実行されている必要があります。この設定を使用して、ユーザーが自分のデスクトップに直接 RDP 接続を作成することを不可にできます。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 デフォルトでは、この設定は有効になっています。
AllowSingleSignon	X		シングル サインオン (SSO) を使用して、ユーザーをデスクトップおよびアプリケーションに接続するかどうかを決定します。この設定が有効になっていると、ユーザーはサーバにログインするときに、自分の認証情報を 1 回入力するだけで済みます。この設定を無効にすると、ユーザーはリモート接続の確立時に再認証する必要があります。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 デフォルトでは、この設定は有効になっています。
CommandsToRunOnConnect	X		セッションに初めて接続するときに実行されるコマンドまたはコマンド スクリプトのリストを指定します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 詳細については、Horizon デスクトップでのコマンドの実行を参照してください。
CommandsToRunOnDisconnect	X		セッションが切断されたときに実行されるコマンドまたはコマンド スクリプトのリストを指定します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 詳細については、Horizon デスクトップでのコマンドの実行を参照してください。

設定	コンピュータ	ユーザー	プロパティ
CommandsToRunOnReconnect	X		セッションが切断された後、再接続されるときに実行されるコマンドまたはコマンド スクリプトのリストを指定します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 詳細については、Horizon デスクトップでのコマンドの実行を参照してください。
ConnectionTicketTimeout	X		Horizon 接続チケットが有効な時間（秒）を指定します。 Horizon Client デバイスは、エージェントに接続するときに、検証とシングル サインオンのために接続チケットを使用します。セキュリティ上の理由から、接続チケットは限られた期間のみ有効です。ユーザーがリモート デスクトップに接続するときは、接続チケットのタイムアウト期間内に認証を行う必要があります。そうでないとセッションがタイムアウトになります。この設定が構成されていない場合、デフォルトのタイムアウト期間は 900 秒になります。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。
CredentialFilterExceptions	X		エージェントの CredentialFilter のロードを許可されていない実行可能ファイルを指定します。ファイル名にパスまたはサフィックスを含めることはできません。複数のファイル名を区切るにはセミコロンを使用します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。
Disable Time Zone Synchronization	X	X	Horizon デスクトップのタイム ゾーンを接続されたクライアントのタイムゾーンと同期するかどうかを指定します。設定を有効にすると、Horizon Client の構成ポリシーの **Disable time zone forwarding** 設定が無効に設定されていない場合にのみ適用されます。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 デフォルトでは、この設定は無効になっています。
DPI Synchronization	X	X	リモート セッションに関するシステム全体の DPI 設定を調整します。この設定が有効にされていたり、構成されていなかったりすると、リモート セッションに関するシステム全体の DPI 設定は、クライアント オペレーティング システムの対応する DPI 設定と一致するように設定されます。この設定が無効になっていると、リモート セッションに関するシステム全体の DPI 設定は決して変更されません。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 デフォルトでは、この設定は構成されていません。 **注:** この設定は、Horizon Client 4.2 以降がインストールされている Windows クライアントにのみ適用されます。

設定	コンピュータ	ユーザー	プロパティ
Enable multi-media acceleration	X		リモート デスクトップでマルチメディア リダイレクト (MMR) を有効にするかどうかを指定します。 MMR は、TCP ソケットを介してリモート システムの固有のコーデックからマルチメディア データをクライアントに直接転送する Windows Media Foundation フィルタです。その後、データはクライアント上で直接デコードされ、そこで再生されます。クライアントがローカル マルチメディア デコーディングを処理するために十分なリソースを持たない場合は、MMR を無効にできます。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 デフォルトでは、この設定は有効になっています。
Force MMR to use software overlay	X		MMR は、パフォーマンス向上のため、ハードウェア オーバーレイを使用してビデオの再生を試みます。複数のディスプレイを使用している場合、ハードウェア オーバーレイは 1 つのディプレイ（プライマリ ディスプレイまたは WMP が開始しているディスプレイ）でのみ有効になります。WMP を別のディスプレイにドラッグすると、ビデオは黒色の四角形で表示されます。すべてのディスプレイで動作するソフトウェア オーバーレイを MMR で強制的に使用する場合には、このオプションを使用します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 デフォルトでは、この設定は構成されていません。
Single sign-on retry timeout	X		シングル サインオンを再試行するまでの時間をミリ秒単位で指定します。シングル サインオンの再試行を無効にするには、値を 0 に設定します。デフォルト値は 5,000 ミリ秒です。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 デフォルトでは、この設定は構成されていません。
ShowDiskActivityIcon	X		この設定は、このリリースではサポートされていません。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。
Toggle Display Settings Control	X		クライアント セッションで PCoIP 表示プロトコルを使用するときに、[Display (画面)] コントロール パネルの [Settings (設定)] タブを無効にするかどうかを指定します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 デフォルトでは、この設定は有効になっています。
UnAuthenticatedAccessEnabled			非認証アクセス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、認証されていないユーザーが、Active Directory の認証情報を要求せずに Horizon Client から公開アプリケーションにアクセスできます。この設定を無効にすると、認証されていないユーザーは、Active Directory の認証情報を要求せずに Horizon Client から公開アプリケーションにアクセスすることはできません。 この設定を有効にするには、RDS ホストを再起動する必要があります。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent の構成] フォルダにあります。 デフォルトでは、この設定は有効になっています。

設定	コンピュータ	ユーザー	プロパティ
Send updates for empty or offscreen windows	X		クライアントが空またはオフスクリーン ウィンドウの更新を受信するかどうかを指定します。この設定を無効にすると、2x2 ピクセルより小さいウィンドウまたは完全にオフスクリーンの位置にあるウィンドウの情報がクライアントに送信されません。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Unity Touch およびホスト型アプリケーション] フォルダにあります。 デフォルトでは、この設定は無効になっています。
Enable Unity Touch	X		リモート デスクトップで Unity Touch 機能を有効にするかどうかを決定します。Unity Touch は、Horizon でリモート アプリケーションの配信をサポートし、モバイル デバイス ユーザーが Unity Touch サイドバーのアプリケーションにアクセスできるようにします。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Unity Touch およびホスト型アプリケーション] フォルダにあります。 デフォルトでは、この設定は有効になっています。
Enable system tray redirection for Hosted Apps	X		ユーザーがリモート アプリケーションを実行しているときに、システム トレイのリダイレクトを有効にするかどうかを決定します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Unity Touch およびホスト型アプリケーション] フォルダにあります。 デフォルトでは、この設定は有効になっています。
Enable user profile customization for Hosted Apps	X	X	リモート アプリケーションの使用時にユーザー プロファイルをカスタマイズ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 プロファイルが生成され、Windows のテーマがカスタマイズされます。また、スタートアップ アプリケーションが登録されます。 このコンピュータの構成は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Unity Touch およびホスト型アプリケーション] フォルダにあります。このユーザーの構成は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent のセキュリティ] - [Unity Touch およびホスト型アプリケーション] フォルダにあります。 デフォルトでは、この設定は無効になっています。
Limit usage of Windows hooks	X		リモート アプリケーションまたは Unity Touch の使用時に大半のフックを無効にします。この設定は、OS レベルのフックを設定したときに互換性の問題が発生するアプリケーションに使用します。たとえば、この設定を有効にすると、大半の Windows Active Accessibility とインプロセス フックが使用できなくなります。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Unity Touch およびホスト型アプリケーション] フォルダにあります。 この設定は、デフォルトで無効になっています。すべての優先フックが使用されます。

設定	コンピュータ	ユーザー	プロパティ
Accept SSL encrypted framework channel		X	SSL 暗号化フレームワーク チャネルを有効にします。次のオプションを使用できます。 ■ [無効化] - SSL を無効にします。 ■ [有効化] - SSL を有効にします。SSL を使用せずにレガシー クライアントとの接続を許可します。 ■ [強制] - SSL を有効にします。レガシー クライアントとの接続を拒否します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Agent のセキュリティ] フォルダにあります。 デフォルトでは、この設定は構成されていません。デフォルト値は [有効化] です。
Default Proxy Server	X		プロキシ サーバのデフォルトの Internet Explorer 接続設定。プロキシ サーバを指定するには、[インターネット オプション] > [ローカル エリア ネットワーク (LAN) の設定] の順に移動します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [VMware クライアント IP アドレスの透過性] フォルダにあります。 デフォルトでは、この設定は有効ではありません。
Enable	X		VMware クライアント IP アドレスの透過性を有効にします。Internet Explorer へのリモート接続で、リモート デスクトップ マシンの IP アドレスの代わりにクライアントの IP アドレスを使用します。この設定は、次回のログイン時に有効になります。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [VMware クライアント IP アドレスの透過性] フォルダにあります。 Horizon Agent インストーラで [VMware クライアント IP アドレスの透過性] カスタム セットアップ オプションが選択されている場合、この設定はデフォルトで有効になります。
Default auto detect proxy	X		Internet Explorer のデフォルトの接続設定。[設定を自動的に検出する] を有効にするには、[インターネット オプション] > [ローカル エリア ネットワーク (LAN) の設定] の順に移動します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [VMware クライアント IP アドレスの透過性] フォルダにあります。 デフォルトでは、この設定は有効ではありません。

設定	コンピュータ	ユーザー	プロパティ
Set proxy for Java applet	X		Java アプレットのプロキシを設定します。次のオプションを使用できます。 ■ [Use client ip transparency for Java proxy] (Java プロキシにクライアント IP 透過性を使用) - Java アプレットのリモート接続に、リモート デスクトップ マシンの IP アドレスではなく、クライアントの IP アドレスを使用します。 ■ [Use direct connection for Java proxy] (Java プロキシに直接接続を使用) - Java アプレットのブラウザ設定を回避し、直接接続を使用します。 ■ [Use the default value for Java proxy] (Java プロキシにデフォルト値を使用) - 元の Java プロキシ設定を復元します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [VMware クライアント IP アドレスの透過性] フォルダにあります。 デフォルトでは、この設定は有効ではありません。
Enable flash multi-media redirection	X		エージェントで Flash リダイレクトを有効にするかどうかを指定します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [VMware FlashMMR] フォルダにあります。
Minimum rect size to enable FlashMMR	X		Flash リダイレクトを有効にする長方形の最小サイズを指定します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [VMware FlashMMR] フォルダにあります。 デフォルトの幅は 320 ピクセル、デフォルトの高さは 200 ピクセルです。
Definition for FlashMMR url list usage		X	URL での Flash リダイレクトの使用を有効または無効にするホワイト リスト ルールまたはブラック リスト ルールを定義します。 [FlashMMR URL リストの使用方法の定義] ドロップダウン メニューから[ホワイト リストを有効にする] を選択すると、URL リストにある URL でのみ Flash リダイレクトの使用が有効になります。 [FlashMMR URL リストの使用方法の定義] ドロップダウン メニューから[ブラック リストを有効にする] を選択すると、URL リストにある URL で Flash リダイレクトは使用できません。 URL リストは、**Hosts Url list to enable FlashMMR** グループ ポリシー設定で指定します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [VMware FlashMMR] フォルダにあります。 この設定には、デフォルトでホワイト リストが指定されています。
Hosts Url list to enable FlashMMR		X	**Definition for FlashMMR url list usage** グループ ポリシーの設定に基づいて Flash リダイレクトの使用を有効または無効にする URL リストを指定します。 [http://] または [https://] を必ず入れてください。正規表現を使用できます。たとえば、 **https://*.google.com** や **http://www.cnn.com** を指定できます。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [VMware FlashMMR] フォルダにあります。

注: `Connect using DNS Name` の設定は、Horizon 6 バージョン 6.1 リリースで削除されました。Horizon 7 LDAP 属性、[pae-PreferDNS] を設定して Horizon 接続サーバが、デスクトップ マシンと RDS ホストのアドレスをクライアントとゲートウェイに送信するときは、DNS 名に環境設定を与えるようにすることができます。『View のインストール』ドキュメントの「Horizon 接続サーバがアドレス情報を返す場合、DNS 名に環境設定を与える」を参照してください。

Horizon Agent の USB 設定

Horizon Agent の構成 ADMX テンプレートの USB 設定を参照してください。

リモート デスクトップに送信されるクライアント システム情報

ユーザーがリモート デスクトップに接続するか、再接続すると、Horizon Client がクライアント システムに関する情報を収集し、接続サーバがその情報をリモート デスクトップに送信します。

Horizon Agent は、クライアント コンピュータ情報を、単一ユーザー マシンにデプロイされたリモート デスクトップのシステム レジストリ パス `HKCU\Volatile Environment` に書き込みます。RDS セッションにデプロイされたリモート デスクトップの場合、Horizon Agent は、クライアント コンピュータ情報をシステム レジストリ パス `HKCU\Volatile Environment\`*x* に書き込みます。この *x* は RDS ホストでのセッション ID です。

Horizon Client がリモート デスクトップ セッション内で実行されている場合、仮想マシン情報ではなくて物理クライアントの情報がリモート デスクトップに送信されます。たとえば、ユーザーがクライアント システムをリモート デスクトップに接続し、リモート デスクトップ内で Horizon Client を起動して別のリモート デスクトップに接続する場合、物理クライアント システムの IP アドレスはこのセカンド リモート デスクトップに送信されます。この機能は、ネスト モードまたはダブルホップ シナリオと呼ばれます。Horizon Client は、1 に設定されている `ViewClient_Nested_Passthrough` をクライアント システム情報と一緒に送信し、ネスト モード情報を送信していることを示します。

注: Horizon Client 4.1 では、最初のプロトコル接続の時に、クライアント システム情報がセカンドホップ デスクトップに渡されます。Horizon Client 4.2 以降では、ファーストホップ プロトコルの接続が切断して再接続すると、クライアント システム情報も更新されます。

Horizon Agent の `CommandsToRunOnConnect`、`CommandsToRunOnReconnect` および `CommandsToRunOnDisconnect` グループ ポリシー設定にコマンドを追加し、ユーザーがデスクトップに接続および再接続するときに、この情報をシステム レジストリから読み取るコマンドまたはコマンド スクリプトを実行することができます。詳細については、Horizon デスクトップでのコマンドの実行を参照してください。

表 5-7. クライアント システム情報に、クライアント システム情報を含むレジストリ キーについて説明し、それらをサポートするデスクトップおよびクライアント システムのタイプを一覧表示します。[サポートされるネスト モード] 列に [はい] が表示される場合、物理クライアントの情報（仮想マシンの情報ではなく）がセカンドホップ デスクトップに送信されることを示します。

表 5-7. クライアント システム情報

レジストリ キー	説明	サポートされるネスト モード	サポートされるデスクトップ	サポートされるクライアント システム
ViewClient_IP_Address	クライアント システムの IP アドレス。	はい	VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_MAC_Address	クライアント システムの MAC アドレス。	はい	VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android
ViewClient_Machine_Name	クライアント システムのマシン名。	はい	VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Machine_Domain	クライアント システムのドメイン。	はい	VDI（シングルユーザー マシン） RDS	Windows、Windows ストア
ViewClient_LoggedOn_Username	クライアント システムへのログインに使用したユーザー名。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac
ViewClient_LoggedOn_Domainname	クライアント システムへのログインに使用したドメイン名。		VDI（シングルユーザー マシン） RDS	Windows、Windows ストア Linux クライアントまたは Mac クライアントの場合、ViewClient_Machine_Domain を参照してください。.ViewClient_LoggedOn_Domainname は、Linux および Mac アカウントが Windows ドメインにバインドされていないため、Linux クライアントまたは Mac クライアントでは指定されません。
ViewClient_Type	クライアント システムのシン クライアント名またはオペレーティング システムの種類。	はい	VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Broker_DNS_Name	View 接続サーバ インスタンスの DNS 名。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Broker_URL	View 接続サーバ インスタンスの URL。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。

レジストリ キー	説明	サポートされるネスト モード	サポートされるデスクトップ	サポートされるクライアント システム
ViewClient_Broker_Tunneled	View 接続サーバのトンネル接続のステータス。true（有効）または false（無効）です。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Broker_Tunnel_URL	View 接続サーバのトンネル接続が有効になっている場合のトンネル接続の URL。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Broker_Remote_IP_Address	View 接続サーバ インスタンスから見えるクライアント システムの IP アドレス。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_TZID	Olson タイム ゾーン ID。 タイム ゾーンの同期を無効にするには、Horizon Agent の Disable Time Zone Synchronization グループ ポリシー設定を有効にします。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS
ViewClient_Windows_Timezone	GMT 標準時間。 タイム ゾーンの同期を無効にするには、Horizon Agent の Disable Time Zone Synchronization グループ ポリシー設定を有効にします。		VDI（シングルユーザー マシン） RDS	Windows、Windows ストア
ViewClient_Broker_DomainName	View 接続サーバの認証に使用されるドメイン名。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Broker_UserName	View 接続サーバの認証に使用されるユーザー名。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Client_ID	ライセンス キーへのリンクとして使用される Unique Client HardwareId を指定します。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Displays.Number	クライアントで使用されているモニターの数を指定します。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Displays.Topology	クライアントのディスプレイの配置、解像度、寸法を指定します。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア

レジストリ キー	説明	サポートされるネスト モード	サポートされるデスクトップ	サポートされるクライアント システム
ViewClient_Keyboard.Type	クライアントで使用されているキーボードの種類を指定します。例：日本語、韓国語。		VDI（シングルユーザー マシン） RDS	Windows
ViewClient_Launch_SessionType	セッション タイプを指定します。指定できるタイプはデスクトップまたはアプリケーションです。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Mouse.Identifier	マウスの種類を指定します。		VDI（シングルユーザー マシン） RDS	Windows
ViewClient_Mouse.NumButtons	マウスでサポートするボタンの数を指定します。		VDI（シングルユーザー マシン） RDS	Windows
ViewClient_Mouse.SampleRate	PS/2 マウスからの入力のサンプリング レートを 1 秒あたりのレポート数で指定します。		VDI（シングルユーザー マシン） RDS	Windows
ViewClient_Protocol	使用されているプロトコルを指定します。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Language	オペレーティング システムの言語を指定します。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Launch_Matched_Tags	1 つ以上のタグを指定します。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Launch_ID	デスクトップまたはアプリケーション プールの一意の ID を指定します。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Broker_Farm_ID	RDS ホストのデスクトップまたはアプリケーション プールのファーム ID を指定します。		RDS	Windows、Linux、Mac、Android、iOS、Windows ストア

注: 表 5-7. クライアント システム情報にある ViewClient_LoggedOn_Username および ViewClient_LoggedOn_Domainname の定義は、Horizon Client 2.2 for Windows 以降のリリースに適用されます。

Horizon Client5.4 for Windows 以前のリリースでは、Horizon Client で入力されたユーザー名が ViewClient_LoggedOn_Username により送信され、Horizon Client で入力されたドメイン名が ViewClient_LoggedOn_Domainname により送信されます。

Horizon Client2.2 for Windows は Horizon Client 5.4 for Windows より後のリリースです。Horizon Client2.2 から、Windows 版のリリース番号は、他のオペレーティング システムおよびデバイスの Horizon Client リリースと整合性が取れています。

Horizon デスクトップでのコマンドの実行

Horizon Agent CommandsToRunOnConnect、CommandsToRunOnReconnect、および CommandsToRunOnDisconnect グループ ポリシー設定を使用して、ユーザーが接続、再接続、切断するときに Horizon デスクトップ上でコマンドおよびコマンド スクリプトを実行できます。

コマンドまたはコマンド スクリプトを実行するには、コマンド名またはスクリプトのファイル パスを、グループ ポリシー設定のコマンド リストに追加します。例：

```
date
```

```
C:\Scripts\myscript.cmd
```

コンソール アクセスが必要なスクリプトを実行するには、先頭に –C または –c オプションと領域を付加します。例：

```
–c C:\Scripts\Cli_clip.cmd
```

```
–C e:\procexp.exe
```

サポートされているファイルのタイプには、.CMD、.BAT、.EXE が含まれます。.VBS ファイルは、cscript.exe または wscript.exe で解析されない限り実行されません。例：

```
–C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

文字列の合計の長さ（–C または –c オプションを含む）が 260 文字を超えないようにする必要があります。

VMware Virtualization Pack for Skype for Business ポリシー設定

VMware View Agent 設定 ADMX テンプレート ファイル (vdm_agent.admx) には、VMware Virtualization Pack for Skype for Business に関連するポリシー設定が含まれています。

これらの設定は、グループ ポリシー管理エディタの [コンピュータの構成] - [管理用テンプレート] - [VMware View Agent の構成] - [VMware Virtualization Pack for Skype for Business] フォルダにあります。

表 5-8. Virtualization Pack for Skype for Business ポリシー設定

設定	説明
Show Icon	Virtualization Pack for Skype for Business のアイコンを表示します。このポリシーは、デフォルトで有効になっています。Virtualization Pack for Skype for Business の「アイコンの表示」ポリシーが無効になっている場合、アイコンは表示されません。無効にした場合、通話の統計情報やメッセージは表示できません。
Show Messages	Virtualization Pack for Skype for Business のメッセージを表示します。このポリシーは、デフォルトで有効になっています。Virtualization Pack for Skype for Business の「アイコンの表示」ポリシーまたは「メッセージの表示」ポリシーが無効になっている場合、メッセージは表示されません。

PCoIP ポリシー設定

PCoIP ADMX テンプレート ファイルには、PCoIP 表示プロトコルに関連するポリシー設定が含まれています。ADMX テンプレート ファイルには名前が付けられています (`pcoip.admx`)。これらの設定をデフォルト値（管理者による上書きが可能）にすることも、上書きできない値にすることもできます。

ADMX ファイルは、`VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` という `.zip` バンドル ファイル内にあり、VMware ダウンロードサイト（https://my.vmware.com/web/vmware/downloads）からダウンロードできます。[Desktop & End-User Computing（デスクトップおよびエンドユーザー コンピューティング）] で VMware Horizon 7 のダウンロードを選択します。これには `.zip` バンドル ファイルが含まれます。

PCoIP セッション変数 ADMX テンプレート ファイルには、次の 2 つのサブカテゴリがあります。

上書き可能な管理者デフォルト
PCoIP ポリシー設定のデフォルト値を指定します。管理者はこれらの設定を上書きできます。これらの設定は、レジストリ キーの値を `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults` に書き込みます。これらの設定はすべて、グループ ポリシー管理エディタの [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [PCoIP セッション変数] - [上書き可能な管理者デフォルト] フォルダにあります。

上書き不可の管理者設定
上書き可能な管理者デフォルトと同じ設定を含みますが、管理者はこれらの設定を上書きできません。これらの設定は、レジストリ キーの値を `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin` に書き込みます。これらの設定はすべて、グループ ポリシー管理エディタの [ユーザーの構成] - [ポリシー] - [管理用テンプレート] - [PCoIP セッション変数] - [上書き不可の管理者設定] フォルダにあります。

テンプレートには、コンピュータの構成とユーザーの構成の両方の設定が含まれています。

ポリシー以外のレジストリ キー

ローカル マシン設定を適用する必要があり、HKLM\Software\Policies\Teradici 下に格納できない場合は、ローカル マシン設定を HKLM\Software\Teradici 内のレジストリ キーに格納できます。HKLM\Software\Policies\Teradici にあるのと同じレジストリ キーを HKLM\Software\Teradici に入れることができます。両方の場所に同じレジストリ キーが存在する場合は、HKLM\Software\Policies\Teradici 内の設定がローカル マシン値に優先されます。

PCoIP の一般的な設定

PCoIP ADMX テンプレート ファイルには、PCoIP イメージの品質、USB デバイス、ネットワーク ポートなどの一般的な設定を行うグループ ポリシー設定が含まれます。

これらの設定はすべて、グループ ポリシー管理エディタの [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [PCoIP セッション変数] - [上書き可能な管理者デフォルト] フォルダにあります。

これらの設定はすべて、グループ ポリシー管理エディタの [ユーザーの構成] - [ポリシー] - [管理用テンプレート] - [PCoIP セッション変数] - [上書き不可の管理者設定] フォルダにあります。

表 5-9. PCoIP の一般的なポリシー設定

設定	説明
Configure PCoIP event log cleanup by size in MB	サイズ (MB) に基づく PCoIP イベント ログ クリーンアップの構成を有効にします。 このポリシーが構成されている場合は、クリーンアップが実行される前のログ ファイルの最大サイズが設定で管理されます。*m* がゼロ以外に設定されている場合は、*m* MB より大きいファイルが自動的かつサイレントに削除されます。0 に設定されている場合は、サイズに基づくファイルのクリーンアップは行われません。 このポリシーが無効になっているか設定されていない場合は、サイズに基づくイベント ログ クリーンアップのデフォルト値は 100 MB です。 ログ ファイルのクリーンアップは、セッション起動時に 1 回実行されます。設定の変更は、次のセッションまで適用されません。
Configure PCoIP event log cleanup by time in days	時間（日数）に基づく PCoIP イベント ログ クリーンアップの構成を有効にします。 このポリシーが構成されている場合は、ログ ファイルのクリーンアップが実行されるまでの日数が管理されます。*n* がゼロ以外に設定されている場合は、日数が *n* 日より長いログ ファイルが自動的かつサイレントに削除されます。0 に設定されている場合は、時間に基づくファイルのクリーンアップは行われません。 このポリシーが無効になっているか設定されていない場合は、イベント ログ クリーンアップのデフォルトの日数は 7 日です。 ログ ファイルのクリーンアップは、セッション起動時に 1 回実行されます。設定の変更は、次のセッションまで適用されません。
Configure PCoIP event log verbosity	PCoIP イベント ログの冗長性を設定します。この値は、0（最も簡素）から 3（最も詳細）です。 この設定を有効にすると、冗長性のレベルを 0 から 3 に設定できます。設定を行わないか、無効にすると、デフォルトのイベント ログの冗長性レベルは 2 になります。 この設定をアクティブ PCoIP セッション中に変更すると、新しい設定が直ちに反映されます。

設定	説明
Configure PCoIP image quality levels	ネットワーク輻輳期間中の PCoIP でのイメージ描画方法を制御します。[最低イメージ品質]、[最高初期イメージ品質]、および [最大フレーム レート] の値の相互作用により、ネットワーク バンド幅に制約のある環境での精密な制御が可能になります。 バンド幅が制限されるシナリオでイメージ品質とフレーム レートのバランスをとるには、[最低イメージ品質] の値を使用します。30 から 100 までの値を指定できます。デフォルト値は 40 です。小さい値を指定するとフレーム レートが高くなりますが、表示の品質が低下する可能性があります。大きい値を指定するとイメージ品質が向上しますが、ネットワーク バンド幅に制約がある場合にフレーム レートが低下する可能性があります。ネットワーク バンド幅に制約がない場合は、この値にかかわらず、PCoIP で最高品質が維持されます。 表示イメージ内の変更された領域の初期品質を制限することで、PCoIP に必要な最大ネットワーク バンド幅を削減するには、[最高初期イメージ品質] の値を使用します。30 から 100 までの値を指定できます。デフォルト値は 80 です。小さい値を指定するとコンテンツの変更部分のイメージ品質が低下し、必要な最大バンド幅が削減されます。大きい値を指定するとコンテンツの変更部分のイメージ品質が向上し、必要な最大バンド幅が増加します。イメージの変更されていない領域は、この値にかかわらず、プログレッシブ方式でロスレス（完全）品質まで構築されます。80 以下の値を指定すると、使用可能なバンド幅を最大限に活用できます。 [最低イメージ品質] の値が [最高初期イメージ品質] の値を超えないようにする必要があります。 1 秒あたりの画面の更新回数を制限して、ユーザーあたりの平均使用バンド幅を管理するには、[最大フレーム レート] の値を使用します。毎秒 1 フレームから 120 フレームまでの値を指定できます。デフォルト値は 30 です。大きい値を指定すると、使用バンド幅が増加する場合がありますが、ジッタが減少するため、ビデオなどの変化するイメージの遷移がスムーズになります。小さい値を指定すると、使用バンド幅が削減されますが、ジッタが増加します。 これらのイメージ品質の値は、ソフト ホストにのみ適用され、ソフト クライアントには影響しません。 この設定を無効にするか、構成しない場合は、デフォルト値が使用されます。 この設定をアクティブ PCoIP セッション中に変更すると、新しい設定が直ちに反映されます。
Configure frame rate vs image quality preference	フレーム レートとイメージ品質の設定を 0（最大フレーム レート）から 100（最高イメージ品質）で構成します。このポリシーが無効になっているか設定されていない場合、デフォルトの設定は 50 です。 大きい値（最大 100）を指定すると、フレーム レートが低い場合でも、高いイメージ品質が優先されます。小さい値（最小 0）を指定すると、高いイメージ品質で滑らかに表示されます。 この設定は、Configure PCoIP image quality levels GPO と連携も可能です。この GPO は、最高初期イメージ品質レベルと最低イメージ品質レベルを指定します。Frame rate and image quality preference では各フレームのイメージ品質レベルを調整できますが、Configure PCoIP image quality levels GPO によって構成された最高/最低品質レベルのしきい値を超えて調整することはできません。 実行時にこのポリシーを変更すると、変更が直ちに反映されることがあります。

設定	説明
Configure PCoIP session encryption algorithms	セッション ネゴシエーション中に PCoIP エンドポイントによってアドバタイズされる暗号化アルゴリズムを制御します。 いずれかのチェック ボックスをオンにすると、関連付けられた暗号化アルゴリズムが無効になります。1 つ以上のアルゴリズムを有効にする必要があります。 この設定はエージェントとクライアントの両方に適用されます。エンドポイントは、使用される実際のセッション暗号化アルゴリズムをネゴシエートします。FIPS140-2 承認モードが有効な場合は、[Disable AES-128-GCM encryption（AES-128-GCM 暗号化を無効にする）] の値が常に上書きされ、AES-128-GCM 暗号化が有効になります。 サポートされている暗号化アルゴリズムは、SALSA20/12-256、AES-GCM-128、AES-GCM-256（優先順位順）です。デフォルトでは、サポートされているすべての暗号化アルゴリズムを、このエンドポイントのネゴシエーションに使用できます。 両方のエンドポイントが 3 つすべてのアルゴリズムをサポートするように構成され、接続でセキュリティ ゲートウェイ (SG) が使用されない場合は、SALSA20 アルゴリズムがネゴシエートされ使用されます。ただし接続で SG が使用される場合は、SALSA20 は自動的に無効になり、AES128 がネゴシエートされ使用されます。一方のエンドポイントまたは SG が SALSA20 を無効に、もう一方のエンドポイントが AES128 を無効にすると、AES256 がネゴシエートされ使用されます。

設定	説明
`Configure PCoIP USB allowed and unallowed device rules`	Teradici ファームウェアを実行するゼロ クライアントを使用する PCoIP セッションで使用を許可する USB デバイスと許可しない USB デバイスを指定します。PCoIP セッションで使用される USB デバイスは、USB 許可テーブルに表示されている必要があります。USB 不許可テーブルに表示されている USB デバイスは、PCoIP セッションで使用できません。 最大 10 の USB 許可ルールと最大 10 の USB 不許可ルールを定義できます。複数のルールは縦棒（¦）文字で区切ります。 各ルールは、ベンダー ID（VID）と製品 ID（PID）の組み合わせ、または USB デバイスのクラスの記述で指定できます。クラス ルールでは、デバイス クラス全体、1 つのサブクラス、またはサブクラス内のプロトコルの許可または不許可を指定できます。 VID/PID を組み合わせたルールの形式は、**1xxxxyyyy** です。ここで **xxxx** は 16 進数形式の VID、**yyyy** は 16 進数形式の PID です。たとえば、VID **0x1a2b**、PID **0x3c4d** のデバイスを許可またはブロックするルールは、**11a2b3c4d** です。 クラス ルールの場合は、次のいずれかの形式を使用します。 **すべての USB デバイスを許可する**　形式：**23XXXXXX**　例：**23XXXXXX** **特定のクラス ID の USB デバイスを許可する**　形式：**22*class*XXXX**　例：**22aaXXXX** **特定のサブクラスを許可する**　形式：**21*class*–*subclass*XX**　例：**21aabbXX** **特定のプロトコルを許可する**　形式：**20*class*–*subclass*–*protocol***　例：**20aabbcc** たとえば、USB HID(マウスおよびキーボード）デバイス（クラス ID 0x03) と Web カメラ（クラス ID 0x0e）を許可する USB 許可文字列は **2203XXXX|220eXXXX** です。USB マス ストレージ デバイス（クラス ID 0x08）を許可しない USB 不許可文字列は、**2208XXXX** です。 空の USB 許可文字列は、どの USB デバイスも許可されないことを意味します。空の USB 不許可文字列は、どの USB デバイスも禁止されないことを意味します。 この設定は、Horizon Agent にのみ、およびリモート デスクトップが Teradici ファームウェアを実行するゼロ クライアントとセッション中の場合にのみ適用されます。デバイスの使用はエンドポイント間でネゴシエートされます。 デフォルトでは、すべてのデバイスが許可され、どのデバイスも禁止されません。

設定	説明
Configure PCoIP virtual channels	PCoIP セッションで動作できる仮想チャネルと動作できない仮想チャネルを指定します。この設定によって、PCoIP ホスト上でのクリップボードの処理を無効にするかどうかも指定されます。 PCoIP セッションで使用される仮想チャネルは、許可仮想チャネルリストに表示されている必要があります。不許可仮想チャネル リストに表示されている仮想チャネルは、PCoIP セッションでは使用できません。 PCoIP セッションで使用する仮想チャネルを 15 まで指定できます。 複数のチャネル名は縦棒（¦）文字で区切ります。たとえば、mksvchan と vdp_rdpvcbridge の仮想チャネルを許可する仮想チャネル許可文字列は、**mksvchan¦vdp_vdpvcbridge** です。 チャネル名に縦棒文字またはバックスラッシュ（\）文字が含まれる場合は、その前にバックスラッシュ文字を入れてください。たとえば、チャネル名 awk¦ward\channel は **awk\¦ward\\channel** として入力します。 許可仮想チャネル リストが空の場合は、すべての仮想チャネルが禁止されます。不許可仮想チャネル リストが空の場合は、すべての仮想チャネルが許可されます。 仮想チャネルの設定はエージェントとクライアントの両方に適用されます。仮想チャネルを使用するには、エージェントとクライアントの両方で仮想チャネルを有効にする必要があります。 仮想チャネルの設定には、PCoIP ホスト上でのクリップボードのリモート処理を無効にできるチェック ボックスが別にあります。この値はエージェントにのみ適用されます。 デフォルトでは、クリップボードの処理を含め、すべての仮想チャネルが有効です。
Configure the PCoIP transport header	PCoIP 転送ヘッダを構成し、転送セッションの優先度を設定します。 PCoIP 転送ヘッダは、すべての PCoIP UDP パケットに追加される 32 ビット ヘッダです（転送ヘッダが有効にされ、両側でサポートされる場合に限ります）。PCoIP 転送ヘッダによって、ネットワーク デバイスは、ネットワークの輻輳を処理するときに、より良い優先順位/QoS 決定を行うことができます。デフォルトでは、転送ヘッダは有効になっています。 転送セッションの優先度は、PCoIP 転送ヘッダで報告される PCoIP セッション優先度を決定します。ネットワーク デバイスは、指定した転送セッション優先度に基づいてより良い優先順位/QoS 決定を行います。 Configure the PCoIP transport header 設定を有効にすると、以下の転送セッション優先度が使用できるようになります。 ■ [高] ■ [中]（デフォルト値） ■ [低] ■ [未定義] 転送セッション優先度値は、PCoIP エージェントとクライアントによって取り決められます。PCoIP エージェントが転送セッション優先度値を指定する場合、セッションはエージェントが指定したセッション優先度を使用します。クライアントだけが転送セッション優先度を指定した場合、セッションはクライアントが指定したセッション優先度を使用します。エージェントとクライアントのどちらもが転送セッション優先度を指定しなければ、または[未定義の優先度] が指定された場合、セッションはデフォルト値である [中] 優先度を使用します。

設定	説明
Configure the TCP port to which the PCoIP host binds and listens	ソフトウェア PCoIP ホストがバインドされる TCP エージェント ポートを指定します。 TCP ポートの値によって、エージェントがバインドを試行するベース TCP ポートが指定されます。TCP ポート範囲の値によって、ベース ポートが使用可能でない場合に使用を試行する追加ポートの数が指定されます。ポート範囲は 1 から 10 までの間にする必要があります。 この範囲は、ベース ポートから、ベース ポートにポート範囲を加えた数値までになります。たとえば、ベース ポートが 4172 でポート範囲が 10 の場合、範囲は 4172 から 4182 までになります。 リトライ ポート範囲の値を 0 に設定しないでください。この値を 0 に設定すると、PCoIP 表示プロトコルでユーザーがデスクトップにログインする時に接続に失敗します。Horizon Client は、**このデスクトップの表示プロトコルは現在使用できません。システム管理者にお問い合わせください。**というエラー メッセージを返します。 この設定は Horizon Agent にのみ適用されます。 シングル ユーザー マシンでは、View 4.5 以降でのデフォルトのベース TCP ポートは 4172 です。View 4.0.*x* 以前でのデフォルトのベース TCP ポートは 50002 です。デフォルトのポート範囲は 1 です。 RDS ホストでは、デフォルトのベース TCP ポートは 4173 です。 PCoIP が RDS ホストで使用される場合、ユーザー接続ごとに個別の PCoIP ポートが使用されます。リモート デスクトップ サービスによって設定されるデフォルトのポート範囲は、同時ユーザー接続の予想される最大数に対応できる十分な大きさです。 **重要:** ベスト プラクティスとして、このポリシー設定を使用して RDS ホストのデフォルトのポート範囲を変更したり、TCP ポート値をデフォルトの 4173 から変更したりしないでください。最も重要なこととして、TCP ポート値を 4172 に設定しないでください。この値を 4172 に設定すると、RDS セッション中の PCoIP パフォーマンスに悪影響を及ぼします。

設定	説明
Configure the UDP port to which the PCoIP host binds and listens	ソフトウェア PCoIP ホストがバインドされる UDP エージェント ポートを指定します。 UDP ポートの値によって、エージェントがバインドを試行するベース UDP ポートが指定されます。UDP ポート範囲の値によって、ベース ポートが使用可能でない場合に使用を試行する追加ポートの数が指定されます。ポート範囲は 1 から 10 までの間にする必要があります。 リトライ ポート範囲の値を 0 に設定しないでください。この値を 0 に設定すると、PCoIP 表示プロトコルでユーザーがデスクトップにログインする時に接続に失敗します。Horizon Client は、**このデスクトップの表示プロトコルは現在使用できません。システム管理者にお問い合わせください。**というエラー メッセージを返します。 この範囲は、ベース ポートから、ベース ポートにポート範囲を加えた数値までになります。たとえば、ベース ポートが 4172 でポート範囲が 10 の場合、範囲は 4172 から 4182 までになります。 この設定は Horizon Agent にのみ適用されます。 シングル ユーザー マシンでは、View 4.5 以降でのデフォルトのベース UDP ポートは 4172、View 4.0.*x* 以前でのデフォルトのベース UDP ポートは 50002 です。デフォルトのポート範囲は 10 です。 RDS ホストでは、デフォルトのベース UDP ポートは 4173 です。 PCoIP が RDS ホストで使用される場合、ユーザー接続ごとに個別の PCoIP ポートが使用されます。リモート デスクトップ サービスによって設定されるデフォルトのポート範囲は、同時ユーザー接続の予想される最大数に対応できる十分な大きさです。 **重要:** ベスト プラクティスとして、このポリシー設定を使用して RDS ホストのデフォルトのポート範囲を変更したり、UDP ポート値をデフォルトの 4173 から変更したりしないでください。 最も重要なこととして、UDP ポート値を 4172 に設定しないでください。 この値を 4172 に設定すると、RDS セッション中の PCoIP パフォーマンスに悪影響を及ぼします。
Enable access to a PCoIP session from a vSphere console	vSphere Client コンソールにアクティブな PCoIP セッションの表示およびデスクトップへの入力の送信を許可するかどうかを決定します。 デフォルトでは、クライアントが PCoIP によって接続されている場合、vSphere Client コンソール画面は空白になり、コンソールは入力を送信できません。デフォルト設定によって、PCoIP セッションがアクティブなときに悪意あるユーザーがユーザーのデスクトップを閲覧したりホストにローカルで入力できなくなります。 この設定は Horizon Agent にのみ適用されます。 この設定を無効にするか、構成しない場合は、コンソール アクセスは許可されません。この設定を有効にすると、コンソールに PCoIP セッションが表示され、コンソール入力が許可されます。 この設定を有効にした場合、Windows 7 システム上で実行している PCoIP セッションは、Windows 7 仮想マシンがハードウェア v8 である場合にのみコンソールに表示できます。ハードウェア v8 は ESXi 5.0 以降でのみ使用できます。一方、Windows 7 システムへのコンソール入力は、仮想マシンがどのハードウェア バージョンであっても許可されます。
Enable/disable audio in the PCoIP session	PCoIP セッションでオーディオを有効にするかどうかを指定します。両方のエンドポイントでオーディオが有効になっている必要があります。この設定を有効にすると、PCoIP オーディオが許可されます。この設定を無効にすると、PCoIP オーディオが無効になります。この設定を構成しないと、デフォルトでオーディオが有効になります。

設定	説明
Enable/disable microphone noise and DC offset filter in PCoIP session	PCoIP セッション中にマイク入力のマイク ノイズ フィルタおよび DC オフセット フィルタを有効にするかどうかを決定します。 この設定は Horizon Agent と Teradici オーディオ ドライバのみに適用されます。 この設定が構成されていない場合、Teradici オーディオ ドライバは、デフォルトでマイク ノイズ フィルタおよび DC オフセット フィルタを使用します。
Turn on PCoIP user default input language synchronization	PCoIP セッションでのユーザーのデフォルト入力言語と、PCoIP クライアント エンドポイントのデフォルト入力言語を同期するかどうかを指定します。この設定を有効にすると、同期が許可されます。この設定を無効にするか、構成しない場合は、同期が許可されません。 この設定は Horizon Agent にのみ適用されます。
Configure SSL Connections to satisfy Security Tools	SSL セッションのネゴシエーション接続の確立方法を指定します。 ポート スキャナを満たすには、この「SSL 接続を構成」を有効にし、Horizon Agent で次のタスクを完了します。 1 Microsoft Management Console で、ローカル マシンのコンピュータ アカウントの個人用ストアに正しい名前の署名付き証明書を保存します。 2 信頼されたルート証明書ストアに認証局の署名付き証明書を保存します。 3 VMware View 5.1 以前との接続を無効にします。 4 証明書ストアから証明書を読み込むように Horizon Agent を設定します。ローカル マシンの個人用ストアを使用する場合、手順 1 と 2 で別の保存場所を使用していなければ、証明書ストアの名前 (MY と ROOT) を変更せず、そのまま使用します。 PCoIP Server がポート スキャナなどの Security Tools を満たします。
Configure SSL Protocols	SSL 暗号化接続を確立する前に、特定の暗号化プロトコルの使用を制限するように、OpenSSL プロトコルを構成します。プロトコル リストは、コロンで区切られた 1 つ以上の openssl プロトコル文字列で構成されています。暗号文字列で大文字と小文字は区別されません。 デフォルト値は TLS1.1:TLS1.2 です。 これは、TLS v1.1 と TLS v1.2 が有効で、SSL v2.0、SSLv3.0、TLS v1.0 が無効であることを意味します。 この設定は、Horizon Agent と Horizon Client の両方に適用されます。 両側で設定すると、OpenSSL プロトコルのネゴシエーション ルールが使用されます。
Configure SSL cipher list	SSL 暗号化接続を確立する前に、暗号の使用を制限する SSL 暗号リストを設定します。このリストは、コロンで区切られた 1 つ以上の暗号文字列で構成されています。すべての暗号文字列は、大文字と小文字が区別されません。 デフォルトの値は、ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH です。 この項目を設定すると、[Security Tools の要件を満たすために SSL 接続を設定] の [SSL 接続ネゴシエーションに AES-256 以上の暗号を強制する] チェック ボックスは無視されます。 この設定は、PCoIP Server と PCoIP クライアントの両方に適用する必要があります。

PCoIP クリップボードの設定

Horizon PCoIP ADMX テンプレート ファイルには、コピーおよび貼り付け操作に関するクリップボード設定を構成するグループ ポリシー設定が含まれます。

これらの設定はすべて、グループ ポリシー管理エディタの [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [PCoIP セッション変数] - [上書き可能な管理者デフォルト] フォルダにあります。

これらの設定はすべて、グループ ポリシー管理エディタの [ユーザーの構成] - [ポリシー] - [管理用テンプレート] - [PCoIP セッション変数] - [上書き不可の管理者設定] フォルダにあります。

表 5-10. PCoIP クリップボード ポリシー設定

設定	説明
Configure clipboard memory size on server (in kilobytes)	キロバイト単位で、サーバのクリップボードのメモリ サイズの値を指定します。クライアントにも、クリップボードのメモリ サイズの値があります。セッション設定後、サーバは自身のクリップボードのメモリ サイズの値をクライアントに送信します。有効なクリップボードのメモリ サイズは、クライアントとサーバのクリップボードのメモリ サイズの値の小さい方となります。 指定できる最小値は 512 KB、最大値は 16384 KB です。0 を指定する場合、または値を指定しない場合、サーバのクリップボードのメモリ サイズは、デフォルトで 1024 KB になります。 この設定は、バージョン 7.0.1 以降、および Horizon Client 4.1 以降がインストールされている Windows、Linux および Mac クライアントのみに適用されます。以前のリリースでは、クリップボードのメモリ サイズは 1 MB です。 **注:** ネットワークによっては、クリップボードのメモリ サイズを大きくすると、パフォーマンスに悪影響が及ぶ場合があります。クリップボードのメモリ サイズは、16 MB を超える値に設定しないことを推奨します。
Configure clipboard redirection	クリップボード リダイレクトを許可する方向を決定します。次のいずれかの値を選択できます。 ■ [クライアントからエージェントの方向のみ有効]（すなわち、クライアント システムからリモート デスクトップにのみ、コピーおよび貼り付けを許可します）。 ■ [どちらの方向も無効] ■ [どちらの方向も有効] ■ [エージェントからクライアントの方向のみ有効]（すなわち、リモート デスクトップからクライアント システムにのみ、コピーおよび貼り付けを許可します）。 クリップボードのリダイレクトは、仮想チャネルとして実装されます。仮想チャネルが無効になっている場合、クリップボードのリダイレクトは機能しません。 この設定は Horizon Agent にのみ適用されます。 この設定が無効または構成されていない場合、デフォルト値は [クライアントからエージェントの方向のみ有効] です。
Filter text out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データからテキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Rich Text Format data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データからリッチ テキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。

設定	説明
Filter images out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データからイメージ データを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Office text data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データから Microsoft Office のテキスト形式データ（BIFF12 形式）を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データから Microsoft Office チャートおよび Smart Art データ (Art::GVML ClipFormat) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Text Effects data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データから Microsoft Office のテキスト エフェクト データ（HTML 形式）を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter text out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データからテキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Rich Text Format data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データからリッチ テキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter images out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データからイメージ データを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Office text data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データから Microsoft Office のテキスト形式データ（BIFF12 形式）を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。

設定	説明
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データから Microsoft Office チャートおよび Smart Art データ (Art::GVML ClipFormat) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Text Effects data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データから Microsoft Office のテキスト エフェクト データ（HTML 形式）を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。

PCoIP のバンド幅設定

Horizon PCoIP ADMX テンプレート ファイルには、PCoIP のバンド幅特性を構成するグループ ポリシー設定が含まれます。

これらの設定はすべて、グループ ポリシー管理エディタの [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [PCoIP セッション変数] - [上書き可能な管理者デフォルト] フォルダにあります。

これらの設定はすべて、グループ ポリシー管理エディタの [ユーザーの構成] - [ポリシー] - [管理用テンプレート] - [PCoIP セッション変数] - [上書き不可の管理者設定] フォルダにあります。

表 5-11. Horizon PCoIP のセッションバンド幅変数

設定	説明
Configure the maximum PCoIP session bandwidth	PCoIP セッションの最大バンド幅をキロビット/秒単位で指定します。このバンド幅には、イメージ、オーディオ、仮想チャネル、USB、および制御 PCoIP のすべてのトラフィックが含まれます。 この値を、想定される同時並行の PCoIP セッションの数を考慮に入れたうえで、エンドポイントが接続されるリンクの合計容量に設定します。たとえば、4 メガビット/秒のインターネット接続を介して接続される単一ユーザーの VDI 構成（単一の PCoIP セッション）では、他のネットワーク トラフィックのための余地を確保するためにこの値を 4 メガビット、またはそれから 10% 引いた値に設定します。複数の VDI ユーザーまたは RDS 構成のいずれかで構成される、複数の同時並行 PCoIP セッションでリンクを共有することを想定している場合には、設定を適宜調整することを推奨します。ただし、この値を低くすると、各アクティブ セッションの最大バンド幅が制限されます。 この値を設定すると、エージェントがリンク容量よりも高い速度での送信を試行して、過剰なパケット損失が発生したり、ユーザーの操作性が低下したりすることがなくなります。この値は対称型です。クライアント側とエージェント側で設定されている 2 つの値のうち、小さい方の値がクライアントとエージェントで強制的に使用されます。たとえば、最大バンド幅を 4 メガビット/秒に設定すると、それがクライアント側で行われた設定でも、エージェントは強制的にそれ以下の速度で送信するようになります。 エンドポイント上でこの設定を無効にするか、構成しない場合、エンドポイントはバンド幅を制限しません。この設定を構成する場合、その設定はエンドポイントの最大バンド幅制限としてキロビット/秒単位で使用されます。 この設定が構成されていない場合のデフォルト値は、900000 キロビット/秒になります。 この設定は Horizon Agent とクライアントに適用されます。2 つのエンドポイントの設定が異なる場合は、小さい方の値が使用されます。
Configure the PCoIP session bandwidth floor	PCoIP セッションによって予約されるバンド幅の下限をキロバイト/秒単位で指定します。 この設定では、エンドポイントのバンド幅で期待される最小送信速度が構成されます。この設定を使用してエンドポイントのバンド幅を予約すると、ユーザーはバンド幅が使用可能になるまで待つ必要がなくなるため、セッションの応答性が向上します。 すべてのエンドポイントの合計予約バンド幅を過剰にサブスクライブしないように注意してください。また、構成内の全接続のバンド幅下限の合計がネットワークの容量を超えないように注意してください。 デフォルト値は 0 です。これは、最小バンド幅が予約されないことを意味します。この設定を無効にするか、構成しない場合、最小バンド幅は予約されません。 この設定は Horizon Agent とクライアントに適用されますが、構成されたエンドポイントにのみ影響します。 この設定をアクティブ PCoIP セッション中に変更すると、変更が直ちに反映されます。
Configure the PCoIP session MTU	PCoIP セッションでの UDP パケットの最大転送ユニット（MTU）サイズを指定します。 この MTU サイズには、IP および UDP のパケット ヘッダーが含まれます。TCP では MTU の設定に標準の MTU 検出メカニズムが使用されるため、この設定による影響を受けません。 最大 MTU サイズは 1500 バイトです。最小 MTU サイズは 500 バイトです。デフォルト値は 1300 バイトです。 通常、MTU サイズを変更する必要はありません。PCoIP パケットの断片化の原因となる、通常と異なるネットワーク設定を使用する場合は、この値を変更してください。 この設定は Horizon Agent とクライアントに適用されます。2 つのエンドポイントの MTU サイズ設定が異なる場合は、小さい方のサイズが使用されます。 この設定を無効にするか、構成しない場合、クライアントでは Horizon Agent とのネゴシエーションにデフォルト値が使用されます。

設定	説明
Configure the PCoIP session audio bandwidth limit	PCoIP セッションでオーディオ（サウンドの再生）に使用できる最大バンド幅を指定します。 オーディオ処理では、オーディオに使用されるバンド幅が監視されます。この処理によって、現在のバンド幅使用率で可能な最善のオーディオを提供するオーディオ圧縮アルゴリズムが選択されます。バンド幅制限が設定されている場合、バンド幅の制限内に収まるようになるまで、圧縮アルゴリズムの選択が変更されて品質が低下します。指定されたバンド幅の制限内で最低品質のオーディオを提供できない場合は、オーディオが無効になります。 圧縮なしの高品質なステレオ オーディオを再生できるようにするには、この値を 1600 キロビット/秒以上に設定します。450 キロビット/秒以上に設定すると、高品質な圧縮ステレオ オーディオを提供できます。50 ～ 450 キロビット/秒の値を設定すると、FM ラジオから電話までの品質のオーディオになります。50 キロビット/秒未満の値を設定すると、オーディオが再生されない可能性があります。 この設定は Horizon Agent にのみ適用されます。この設定による効果を得るには、両方のエンドポイントでオーディオを有効にする必要があります。 また、この設定は USB オーディオには影響しません。 この設定を無効にするか、構成しない場合、デフォルトのオーディオ バンド幅制限である 500 キロビット/秒が構成され、オーディオ圧縮アルゴリズムの選択が制限されます。この設定を構成すると、値がキロビット/秒単位で計測され、デフォルトのオーディオ バンド幅制限は 500 キロビット/秒となります。 この設定は View 4.6 以降に適用されます。それ以前のバージョンの View では影響がありません。 この設定をアクティブ PCoIP セッション中に変更すると、変更が直ちに反映されます。
Turn off Build-to-Lossless feature	PCoIP プロトコルのロスレス構築機能をオフまたはオンのどちらにするかを指定します。この機能は、デフォルトでオフになっています。 この設定を有効にするか、構成しない場合、ロスレス構築機能はオフになり、イメージやその他のデスクトップおよびアプリケーション コンテンツがロスレス状態まで構築されることはありません。バンド幅が制約されたネットワーク環境では、ロスレス構築機能をオフにすることでバンド幅を節約できます。 この設定を無効にするとロスレス構築機能がオンになります。イメージおよびその他のデスクトップおよびアプリケーション コンテンツをロスレス状態まで構築することが必要な環境では、ロスレス構築機能をオンにすることが推奨されています。 この設定をアクティブ PCoIP セッション中に変更すると、変更が直ちに反映されます。 PCoIP のロスレス構築機能の詳細については、PCoIP ロスレス構築機能を参照してください。

PCoIP のキーボード設定

View PCoIP ADMX テンプレート ファイルには、キーボードの使用方法に影響を及ぼす PCoIP の設定を構成するグループ ポリシー設定が含まれます。

これらの設定はすべて、グループ ポリシー管理エディタの [コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [PCoIP セッション変数] - [上書き可能な管理者デフォルト] フォルダにあります。

これらの設定はすべて、グループ ポリシー管理エディタの [ユーザーの構成] - [ポリシー] - [管理用テンプレート] - [PCoIP セッション変数] - [上書き不可の管理者設定] フォルダにあります。

表 5-12. キーボード用の Horizon PCoIP のセッション変数

設定	説明
`Disable sending CAD when users press Ctrl+Alt+Del`	このポリシーが有効になっている場合、PCoIP セッション中に Secure Attention Sequence (SAS) をリモート デスクトップに送信するには、Ctrl+Alt+Del ではなく Ctrl+Alt+Insert を押す必要があります。 ユーザーがクライアント エンドポイントをロックするために Ctrl+Alt+Del を押したとき、ホストとゲストの両方に SAS が送信されるために混乱が生じる場合は、この設定を有効にすることを推奨します。 この設定は Horizon Agent にのみ適用されて、クライアントには影響しません。 このポリシーが構成されていない、または無効になっている場合は、Ctrl+Alt+Del または Ctrl+Alt+Insert を押して SAS をリモート デスクトップに送信できます。
`Use alternate key for sending Secure Attention Sequence`	Secure Attention Sequence (SAS) を送信するための、Insert キーの代替キーを指定します。 この設定を使用して、PCoIP セッション中にリモート デスクトップの内部から起動された仮想マシンで Ctrl+Alt+Ins のキー シーケンスを保持できます。 たとえば、ユーザーが PCoIP デスクトップ内から vSphere Client を起動し、vCenter Server で仮想マシンのコンソールを開くことができます。vCenter Server 仮想マシン上のゲスト オペレーティング システム内で Ctrl+Alt+Ins シーケンスを使用すると、仮想マシンに Ctrl+Alt+Del の SAS が送信されます。この設定を構成すると、Ctrl + Alt + *Alternate Key* のシーケンスで PCoIP デスクトップに Ctrl+Alt+Del の SAS を送信できます。 この設定を有効にする場合は、代替キーをドロップダウン メニューから選択する必要があります。この設定を有効にして、値を未指定のままにすることはできません。 この設定を無効にするか、構成しない場合は、Ctrl+Alt+Ins のキー シーケンスが SAS として使用されます。 この設定は Horizon Agent にのみ適用されて、クライアントには影響しません。

PCoIP ロスレス構築機能

PCoIP 表示プロトコルを構成して、プログレッシブ構築またはロスレス構築と呼ばれるエンコーディング方法を使用できます。この方法により、制約のあるネットワーク条件下でも全体的に最適なユーザー体験を提供できます。この機能は、デフォルトでオフになっています。

ロスレス構築機能ではロッシー イメージと呼ばれる高度に圧縮された初期イメージを提供し、その後プログレッシブに完全なロスレス状態まで構築します。ロスレス状態とは、イメージが意図したとおり完全に忠実に表示されることです。

LAN 上では、PCoIP は、テキストを常にロスレス圧縮を使用して表示します。ロスレス機能が有効になっていて、セッションあたりの使用可能帯域幅が 1Mbs を下回った場合には、PCoIP は最初にロッシー テキスト イメージを表示し、そのイメージを素早くロスレス状態に構築します。このアプローチにより、ネットワーク条件が変化する中でもデスクトップの応答が早い状態に保ち、可能な限り最高の状態のイメージを表示することで、ユーザーに最適な体験を提供できます。

ロスレス構築機能には次の特長があります。

- 動的にイメージ品質を調整
- 混雑しているネットワーク上でイメージ品質を低減
- 画面更新の待ち時間を減らすことにより、応答性を維持

- ネットワークの混雑解消時には最大イメージ品質を回復

`Turn off Build-to-Lossless feature` グループ ポリシー設定を無効にして、ロスレス構築機能をオンにすることができます。PCoIP のバンド幅設定を参照してください。

VMware Blast ポリシー設定

VMware Blast グループ ポリシー ADMX テンプレート ファイルの `vdm_blast.admx` には、VMware Blast 表示プロトコルのポリシー設定が含まれています。ポリシーを適用すると、設定がレジストリ キー `HKLM\Software\Policies\VMware, Inc.\VMware Blast\config` に保存されます。

これらの設定は、HTML Access およびすべての Horizon Client に適用されます。

表 5-13. VMware Blast ポリシー設定

設定	説明
`Max Session Bandwidth`	VMware Blast セッションの最大バンド幅をキロビット/秒 (kbps) 単位で指定します。このバンド幅には、イメージ、オーディオ、仮想チャネル、USB、および VMware Blast 制御のすべてのトラフィックが含まれます。デフォルトは 1 Gbps です。
`Min Session Bandwidth`	VMware Blast セッション用に予約された最小バンド幅をキロビット/秒 (kbps) 単位で指定します。デフォルトは 256 kbps です。
`Max Bandwidth Slope for the Kbps Per Megapixel`	VMware Blast セッション用に予約された最大バンド幅スロープをキロビット/秒 (kbps) 単位で指定します。最小値は 100 です。最大値は 100000 です。デフォルト値は 6200 です。
`Max Frame Rate`	画面更新の最大レートを指定します。この設定を使用して、ユーザーが使用する平均バンド幅を管理します。デフォルトは 1 秒あたり 30 回の更新です。
`UDP Protocol`	UDP プロトコルまたは TCP プロトコルを使用するかどうかを指定します。デフォルトでは、UDP プロトコルが使用されます。この設定では、レジストリ キーがある Horizon Agent マシンの再起動が必要となります。この設定は、常に TCP プロトコルが使用される HTML Access には適用されません。
`H264`	H.264 エンコードまたは JPEG/PNG エンコードを使用するかどうかを指定します。デフォルトでは、H.264 エンコードを使用します。
`PNG`	この設定を有効にしない、あるいは構成しない場合、PNG エンコードをリモート セッションに利用できます。この設定を無効にすると、JPEG/PNG モードにおけるエンコードでは、JPEG エンコードのみが使用されます。H.264 エンコーダが有効な場合、このポリシーは適用されません。デフォルトでは、この設定は構成されていません。 この設定は 7.0.2 以降に適用されます。
`Screen Blanking`	デスクトップにアクティブなセッションがある場合に、デスクトップ仮想マシンのコンソールに、ユーザーに表示される実際のデスクトップを表示するか、空の画面を表示するかを指定します。デフォルトでは、空の画面を表示します。
`Cookie Cleanup Interval`	アクティブではないセッションに関連付けられている Cookie を削除する頻度（ミリ秒）を決定します。デフォルトは 100 ミリ秒です。

設定	説明
Image Quality	リモート ディスプレイのイメージ品質を指定します。2 つの低品質設定、2 つの高品質設定、および 1 つの中品質設定を指定できます。低品質設定は、スクロール発生時など、頻繁に変化する画面の領域に適しています。高品質設定は、より静的な画面の領域に適していて、イメージ品質がより高くなります。次の設定を指定できます。 ■ [Low JPEG Quality（低品質 JPEG）]（使用可能な値の範囲：1 ～ 100、デフォルト：25） ■ [Low JPEG Chroma Subsampling（低い JPEG 彩度のサブサンプリング）]（使用可能な値の範囲：4:1:0（最低）、4:1:1、4:2:0、4:2:2、および 4:4:4（最高）、デフォルト：4:1:0） ■ [Mid JPEG Quality（中品質 JPEG）]（使用可能な値の範囲：1 ～ 100、デフォルト：35） ■ [High JPEG Quality（高品質 JPEG）]（使用可能な値の範囲：1 ～ 100、デフォルト：90） ■ [High JPEG Chroma Subsampling（高い JPEG 彩度のサブサンプリング）]（使用可能な値の範囲：4:1:0（最低）、4:1:1、4:2:0、4:2:2、および 4:4:4（最高）、デフォルト：4:4:4）
H.264 Quality	H.264 エンコードを使用するように構成されたリモート ディスプレイのイメージ品質を指定します。ロスレス圧縮でイメージをどれだけ制御するかを決定する量子化の最小および最大値を指定できます。最高のイメージ品質には量子化の最小値を指定できます。最低のイメージ品質には量子化の最大値を指定できます。次の設定を指定できます。 ■ [H264maxQP]（使用可能な値の範囲：0 ～ 51、デフォルト：36） ■ [H264minQP]（使用可能な値の範囲：0 ～ 51、デフォルト：10） 最高のイメージ品質のためには、使用可能な値の範囲の +5 または -5 以内の量子化値を設定します。
HTTP Service	セキュリティ サーバまたは Access Point アプライアンスとデスクトップの間の安全な通信 (HTTPS) に使用されるポートを指定します。このポートを開くようにファイアウォールを構成する必要があります。デフォルトは 22443 です。
Audio playback	オーディオ再生をリモート デスクトップに対して有効にするかどうかを指定します。この設定では、オーディオ再生を有効にします。
Configure clipboard redirection	クリップボード リダイレクトの許容される動作を指定します。次のオプションがあります。 ■ [どちらの方向も有効] ■ [どちらの方向も無効] ■ [Enabled client to server only（クライアントからサーバの方向のみ有効）]（ユーザーはクライアントからデスクトップへのみコピー/貼り付けを実行できます。） ■ [Enabled server to client only（サーバからクライアントの方向のみ有効）]（ユーザーはデスクトップからクライアントへのみコピー/貼り付けを実行できます。） デフォルトは [Enabled client to server only（クライアントからサーバの方向のみ有効）] です。
Clipboard memory size on server(in kilobytes)	キロバイト単位で、サーバのクリップボードのメモリ サイズの値を指定します。クライアントにも、クリップボードのメモリ サイズの値があります。セッション設定後、サーバは自身のクリップボードのメモリ サイズの値をクライアントに送信します。有効なクリップボードのメモリ サイズは、クライアントとサーバのクリップボードのメモリ サイズの値の小さい方となります。 指定できる最小値は 512 KB、最大値は 16384 KB です。0 を指定する場合、または値を指定しない場合、サーバのクリップボードのメモリ サイズは、デフォルトで 1024 KB になります。 この設定は、バージョン 7.0.1 以降、および Horizon Client 4.1 以降がインストールされている Windows、Linux および Mac クライアントのみに適用されます。以前のリリースでは、クリップボードのメモリ サイズは 1 MB です。 **注:** ネットワークによっては、クリップボードのメモリ サイズを大きくすると、パフォーマンスに悪影響が及ぶ場合があります。クリップボードのメモリ サイズは、16 MB を超える値に設定しないことを推奨します。
Keyboard locale synchronization	クライアントのキーボード ロケール リストやデフォルト キーボード ロケールを、リモート デスクトップまたはアプリケーションに同期させるかどうかを指定します。この設定を有効にすると、同期が発生します。この設定は Horizon Agent のみに適用されます。 **注:** この機能は、Horizon Client for Windows のみにサポートされます。

設定	説明
Configure file transfer	リモート デスクトップと HTML Access クライアント間のファイル転送について許可される動作を指定します。次のいずれかの値を選択できます。 ■ [アップロードとダウンロードの両方を無効にする] ■ [アップロードとダウンロードの両方を有効にする] ■ [ファイルのアップロードのみを有効にする] (ユーザーはクライアントシステムからリモート デスクトップにのみファイルをアップロードできます)。 ■ [ファイルのダウンロードのみを有効にする] (ユーザーはリモート デスクトップからクライアントシステムにのみファイルをダウンロードできます)。 デフォルトは、[ファイルのアップロードのみを有効にする] です。 この設定は、バージョン 7.0.1 以降と HTML Access 4.1 以降にのみ適用されます。
Filter text out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データからテキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Rich Text Format data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データからリッチ テキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter images out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データからイメージ データを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Office text data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データから Microsoft Office のテキスト形式データ (BIFF12 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データから Microsoft Office チャートおよび Smart Art データ (Art::GVML ClipFormat) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Text Effects data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データから Microsoft Office のテキスト エフェクト データ (HTML 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter text out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データからテキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Rich Text Format data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データからリッチ テキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。

設定	説明
Filter images out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データからイメージ データを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Office text data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データから Microsoft Office のテキスト形式データ (BIFF12 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データから Microsoft Office チャートおよび Smart Art データ (Art::GVML ClipFormat) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Text Effects data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データから Microsoft Office のテキスト エフェクト データ (HTML 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。

VMware Blast ポリシー設定の適用

クライアントのセッション中に、次の VMware Blast ポリシーの変更があった場合、Horizon Client は変更を検出し、直ちに新しい設定を適用します。

- H264
- Audio Playback
- Max Session Bandwidth
- Min Session Bandwidth
- Max Frame Rate
- Image Quality

他のすべての VMware Blast ポリシーについては、マイクロソフト GPO 更新ルールが適用されます。GPO は、手動または Horizon Agent マシンの再起動により更新できます。詳細については、Microsoft ドキュメントを参照してください。

リモート デスクトップ サービス グループ ポリシーの使用

リモート デスクトップ サービス グループ ポリシーを使用し、RDS ホスト、RDS デスクトップ セッション、および RDS アプリケーション セッションの構成とパフォーマンスを制御できます。Horizon 7 には、Horizon 7 でサポートされる Microsoft RDS グループ ポリシーが含まれている ADMX ファイルが提供されています。

ベスト プラクティスとして、対応する Microsoft グループ ポリシーではなく Horizon 7 ADMX ファイルで提供されているグループ ポリシーを設定することをお勧めします。Horizon 7 グループ ポリシーは、Horizon 7 環境をサポートすることが保証されています。

Active Directory へのリモート デスクトップ サービス ADMX ファイルの追加

リモート デスクトップ サービス ADMX ファイルのポリシー設定を Active Directory のグループ ポリシー オブジェクト (GPO) に追加することができます。

また、個々の RDS ホストにリモート デスクトップ サービス ADMX ファイルをインストールすることもできます。個々の RDS ホストでローカル グループ ポリシー エディタ (`gpedit.msc`) を使用して、グループ ポリシー設定を編集します。

前提条件

- リモート デスクトップ サービス グループ ポリシー設定の GPO を作成し、RDS ホストを含む OU にリンクします。
- Active Directory サーバをホストするマシンに管理者ドメイン ユーザーとしてログインできることを確認します。
- MMC およびグループ ポリシー管理スナップインが Active Directory サーバで使用できることを確認します。

手順

1 Horizon 7 GPO Bundle `.zip` ファイルを https://my.vmware.com/web/vmware/downloads の VMware ダウンロード サイトからダウンロードします。

[Desktop & End-User Computing（デスクトップおよびエンドユーザー コンピューティング）] で VMware Horizon 7 のダウンロードを選択します。これには GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` で、*x.x.x* はバージョン、*yyyyyyy* はビルド番号を表します。Horizon 7 のグループ ポリシー設定用の ADMX ファイルはすべて、このファイルで提供されています。

2 `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` ファイルを解凍して、リモート デスクトップ サービス ADMX および ADML ファイルを Active Directory サーバにコピーします。

a Active Directory サーバの `C:\Windows\PolicyDefinitions` フォルダに `vmware_rdsh_server.admx` ファイルをコピーします。

b （オプション） Active Directory サーバで、`C:\Windows\PolicyDefinitions\` 内の適切なサブフォルダに `vmware_rdsh_server.adml` 言語リソース ファイルをコピーします。

3 Active Directory サーバで、[グループ ポリシー管理エディタ] を開きます。

リモート デスクトップ サービス グループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [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] フォルダにインストールされています。

リモート デスクトップ サービス グループ ポリシー設定の一部は、[ユーザーの構成] - [管理用テンプレート] - [Windows コンポーネント] - [リモート デスクトップ サービス] - [リモート デスクトップ セッション ホスト] フォルダにもインストールされています。

4 （オプション）[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] [] フォルダで、グループ ポリシー設定を構成します。

RDS アプリケーションの互換性の設定

RDS アプリケーションの互換性グループ ポリシー設定は、Windows インストーラの互換性、リモート デスクトップの IP 仮想化、ネットワーク アダプタの選択、RDS ホスト IP アドレスの使用などを制御します。

表 5-14. RDS アプリケーションの互換性グループ ポリシー設定

設定	説明
`Turn off Windows Installer RDS Compatibility`	このポリシー設定は、Windows Installer RDS Compatibility が、フルインストールされたアプリケーションのユーザーごとに実行されるかどうかを指定します。Windows インストーラで一度に実行できる `msiexec` プロセス インスタンスは 1 つです。デフォルトでは、Windows Installer RDS Compatibility が有効になります。 このポリシー設定を有効にすると、Windows Installer RDS Compatibility が無効になり、一度に実行できる `msiexec` プロセス インスタンスは 1 つになります。 このポリシー設定を無効にするか、または構成しないままにすると、Windows Installer RDS Compatibility が有効になり、複数のユーザーごとのアプリケーションのインストール要求が待機中になり、それらが受け取られた順に `msiexec` プロセスによって処理されます。

`Turn on Remote Desktop IP Virtualization`	このポリシー設定は、リモート デスクトップの IP 仮想化を有効にするかどうかを指定します。
	デフォルトでは、リモート デスクトップの IP 仮想化は無効です。
	このポリシー設定を有効にすると、リモート デスクトップの IP 仮想化が有効になります。この設定が適用されるモードを選択できます。プログラム単位モードを使用する場合は、仮想 IP アドレスを使用するプログラムのリストを入力する必要があります。各プログラムを個別の行に入力してください（プログラム間に空の行を入れないでください）。例：
	`explorer.exe`
	`mstsc.exe`
	このポリシー設定を無効にするか、または構成しないままにすると、リモート デスクトップの IP 仮想化は無効になります。

設定	説明
Select the network adapter to be used for Remote Desktop IP Virtualization	このポリシー設定は、仮想 IP アドレスに使用されるネットワーク アダプタに対応する IP アドレスとネットワーク マスクを指定します。IP アドレスとネットワーク マスクは、Classless Inter-Domain Routing の表記で入力する必要があります。例： 192.0.2.96/24. このポリシー設定を有効にすると、指定した IP アドレスとネットワーク マスクが使用されて、仮想 IP アドレスに使用されるネットワーク アダプタが選択されます。 このポリシー設定を無効にするか、または構成しないままにすると、リモート デスクトップの IP 仮想化は無効になります。リモート デスクトップの IP 仮想化を機能させるためには、ネットワーク アダプタを構成する必要があります。
Do not use Remote Desktop Session Host server IP address when virtual IP address is not available	このポリシー設定は、仮想 IP アドレスが使用できない場合に RDS ホストの IP アドレスをセッションが使用するかどうかを指定します。 このポリシー設定を有効にすると、仮想 IP アドレスが使用できない場合に RDS ホストの IP アドレスが使用されません。このセッションではネットワーク接続が確立されていません。 このポリシー設定を無効にするか、または構成しないままにすると、仮想 IP アドレスが使用できない場合、RDS ホストの IP アドレスが使用されます。

RDS 接続の設定

RDS 接続のグループ ポリシー設定を使用すると、RDS ホストのセッション接続にポリシーを設定できます。

Horizon 7 RDS グループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [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] - [接続] フォルダにインストールされています。

Horizon 7 RDS グループ ポリシー設定は、[ユーザーの構成] - [管理用テンプレート] - [Windows コンポーネント] - [リモート デスクトップ サービス] - [リモート デスクトップ セッション ホスト] - [接続] フォルダにもインストールされています。

表 5-15. RDS 接続グループ ポリシー設定

設定	説明
Automatic reconnection	ネットワーク リンクが一時的に失われた場合に、リモート デスクトップ接続クライアントが RDS ホストのセッションに自動的に再接続するかどうかを指定します。デフォルトでは、最大 20 個の接続が 5 分間隔で試行されます。 このポリシー設定を有効にすると、リモート デスクトップ接続を実行しているすべてのクライアントで、ネットワーク接続の消失時に自動的に再接続を試みます。 このポリシー設定を無効にすると、クライアントの自動接続は禁止されます。 このポリシー設定を構成しないと、グループ ポリシー レベルで自動再接続が指定されません。ただし、リモート デスクトップ接続の [エクスペリエンス] タブで [接続が損なわれた場合は再接続する] チェックボックスをオンにすると、自動再接続を構成できます。
Allow users to connect remotely using Remote Desktop Services	このポリシー設定は、リモート デスクトップ サービスを使用するコンピュータへのリモート接続を設定します。 このポリシー設定を有効にすると、対象コンピュータのリモート デスクトップ ユーザー グループメンバーであれば、リモート デスクトップ サービスを使用して対象コンピュータにリモートから接続できます。 このポリシー設定を無効にすると、リモート デスクトップ サービスを使用して対象コンピュータにリモートから接続できなくなります。対象コンピュータは現在の接続を維持しますが、新しい受信接続は受け入れません。 このポリシー設定を構成しない場合、リモート デスクトップ サービスは対象コンピュータのリモート デスクトップ設定を確認し、リモート接続を許可するかどうか決めます。この設定は、[システム プロパティ] の [リモート] タブにあります。デフォルトでは、リモート接続は許可されません。 **注:** 「リモート接続にネットワーク レベル認証を使用したユーザー認証を必要とする」ポリシー設定を構成すると、リモート デスクトップ サービスを使用してリモート クライアントからの接続を制限できます。この設定を行うには、[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] - [セキュリティ] の順に移動します。同時に接続できるユーザーの数を制限するには、リモート デスクトップ セッション ホスト構成ツールの [ネットワーク アダプター] タブにある [最大接続数] オプションを構成するか、「接続数を制限する」ポリシー設定を構成します。この設定を行うには、[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] - [接続] の順に移動します。

設定	説明
Deny logoff of an administrator logged in to the console session	このポリシー設定では、サーバのコンソールにリモート接続しようとしている管理者が、そのコンソールに現在ログインしている管理者をログオフできるかどうかを指定します。 このポリシーは、現在接続している管理者が別の管理者によってログオフされないようにする場合に役立ちます。接続中の管理者がログオフすると、未保存のデータはすべて失われます。 このポリシー設定を有効にすると、接続している管理者のログオフはできません。 このポリシー設定を無効にするか、構成しない場合、接続している管理者をログオフできます。 **注:** コンソール セッションはセッション 0 となります。コンソール アクセスは、コンピュータ フィールド名のリモート デスクトップ接続またはコマンド ラインから /console スイッチを使用して取得できます。
Configure keep-alive connection interval	このポリシー設定では、キープアライブ間隔を入力し、RDS ホスト上のセッション状態とクライアント状態の一貫性を保つことができます。 クライアントが RDS ホストとの接続を失った後、クライアントが物理的に RDS ホストから切断されていても、RDS ホストのセッションが切断状態にはならず、引き続きアクティブなままである可能性があります。クライアントが再び同じ RDS ホストにログインすると、新しいセッションが確立され (RDS ホストが複数のセッションを許可している場合)、元のセッションがアクティブなまま残る可能性があります。 このポリシー設定を有効にする場合、キープアライブ間隔を入力する必要があります。キープアライブ間隔により、サーバがセッション状態を確認する間隔（分単位）が決まります。入力可能な値の範囲は 1 から 999,999 です。 このポリシー設定を無効にするか、構成しない場合は、キープアライブ間隔は設定されず、サーバはセッションの状態を確認しません。
Limit number of connections	リモート デスクトップ サービスがサーバへの同時接続数を制限するかどうかを指定します。 この設定を使用すると、サーバでアクティブなリモート デスクトップ サービス セッションの数を制限できます。この数値を超過し、別のユーザーが接続を試みると、サーバがビジー状態のため後でもう一度やり直すように指示するエラー メッセージが表示されます。セッション数を制限すると、システム リソースを必要とするセッションが減るため、パフォーマンスが向上します。デフォルトでは、RDS ホストには数に制限のないリモート デスクトップ サービス セッションが許可され、管理用リモート デスクトップには 2 つのリモート デスクトップ サービス セッションが許可されます。 この設定を使用するには、サーバの最大接続数を入力します。接続数を制限しない場合は 999999 を入力します。 このポリシー設定を有効にすると、サーバで実行している Windows のバージョンおよびリモート デスクトップ サービスのモードに応じて、指定された数に接続の最大数が制限されます。 このポリシー設定を無効にするか、構成しない場合、グループ ポリシー レベルで接続数の制限は強制的に適用されません。 **注:** この設定は、RDS ホスト（リモート デスクトップ セッション ホスト ロール サービスがインストールされた Windows オペレーティング システムを実行しているサーバ）で使用されるように設計されています。

設定	説明
Set rules for remote control of Remote Desktop Services user sessions	このポリシー設定では、リモート デスクトップ サービス セッションで許可されるリモート制御レベルを指定します。 このポリシー設定を使用すると、「セッション表示」と「フル コントロール」のいずれかのリモート制御レベルを選択できます。セッション表示では、リモート制御のユーザーにセッションの表示を許可します。フル コントロールでは、管理者にセッションの操作を許可します。リモート制御は、ユーザー権限の有無にかかわらず確立できます。 このポリシー設定を有効にすると、管理者は、指定されたルールに従ってユーザーのリモート デスクトップ サービス セッションをリモートから操作できます。これらのルールを設定するには、オプション リストから必要な制御と権限のレベルを選択します。リモート制御を無効にするには、[リモート制御を許可しない] を選択します。 このポリシー設定を無効にするか、構成しない場合、リモート制御のルールは、リモート デスクトップ セッション ホスト構成ツールの [リモート制御] タブの設定で決まります。デフォルトでは、ユーザーの権限があれば、セッションに対するフル コントロールがリモート制御のユーザーに許可されます。 **注:** このポリシー設定は、[コンピュータの構成] と [ユーザーの構成] の両方に表示されます。両方のポリシー設定を指定した場合、[コンピュータの構成] のポリシー設定が優先されます。
Restrict Remote Desktop Services users to a single Remote Desktop Services session	このポリシー設定では、ユーザーに 1 つのリモート デスクトップ サービス セッションのみを許可します。 このポリシー設定を有効にすると、リモート デスクトップ サービスを使用してリモートからログインするユーザーは、そのサーバ上で 1 つのセッション（アクティブまたは切断状態）のみを使用できます。ユーザーが切断状態でセッションを離れると、次のログイン時に同じセッションに自動的に接続されます。 このポリシー設定を無効にすると、数に制限なく、リモート デスクトップ サービスを使用してリモートから同時接続を確立できます。 このポリシー設定を構成しないと、リモート デスクトップ セッション ホスト構成ツールの [各ユーザーを 1 セッションに制限する] 設定により、ユーザーが 1 つのリモート デスクトップ サービス セッションに制限されるかどうかが決まります。

設定	説明
Allow remote start of unlisted programs	このポリシー設定では、リモート デスクトップ サービス セッションの開始時にリモート ユーザーが RDS ホスト上の任意のプログラムを開始できるか、RemoteApp プログラムのリストにあるプログラムのみを開始できるかを指定します。 RemoteApp マネージャで RemoteApp プログラムのリストを作成することで、RDS ホストでリモートから開始可能なプログラムを制御できます。デフォルトでは、ユーザーがリモート デスクトップ サービス セッションの開始時に開始できるプログラムは RemoteApp プログラムのリストにあるプログラムのみです。 このポリシー設定を有効にすると、リモート ユーザーはリモート デスクトップ サービス セッションの開始時に RDS ホスト上の任意のプログラムを開始できます。たとえば、リモート デスクトップ接続のクライアントを使用して、接続時にプログラムの実行可能ファイルのパスを指定すると、そのプログラムを開始できます。 このポリシー設定を無効にするか、構成しない場合、リモート ユーザーはリモート デスクトップ サービス セッションの開始時に RemoteApp マネージャの RemoteApp プログラム リストにあるプログラムのみを開始できます。
Turn off Fair Share CPU Scheduling	CPU スケジュール設定の公平なシェアは、同じ RDS ホスト上のすべてのリモート デスクトップ サービス セッション間で、セッションの数と、各セッション内でのプロセッサ時間の要求に基づき、プロセッサ時間を動的に分散します。 このポリシー設定を有効にすると、CPU スケジュール設定の公平なシェアはオフになります。 このポリシー設定を無効にするか、または構成しない場合、CPU スケジュール設定の公平なシェアはオンになります。

RDS デバイスおよびリソースのリダイレクトの設定

RDS デバイスおよびリソース リダイレクト グループ ポリシー設定により、リモート デスクトップ サービス セッションのクライアント コンピュータのデバイスおよびリソースへのアクセスを制御します。

Horizon 7 RDS グループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [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] フォルダにインストールされています。

Horizon 7 RDS グループ ポリシー設定は、[ユーザーの構成] - [管理用テンプレート] - [Windows コンポーネント] - [リモート デスクトップ サービス] - [リモート デスクトップ セッション ホスト] - [デバイスとリソースのリダイレクト] フォルダにもインストールされています。

表 5-16. RDS デバイスおよびリソース リダイレクト グループ ポリシー設定

設定	説明
Allow audio and video playback redirection	このポリシー設定では、リモート デスクトップ サービス セッションでユーザーがリモート コンピュータのオーディオ出力とビデオ出力をリダイレクトできるかどうかを指定します。 リモート デスクトップ接続 (RDC) の [ローカル リソース] タブでリモート オーディオの設定を構成すると、リモート コンピュータのオーディオ出力の再生場所を指定できます。また、リモート オーディオをリモート コンピュータで再生するか、ローカル コンピュータで再生するかも選択できます。オーディオを再生しないように選択することもできます。ビデオ再生を構成するには、リモート デスクトップ プロトコル (.rdp) ファイルの videoplayback 設定を使用します。デフォルトでは、ビデオ再生は有効になっています。 デフォルトでは、Windows Server 2008 R2、Windows Server 2008 または Windows Server 2003 を実行しているコンピュータに接続している場合、オーディオ再生とビデオ再生のリダイレクトは許可されません。デフォルトでは、Windows 7、Windows Vista または Windows XP Professional を実行しているコンピュータに接続している場合、オーディオ再生とビデオ再生のリダイレクトが許可されます。 このポリシー設定を有効にすると、オーディオ再生とビデオ再生のリダイレクトが許可されます。 このポリシー設定を無効にすると、オーディオ再生のリダイレクトが RDC で指定されている場合またはビデオ再生が .rdp ファイルで指定されている場合でも、オーディオ再生とビデオ再生のリダイレクトは許可されません。 このポリシー設定を構成しない場合、リモート デスクトップ セッション ホスト構成ツールの [クライアントの設定] タブにある [オーディオおよびビデオの再生] の設定で、オーディオ再生とビデオ再生のリダイレクトが許可されるかどうかが決まります。
Allow audio recording redirection	このポリシー設定では、リモート デスクトップ サービス セッション中にリモート コンピュータにオーディオ録音を行うかどうかを指定します。 リモート デスクトップ接続 (RDC) の [ローカル リソース] タブでリモート オーディオの設定を構成すると、リモート コンピュータにオーディオ録音を行うかどうかを指定できます。ローカル コンピュータで内蔵マイクなどのオーディオ入力デバイスを使用してオーディオを録音できます。 デフォルトでは、Windows Server 2008 R2 を実行しているコンピュータに接続している場合、オーディオ録音のリダイレクトは許可されません。デフォルトでは、Windows 7 を実行しているコンピュータに接続している場合、オーディオ録音のリダイレクトが許可されます。 このポリシー設定を有効にすると、オーディオ録音のリダイレクトが許可されます。 このポリシー設定を無効にすると、オーディオ録音のリダイレクトが RDC で指定されている場合でも、オーディオ録音のリダイレクトは許可されません。 このポリシー設定を構成しない場合、リモート デスクトップ セッション ホスト構成ツールの [クライアントの設定] タブにある [オーディオ録音の再生] の設定で、オーディオ録音のリダイレクトが許可されるかどうかが決まります。

設定	説明
Limit audio playback quality	このポリシー設定では、リモート デスクトップ サービス セッションのオーディオ再生品質を制限します。オーディオ再生品質を制限すると、接続のパフォーマンスが向上します（特に低速リンクの場合）。 このポリシー設定を有効にする場合、[高]、[中] または [動的] のいずれかを選択する必要があります。[高] を選択すると、オーディオは圧縮されずに送信され、待ち時間が最小になります。この場合は、大量のバンド幅が必要になります。[中] を選択すると、使用されているコーデックに応じてオーディオが圧縮されて送信されます。待ち時間も最小になります。[動的] を選択すると、オーディオ送信時に圧縮レベルがリモート接続のバンド幅によって決まります。 このポリシー設定を使用してリモート コンピュータで指定したオーディオの再生品質は、クライアント コンピュータのオーディオ再生品質に関係なく、リモート デスクトップ サービス セッションで使用可能な最高音質になります。たとえば、クライアント コンピュータのオーディオ再生品質がリモート コンピュータのオーディオ再生品質よりも高い場合、使用されるオーディオ再生品質は低くなります。 オーディオ再生品質は、クライアント コンピュータでリモート デスクトップ プロトコル (.rdp) ファイルの audioqualitymode 設定で構成します。デフォルトのオーディオ再生品質は [動的] に設定されています。
Do not allow clipboard redirection	リモート デスクトップ サービス セッションで、リモート コンピュータとクライアント コンピュータ間でクリップボード共有（クリップボードのリダイレクト）を防止するかどうかを指定します。 この設定を使用すると、リモート コンピュータやローカル コンピュータへのクリップボード データのリダイレクトを防止できます。デフォルトでは、リモート デスクトップ サービスによるクリップボードのリダイレクトは許可されています。 このポリシー設定を有効にすると、クリップボード データのリダイレクトはできません。 このポリシー設定を無効にすると、リモート デスクトップ サービスは常にクリップボードのリダイレクトを許可します。 この設定を構成しないと、グループ ポリシー レベルでクリップボードのリダイレクトが指定されません。ただし、管理者がリモート デスクトップ セッション ホスト構成ツールを使用して、クリップボードのリダイレクトを無効にできます。
Do not allow COM port redirection	リモート デスクトップ サービス セッションのリモート コンピュータからクライアント COM ポートへのデータのリダイレクトを防止するかどうかを指定します。 この設定を使用すると、リモート デスクトップ サービス セッションにログイン中、COM ポート周辺機器へのデータのリダイレクトや、ローカル COM ポートのマッピングを防止できます。デフォルトでは、リモート デスクトップ サービスによる COM ポートのリダイレクトは許可されています。 このポリシー設定を有効にすると、サーバ データをローカル COM ポートにリダイレクトできません。 このポリシー設定を無効にすると、リモート デスクトップ サービスは常に COM ポートのリダイレクトを許可します。 この設定を構成しないと、グループ ポリシー レベルで COM ポートのリダイレクトが指定されません。ただし、管理者がリモート デスクトップ セッション ホスト構成ツールを使用して、COM ポートのリダイレクトを無効にできます。

設定	説明
Do not allow drive redirection	リモート デスクトップ サービス セッションで、クライアント ドライブのマッピング（ドライブ リダイレクト）を防止するかどうかを指定します。 デフォルトでは、接続時に RD セッション ホスト サーバが自動的にクライアント ドライブをマッピングします。マッピングされたドライブは、Windows エクスプローラまたは [コンピュータ] のセッション フォルダ ツリーに、<コンピュータ名> の <ドライブ文字> という形式で表示されます。この設定を使用すると、この動作を上書きできます。 このポリシー設定を有効にすると、リモート デスクトップ サービス セッションでクライアント ドライブのリダイレクトが許可されません。 このポリシー設定を無効にすると、クライアント ドライブのリダイレクトは常に許可されます。 この設定を構成しないと、グループ ポリシー レベルでクライアント ドライブのリダイレクトが指定されません。ただし、管理者がリモート デスクトップ セッション ホスト構成ツールを使用して、クライアント ドライブのリダイレクトを無効にできます。
Do not allow LTP Port redirection	リモート デスクトップ サービス セッションでクライアント LPT ポートへのデータのリダイレクトを防止するかどうかを指定します。 この設定を使用すると、ローカル LPT ポートへのマッピングや、リモート コンピューターからローカル LPT ポート周辺機器へのデータ リダイレクトを防止できます。デフォルトでは、リモート デスクトップ サービスによる LPT ポートのリダイレクトは許可されています。 このポリシー設定を有効にすると、リモート デスクトップ サービス セッションでサーバ データをローカル LPT ポートにリダイレクトできません。 このポリシー設定を無効にすると、LPT ポートのリダイレクトは常に許可されます。 この設定を構成しないと、グループ ポリシー レベルで LPT ポートのリダイレクトが指定されません。ただし、管理者がリモート デスクトップ セッション ホスト構成ツールを使用して、LPT ポートのリダイレクトを無効にできます。
Do not allow supported Plug and Play device redirection	このポリシー設定では、リモート デスクトップ サービス セッションでサポートされているプラグ アンド プレイ デバイス（Windows ポータブル デバイスなど）のリモート コンピュータへのリダイレクトを制御します。 デフォルトでは、サポートされているプラグ アンド プレイ デバイスのリダイレクトは、リモート デスクトップ サービスに許可されています。リモート デスクトップ接続の [ローカル リソース] タブにある [その他] のオプションを使用すると、サポートされているプラグ アンド プレイ デバイスを選択して、リモート コンピュータにリダイレクトできます。 このポリシー設定を有効にすると、サポートされているプラグ アンド プレイ デバイスをリモート コンピュータにリダイレクトできません。 このポリシー設定を無効にするか、構成しない場合、サポートされているプラグ アンド プレイ デバイスをリモート コンピュータにリダイレクトできます。 **注:** リモート デスクトップ セッション ホスト構成ツールの [クライアントの設定] タブで、サポートされているプラグ アンド プレイ デバイスのリダイレクトを許可しないように設定できます。サポート対象の特定のプラグ アンド プレイ デバイスのリダイレクトを許可しないように設定するには、[コンピューターの構成] - [管理用テンプレート] - [システム] - [デバイスのインストール] - [デバイスのインストールの制限] の順に移動します。

設定	説明
Do not allow smart card device redirection	このポリシー設定では、リモート デスクトップ サービス セッションでスマート カード デバイスのリダイレクトを制御します。 このポリシー設定を有効にすると、リモート デスクトップ サービスのユーザーは、スマート カードでリモート デスクトップ サービス セッションにログインできなくなります。 このポリシー設定を無効にするか、構成しない場合、スマート カード デバイスのリダイレクトは許可されます。デフォルトでは、接続時にリモート デスクトップ サービスはスマート カード デバイスを自動的にリダイレクトします。 **注:** クライアント コンピュータで、Microsoft Windows 2000 Server 以降または Microsoft Windows XP Professional 以降が実行され、ターゲット サーバがドメインに参加している必要があります。
Allow time zone redirection	このポリシー設定は、クライアント コンピュータがタイム ゾーン設定をリモート デスクトップ サービス セッションにリダイレクトするかどうかを決定します。 このポリシー設定を有効にすると、タイム ゾーン リダイレクトが可能なクライアントはタイム ゾーン情報をサーバに送信します。サーバ ベースの時間は現在のセッション時間を計算するために使用されます（現在のセッション時間 = サーバ ベースの時間 + クライアント タイム ゾーン）。 このポリシー設定を無効にする場合、または構成しない場合、クライアント コンピュータはタイム ゾーン情報をリダイレクトしません。セッション タイム ゾーンはサーバ タイム ゾーンと同じです。

RDS ライセンスの設定

RDS ライセンス グループ ポリシー設定では、RDS ライセンス サーバが参照される順番、問題通知を表示するかどうか、RDS クライアント アクセス ライセンス (CAL) でユーザーごとのライセンスまたはデバイスごとのライセンスのどちらを使用するかを管理します。

Horizon 7 RDS グループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [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] - [ライセンス] フォルダにインストールされています。

表 5-17. RDS ライセンス グループ ポリシー設定

設定	説明
Use the specified Remote Desktop license servers	このポリシー設定により、リモート デスクトップ ライセンス サーバが RDS ホスト サーバを探す順番を指定できます。 このポリシーを有効にすると、RDS ホスト サーバは指定されたライセンス サーバを最初に探します。指定されたライセンス サーバが見つからない場合、RDS ホスト サーバにより自動ライセンス サーバ検出が試行されます。 自動ライセンス サーバ検出では、Windows Server ベースのドメイン内の RDS ホスト サーバにより、次の順番でライセンス サーバへのアクセスが試行されます。 1 リモート デスクトップ セッション ホスト構成ツールで指定されたライセンス サーバ。 2 Active Directory ドメイン サービスで公開されたライセンス サーバ。 3 RDS ホストと同じドメインのドメイン コントローラ上にインストールされたライセンス サーバ。 このポリシー設定を無効にするか、構成しなかった場合、RDS ホストでは、リモート デスクトップ セッション ホスト構成ツールで指定されたライセンス サーバ検出モードが使用されます。
Hide notifications about RD Licensing problems that affect the RD Session Host server	このポリシー設定により、RDS ホストに影響する RD ライセンスに問題がある場合、RDS ホストに通知を表示するかどうかを決定します。 デフォルトでは、RDS ホストに影響する RD ライセンスに問題がある場合、ローカル管理者としてログインした後に RDS ホストに通知が表示されます。RDS ホストのライセンス有効期間が切れるまでの日数も通知されます（該当する場合）。 このポリシー設定を有効にすると、これらの通知は RDS ホストに表示されません。 このポリシー設定を無効にするか、構成しなかった場合、ローカル管理者としてログインした後に、RDS ホストにこれらの通知が表示されます。
Set the Remote Desktop licensing mode	このポリシー設定により、この RDS ホストへの接続に必要なリモート デスクトップ サービス クライアント アクセス ライセンス (RDS CAL) のタイプを指定できます。 このポリシー設定では、ユーザーごとまたはデバイスごとのいずれかのライセンス モデルを選択できます。 接続ユーザー数によるライセンス モードでは、この RDS ホストに接続する各ユーザー アカウントには、RDS CAL（接続ユーザー数）が必要になります。 接続デバイス数によるライセンス モードでは、この RDS ホストに接続する各デバイスには、RDS CAL（接続デバイス数）が必要になります。 このポリシー設定を有効にすると、ここで指定したライセンス モードは、リモート デスクトップ セッション ホストのインストール時に指定した、またはリモート デスクトップ セッション ホスト構成ツールで指定したライセンス モードに優先します。 このポリシー設定を無効にするか、構成しなかった場合、リモート デスクトップ セッション ホスト ロール サービスのインストール時に指定した、またはリモート デスクトップ セッション ホスト構成ツールで指定したライセンス モードが使用されます。

RDS プリンタ リダイレクトの設定

RDS プリンタ リダイレクトのグループ ポリシー設定を使用すると、プリンタ リダイレクトのポリシーを設定できます。

Horizon 7 RDS グループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [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] - [プリンタ リダイレクト] フォルダにインストールされています。

Horizon 7 RDS グループ ポリシー設定は、[ユーザーの構成] - [管理用テンプレート] - [Windows コンポーネント] - [リモート デスクトップ サービス] - [リモート デスクトップ セッション ホスト] - [プリンタ リダイレクト] フォルダにもインストールされています。

表 5-18. RDS プリンタ リダイレクトのグループ ポリシー設定

設定	説明
Do not set default client printer to be default printer in a session	このポリシー設定では、クライアントのデフォルト プリンタが RDS ホスト セッションのデフォルト プリンタに自動的に設定されるかどうかを指定します。 デフォルトでは、リモート デスクトップ サービスはクライアントのデフォルト プリンタを RDS ホスト セッションのデフォルト プリンタに自動的に設定します。このポリシー設定を使用すると、この動作を上書きできます。 このポリシー設定を有効にすると、リモート コンピュータで指定されたプリンタがデフォルト プリンタになります。 このポリシー設定を無効にすると、RDS ホストがクライアントのデフォルト プリンタを自動的にマッピングし、接続時にこのプリンタをデフォルト プリンタに設定します。 このポリシーを設定しない場合、グループ ポリシー レベルではデフォルト プリンタが指定されません。ただし、管理者がリモート デスクトップ セッション ホスト構成ツールを使用して、クライアント セッションのデフォルト プリンタを構成できます。
Do not allow client printer redirection	このポリシー設定では、リモート デスクトップ サービス セッションでのクライアント プリンタのマッピングを無効にするかどうかを指定します。 このポリシー設定を使用すると、リモート コンピュータからローカル (クライアント) コンピュータに接続されているプリンタへの印刷ジョブのリダイレクトを防ぐことができます。デフォルトでは、リモート デスクトップ サービスはこのクライアント プリンタ マッピングを許可します。 このポリシー設定を有効にすると、ユーザーは、リモート デスクトップ サービス セッションで、リモート コンピュータからローカル クライアントのプリンタに印刷ジョブをリダイレクトできません。 このポリシー設定を無効にすると、ユーザーはクライアント プリンタ マッピングを使用して印刷ジョブをリダイレクトできます。 このポリシーを設定しない場合、グループ ポリシー レベルではクライアント プリンタ マッピングが指定されません。ただし、管理者がリモート デスクトップ セッション ホスト構成ツールを使用して、クライアント プリンタ マッピングを無効にできます。

設定	説明
Use Remote Desktop Easy Print printer driver first	このポリシー設定では、クライアント プリンタのインストール時にリモート デスクトップ Easy Print プリンタ ドライバを最初に使用するかどうかを指定します。 このポリシー設定を有効にするか、構成しない場合、クライアント プリンタのインストール時に RDS ホストは最初にリモート デスクトップ Easy Print プリンタ ドライバを使用します。何らかの理由でリモート デスクトップ Easy Print プリンタ ドライバが使用できない場合、RDS ホスト上でクライアント プリンタに対応するプリンタ ドライバが使用されます。クライアント プリンタに対応するプリンタ ドライバが RDS ホストにない場合、リモート デスクトップ セッションでクライアント プリンタを使用することはできません。 このポリシー設定を無効にすると、RDS ホストは適切なプリンタ ドライバを検索して、クライアント プリンタをインストールします。クライアント プリンタに対応するプリンタ ドライバが RDS ホストにない場合、RDS ホストはリモート デスクトップ Easy Print ドライバを使用してクライアント プリンタのインストールを試みます。何らかの理由でリモート デスクトップ Easy Print プリンタ ドライバが使用できない場合、リモート デスクトップ サービス セッションでクライアント プリンタを使用することはできません。 **注:** 「クライアント プリンタのリダイレクトを許可しない」ポリシー設定を有効にすると、「リモート デスクトップ Easy Print プリンタ ドライバを最初に使う」ポリシー設定は無視されます。

設定	説明
Specify RD Session Host Server fallback printer driver behavior	このポリシー設定では、RDS ホストのフォールバック プリンタ ドライバの動作を指定します。 デフォルトでは、RDS ホストのフォールバック プリンタ ドライバは無効になっています。クライアント プリンタに対応するプリンタ ドライバが RDS ホストにない場合、リモート デスクトップ サービス セッションでプリンタを使用することはできません。 このポリシー設定を有効にすると、フォールバック プリンタ ドライバが有効になります。デフォルトでは、RDS ホストが適切なプリンタ ドライバを検索します。プリンタ ドライバが見つからない場合、クライアントのプリンタは使用できません。このデフォルトの動作は変更できます。使用可能なオプションは次のとおりです。 ■ Do nothing if one is not found。プリンタ ドライバが一致しない場合、RDS ホストは適切なドライバを検索します。見つからない場合、クライアントのプリンタは使用できません。これがデフォルトの動作です。 ■ Default to PCL if one is not found。適切なプリンタ ドライバが見つからない場合、プリンタ制御言語 (PCL) のフォールバック プリンタ ドライバがデフォルトで使用されます。 ■ Default to PS if one is not found。適切なプリンタ ドライバが見つからない場合、PostScript (PS) のフォールバック プリンタ ドライバがデフォルトで使用されます。 ■ Show both PCL and PS if one is not found。適切なプリンタ ドライバが見つからない場合、PS と PCL の両方のフォールバック プリンタ ドライバが表示されます。 このポリシー設定を無効にすると、RDS ホスト フォールバック ドライバが無効になり、RDS ホストはフォールバック プリンタ ドライバを使用しません。 このポリシーを設定しない場合、デフォルトのフォールバック プリンタ ドライバの動作は無効になります。 **注:** 「クライアント プリンタのリダイレクトを許可しない」設定を有効にすると、このポリシー設定は無視され、フォールバック プリンタ ドライバが無効になります。
Redirect only the default client printer	このポリシー設定では、リモート デスクトップ サービス セッションへのリダイレクトをデフォルトのクライアント プリンタに限定するかどうかを指定します。 このポリシー設定を有効にすると、デフォルトのクライアント プリンタだけがリモート デスクトップ サービス セッションにリダイレクトされます。 このポリシー設定を無効にするか、構成しない場合、すべてのクライアント プリンタがリモート デスクトップ サービス セッションでリダイレクトされます。

RDS プロファイルの設定

RDS プロファイル グループ ポリシー設定では、リモート デスクトップ サービス セッションの移動プロファイルおよびホーム ディレクトリの設定を制御します。

表 5-19. RDS プロファイル グループ ポリシー設定

設定	説明
Limit the size of the entire roaming user profile cache	このポリシー設定により、ローカル ドライブ上の移動ユーザー プロファイルのキャッシュ全体のサイズを制限できます。このポリシー設定は、リモート デスクトップ セッション ホスト ロール サービスがインストールされているコンピュータにのみ適用されます。 **注:** 個別のユーザー プロファイルのサイズを制限する場合は、[User Configuration\Policies\Administrative Templates\System\User Profiles] にある `Limit profile size` ポリシー設定を使用します。 このポリシー設定を有効にする場合は、移動ユーザー プロファイルのキャッシュ全体の監視間隔（分単位）と最大サイズ（ギガバイト単位）を指定する必要があります。監視間隔で、移動ユーザー プロファイルのキャッシュ全体のサイズをチェックする頻度を決定します。移動ユーザー プロファイルのキャッシュ全体のサイズが指定した最大サイズを超えると、下回るまで最も古い（最も長く使われていない）移動ユーザー プロファイルが削除されます。 このポリシー設定を無効にする、または構成しない場合、ローカル ドライブ上の移動ユーザー プロファイルのキャッシュ全体のサイズに制限は設定されません。 注：[Computer Configuration\Policies\Administrative Templates\System\User Profiles] にある `Prevent Roaming Profile changes from propagating to the server` ポリシー設定が有効になっている場合、このポリシー設定は無視されます。
Set Remote Desktop Services User Home Directory	リモート デスクトップ サービスが、指定されたネットワーク共有またはローカル ディレクトリ パスを、リモート デスクトップ サービス セッションでユーザーのホーム ディレクトリのルートとして使用するかどうかを指定します。 この設定を使用するには、[場所] ドロップダウン リストからホーム ディレクトリ（ネットワークまたはローカル）の場所を選択します。ディレクトリをネットワーク共有に置く場合は、ホーム ディレクトリのルート パスを `\\Computername\Sharename` の形式で入力してから、ネットワーク共有をマッピングするドライブ文字を選択します。 ホーム ディレクトリをローカル コンピュータに保持する場合は、ホーム ディレクトリのルート パスを環境変数や省略記号なしで `Drive:\Path` の形式で入力します。ログイン時にリモート デスクトップ サービスで自動的に追加されるため、ユーザー エイリアスのプレースホルダは指定しないでください。 **注:** ローカル パスを指定する場合、[ドライブ レター] フィールドは無視されます。ローカル パスを指定することを選択したが、ホーム ディレクトリのルート パスにネットワーク共有名を入力した場合、リモート デスクトップ サービスはユーザーのホーム ディレクトリをネットワーク上の場所に配置します。 ステータスが [有効] に設定されている場合、リモート デスクトップ サービスはユーザーのホーム ディレクトリを、ローカル コンピュータまたはネットワーク上で指定した場所に作成します。各ユーザーのホーム ディレクトリのパスは、指定されたホーム ディレクトリのルート パスおよびユーザーのエイリアスです。 ステータスが [無効] または [構成されていません] に設定されている場合、ユーザーのホーム ディレクトリはサーバで指定されたものになります。

設定	説明
Use mandatory profiles on the RD Session Host server	このポリシー設定により、RDS ホストにリモートで接続しているすべてのユーザーについて、リモート デスクトップ サービスが必須のプロファイルを使用するかどうかを指定できます。 このポリシー設定を有効にした場合、リモート デスクトップ サービスは Set path for Remote Desktop Services Roaming User Profile ポリシー設定で指定したパスを、必須のユーザー プロファイルのルート フォルダとして使用します。RDS ホストにリモートで接続しているすべてのユーザーは、同じユーザー プロファイルを使用します。 このポリシー設定を無効にする、または構成しない場合、RDS ホストにリモートで接続しているユーザーは必須のユーザー プロファイルを使用しません。 **注:** このポリシー設定を有効にするには、Set path for Remote Desktop Services Roaming User Profile ポリシー設定も有効にして構成する必要があります。
Set path for Remote Desktop Services Roaming User Profile	このポリシー設定では、リモート デスクトップ サービスが移動ユーザー プロファイルに使用するネットワーク パスを指定できます。 デフォルトでは、リモート デスクトップ サービスはすべてのユーザー プロファイルを RDS ホストのローカルに保存します。このポリシー設定を使用して、ユーザープロファイルを一元的に保存できるネットワーク共有を指定できます。これにより、ユーザーはユーザー プロファイルにネットワーク共有を使用するように構成されているすべての RDS ホスト上のセッションで、同じプロファイルにアクセスできます。 このポリシー設定を有効にすると、リモート デスクトップ サービスは指定されたパスをすべてのユーザー プロファイルのルート ディレクトリとして使用します。このプロファイルは、各ユーザーのアカウント名が名前として付けられたサブフォルダに含まれます。 このポリシー設定を行うには、ネットワーク共有へのパスを \\Computername\Sharename の形式で入力します。ユーザーがログインしてプロファイルが作成される際にリモート デスクトップ サービスで自動的に追加されるため、ユーザー アカウント名のプレースホルダは指定しないでください。指定したネットワーク共有が存在しない場合、リモート デスクトップ サービスにより RDS ホストにエラー メッセージが表示され、ユーザー プロファイルは RDS ホスト上のローカルに保存されます。 このポリシー設定を無効にする、または構成しない場合、ユーザー プロファイルは RDS ホスト上のローカルに保存されます。ユーザーのアカウントの [プロパティ] ダイアログ ボックスの [リモート デスクトップ サービス プロファイル] タブで、ユーザーのプロファイルのパスを構成できます。 注： 1 ポリシー設定によって有効になる移動ユーザー プロファイルは、リモート デスクトップ サービス接続にのみ適用されます。Windows 移動ユーザー プロファイルを構成させる場合もあります。リモート デスクトップ サービスの移動ユーザー プロファイルは、常にリモート デスクトップ サービス セッションで優先されます。 2 RDS ホストにリモートで接続しているすべてのユーザーについて、必須のリモート デスクトップ サービスの移動ユーザー プロファイルを構成するには、このポリシー設定を [Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\RD Session Host\Profiles] にある Use mandatory profiles on the RD Session Host server ポリシー設定とともに使用します。Set path for Remote Desktop Services Roaming User Profile ポリシー設定で設定するパスには、必須のプロファイルを含める必要があります。

RDS 接続サーバ設定

RDS 接続サーバのグループ ポリシー設定を使用すると、接続サーバのポリシーを設定できます。

Horizon 7 RDS グループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [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] - [RD 接続ブローカ] フォルダにインストールされています。

表 5-20. RDS 接続サーバのグループ ポリシー設定

設定	説明
Join RD Connection Broker	このポリシー設定では、RDS ホストが RDS ホストにインストールされた接続サーバのファームに参加するかどうかを指定します。RDS ホストの接続サーバは、ユーザー セッションを追跡し、ロードバランシングされた RDS ファームの既存セッションへの再接続をユーザーに許可します。RDS ホストの接続サーバに参加するには、リモート デスクトップ セッション ホスト ロール サービスが RDS ホストにインストールされている必要があります。 このポリシー設定を有効にすると、RDS ホストは「RD 接続ブローカ ファーム名を構成する」設定で指定されたファームに参加します。このファームは、「RD 接続ブローカ サーバ名を構成する」ポリシー設定に指定された接続サーバ上にあります。 このポリシー設定を無効にすると、RDS ホストは接続サーバのファームに参加せず、ユーザー セッションは追跡されません。この設定を無効にすると、リモート デスクトップ セッション ホスト構成ツールまたはターミナル サービス WMI プロバイダを使用して、接続サーバに参加するように RDS ホストを構成できなくなります。 このポリシー設定を構成しない場合、この設定はグローバル ポリシー レベルで指定されません。この場合、リモート デスクトップ セッション ホスト構成ツールまたはターミナル サービス WMI プロバイダを使用して、RDS ホストの接続サーバに参加するように RDS ホストを構成できます。 **注:** 1 この設定を有効にする場合には、「RD 接続ブローカ ファーム名を構成する」と「RD 接続ブローカ サーバ名を構成する」ポリシー設定も有効にする必要があります。あるいは、リモート デスクトップ セッション ホスト構成ツールまたはターミナル サービス WMI プロバイダを使用して、これらの設定を構成する必要があります。 2 Windows Server 2008 の場合、このポリシーを使用するには Windows Server 2008 Standard 以上が必要です。
Configure RD Connection Broker farm name	このポリシー設定では、RDS ホストが参加する接続サーバのファーム名を指定します。接続サーバは、ファーム名を使用して、同じ RDS ファームにある RDS ホストを特定します。したがって、ロードバランシングされた同じファームの RDS ホストには、同じファーム名を使用する必要があります。ファーム名は、Active Directory ドメイン サービスの名前に対応していません。 新しいファーム名を指定すると、RDS ホストの新しいファームが接続サーバに作成されます。既存のファーム名を指定すると、RDS ホストは RDS ホストの接続サーバのファームに参加します。 このポリシー設定を有効にした場合、RDS ホストに接続サーバのファーム名を指定する必要があります。 このポリシー設定を無効にするか、構成しない場合、ファーム名はグループ ポリシー レベルで指定されません。この場合、リモート デスクトップ セッション ホスト構成ツールまたはターミナル サービス WMI プロバイダを使用してファーム名を調整できます。 **注:** Windows Server 2008 の場合、このポリシーを使用するには Windows Server 2008 Standard 以上が必要です。この設定は、「RD 接続ブローカーへの参加」と「RD 接続ブローカ サーバ名を構成する」の設定がともに有効で、グループ ポリシー、リモート デスクトップ セッション ホスト構成ツールまたはターミナル サービス WMI プロバイダで構成されていない限り、無効になります。

設定	説明
Use IP Address Redirection	このポリシー設定では、クライアント デバイスがロードバランシングされた RDS ファームの既存のリモート デスクトップ サービス セッションに再接続するときのリダイレクト方法を指定します。この設定は、RDS ホストの接続サーバを使用する RDS ホストに適用されます。リモート デスクトップの接続サーバを使用するホストには適用されません。 このポリシー設定を有効にした場合、リモート デスクトップ サービス クライアントは RDS ホストの接続サーバにクエリを送信し、セッションがある RDS ホストの IP アドレスを使用して既存のセッションにリダイレクトします。このリダイレクト方法では、クライアント コンピュータが IP アドレスでファーム内の RDS ホストに直接接続できる必要があります。 このポリシー設定を無効にすると、RDS ホストの IP アドレスはクライアントに送信されません。代わりに、IP アドレスはトークンに埋め込まれます。クライアントがロード バランサに再接続すると、ルーティング トークンを使用してファーム内の正しい RDS ホストの既存セッションにクライアントがリダイレクトされます。ネットワークのロードバランス ソリューションで RDS ホストの接続サーバ ルーティング トークンを使用でき、ロード バランシングされたファーム内の RDS ホストに IP アドレスで直接接続しない場合にのみ、この設定を無効にしてください。 このポリシー設定を構成しないと、リモート デスクトップ セッション ホスト構成ツールの「IP アドレス リダイレクトを使用する」の設定が使用されます。デフォルトでは、リモート デスクトップ セッション ホスト構成ツールのこの設定は有効になっています。 **注:** Windows Server 2008 の場合、このポリシーを使用するには Windows Server 2008 Standard 以上が必要です。

設定	説明
Configure RD Connection Broker Server name	このポリシー設定では、ロードバランシングされた RDS ファームの RDS ホストがユーザー セッションの追跡とリダイレクトに使用する接続サーバを指定します。指定する RDS ホストで接続サーバ サービスが実行されている必要があります。ロードバランシングされたファーム内のすべての RDS ホストは、同じ接続サーバを使用する必要があります。 このポリシー設定を有効にする場合、ホスト名、IP アドレスまたは完全修飾ドメイン名を使用して、RDS ホストの接続サーバを指定する必要があります。接続サーバに指定した名前または IP アドレスが無効な場合、RDS ホストのイベント ビューアにエラー メッセージが記録されます。 このポリシー設定を無効にするか、構成しない場合、リモート デスクトップ セッション ホスト構成ツールまたはターミナル サービス WMI プロバイダを使用して、RDS ホストの接続サーバ名または IP アドレスを調整できます。 **注:** ■ Windows Server 2008 の場合、このポリシーを使用するには Windows Server 2008 Standard が必要です。 ■ 「RD 接続ブローカーへの参加」ポリシー設定が有効か、リモート デスクトップ セッション ホスト構成ツールまたはターミナル サービス WMI プロバイダを使用して RDS ホストが RDS ホストの接続サーバに参加するように構成されていない限り、このポリシー設定は無効になります。 ■ RDS ファームで接続サーバが有効になっているセッションのアクティブ メンバーにするには、ファーム内の各 RDS ホストのコンピュータ アカウントが、RDS ホストの接続サーバの「Session Directory Computers」(セッション ディレクトリ コンピュータ) ローカル グループのメンバーにする必要があります。
Use RD Connection Broker load balancing	このポリシー設定では、RDS ホストの接続サーバでロード バランシング機能を使用し、RDS ファーム内のサーバ間で負荷分散を行うかどうかを指定します。 このポリシー設定を有効にすると、RDS ホストの接続サーバは、既存のセッションがないユーザーをファーム内でセッション数の最も少ないファームの RDS ホストにリダイレクトします。既存セッションのユーザーに対するリダイレクト動作の影響はありません。RDS ホストの接続サーバを使用するようにサーバを構成すると、既存セッションのユーザーはセッションがある RDS ホストにリダイレクトされます。 このポリシー設定を無効にすると、既存セッションのないユーザーは、接続した最初の RDS ホストにログインします。 このポリシー設定を構成しない場合、リモート デスクトップ セッション ホスト構成ツールまたはターミナル サービス WMI プロバイダを使用して、RDS ホストの接続サーバ ロード バランシングに参加するように、RDS ホストを構成できます。 **注:** このポリシー設定を有効にする場合、「RD 接続ブローカーへの参加」、「RD 接続ブローカー ファーム名を構成する」、「RD 接続ブローカ サーバ名を構成する」ポリシー設定も有効にする必要があります。

RDS リモート セッション環境の設定

RDS リモート セッション環境のグループ ポリシー設定では、リモート デスクトップ サービス セッションでのユーザー インターフェイスの構成を制御します。

Horizon 7 RDS グループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [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] フォルダにインストールされています。

Horizon 7 RDS グループ ポリシー設定は、[ユーザーの構成] - [管理用テンプレート] - [Windows コンポーネント] - [リモート デスクトップ サービス] - [リモート デスクトップ セッション ホスト] - [リモート セッション環境] フォルダにもインストールされています。

表 5-21. RDS リモート セッション環境のグループ ポリシー設定

設定	説明
Limit maximum color depth	このポリシー設定では、リモート デスクトップ サービス接続で利用できる色の解像度（色の深度）の最大値を指定します。 このポリシー設定では、RDP を使用した接続で使用する色の深度を制限できます。色の深度を制限すると、接続のパフォーマンスが向上し（特に低速リンクの場合）、サーバの負荷が軽減されます。 このポリシー設定を有効にすると、指定した色の深度がユーザーの RDP 接続で使用可能な色の最大深度になります。接続の実際の色の深度は、クライアント コンピュータで利用できる色のサポートによってきまします。[クライアント互換] を選択すると、クライアントで利用できる最高の色の深度が使用されます。 **注:** 24 ビットの色の深度は、Windows XP Professional と Windows Server 2003 でのみサポートされます。 このポリシー設定を無効にするか、または構成しない場合、接続で使用される色の深度は、ユーザーが接続にさらに低いレベルを指定している場合を除き、リモート デスクトップ セッション ホスト構成ツールの [クライアントの設定] タブにある [色の深度の最大値を制限する] 設定によって決まります。
Enforce Removal of Remote Desktop Wallpaper	リモート デスクトップ サービスで接続しているリモート クライアントにデスクトップの壁紙を表示するかどうかを指定します。 この設定を使用すると、リモート デスクトップ サービス セッション中に壁紙を表示しないように設定できます。Windows XP Professional の場合、デフォルトでは、クライアントの構成に応じてリモート デスクトップで接続しているリモート クライアントに壁紙を表示します。詳細については、リモート デスクトップ接続オプションの [エクスペリエンス] タブを参照してください。Windows Server 2003 を実行しているサーバの場合、デフォルトでは、リモート デスクトップ サービス セッションに壁紙を表示しません。 この設定を有効にすると、リモート デスクトップ サービス セッションに壁紙は表示されません。 この設定を無効にすると、クライアントの構成に応じてリモート デスクトップ サービス セッションに壁紙が表示されます。 この設定を構成しない場合、デフォルトの動作が適用されます。

設定	説明
Configure RemoteFX	このポリシー設定では、リモート デスクトップ仮想化ホスト（RD 仮想化ホスト）と RDS ホストの両方での RemoteFX の可用性を制御します。 RD 仮想化ホストに展開された場合、RemoteFX は、グラフィックス処理ユニット (GPU) を使用してサーバ上のコンテンツをレンダリングし、ユーザーの操作性を向上します。デフォルトでは、RD 仮想化ホストの RemoteFX は、サーバ側の GPU またはハードウェアを使用して LAN 接続と RDP 7.1 での操作性を向上します。 RDS ホストに展開された場合、RemoteFX は、ハードウェア アクセラレータによる圧縮スキームを使用して操作性を向上します。 このポリシー設定を有効にすると、LAN 接続と RDP 7.1 での操作性を向上するため、RemoteFX が使用されます。 このポリシー設定を無効にすると、RemoteFX は無効になります。 このポリシー設定を構成しない場合、デフォルトの動作が使用されます。デフォルトでは、RD 仮想化ホストの RemoteFX は有効になります。RDS ホストの RemoteFX は無効になります。
Limit maximum display resolution	このポリシー設定では、リモート デスクトップ サービス セッションの表示に使用する各モニターの最高解像度を指定します。リモート セッションの表示に使用する解像度を制限すると、接続のパフォーマンスが向上し（特に低速リンクの場合）、サーバの負荷が軽減されます。 このポリシー設定を有効にする場合、画面解像度の幅と高さを指定する必要があります。指定した解像度は、リモート デスクトップ サービス セッションの表示に使用する各モニターの最高解像度になります。 このポリシー設定を無効にするか、構成しない場合、リモート デスクトップ セッション ホスト構成ツールの [表示設定] タブに指定されている値に応じて、各モニターでリモート デスクトップ サービス セッションの表示に使用できる最高解像度が決まります。
Limit maximum number of monitors	このポリシー設定では、リモート デスクトップ サービス セッションの表示に使用できるモニターの数を制限します。リモート デスクトップ サービス セッションの表示に使用するモニター数を制限すると、接続のパフォーマンスが向上し（特に低速リンクの場合）、サーバの負荷が軽減されます。 このポリシー設定を有効にすると、リモート デスクトップ サービス セッションの表示に使用できるモニターの数を指定できます。1 から 10 の数値を指定できます。 このポリシー設定を無効にするか、構成しない場合、リモート デスクトップ サービス セッションの表示に使用できるモニター数は、リモート デスクトップ セッション ホスト構成ツールの [表示設定] タブにある [セッションごとのモニターの最大数] ボックスの値によって決まります。

設定	説明
Remove "Disconnect" option from Shut Down dialog	このポリシー設定では、リモート デスクトップ サービス セッションの [Windows のシャットダウン] ダイアログ ボックスから [切断] オプションを削除します。 このポリシー設定を使用すると、この一般的な方法で RDS ホストからクライアントを切断できなくなります。 このポリシー設定を有効にすると、[Windows のシャットダウン] ダイアログ ボックスのドロップダウン リストから [切断] オプションが削除されます。 このポリシー設定を無効にするか、構成しない場合、[Windows のシャットダウン] ダイアログ ボックスのドロップダウン リストから [切断] オプションは削除されません。 **注:** このポリシー設定は、[Windows のシャットダウン] ダイアログ ボックスのみに適用されます。他の方法によるリモート デスクトップ サービス セッションからの切断を防止することはできません。このポリシー設定は、サーバで切断状態のセッションを防止しません。切断状態のセッションがサーバ上で維持される時間を制御するには、「切断されたセッションの制限時間を設定する」ポリシー設定を構成します。この設定を行うには、[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] - [RD セッション ホスト] - [セッションの制限時間] の順に移動します。
Optimize visual experience when using RemoteFX	このポリシー設定では、RemoteFX を使用するリモート デスクトップ接続 (RDC) でリモート ユーザーに提供される視覚体験を指定します。このポリシーを使用すると、提供するグラフィックス環境の種類とネットワーク バンド幅の使用量のバランスを取ることができます。 ユーザー要件に応じて、画面キャプチャ レートを下げてネットワーク バンド幅の使用量を減らすことができます。画質を下げる（画像の圧縮率を上げる）ことでネットワーク バンド幅の使用量を減らすこともできます。 標準よりもバンド幅が広いネットワークを使用する場合、画面キャプチャ レートと画質の設定で最高値を選択すると、バンド幅を最大限に利用できます。 デフォルトでは、LAN 上でバランスの取れた体験を提供するように、RemoteFX を使用するリモート デスクトップ接続セッションが最適化されます。このポリシー設定を無効にするか、構成しない場合、RemoteFX を使用するリモート デスクトップ接続セッションは、画面キャプチャ レートと画像圧縮の設定に「中」を選択した場合（デフォルトの動作）と同じになります。

設定	説明
Set compression algorithm for RDP data	このポリシー設定では、使用するリモート デスクトップ プロトコル (RDP) 圧縮アルゴリズムを指定します。 デフォルトでは、サーバはサーバのハードウェア構成に基いて RDP 圧縮アルゴリズムを使用します。 このポリシー設定を有効にすると、使用する RDP 圧縮アルゴリズムを指定できます。メモリの使用量を抑えるように最適化されたアルゴリズムを選択すると、メモリの使用量は少なくなりますが、使用するネットワーク バンド幅は増加します。ネットワーク バンド幅の使用量を抑えるように最適化されたアルゴリズムを選択すると、使用するネットワーク バンド幅は少なくなりますが、メモリの使用量は増加します。また、メモリの使用量とネットワーク バンド幅のバランスが取れた 3 つ目の選択肢もあります。 RDP 圧縮アルゴリズムを使用しないことも選択できます。RDP 圧縮アルゴリズムを使用しないように選択すると、使用するネットワーク バンド幅が増加します。この設定は、ネットワーク トラフィックを最適化するように設計されたハードウェアを使用している場合にのみ推奨します。RDP 圧縮アルゴリズムを使用しないように選択した場合でも、一部のグラフィック データは圧縮されます。 このポリシー設定を無効にするか、構成しない場合、デフォルトの RDF 圧縮アルゴリズムが使用されます。
Optimize visual experience for Remote Desktop Services sessions	このポリシー設定では、リモート デスクトップ サービス セッションでリモート ユーザーに提供される視覚体験を指定します。リモート コンピュータのリモート セッションは、その視覚体験をサポートするように最適化されます。 デフォルトでは、リモート デスクトップ サービス セッションはリッチ マルチメディア（Silverlight や Windows Presentation Foundation を使用するアプリケーションなど）用に最適化されます。 このポリシー設定を有効にする場合、リモート デスクトップ サービス セッションを最適化する視覚体験を選択する必要があります。[リッチ マルチメディア] または [テキスト] を選択できます。 このポリシー設定を無効にするか、構成しない場合、リモート デスクトップ サービス セッションはリッチ マルチメディア用に最適化されます。

設定	説明
Start a program on connection	接続時に指定のプログラムを自動的に実行するようにリモート デスクトップ サービスを構成します。 この設定を使用すると、ユーザーがリモート コンピュータにログインしたときに自動的に実行されるプログラムを指定できます。 デフォルトでは、サーバ管理者またはクライアント接続を構成しているユーザーがこの設定を指定しない限り、リモート デスクトップ サービス セッションは Windows デスクトップに対するフル アクセスをユーザーに提供します。この設定を有効にすると、サーバ管理者またはユーザーが設定した [スタートアップ プログラム] の設定が上書きされます。[スタート] メニューと Windows デスクトップは表示されません。ユーザーがプログラムを終了すると、セッションが自動的にログオフされます。 この設定を使用するには、[プログラムのパスとファイル名] にユーザーのログイン時に実行する実行可能ファイルの完全修飾名（パスとファイル名）を指定します。必要であれば、[作業ディレクトリ] にプログラムの開始ディレクトリの完全修飾パスを入力します。[作業ディレクトリ] を空欄のままにすると、プログラムはそのデフォルトの作業ディレクトリで実行されます。指定したプログラム パス、ファイル名、作業ディレクトリが有効なディレクトリ名でない場合、RDS ホスト接続に失敗し、エラー メッセージが表示されます。 この状態が有効に設定されている場合、リモート デスクトップ サービス セッションは指定のプログラムを自動的に実行し、指定の作業ディレクトリ（作業ディレクトリが指定されていない場合はプログラムのデフォルト ディレクトリ）をプログラムの作業ディレクトリとして使用します。 状態が無効に設定されているか、構成に設定されていない場合、サーバ管理者またはユーザーが指定しない限り、リモート デスクトップ サービス セッションが完全なデスクトップで開始します。詳細については、「ユーザーのログイン時に実行するプログラムを指定する」ポリシー設定を参照してください。この設定を確認するには、[コンピュータの構成] - [管理用テンプレート] - [システム] - [ログイン] の順に移動します。 **注:** この設定は、[コンピュータの構成] と [ユーザーの構成] の両方に表示されます。両方の設定を構成すると、[ユーザーの構成] よりも [コンピュータの構成] の設定が優先します。
Always show desktop on connection	このポリシー設定では、クライアントがリモート コンピュータに接続した後、常にデスクトップを表示するか、初期プログラムを実行可能にするかを指定します。この設定は、デフォルトのユーザー プロファイル、リモート デスクトップ接続、リモート デスクトップ サービス クライアントまたはグループ ポリシーですでに初期プログラムが指定されていても、クライアントがリモート コンピュータに接続した後にデスクトップを表示する必要がある場合に使用します。 このポリシーを有効にすると、クライアントがリモート コンピュータに接続した後に常にデスクトップが表示されます。このポリシー設定は、初期プログラムのポリシー設定よりも優先されます。 このポリシーを無効にするか、構成しない場合、クライアントがリモート コンピュータに接続した後にリモート コンピュータで実行する初期プログラムを指定できます。初期プログラムを指定しないと、クライアントがリモート コンピュータに接続した後に常にデスクトップが表示されます。 **注:** このポリシー設定を有効にすると、[接続時にプログラムを起動する] ポリシー設定は無視されます。

設定	説明
Allow desktop composition for remote desktop sessions	このポリシー設定では、リモート デスクトップ セッションでデスクトップ コンポジションを許可するかどうかを指定します。このポリシー設定は、RemoteApp セッションに適用されません。 デスクトップ コンポジションは、Windows Aero のユーザー インターフェイス要素（半透明のウィンドウなど）をリモート デスクトップ セッションに提供します。Windows Aero を使用すると、追加のシステム リソースとバンド幅が必要になります。このため、リモート デスクトップ セッションにデスクトップ コンポジションを許可すると、接続のパフォーマンスが低下し（特に低速リンクの場合）、リモート コンピュータの負荷が増加する可能性があります。 このポリシー設定を有効にすると、リモート デスクトップ セッションでデスクトップ コンポジションが使用可能になります。クライアント コンピュータでデスクトップ コンポジションを構成するには、リモート デスクトップ接続 (RDC) の [エクスペリエンス] タブで設定します。あるいは、リモート デスクトップ プロトコル (.rdp) ファイルでデスクトップ コンポジションを許可する設定を使用します。また、クライアント コンピュータに Windows Aero 機能に対応するハードウェアも必要です。 **注:** リモート デスクトップ セッションで Windows Aero 機能を使用するには、リモート コンピュータで追加の設定が必要になる場合があります。たとえば、リモート コンピュータにデスクトップ エクスペリエンス機能をインストールして、色の深度の最大値を 32 bpp に設定する必要があります。また、リモート コンピュータでテーマ サービスを開始する必要もあります。 このポリシー設定を無効にするか、構成しない場合、RDC または .rdp ファイルでデスクトップ コンポジションを有効にしても、リモート デスクトップ セッションでデスクトップ コンポジションを使用できません。

設定	説明
Do not allow font smoothing	このポリシー設定では、リモート接続でフォント スムージングを許可するかどうかを指定します。 フォント スムージングはリモート接続に ClearType 機能を提供します。ClearType はコンピュータのフォントを表示するテクノロジーで、特に LCD モニターを使用している場合に、きれいで滑らかなフォントを表示できます。フォント スムージングには追加のバンド幅が必要になるため、リモート接続でフォント スムージングを禁止すると、接続のパフォーマンスが向上する可能性があります（特に低速リンクの場合）。 デフォルトでは、フォント スムージングはリモート接続で許可されています。フォント スムージングを構成するには、リモート デスクトップ接続 (RDC) の [エクスペリエンス] タブで設定します。あるいは、リモート デスクトップ プロトコル (.rdp) ファイルでフォント スムージングを許可する設定を使用します。 このポリシー設定を有効にすると、RDC または .rdp ファイルでフォント スムージングを有効にしても、リモート接続でフォント スムージングを使用することはできません。 このポリシー設定を無効にするか、構成しない場合、フォント スムージングはリモート接続で許可されます。
Remove Windows Security item from Start menu	リモート デスクトップ クライアントの [設定] メニューから [Windows セキュリティ] の項目を削除するかどうかを指定します。この設定を使用して、未熟なユーザーがリモート デスクトップ サービスから間違ってログオフするのを防ぐことができます。 ステータスが [有効] に設定されている場合、[スタート] メニューの [設定] に [Windows セキュリティ] は表示されません。このため、クライアント コンピュータで [Windows セキュリティ] ダイアログ ボックスを開くには、Ctrl+Alt+End などの Secure Attention Sequence (SAS) を入力する必要があります。 ステータスが [無効] または [構成されていません] に設定されている場合、[Windows セキュリティ] は [設定] メニューに残ります。

RDS セキュリティの設定

RDS Security group ポリシー設定で、ローカル管理者が権限のカスタマイズをできるようにするかどうかを制御します。

Horizon 7 RDS グループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [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] - [セキュリティ] フォルダにインストールされています。

表 5-22. RDS Security Group ポリシー設定

設定	説明
Server Authentication Certificate Template	このポリシー設定では、RDS ホストの認証で自動的に選択される証明書を決める証明書テンプレートの名前を指定します。 RDP 接続中にクライアントと RDS ホスト間の通信を保護するために SSL (TLS 1.0) を使用する場合、RDS ホストの認証に証明書が必要になります。 このポリシー設定を有効にすると、証明書テンプレートの名前を指定する必要があります。RDS ホストの認証に使用する証明書が自動的に選択される場合、指定した証明書テンプレートで作成された証明書のみ対象となります。証明書の自動選択は、特定の証明書が選択されていない場合にのみ行われます。 指定した証明書テンプレートで作成された証明書が見つからない場合、RDS ホストは証明書の登録要求を発行します。この要求が完了されるまでは現在の証明書が使用されます。指定した証明書テンプレートで作成された証明書が複数見つかった場合は、有効期限が最も長く、RDS ホストの現在の名前に一致する証明書が選択されます。 このポリシー設定を無効にするか、構成しない場合、自己署名証明書が RDS ホストの認証にデフォルトで使用されます。リモート デスクトップ セッション ホスト構成ツールの [全般] タブで、RDS ホストの認証に使用する特定の証明書を選択できます。 **注:** RDS ホストの認証に使用される特定の証明書を選択した場合、この証明書がポリシー設定より優先されます。
Set client connection encryption level	リモート デスクトップ プロトコル (RDP) 接続時にクライアントと RDS ホスト間の通信を保護するため、特定の暗号化レベルの使用を必要とするかどうかを指定します。 このポリシー設定を有効にした場合、リモート接続時のクライアントと RDS ホスト間のすべての通信で、ここで指定した暗号化方法を使用する必要があります。デフォルトでは、暗号化レベルは [高] に設定されています。次の暗号化方法を使用できます。 ■ High。[高] を設定すると、クライアントとサーバ間で送受信されるデータは強固な 128 ビット暗号化で保護されます。この暗号化レベルは、128 ビット暗号化をサポートするクライアント（たとえば、リモート デスクトップ接続を実行するクライアント）のみを含む環境で使用します。この暗号化レベルをサポートしていないクライアントは RDS ホスト サーバに接続できません。 ■ Client Compatible。[クライアント互換] を設定すると、クライアントとサーバ間で送受信されるデータは、クライアントでサポートされている最高のキー強度で暗号化されます。この暗号化レベルは、128 ビット暗号化をサポートしていないクライアントを含む環境で使用します。 ■ Low。[低] を設定すると、クライアントからサーバに送信されるデータのみ 56 ビット暗号化で暗号化されます。 この設定を無効にするか、構成しない場合、RDS ホストへのリモート接続に使用される暗号化レベルは、グループ ポリシーで強制的に適用されません。ただし、リモート デスクトップ セッション ホスト構成ツールを使用すると、これらの接続に必要な暗号化レベルを設定できます。 **重要:** FIPS 準拠は、[暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う] ポリシー設定で構成できます。設定するには、[コンピュータの構成] - [Windows の設定] - [セキュリティの設定] - [ローカル ポリシー] - [セキュリティ オプション] の順に移動するか、リモート デスクトップ セッション ホスト構成で [FIPS 準拠] を使用します。[FIPS 準拠] 設定では、Microsoft 暗号化モジュールを使用して、FIPS (Federal Information Processing Standard) 140-1 暗号化アルゴリズムにより、クライアントとサーバ間で送受信されるデータの暗号化と暗号化解除を行います。この暗号化レベルは、クライアントと RDS ホスト間の通信で最高レベルの暗号化が必要な場合に使用します。FIPS 準拠が、グループ ポリシーの [システム暗号化: 暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う] 設定によっ

設定	説明
Always prompt for password upon connection	接続時に、リモート デスクトップ サービスがクライアントに常にパスワードの入力を要求するかどうかを指定します。 この設定を使用すると、リモート デスクトップ サービスにログインしているユーザーがリモート デスクトップ接続のクライアントでパスワードをすでに入力していても、パスワードの入力を強制的に要求できます。 デフォルトでは、リモート デスクトップ接続クライアントでパスワードを入力すると、リモート デスクトップ サービスに自動的にログインできます。 このポリシー設定を有効にすると、リモート デスクトップ接続のクライアントでパスワードを入力しても、リモート デスクトップ サービスに自動的にログインできません。ログイン パスワードが要求されます。 このポリシー設定を無効にすると、リモート デスクトップ接続のクライアントでパスワードを入力すると、リモート デスクトップ サービスに自動的にログインできます。 この設定を行わない場合、グループ ポリシー レベルで自動ログインが指定されません。ただし、管理者がリモート デスクトップ セッション ホスト構成ツールを使用して、パスワードを強制的に要求できます。
Require secure RPC communication	RDS ホストがすべてのクライアントとの RPC 通信の保護を要求するのか、保護されていない通信を許可するのかを指定します。 この設定を使用すると、クライアントとの RPC 通信をセキュリティで保護し、認証済みで暗号化された要求のみを許可できます。 この設定を有効にすると、リモート デスクトップ サービスは、保護された要求をサポートする RPC クライアントからの要求を受け入れます。信頼されていないクライアントとの保護されていない通信は許可されません。 この設定を無効にすると、リモート デスクトップ サービスは、すべての RPC トラフィックにセキュリティを要求します。ただし、RPC クライアントが要求に応答しない場合には、保護されていない通信が許可されます。 この設定を行わない場合、保護されていない通信が許可されます。 **注:** リモート デスクトップ サービスの管理と構成には RPC インターフェイスが使用されます。

設定	説明
Require use of specific security layer for remote (RDP) connections	リモート デスクトップ プロトコル (RDP) 接続時にクライアントと RDS ホスト間の通信を保護するため、特定のセキュリティ レイヤーの使用を必要とするかどうかを指定します。 このポリシー設定を有効にした場合、リモート接続時のクライアントと RDS ホスト間のすべての通信で、ここで指定したセキュリティ方法を使用する必要があります。次のセキュリティ方法を使用できます。 ■ Negotiate。ネゴシエートでは、クライアントでサポートされている最も安全性の高い方法が強制的に実行されます。Transport Layer Security (TLS) バージョン 1.0 がサポートされている場合、RDS ホストの認証に使用されます。TLS がサポートされていない場合、ネイティブのリモート デスクトップ プロトコル (RDP) 暗号化を使用して通信が保護されますが、RDS ホストは認証されません。 ■ RDP。RDP では、ネイティブの RDP 暗号化を使用して、クライアントと RDS ホスト間の通信が保護されます。この設定を選択すると、RDS ホストは認証されません。 ■ SSL (TLS 1.0)。SSL の場合、TLS 1.0 を使用して RDS ホストを認証する必要があります。TLS がサポートされていない場合、接続に失敗します。 この設定を無効にするか、構成しない場合、RDS ホストへのリモート接続に使用されるセキュリティ方法はグループ ポリシーで強制的に適用されません。ただし、リモート デスクトップ セッション ホスト構成ツールを使用すると、これらの接続に必要なセキュリティ方法を設定できます。

設定	説明
Require user authentication for remote connections by using Network	このポリシー設定では、RDS ホストへのリモート接続でネットワーク レベルの認証を使用したユーザー認証が必要かどうかを指定します。このポリシー設定を使用すると、リモート接続プロセスの初期段階でユーザーの認証が要求されるため、セキュリティが強化されます。 このポリシー設定を有効にすると、ネットワーク レベルの認証をサポートするクライアント コンピュータのみが RDS ホストに接続できます。 クライアント コンピュータがネットワーク レベルの認証に対応しているどうかを確認するには、クライアント コンピュータでリモート デスクトップ接続を起動して、[リモート デスクトップ接続] ダイアログ ボックスの左上のアイコンをクリックし、[バージョン情報] をクリックします。[バージョン情報] ダイアログ ボックスで、「ネットワーク レベル認証はサポートされています」というテキストを探します。 このポリシー設定を無効にするか、構成しない場合、RDS ホストへのリモート接続を許可する前のユーザー認証で、ネットワーク レベルの認証が不要になります。 リモート デスクトップ セッション ホスト構成ツールまたは、[システムのプロパティ] の [リモート] タブを使用すると、ユーザー認証にネットワーク レベルの認証が必要であることを指定できます。 **重要:** このポリシー設定を無効にするか、構成しない場合、ユーザー認証がリモート接続処理の後半で行われるため、セキュリティが低下します。
Do not allow local administrators to customize permissions	リモート デスクトップ セッション ホスト構成ツールで、セキュリティ権限をカスタマイズする管理者権限を無効にするかどうかを指定します。 この設定を使用して、管理者がリモート デスクトップ セッション ホスト構成ツールの [アクセス権限] タブでユーザー グループを変更できないようにすることができます。デフォルトでは、管理者はこのような変更を行うことができます。 ステータスが [有効] に設定されている場合、リモート デスクトップ セッション ホスト構成ツールの [アクセス権限] タブでは、接続ごとのセキュリティ記述子をカスタマイズしたり、既存のグループのデフォルトのセキュリティ記述子を変更したりすることはできません。すべてのセキュリティ記述子は読み取り専用です。 ステータスが [無効] または [構成されていません] に設定されている場合でも、サーバ管理者にはリモート デスクトップ セッション ホスト構成ツールの [アクセス権限] タブのユーザーのセキュリティ記述子へのすべての読み取り/書き込み権限があります。 **注:** ユーザーのアクセスを管理する際には、リモート デスクトップ ユーザー グループにユーザーを追加することをお勧めします。

RDS セッションの時間制限

RDS セッションの時間制限のグループ ポリシー設定を使用すると、RDS ホストのセッションに時間制限ポリシーを設定できます。

Horizon 7 RDS グループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [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] - [セッションの時間制限] フォルダにインストールされています。

Horizon 7 RDS グループ ポリシー設定は、[ユーザーの構成] - [管理用テンプレート] - [Windows コンポーネント] - [リモート デスクトップ サービス] - [リモート デスクトップ セッション ホスト] - [セッションの時間制限] フォルダにもインストールされています。

表 5-23. RDS セッションの時間制限のグループ ポリシー設定

設定	説明
Set time limit for disconnected sessions	このポリシー設定を使用すると、切断されたリモート デスクトップ サービス セッションに制限時間を設定できます。 このポリシー設定を使用すると、切断されたセッションがサーバでアクティブになっている最大時間を指定できます。デフォルトでは、セッションからログオフして終了しなくても、リモート デスクトップ サービスを切断できます。 セッションが切断状態の場合、ユーザーが接続していなくても、実行中のプログラムはアクティブのままになります。デフォルトでは、切断されたセッションはサーバ上に無期限で保持されます。 このポリシー設定を有効にした場合、指定した時間が経過すると、切断状態のセッションがサーバから削除されます。切断状態のセッションを無期限で維持するデフォルトの動作を強制的に実行するには、「無期限」を選択します。コンソール セッションには、切断されたセッションの制限時間は適用されません。 このポリシー設定を無効にするか、構成しない場合、切断されたセッションは無期限で維持されます。切断されたセッションの制限時間は、リモート デスクトップ セッション ホスト構成ツールの [セッション] タブで指定できます。 **注:** このポリシー設定は、[コンピュータの構成] と [ユーザーの構成] の両方に表示されます。両方のポリシー設定を指定した場合、[コンピュータの構成] のポリシー設定が優先されます。
Set time limit for active but idle Remote Desktop Services sessions	このポリシー設定では、アクティブなリモート デスクトップ サービス セッションに許可するアイドル状態（ユーザーの入力がない状態）の最大時間を指定します。この時間が経過すると、セッションが自動的に切断されます。 このポリシー設定を有効にすると、[アイドル セッションの制限] ドロップダウン リストで制限時間を選択する必要があります。指定した時間が経過すると、リモート デスクトップ サービスはアイドル状態のセッションを自動的に切断します。セッションを切断する 2 分前に警告が表示されます。キーを押すか、マウスを動かすと、セッションをアクティブのまま継続できます。コンソール セッションには、アイドル セッションの制限時間は適用されません。 このポリシー設定を無効にするか、構成しない場合、リモート デスクトップ サービスはアイドル状態のセッションを無期限で維持します。アイドル セッションの制限時間は、リモート デスクトップ セッション ホスト構成ツールの [セッション] タブで指定できます。 制限時間に達したときに、リモート デスクトップ サービスがセッションの切断ではなく、セッションを終了するように設定するには、「制限時間に達したらセッションを中止する」ポリシー設定を使用します。この設定を行うには、[コンピュータの構成] - [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] - [セッションの時間制限] の順に移動します。 **注:** このポリシー設定は、[コンピュータの構成] と [ユーザーの構成] の両方に表示されます。両方のポリシー設定を指定した場合、[コンピュータの構成] のポリシー設定が優先されます。

設定	説明
Set time limit for active Remote Desktop Services sessions	このポリシー設定では、リモート デスクトップ サービス セッションの最大持続時間を指定します。この時間が経過すると、セッションが自動的に切断されます。 このポリシー設定を有効にすると、[アクティブ セッションの最大時間] ドロップダウン リストで必要な制限時間を選択する必要があります。指定した時間が経過すると、リモート デスクトップ サービスはアクティブ セッションを自動的に切断します。リモート デスクトップ サービス セッションが切断される 2 分前に警告が表示されます。この間に、使用中のファイルを保存し、プログラムを終了できます。コンソール セッションには、アクティブ セッションの最大時間は適用されません。 このポリシー設定を無効にするか、構成しない場合、リモート デスクトップ サービスはセッションを無期限で維持します。アクティブ セッションの最大時間は、リモート デスクトップ セッション ホスト構成ツールの [セッション] タブで指定できます。 制限時間に達したときに、リモート デスクトップ サービスがセッションの切断ではなく、セッションを終了するように設定するには、「制限時間に達したらセッションを中止する」ポリシー設定を使用します。この設定を行うには、[コンピュータの構成] - [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] - [セッションの時間制限] の順に移動します。 **注:** このポリシー設定は、[コンピュータの構成] と [ユーザーの構成] の両方に表示されます。両方のポリシー設定を指定した場合、[コンピュータの構成] のポリシー設定が優先されます。

設定	説明
Terminate session when time limits are reached	期限付きのリモート デスクトップ サービス セッションを切断ではなく終了するかどうかを指定します。 この設定を使用すると、アクティブ セッションまたはアイドル セッションの制限時間に達したときに、リモート デスクトップ サービスがセッションを終了します（ユーザーはログオフされ、サーバからセッションが削除されます）。デフォルトでは、リモート デスクトップ サービスは、制限時間に達したセッションを切断します。 制限時間は、サーバ管理者がローカルのグループ ポリシーで設定します。「アクティブなリモート デスクトップ サービス セッションの制限時間を設定する」と「アクティブでアイドル状態になっているリモート デスクトップ サービス セッションの制限時間を設定する」の設定を参照してください。 この設定を有効にすると、リモート デスクトップ サービスは制限時間に達したすべてのセッションを終了します。 この設定を無効にすると、サーバ管理者の設定に関わらず、リモート デスクトップ サービスはタイムアウトしたセッションを切断します。 この設定を行わない場合、ローカルの設定で別の指定がない限り、リモート デスクトップ サービスはタイムアウトしたセッションを切断します。 **注:** この設定は、リモート デスクトップ セッション ホスト構成ツールまたはグループ ポリシー管理コンソールで明示的に設定した時間制限にのみ適用されます。接続条件またはネットワーク条件で発生したタイムアウト イベントには適用されません。この設定は、[コンピュータの構成] と [ユーザーの構成] の両方に表示されます。両方の設定を指定した場合、[コンピュータの構成] の設定が優先します。
Set time limit for logoff of RemoteApp sessions	このポリシー設定では、ユーザーのリモート アプリケーション セッションが切断状態を維持できる時間を指定します。この時間が経過すると、セッションは RDS ホストからログオフされます。 デフォルトでは、ユーザーがリモート アプリケーションを終了したときに、セッションが RDS ホストから切断されます。 このポリシー設定を有効にした場合、ユーザーがリモート アプリケーションを終了した後も、リモート アプリケーション セッションは指定した制限時間まで切断状態を維持します。指定した制限時間に達すると、リモート アプリケーション セッションは RDS ホストからログオフされます。制限時間に達する前にユーザーがリモート アプリケーションを開始すると、ユーザーは RDS ホストで切断状態のセッションに再接続します。 このポリシー設定を無効にするか、構成しない場合、ユーザーがリモート アプリケーションを終了すると、セッションが RDS ホストから切断されます。 **注:** このポリシー設定は、[コンピュータの構成] と [ユーザーの構成] の両方に表示されます。両方のポリシー設定を指定した場合、[コンピュータの構成] のポリシー設定が優先されます。

RDS 一時フォルダの設定

RDS 接続グループ ポリシー設定は、リモート デスクトップ サービス セッション用の一時フォルダの作成および削除を制御します。

表 5-24. RDS 一時フォルダのグループ ポリシー設定

設定	説明
Do not delete temp folder upon exit	リモート デスクトップ サービスで、ユーザーのセッションごとの一時フォルダをログオフ時に保持するかどうかを指定します。 この設定を使用して、ユーザーがセッションからログオフしても、リモート コンピュータ上のユーザーのセッション固有の一時フォルダを保持することができます。デフォルトでは、リモート デスクトップ サービスは、ユーザーがログオフする際にユーザーの一時フォルダを削除します。 このステータスが [有効] に設定されている場合、ユーザーのセッションごとの一時フォルダは、ユーザーがセッションからログオフしても保持されます。 このステータスが [無効] に設定されている場合、管理者がリモート デスクトップ セッション ホスト構成ツールで他の設定をしたとしても、一時フォルダはユーザーがログオフするときに削除されます。 このステータスが [構成されていません] に設定されている場合、サーバ管理者が他の設定をしない限り、リモート デスクトップ サービスはログオフ時に一時フォルダをリモート コンピュータから削除します。 **注:** この設定は、セッションごとの一時フォルダがサーバで使用されている場合のみ有効になります。つまり、[セッションごとの一時フォルダを使用しない] 設定を有効にした場合、この設定は無効になります。
Do not use temporary folders per session	このポリシー設定により、リモート デスクトップ サービスがセッション固有の一時フォルダを作成することを防止できます。 このポリシー設定を使用して、各セッション用の別の一時フォルダをリモート コンピュータ上に作成することを無効にできます。デフォルトでは、リモート デスクトップ サービスは、ユーザーがリモート コンピュータに保持する、各アクティブ セッション用の別の一時フォルダを作成します。これらの一時フォルダは、ユーザーのプロファイルフォルダ内一時フォルダにあるリモート コンピュータ上で、sessionid という名前で作成されます。 このポリシー設定を有効にすると、セッションごとの一時フォルダは作成されません。その代わりに、リモート コンピュータ上のすべてのセッション用のユーザーの一時ファイルが、リモート コンピュータ上のユーザーのプロファイルフォルダ内の共通の一時フォルダに保存されます。 このポリシー設定を無効にすると、リモート デスクトップ セッション ホスト構成ツールで他の設定をしたとしても、セッションごとの一時フォルダが常に作成されます。 このポリシー設定を構成しないと、リモート デスクトップ セッション ホスト構成ツールで他の設定をしない限り、セッションごとの一時フォルダが作成されます。

仮想印刷でプリンタのフィルタリング

仮想印刷機能を有効にすると、ユーザーはクライアント システムで使用可能な任意のプリンタをリモート デスクトップおよびアプリケーションから使用できます。[クライアント プリンタのリダイレクトに適用するフィルタを指定] エージェント グループ ポリシー設定を使用すると、仮想印刷機能で特定のクライアント プリンタからリモート デスクトップ/アプリケーションへのリダイレクトを防ぐことができます。

[クライアント プリンタのリダイレクトに適用するフィルタを指定] グループ ポリシー設定は、VMware Horizon プリンタ リダイレクト ADMX テンプレート ファイル (`vdm_agent_printing.admx`) に含まれています。これは、`VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` ファイルにバンドルされています。インストール手順については、Active Directory への ADMX テンプレート ファイルの追加を参照してください。

[クライアント プリンタのリダイレクトに適用するフィルタを指定] グループ ポリシー設定を有効にする場合には、[レジストリ値名: PrinterFilterString] テキスト ボックスにフィルタリング ルールを入力する必要があります。フィルタリング ルールは、リダイレクトしないプリンタを指定する正規表現です（ブラック リスト）。フィルタリング ルールで一致しないプリンタにリダイレクトされます。デフォルトでは、フィルタリング ルールは空で、すべてのクライアント プリンタがリダイレクトされます。

次の表に、フィルタリング ルールで使用できる属性、演算子、ワイルドカードを示します。

表 5-25. フィルタリング ルールでサポートされている属性、演算子、ワイルドカード

属性	演算子	ワイルドカード
DriverName、VendorName、PrinterName	AND、OR、NOT	*、?

以下は、フィルタリング ルールの例です。

```
(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e"

PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF"

PrinterName!=".*PDFCreator.*"
```

仮想デスクトップまたは RDS ホストに Horizon Agent インストールするときに、仮想印刷機能を有効にします。インストール手順については、『Horizon 7 での仮想デスクトップのセットアップ』と『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』を参照してください。

ロケーションベースの印刷の設定

ロケーション ベースの印刷機能は、物理的に近いクライアント システムであるプリンタをリモート デスクトップにマッピングして、ユーザーがリモート デスクトップからローカル プリンタやネットワーク プリンタに印刷できるようにします。

ロケーション ベースの印刷により、IT 組織は、エンドポイントのクライアント デバイスに最も近いプリンタにリモート デスクトップをマッピングすることができます。たとえば、病院の医師が次々と部屋を移動している場合、その医師がドキュメントを印刷する度に、印刷ジョブはその医師が現在いる部屋に最も近いプリンタに送信されます。

ロケーションベースの印刷機能は、Windows、Mac、Linux、およびモバイル クライアント デバイスで使用できます。

ロケーション ベースの印刷は、次のリモート デスクトップおよびアプリケーションでサポートされます。

- Windows Desktop や Windows Server マシンなど、単一ユーザーのマシンに展開されたデスクトップ
- 仮想マシンである RDS ホストに展開されたデスクトップ
- 公開アプリケーション

- リモート デスクトップ内部の Horizon Client から起動される公開アプリケーション

ロケーション ベースの印刷機能を使用するには、デスクトップに Horizon Agent と一緒に仮想印刷セットアップ オプションをインストールするとともに、正しいプリンタ ドライバをインストールする必要があります。

ロケーションベースの印刷を設定するには、Active Directory グループ ポリシー設定 `AutoConnect Map Additional Printers for VMware View` を設定します。この設定は、Microsoft グループ ポリシー オブジェクト エディタの [コンピュータの構成] の下の [ソフトウェアの設定] フォルダにあります。

注: `AutoConnect Map Additional Printers for VMware View` はコンピュータ固有のポリシーです。コンピュータ固有のポリシーは、デスクトップに接続するユーザーに関係なく、すべてのリモート デスクトップに適用されます。

`AutoConnect Map Additional Printers for VMware View` は名前変換表として実装されます。表の各行を使用して、特定のプリンタを識別し、そのプリンタの一連の変換ルールを定義します。変換ルールは、プリンタが特定のクライアント システムのリモート デスクトップにマッピングされているかどうかを判定します。

ユーザーがリモート デスクトップに接続すると、Horizon 7 は、クライアント システムを表の各プリンタに関連付けられている変換ルールと比較します。クライアント システムがプリンタに設定されているすべての変換ルールに該当する場合、またはプリンタに変換ルールが関連付けられていない場合、Horizon 7 はユーザーのセッション中にプリンタをリモート デスクトップにマッピングします。

クライアント システムの IP アドレス、名前、および MAC アドレス、さらにユーザーの名前とグループに基づいて変換ルールを定義できます。特定のプリンタに対し、1 つの変換ルールまたは複数の変換ルールを組み合わせて指定できます。

プリンタをリモート デスクトップにマッピングするために使われる情報は、リモート デスクトップの `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect` のレジストリ エントリに保存されます。

ロケーションベースの印刷のプリンタ設定

場所ベースのプリンタのプリンタ設定は、ユーザーのログアウト後またはデスクトップからの切断後も保持されます。たとえば、白黒モードを使用するようにユーザーがロケーションベースのプリンタを設定したとします。ユーザーがデスクトップからログアウトして再度ログインした後も、ロケーションベースのプリンタでは引き続き白黒モードが使用されます。

公開アプリケーションのセッション間でプリンタの設定を保存するには、ユーザーはアプリケーションの印刷ダイアログ ボックスからロケーションベースのプリンタを選択し、選択したプリンタを右クリックして、[印刷設定] を選択する必要があります。ユーザーがプリンタを選択し、アプリケーションの印刷ダイアログ ボックスで [環境設定] ボタンをクリックした場合、プリンタの設定は保存されません。

設定が、Microsoft が推奨するプリンタ ドライバの DEVMODE の拡張部分ではなく、プリンタ ドライバのプライベート空間に保存される場合、ロケーションベースのプリンタの永続設定はサポートされません。永続設定をサポートするには、プリンタ ドライバの DEVMODE 部分に設定が保存されるプリンタを展開します。

ロケーションベースの印刷グループ ポリシー DLL ファイルの登録

ロケーションベースの印刷のグループ ポリシー設定を構成する前に、DLL ファイル TPVMGPoACmap.dll を登録する必要があります。

32 ビット版と 64 ビット版の TPVMGPoACmap.dll は、VMware-Horizon-Extras-Bundle-*x.x.x*-*yyyyyyy*.zip というバンドル化された .zip ファイルで提供されます。*x.x.x* はバージョン、*yyyyyyy* はビルド番号です。このファイルは、http://www.vmware.com/go/downloadview の VMware ダウンロード サイトからダウンロードできます。

手順

1 Active Directory サーバまたはグループ ポリシーの構成に使用するドメイン コンピュータに、TPVMGPoACmap.dll の適切なバージョンをコピーします。

2 regsvr32 ユーティリティを使用して TPVMGPoACmap.dll ファイルを登録します。

例：regsvr32 "C:\TPVMGPoACmap.dll"

次のステップ

ロケーションベースの印刷のグループ ポリシーを構成します。

ロケーションベースの印刷グループ ポリシーの構成

ロケーションベースの印刷を設定するには、AutoConnect Map Additional Printers for VMware View グループ ポリシー設定を構成します。このグループ ポリシー設定は、プリンタを Horizon デスクトップにマッピングする名前変換表です。

前提条件

- Active Directory サーバまたはグループ ポリシーの構成に使用するドメイン コンピュータで、Microsoft MMC およびグループ ポリシー オブジェクト エディタ スナップインが使用できることを確認します。
- Active Directory サーバまたはグループ ポリシーの構成に使用するドメイン コンピュータに、DLL ファイル TPVMGPoACmap.dll を登録します。ロケーションベースの印刷グループ ポリシー DLL ファイルの登録を参照してください。
- AutoConnect Map Additional Printers for VMware View グループ ポリシー設定の構文について理解しておきます。ロケーションベースの印刷グループ ポリシー設定の構文を参照してください。
- ロケーションベースのグループ ポリシー設定の GPO を作成し、それを Horizon デスクトップが格納されている OU にリンクします。Horizon グループ ポリシーの GPO の作成方法の例については、 Horizon 7 グループ ポリシーの GPO の作成を参照してください。
- デスクトップに Horizon Agent と共に仮想印刷設定オプションがインストールされていることを確認します。確認するには、デスクトップ オペレーティング システムに TP AutoConnect サービスおよび TP VC Gateway サービスがインストールされているか確認してください。
- 印刷ジョブは Horizon デスクトップからプリンタに直接送信されるため、必要なプリンタ ドライバがデスクトップにインストールされていることを確認します。

手順

1 Active Directory サーバで GPO を編集します。

Active Directory のバージョン	ナビゲーション パス
Windows 2003	a [スタート] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] の順に選択します。 b Horizon デスクトップを格納する OU を右クリックし、[プロパティ] を選択します。 c [グループ ポリシ] タブで、[開く] をクリックして Group Policy Management プラグインを開きます。 d 右ペインで、ロケーションベースの印刷グループ ポリシー設定用に作成した GPO を右クリックし、[編集] を選択します。
Windows 2008	a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、ロケーション ベースの印刷のグループ ポリシー設定で作成した GPO を右クリックして、[編集] を選択します。

[グループ ポリシー オブジェクト エディタ] ウィンドウが表示されます。

2 [コンピュータの構成] を展開し、[ソフトウェアの設定] フォルダを開き、[VMware View の追加のプリンタを自動接続マッピングする] を選択します。

3 ポリシー ペインで、[追加のプリンタの自動接続マッピングを構成する] をダブルクリックします。

[VMware View の追加のプリンタを自動接続マッピングする] ウィンドウが表示されます。

4 [有効化] を選択してグループ ポリシー設定を有効にします。

グループ ポリシー ウィンドウに変換表の見出しとボタンが表示されます。

重要: [無効化] をクリックすると、すべての表エントリが削除されます。万一のため、後でインポートできるように構成を保存してください。

5 Horizon デスクトップにマッピングするプリンタを追加し、それらの関連変換ルールを定義します。

6 [OK] をクリックして変更を保存します。

ロケーションベースの印刷グループ ポリシー設定の構文

`AutoConnect Map Additional Printers for VMware View` グループ ポリシー設定を使用して、プリンタをリモート デスクトップにマッピングします。

`AutoConnect Map Additional Printers for VMware View` は、プリンタを識別し、関連付けられた変換ルールを定義する名前変換表です。表 5-26. 変換表の列と値では、変換表の構文について説明します。

ロケーションベースの印刷により、ローカル プリンタがリモート デスクトップにマッピングされますが、UNC パスを使用して構成されたネットワーク プリンタのマッピングはサポートされません。

表 5-26. 変換表の列と値

列	説明
IP Range	クライアント システムの IP アドレスの範囲を指定する変換ルール。 特定の範囲の IP アドレスを指定するには、次の表記を使用します。 ***ip_address-ip_address*** 例： **10.112.116.0-10.112.119.255** 特定のサブネットのすべての IP アドレスを指定するには、次の表記を使用します。 *ip_address/subnet_mask_bits* 例： **10.112.4.0/22** この表記は、10.112.4.1 から 10.112.7.254 までの使用可能な IPv4 アドレスを指定しています。 任意の IP アドレスに一致させるには、アスタリスクを入力します。
Client Name	コンピュータ名を指定する変換ルール。 例：**Mary's Computer** 任意のコンピュータ名に一致させるには、アスタリスクを入力します。
Mac Address	MAC アドレスを指定する変換ルール。GPO エディタでは、クライアント システムで使用されている形式と同じものを使用する必要があります。例： ■ Windows クライアントではハイフンを使用します：**01-23-45-67-89-ab** ■ Linux クライアントではコロンを使用します：**01:23:45:67:89:ab** 任意の MAC アドレスに一致させるには、アスタリスクを入力します。
User/Group	ユーザーまたはグループ名を指定する変換ルール。 特定のユーザーまたはグループを指定するには、次の表記を使用します。 *\\domain\user_or_group* 例：**\\mydomain\Mary** 完全修飾ドメイン名 (FQDN) は、ドメイン名の表記としてサポートされていません。 任意のユーザー名またはグループ名を指定するには、アスタリスクを入力します。
Printer Name	リモート デスクトップにマッピングするプリンタの名前。 例：**PRINTER-2-CLR** マッピングされる名前は、クライアント システム上のプリンタ名と一致している必要はありません。 プリンタはクライアント デバイスのローカル プリンタである必要があります。ネットワーク プリンタの UNC パスへのマッピングはサポートされていません。
Printer Driver	プリンタで使用するドライバの名前。 例：**HP Color LaserJet 4700 PS** **重要:** 印刷ジョブはデスクトップからプリンタに直接送られるため、プリンタ ドライバをデスクトップにインストールする必要があります。
IP Port/ThinPrint Port	ネットワーク プリンタの場合は、先頭に **IP_** が付いたプリンタの IP アドレス。 例：**IP_10.114.24.1** デフォルトのポートは 9100 です。ポート番号を IP アドレスに付加することで、デフォルト以外のポートを指定できます。 例：**IP_10.114.24.1:9104**
Default	プリンタがデフォルトのプリンタであるかどうかを示します。

列見出しの上に表示されるボタンを使用して、行を追加、削除、移動し、表エントリを保存およびインポートします。各ボタンには対応するキーボード ショートカットがあります。各ボタンの上にマウスを置くと、ボタンの説明とその対応するキーボード ショートカットが表示されます。たとえば、表の末尾に行を挿入するには、先頭の表ボタンをクリックするか、<Alt> + <A> を押します。表エントリをインポートして保存するには、最後の 2 つのボタンをクリックします。

表 5-27. ロケーションベースの印刷グループ ポリシー設定の例に 2 つの変換表の行の例を示します。

表 5-27. ロケーションベースの印刷グループ ポリシー設定の例

IP Range（IP 範囲）	Client Name（クライアント名）	Mac Address（Mac アドレス）	User/Group（ユーザー/グループ）	Printer Name（プリンタ名）	Printer Driver（プリンタ ドライバ）	IP Port/ThinPrint Port（IP ポート/ThinPrint ポート）	デフォルト
*	*	*	*	PRINTER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	PRINTER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

最初の行に指定されているネットワーク プリンタは、すべての変換ルール列にアスタリスクが表示されているため、すべてのクライアント システムのリモート デスクトップにマッピングされます。2 行目に指定されているネットワーク プリンタは、クライアント システムの IP アドレスが 10.112.116.140 から 10.112.116.145 の範囲である場合のみ、リモート デスクトップにマッピングされます。

Active Directory グループ ポリシーの例

Horizon 7 で Active Directory グループ ポリシーを実装するには、リモート デスクトップ セッションを配信するマシンの組織単位 (OU) を作成して、その OU に 1 つ以上の GPO をリンクします。これらの GPO を使用して、Horizon 7 マシンにグループ ポリシー設定を適用します。

ポリシー設定をドメイン内のすべてのコンピュータに適用している場合は、GPO をドメインに直接リンクできます。ただし、ベスト プラクティスでは、ドメイン内のすべてのコンピュータでのポリシー処理を回避するために、ほとんどの環境では GPO を個別の OU にリンクする必要があります。

Active Directory サーバまたはドメイン内の任意のコンピュータでポリシーを構成できます。次の例に、Active Directory サーバで直接ポリシーを構成する方法を示します。

注: Horizon 7 環境はそれぞれ異なるため、組織固有のニーズに合わせて異なる手順の実行が必要な場合があります。

Horizon 7 マシンの組織単位 (OU) の作成

同じ Active Directory ドメインのその他の Windows コンピュータに影響を与えずにリモート デスクトップ セッションを提供するマシンにグループ ポリシーを適用するには、Horizon 7 マシン専用の組織単位 (OU) を作成します。Horizon 7 環境の全体に対して 1 つの OU を作成することや、仮想デスクトップ マシンと RDS ホスト用に個別の OU を作成することができます。

手順

1 Active Directory サーバで、[スタート] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーおよびコンピュータ] を選択します。

2 Horizon 7 マシンを含むドメインを右クリックし、[新規] - [組織単位 (OU)] を選択します。

3 OU の名前を入力し、[OK] をクリックします。

左ペインに新しい OU が表示されます。

4 Horizon 7 マシンを新しい OU に追加します。

a 左ペインの [コンピュータ] をクリックします。

ドメイン内のすべてのコンピュータ オブジェクトが右ペインに表示されます。

b 右パネルの Horizon 7 マシンを表すコンピュータ オブジェクトの名前を右クリックし、[移動] を選択します。

c OU を選択し、[OK] をクリックします。

OU を選択すると、右ペインに Horizon 7 マシンが表示されます。

次のステップ

Horizon 7 グループ ポリシーの GPO を作成します。

Horizon 7 グループ ポリシーの GPO の作成

Horizon 7 コンポーネントとロケーションベースの印刷のグループ ポリシーを格納する GPO を作成し、それらを Horizon 7 マシンの組織単位 (OU) にリンクします。

前提条件

- Horizon 7 マシンの OU を作成します。
- Active Directory サーバをホストするマシンに管理者ドメイン ユーザーとしてログインできることを確認します。
- MMC およびグループ ポリシー管理スナップインが Active Directory サーバで使用できることを確認します。

手順

1 Active Directory サーバで、グループ ポリシー管理コンソールを開きます。

2 ドメインを展開し、Horizon 7 マシンを格納する OU を右クリックし、[このドメインに GPO を作成し、このコンテナにリンクする] を選択します。

3 GPO の名前を入力し、[OK] をクリックします。

左ペインの OU の下に新しい GPO が表示されます。

4 （オプション） OU の特定の Horizon 7 マシンに GPO を適用します。

a 左ペインで GPO を選択します。

b [セキュリティ フィルタ処理] - [追加] を選択します。

c Horizon 7 マシンのコンピュータ名を入力し、[OK] をクリックします。

[セキュリティ フィルタ処理] ペインに Horizon 7 マシンが表示されます。GPO の設定はこれらのマシンにのみ適用されます。

次のステップ

Horizon ADMX テンプレートを GPO に追加します。

GPO への Horizon 7 ADMX テンプレート ファイルの追加

Horizon 7 コンポーネントのグループ ポリシー設定をリモート デスクトップおよびアプリケーションに適用するには、その ADMX テンプレート ファイルを GPO に追加します。

前提条件

- Horizon 7 コンポーネントのグループ ポリシー設定のための GPO を作成し、それらを Horizon 7 マシンが格納されている OU にリンクします。
- Active Directory サーバをホストするマシンに管理者ドメイン ユーザーとしてログインできることを確認します。
- MMC およびグループ ポリシー管理スナップインが Active Directory サーバで使用できることを確認します。

手順

1 Horizon 7 GPO Bundle `.zip` ファイルを https://my.vmware.com/web/vmware/downloads の VMware ダウンロード サイトからダウンロードします。

[Desktop & End-User Computing（デスクトップおよびエンドユーザー コンピューティング）] で VMware Horizon 7 のダウンロードを選択します。これには GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` で、*x.x.x* はバージョン、*yyyyyyy* はビルド番号を表します。Horizon 7 のグループ ポリシー設定用の ADMX ファイルはすべて、このファイルで提供されています。

2 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` ファイルを解凍して、ADMX ファイルを Active Directory サーバにコピーします。

a `.admx` ファイルと `en-US` フォルダを Active Directory サーバの `%systemroot%\PolicyDefinitions` フォルダにコピーします。

b 言語リソース (`.adml`) を Active Directory サーバの `%systemroot%\PolicyDefinitions\` 内の適切なサブフォルダにコピーします。

3 Active Directory サーバで、グループ ポリシー管理エディタを開き、インストール後にエディタに表示される場所となるテンプレート ファイルのパスを入力します。

次のステップ

グループ ポリシー設定を構成し、Horizon 7 マシンのループバック処理を有効にします。

リモート デスクトップのループバック処理の有効化

通常はある特定のコンピュータに適用されるユーザーの設定が、そのコンピュータにログインするすべてのユーザーに適用されるようにするには、ループバック処理を有効にします。

前提条件

- Horizon 7 コンポーネントのグループ ポリシー設定のための GPO を作成し、それらを Horizon 7 マシンが格納されている OU にリンクします。
- Active Directory サーバをホストするマシンに管理者ドメイン ユーザーとしてログインできることを確認します。
- MMC およびグループ ポリシー管理スナップインが Active Directory サーバで使用できることを確認します。

手順

1 Active Directory サーバで、グループ ポリシー管理コンソールを開きます。

2 ドメインを展開し、グループ ポリシー設定を作成した GPO を右クリックして、[編集] を選択します。

3 グループ ポリシー管理エディタで、[コンピュータの構成] - [ポリシー] - [管理用テンプレート: ポリシー定義] - [システム] - [グループ ポリシー] の順に移動します。

4 右側のペインで、[ユーザー グループ ポリシー ループバックの処理モード] をダブルクリックします。

5 [有効化] を選択し、[モード] ドロップダウン メニューからループバック処理モードを選択します。

オプション	アクション
Merge（マージ）	適用されるユーザー ポリシー設定は、コンピュータ GPO とユーザー GPO の両方に含まれるものを組み合わせたものです。競合がある場合は、コンピュータ GPO が優先されます。
Replace（置き換える）	ユーザー ポリシーはコンピュータに関連付けられている GPO からすべて定義されます。ユーザーに関連付けられているすべての GPO が無視されます。

6 [OK] をクリックして変更を保存します。