VMware Horizon Client for Windows のインストールとセットアップ ガイド

変更日：2019 年 1 月 09 日

VMware Horizon Client for Windows 4.10

vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。
https://docs.vmware.com/jp/
VMware の Web サイトでは、最新の製品アップデートを提供しています。
本書に関するご意見、ご要望をお寄せください。フィードバック送信先：
docfeedback@vmware.com

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

内容

VMware Horizon Client for Windows のインストールとセットアップ ガイド

この『VMware Horizon Client for Windows のインストールとセットアップ ガイド』では、VMware Horizon® Client™ ソフトウェアを Microsoft Windows クライアント システムにインストールして設定し、使用する方法について説明します。

この情報は、デスクトップやノート PC などの Microsoft Windows クライアント システムを含む Horizon の導入設定を行う必要がある管理者向けです。本書に記載されている内容は、仮想マシン　テクノロジーおよびデータセンターの運用に精通している経験豊富なシステム管理者向けに書かれています。

エンドユーザーの場合は、VMware Docs にある『VMware Horizon Client for Windows ユーザー ガイド』ドキュメントを参照するか、Horizon Client オンライン ヘルプを参照してください。

Windows ベースのクライアントのシステム要件とセットアップ

1

Horizon Client を実行するシステムは、一定のハードウェアおよびソフトウェア要件を満たす必要があります。

Windows システムの Horizon Client は、サーバに接続するときに、Internet Explorer のインターネット設定（プロキシ設定を含む）を使用します。Internet Explorer の設定が適切で、Internet Explorer からサーバの URL にアクセスできることを確認してください。

この章には、次のトピックが含まれています。

Windows クライアント システムのシステム要件

サポート対象の Microsoft Windows オペレーティング システムを使用している PC またはラップトップに Horizon Client for Windows をインストールできます。

Horizon Client をインストールする PC またはノート PC とその周辺機器は、一定のシステム要件を満たしている必要があります。

モデル	すべての x86 または x86-64 Windows デバイス
メモリ	1GB 以上の RAM
オペレーティング システム	Horizon Client は、次のオペレーティング システムをサポートします。

OS	バージョン	サービス パックまたはサービス オプション	サポートされるエディション
Windows 10	32 ビットまたは 64 ビット	バージョン 1809 SAC バージョン 1803 SAC (Spring Creators Update) バージョン 1709 SAC（Fall Creators Update） バージョン 1809 LTSC バージョン 1607 LTSB (Anniversary Update)	Home、Pro、Pro for Workstations、Enterprise および IoT Enterprise
Windows 8 または 8.1	32 ビットまたは 64 ビット	なし、または Update 2	Pro、Enterprise、および Industry Embedded
Windows 7	32 ビットまたは 64 ビット	SP1	Home、Enterprise、Professional、Ultimate
Windows Server 2008 R2	64 ビット	最新の更新	Standard
Windows Server 2012 R2	64 ビット	最新の更新	Standard

Windows Server 2008 R2 および Windows Server 2012 R2 は、Horizon Client をネスト モードで実行するためにサポートされます。詳細については、「ネスト モードでサポートされる機能」を参照してください。

Connection Server、セキュリティ サーバ、および View Agent または Horizon Agent

Horizon 6 バージョン 6.2.x 以降の最新メンテナンス リリース。

クライアント システムが企業のファイアウォールの外部から接続する場合は、クライアント システムで VPN 接続が不要となるようにセキュリティ サーバや Unified Access Gateway アプライアンスを使用します。

表示プロトコル

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

ネットワーク プロトコル

- IPv4
- IPv6

Horizon Client のカスタム インストールを実行するときに、インターネット プロトコルの自動選択を有効にできます。詳細については、「インターネット プロトコルの自動選択の有効化」を参照してください。IPv6 環境で Horizon を使用する方法については、『Horizon 7 のインストール』ドキュメントを参照してください。

PCoIP と VMware Blast のハードウェア要件

- SSE2 拡張命令に対応する x86 ベースのプロセッサ。800 MHz 以上のプロセッサ処理速度。

- さまざまなモニター セットアップをサポートするための、システム要件を超える RAM 空き容量。一般的な目安として次の式を使用してください。

```
20MB + (24 * (# monitors) * (monitor width) * (monitor height))
```

一般に、次のように計算します。

```
1 monitor: 1600 x 1200: 64MB
2 monitors: 1600 x 1200: 128MB
3 monitors: 1600 x 1200: 256MB
```

RDP のハードウェア要件

- SSE2 拡張命令に対応する x86 ベースのプロセッサ。800 MHz 以上のプロセッサ処理速度。
- 128MB RAM。

RDP のソフトウェア要件

- Windows 7 の場合は、RDP 7.1 または 8.0 を使用します。Windows 7 には RDP 7 が含まれます。Windows 7 SP1 には RDP 7.1 が含まれます。
- Windows 8 の場合は、RDP 8.0 を使用します。Windows 8.1 の場合は、RDP 8.1 を使用します。
- Windows 10 の場合は、RDP 10.0 を使用します。
- （View Agent 6.0.2 以前でのみサポートされる）Windows XP デスクトップ仮想マシンの場合、Microsoft サポート技術情報 (KB) の記事 323497 および 884020 に記載されている RDP パッチをインストールする必要があります。RDP パッチをインストールしないと、**Windows ソケットの失敗エラー** メッセージがクライアントに表示される可能性があります。
- エージェント インストーラによって、ホスト オペレーティング システムの現在の RDP ポート（通常は 3389）に合わせて受信 RDP 接続のローカル ファイアウォール ルールが構成されます。この RDP ポート番号を変更する場合は、関連するファイアウォール ルールも変更する必要があります。

リモート デスクトップ クライアントのバージョンは、Microsoft ダウンロード センターからダウンロードできます。

ビデオとグラフィックの要件

- Direct3D 11 ビデオをサポートするグラフィック カード。
- 最新のビデオ グラフィック カード ドライバ。
- Windows 7 SP1 の場合、Windows 7 SP1 と Windows Server 2008 R2 SP1 のプラットフォーム更新をインストールします。詳細については、https://support.microsoft.com/ja-jp/kb/2670838 を参照してください。

ビデオとグラフィックの要件

- Direct3D 11 ビデオをサポートするグラフィック カード。
- 最新のビデオ グラフィック カード ドライバ。

- Windows 7 SP1 の場合、Windows 7 SP1 と Windows Server 2008 R2 SP1 のプラットフォーム更新をインストールします。詳細については、https://support.microsoft.com/ja-jp/kb/2670838 を参照してください。

.NET Framework の要件

Horizon Client インストーラには .NET Framework バージョン 4.5 以降が必要です。このインストーラは、インストールを開始する前に、.NET Framework バージョン 4.5 以降がインストールされているかどうか確認します。クライアント コンピュータがこの前提条件を満たしていない場合、インストーラは .NET Framework の最新バージョンを自動的にダウンロードします。

Horizon Client 機能のシステム要件

Horizon Client 機能には、特定のハードウェアおよびソフトウェア要件があります。

スマート カード認証の要件

ユーザー認証にスマート カードを使用するクライアント デバイスは、特定の要件を満たす必要があります。

クライアントのハードウェア要件とソフトウェア要件

ユーザー認証にスマート カードを使用する各クライアント デバイスには、次のハードウェアおよびソフトウェアが必要です。

- Horizon Client
- 互換性のあるスマート カード リーダー

  Horizon Client では、PKCS#11 または Microsoft CryptoAPI プロバイダを使用するスマート カードおよびスマート カード リーダーがサポートされています。必要に応じて、ActivIdentity ActivClient ソフトウェア スイートをインストールできます。このソフトウェアは、スマート カードと対話するためのツールを提供します。
- 製品固有のアプリケーション ドライバ

スマート カードで認証を行うユーザーはスマート カードまたは USB スマート カード トークンを所有している必要があり、各スマート カードにはユーザー証明書が含まれる必要があります。

スマート カード登録の要件

スマート カードに証明書をインストールするには、管理者が登録局として機能するようにコンピュータを設定する必要があります。このコンピュータは、ユーザーにスマート カードを発行するための権限を持っている必要があり、証明書を発行するドメインのメンバーである必要があります。

スマート カードを登録するときに、生成される証明書のキー サイズを選択できます。ローカル デスクトップでスマート カードを使用するには、スマートカードの登録時に 1024 ビットまたは 2048 ビットのキー サイズを選択する必要があります。512 ビットの鍵の証明書はサポートされていません。

Microsoft TechNet の Web サイトでは、Windows システム用にスマート カード認証を計画して実装する方法についての詳細情報が提供されています。

リモート デスクトップおよび公開アプリケーションのソフトウェア要件

Horizon 管理者は、仮想デスクトップまたは RDS ホストに製品固有のアプリケーション ドライバをインストールする必要があります。

Horizon Client で、[ユーザー名のヒント] テキスト ボックスを有効にする

いくつかの環境では、スマート カード ユーザーは、単一のスマート カード証明書を使用して、複数のユーザーアカウントを認証できます。スマート カードでログインするときに、[ユーザー名のヒント] テキスト ボックスにユーザー名を入力します。

[ユーザー名のヒント] テキスト ボックスが Horizon Client のログイン ダイアログ ボックスに表示されるようにするには、接続サーバでスマート カードのユーザー名のヒント機能を有効にする必要があります。スマート カード ユーザー名のヒント機能は、Horizon 7 バージョン 7.0.2 以降のサーバとエージェントでのみサポートされます。スマート カード ユーザー名のヒント機能を有効にする方法については、『Horizon 7 の管理』を参照してください。

外部アクセスのセキュリティを確保するために、お使いの環境でセキュリティ サーバではなく Unified Access Gateway アプライアンスを使用している場合、スマート カード ユーザー名のヒント機能をサポートするように、Unified Access Gateway アプライアンスを構成する必要があります。スマート カード ユーザー名のヒント機能は、Unified Access Gateway 2.7.2 以降でのみサポートされます。Unified Access Gateway でスマート カード ユーザー名のヒント機能を有効にする方法については、『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。

Horizon Client は、スマート カード ユーザー名のヒント機能が有効な場合、単一アカウントのスマート カード証明書も引き続きサポートします。

スマート カード認証の追加要件

Horizon Client システムのスマート カード要件以外に、他の Horizon コンポーネントは、スマート カードをサポートするための特定の構成要件を満たす必要があります。

接続サーバおよびセキュリティ サーバ ホスト	管理者は、すべての信頼されたユーザー証明書に適用可能なすべての認証局 (CA) 証明書を接続サーバまたはセキュリティ サーバ ホスト上のサーバ信頼ストア ファイルに追加する必要があります。これらの証明書にはルート証明書が含まれています。を中間認証局がユーザーのスマート カードの証明書を発行している場合は、中間証明書も含まれます。 スマート カードの使用をサポートするように接続サーバを構成する方法については、『Horizon 7 の管理』を参照してください。
Active Directory	スマート カード認証のために管理者が Active Directory で実行する必要があるタスクについては、『Horizon 7 の管理』ドキュメント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 Web カメル、USB オーディオ、アナログ オーディオ デバイスで動作します。この機能は、Skype、WebEx、Google ハングアウトなどの標準的な会議アプリケーションにも対応しています。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。

仮想デスクトップ	仮想デスクトップには、View Agent 6.0 または Horizon Agent 7.0 以降がインストールされている必要があります。
公開されたデスクトップおよびアプリケーション	リアルタイム オーディオビデオ機能で公開デスクトップおよびアプリケーションで使用するには、RDS ホストに Horizon Agent 7.0.2 以降をインストール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	■ リアルタイム オーディオビデオは、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、「Windows クライアント システムのシステム要件」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。エージェントがインストールされているマシンにデバイス 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）

スキャナ リダイレクトのシステム要件

エンド ユーザーは、ローカル クライアント システムに接続されているスキャナを使用して、リモート デスクトップおよび公開アプリケーションの情報をスキャンできます。この機能を使用するには、リモート デスクトップ、アプリケーション、クライアント コンピュータが一定のシステム要件を満たしている必要があります。

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または RDS ホスト上のリモート デスクトップには、View Agent 6.0.2 以降または Horizon Agent 7.0 以降をインストールし、スキャナ リダイレクト セットアップ オプションを設定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。 仮想デスクトップおよび RDS ホストでサポートされているゲスト OS について、およびリモート デスクトップと公開アプリケーションでのスキャナ リダイレクトの設定については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントの「スキャナ リダイレクトの設定」を参照してください。
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	■ スキャナ リダイレクトは、Windows 7、Windows 8/8.1、および Windows 10 でサポートされています。

- 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。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 システムにスキャナのデバイス ドライバをインストールする必要はありません。

スキャン デバイスの標準

TWAIN または WIA

表示プロトコル

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

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。

シリアル ポート リダイレクトのシステム要件

シリアル ポート リダイレクト機能を使用すると、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 デスクトップと公開アプリケーション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。

仮想デスクトップ

仮想デスクトップ（シングルセッションの仮想マシン）に View Agent 6.1.1 以降または Horizon Agent 7.0 以降がインストールされ、シリアル ポート リダイレクトのセットアップ オプションが選択されている必要があります。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。

次のオペレーティング システムが仮想デスクトップでサポートされます。

- 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
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

シリアル ポート デバイス ドライバを仮想デスクトップにインストールする必要はありません。

公開デスクトップと公開アプリケーション

RDS ホストに Horizon Agent 7.6 以降がインストールされ、シリアル ポート リダイレクトのセットアップ オプションが選択されている必要があります。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。

次のオペレーティング システムが公開デスクトップと公開アプリケーションでサポートされます。

- Windows Server 2008 R2

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

RDS ホストにシリアル ポート デバイス ドライバがインストールされてい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、Windows 10 クライアント システム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 ポートが操作可能である必要があります。シリアル ポート リダイレクトは、Horizon Client for Windows 3.4 以降のリリースで利用できます。

表示プロトコル

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

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 リダイレクトの設定については、『Horizon 7 でのリモート デスクトップ機能の構成』 ドキュメントの「シリアル ポート リダイレクトの設定」を参照してください。

マルチメディア リダイレクト (MMR) のシステム要件

マルチメディア リダイレクト (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、ESXi ホストのロードを低減します。

リモート デスクトップ

- 仮想デスクトップには、View Agent 6.0.2 以降、または Horizon Agent 7.0 以降がインストールされている必要があります。
- 公開デスクトップの場合、RDS ホストに View Agent 6.1.1 以降または Horizon Agent 7.0 以降がインストールされている必要があります。

	オペレーティング システムの要件と他のソフトウェア要件、構成の詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントで Windows メディアのマルチメディア リダイレクトに関するトピックを参照してください。
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	32 ビットまたは 64 ビット Windows 7、Windows 8.x、または Windows 10
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 および 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。

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。

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。

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。『Horizon 7 でのリモート デスクトップ機能の構成』の Flash リダイレクトの構成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、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 がインストールされ、Flash リダイレクト オプションが有効になっ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。

	■ 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 URL リダイレクトの使用の要件

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ー ESXi ホストへの負荷が低減され、データセンター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 エンドポイントにライブ ビデオ イベントを同時にストリームするために必要となるバンド幅が削減されます。

フラッシュ URL リダイレクト機能は、Web ページの管理者によって Web ページ内に組み込まれた JavaScript を使用します。リモート デスクトップのユーザーが Web ページ内に指定された URL リンクをクリックすると、スクリプトは、ShockWave ファイル (SWF) 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 VMware 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。マルチキャストとユニキャストの両方がサポートされます。

フラッシュ URL リダイレクト機能は、エージェント ソフトウェアの正しいバージョンがインストールされている場合にのみ使用可能です。この機能は、View Agent 6.0 以降のエージェント ソフトウェアに含まれます。

フラッシュ URL リダイレクト機能を使用するには、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。クライアント システムが次のソフトウェア要件を満たしている必要があります。

- クライアント システムは、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 ファイル (SWF) をホストする Adobe Web サーバに IP 接続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。
- クライアント システムには、Internet Explorer (ActiveX を使用している) 用の Adobe Flash Player 10.1 以降が必要です。

フラッシュ URL リダイレクトのリモート デスクトップ要件のリスト、および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ために Web ページを構成する方法については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。

URL コンテンツ リダイレクトを使用するための要件

URL コンテンツ リダイレクト機能を使用すると、URL コンテンツをクライアント マシンからリモート デスクトップまたは公開アプリケーションにリダイレクトしたり（クライアントからエージェントへのリダイレクト）、リモート デスクトップまたは公開アプリケーションからクライアント マシンにリダイレクトできます（エージェントからクライアントへのリダイレクト）。

たとえば、エンド ユーザーは、クライアントでネイティブ Microsoft Word アプリケーションのリンクをクリックして、リモートの Internet Explorer アプリケーションでリンクを開くことができます。また、リモートの Internet Explorer アプリケーションのリンクをクリックして、クライアント マシンのネイティブ ブラウザでリンクを開くこともできます。リダイレクトには、HTTP、mailto、callto など、任意の数のプロトコルを設定できます。

注: callto プロトコルは Chrome ブラウザでの URL コンテンツ リダイレクトには対応していません。

Web ブラウザ

次のブラウザで URL を入力またはクリックすると、この URL にリダイレクトされます。

- Internet Explorer 9、10 および 11
- 64 ビットまたは 32 ビットの Chrome 60.0.3112.101 公式ビルド（Horizon 7 バージョン 7.4 以降が必要）

URL コンテンツ リダイレクトは、Microsoft Edge ブラウザなどの、Windows 10 ユニバーサル アプリケーション内でクリックされるリンクには動作しません。

クライアント システム

Horizon Client をインストールする場合は、URL コンテンツ リダイレクトを有効にする必要があります。URL コンテンツ リダイレクトを有効にするには、コマンド ラインから Horizon Client をインストールする必要があります。詳細については、「コマンド ラインからの Horizon Client のインストール」を参照してください。

Chrome ブラウザで URL コンテンツ リダイレクトを使用するには、Horizon 管理者が Chrome に VMware Horizon URL コンテンツ リダイレクト ヘルパー拡張機能をインストールし、有効にしておく必要があります。削除後も、拡張機能は Chrome Web ストアから手動でインストールできます。詳細については、Horizon 7 バージョン 7.4 以降の『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。

初めて Chrome ブラウザから URL がリダイレクトされる際は、URL を Horizon Client で開くよう求められます。URL コンテンツ リダイレクトを行うには、[URL:VMware Hori...lient Protocol を開く] をクリックしてください。[URL:VMware Hori...lient Protocol リンクの選択内容を保存] チェック ボックスを選択すると、このプロンプトは次回から表示されなくなります。

リモート デスクトップまたは公開アプリケーション

Horizon Agent がインストールされている場合、Horizon 管理者は URL コンテンツ リダイレクトを有効にする必要があります。詳細については、『Horizon 7 での仮想デスクトップのセットアップ』または『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』ドキュメントを参照してください。

Chrome ブラウザで URL コンテンツ リダイレクトを使用するには、Horizon 管理者側で Windows エージェント マシンに VMware Horizon URL コンテンツ リダイレクト ヘルパー拡張機能をインストールし有効にしておく必要があります。詳細は、Horizon 7 バージョン 7.4 以降の『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。

また、Horizon 管理者は、Horizon Client がクライアントからリモート デスクトップまたは公開アプリケーションに URL コンテンツをリダイレクトする方法、または Horizon Agent がリモート デスクトップまたは公開アプリケーションからクライアントに URL コンテンツをリダイレクトする方法も設定する必要があります。全詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントの「URL コンテンツ リダイレクトの構成」を参照してください。

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。

エンドユーザーが Google Chrome または Microsoft Edge 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。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、ESXi ホストの負荷が軽減され、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。

リモート デスクトップ

- 仮想デスクトップに Horizon Agent 7.3.2 以降（Chrome の場合）または Horizon Agent 7.5 以降（Edge の場合）がインストールされ、HTML5 マルチメディア リダイレクトのカスタム セットアップ オプションが選択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。
- 公開デスクトップの RDS ホストには Horizon Agent 7.3.2 以降をインストールし、HTML5 マルチメディア リダイレクトのカスタム セットアップ オプションを選択しておく必要があります。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。『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントで、HTML5 マルチメディア リダイレクトの設定に関するトピックを参照してください。
- Chrome または Edge ブラウザがインストールされている必要があります。

- Chrome または Edge 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。『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントで、HTML5 マルチメディア リダイレクトの設定に関するトピックを参照してください。

クライアント システム

- Horizon Client をインストールするときに、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 オプションを選択する必要があります。このオプションはデフォルトで選択されています。

リモート セッションの表示プロトコル

- PCoIP
- VMware Blast

位置情報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仮想デスクトップまたは RDS ホストとクライアント コンピュータは、位置情報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。

位置情報リダイレクトでは、位置情報がクライアント システムからリモート デスクトップまたは公開アプリケーションに送信されます。

仮想デスクトップまたは RDS ホスト

- [設定] - [プライバシー] - [位置情報] の順に移動し、Windows の [位置情報サービス] を [オン] に設定する必要があります。
- 位置情報リダイレクト機能は、次のリモート デスクトップ アプリケーションをサポートします。

アプリケーション	プラットフォーム
Google Chrome（最新バージョン）	すべての仮想デスクトップまたは RDS ホスト
Internet Explorer 11	すべての仮想デスクトップまたは RDS ホスト
Edge、マップ、天気などの Win32 および UWP アプリ	Windows 8.1、Windows 10

  必要であれば、サポート対象の各ブラウザで [位置情報] の権限設定を有効にする必要があります。

- 位置情報リダイレクトのカスタム セットアップ オプションを選択して、Horizon Agent 7.6 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』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』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 VMware 位置情報リダイレクト グループ ポリシー設定が行われている必要があります。『Horizon 7 でのリモート デスクトップ機能の構成』で位置情報リダイレクトの構成に関するトピックを参照してください。
- Internet Explorer 11 の場合、Windows 7 仮想デスクトップと RDS ホストで VMware Horizon 位置情報 IE プラグインを有効にする必要があります。Windows 8.1 と Windows 10 の仮想デスクトップの場合、VMware Horizon 位置情報リダイレクト IE プラグインを有効にする必要はありません。Internet Explorer は、VMware 位置情報リダイレクト ドライバがインストールされた Windows 8.1 および Windows 10 仮想デスクトップでサポートされます。『Horizon 7 でのリモート デスクトップ機能の構成』で位置情報リダイレクトの構成に関するトピックを参照してください。
- Chrome の場合、VMware Horizon 位置情報リダイレクトの Chrome プラグインを有効にする必要があります。『Horizon 7 でのリモート デスクトップ機能の構成』で位置情報リダイレクトの構成に関するトピックを参照してください。

クライアント システム

- Windows 8.1 および Windows 10 のクライアント システムの場合、Horizon が位置情報にアクセスできるように、[設定] - [プライバシー] - [位置情報] の順に移動して、Windows の [位置情報サービス] の設定を [オン] にする必要があります。
- クライアント システムの位置情報を共有するには、Horizon Client で [地理位置情報] を設定する必要があります。詳細については、「位置情報の共有」を参照してください。

リモート セッションの表示プロトコル

- PCoIP
- VMware Blast

セッション共同作業機能の要件

セッション共同作業機能を使用すると、他のユーザーを既存の Windows リモート デスクトップ セッションに招待できます。セッション共同作業機能を使用するには、Horizon 環境が特定の要件を満たしている必要があります。

セッション共同作業者

共同作業セッションに参加するには、ユーザーがクライアント システムに 4.7 以降の Horizon Client for Windows、Mac、または Linux をインストールしているか、HTML Access 4.7 以降を使用する必要があります。

Windows リモート デスクトップ

- Horizon Agent 7.4 以降を Windows 仮想デスクトップまたは公開デスクトップの RDS ホストにインストールする必要があります。

- セッション共同作業機能をデスクトップ プールまたはファーム レベルで有効にしておく必要があります。デスクトップ プールでセッション共同作業機能を有効にする方法については、『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。ファームでセッション共同作業機能を有効にする方法については、『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』ドキュメントを参照してください。

Horizon Agent グループ ポリシー設定を使用して、セッション共同作業機能を設定します。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。

Linux リモート デスクトップ	Linux リモート デスクトップの要件については、『Horizon 7 for Linux 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。
接続サーバ	セッション共同作業機能を利用するには、接続サーバ インスタンスでエンタープライズ ライセンスを使用している必要があります。
表示プロトコル	VMware Blast

セッション共同作業機能は、公開アプリケーション セッションをサポートしません。

Horizon Client で Microsoft Lync を使用するための要件

エンド ユーザーは、Microsoft Lync 2013 クライアントをリモート デスクトップで使用して、Unified Communications (UC) VoIP (voice over IP) および Lync 認定の USB オーディオおよびビデオ デバイスでビデオ チャット電話に参加できます。専用の IP 電話が不要になります。

このアーキテクチャでは、リモート デスクトップに Microsoft Lync 2013 クライアントをインストールし、クライアント エンドポイントに Microsoft Lync VDI プラグインをインストールする必要があります。エンド ユーザーは Microsoft Lync 2013 クライアントを使用して、プレゼンス、インスタント メッセージ、Web 会議、および Microsoft Office 機能を使用できます。

Lync VoIP またはビデオ チャットが行われると、Lync VDI プラグインはデータセンター サーバからクライアント エンドポイントにすべてのメディア処理をオフロードし、すべてのメディアを Lync で最適化されたオーディオおよびビデオ codec にエンコードします。この最適化されたアーキテクチャは拡張性が高く、低いネットワーク バンド幅を使用し、品質の高いリアルタイム VoIP およびビデオがサポートされたポイントツーポイントのメディア配信を提供します。詳細については、
http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf
に掲載されている Horizon 6 および Microsoft Lync 2013 に関するホワイト ペーパーを参照してください。

注: オーディオ録音はサポートされません。この統合は、PCiIP 表示プロトコルでのみサポートされます。

この機能には次の要件があります。

オペレーティング システム

- クライアントのオペレーティング システムで Microsoft Lync VDI プラグインをサポートしている必要があります。32 ビット クライアントのオペレーティング システムの要件については、https://www.microsoft.com/ja-jp/download/details.aspx?id=35457 を参照してください。64 ビット クライアントのオペレーティング システムの要件については、https://www.microsoft.com/ja-jp/download/details.aspx?id=35454 を参照してください。

  注: Windows 10 クライアントには対応していません。Windows 10 クライアントの場合は、Microsoft Lync ではなく Skype for Business が使用できます。詳細については、「Horizon Client と Skype for Business を使用するための要件」を参照してください。

- リモート デスクトップ（エージェント）のオペレーティング システムは、エージェントのバージョンによって異なります。

バージョン	ゲスト OS
View Agent 6.2 以降、または Horizon Agent 7.0 以降	32 ビットまたは 64 ビットの Windows 7 SP1、Windows 8.x、Windows 10、または 64 ビットの Windows Server 2008 R2 SP1、Windows Server 2012 R2 Microsoft RDS ホストの場合、Windows Server 2008 R2、Windows Server 2012、または Windows 2012 R2
View Agent 6.0 または 6.1	32 ビットまたは 64 ビットの Windows 7 SP1、Windows 8.x、または 64 ビットの Windows Server 2008 R2 SP1、Windows Server 2012 R2

クライアント システム ソフトウェア

- Microsoft Lync VDI プラグインの 32 ビットまたは 64 ビット バージョン。Horizon Client の 32 ビット バージョンをインストールする場合は、32 ビット プラグインをインストールします。Horizon Client の 64 ビット バージョンをインストールする場合は、64 ビット プラグインをインストールします。

  重要: 32 ビットの Microsoft Lync VDI プラグインをインストールする場合、Microsoft Office の 64 ビット バージョンをクライアント マシンにインストールしないでください。32 ビット の Microsoft Lync VDI プラグインは、64 ビットの Microsoft Office 2013 と互換性がありません。

- Microsoft Lync Server 2013 展開中に生成されたセキュリティ証明書は、信頼されたルート証明機関のディレクトリにインポートする必要があります。

リモート デスクトップ（エージェント）ソフトウェア

- View Agent 6.0 以降、または Horizon Agent 7.0 以降
- Microsoft Lync 2013 クライアント
- Microsoft Lync Server 2013 展開中に生成されたセキュリティ証明書は、信頼されたルート証明機関のディレクトリにインポートする必要があります

必要なサーバ	■ 接続サーバ 6.0 以降を実行しているサーバ ■ Microsoft Lync Server 2013 を実行しているサーバ ■ 仮想マシンをホストするための vSphere インフラストラクチャ vCenter Server および ESXi ホストは、vSphere 5.0 以降を実行する必要があります。
ハードウェア	■ 以前にリストした必要なソフトウェア コンポーネントのそれぞれをサポートするハードウェア ■ クライアント エンドポイント： 1.5GHz またはそれより高速の CPU および Microsoft Lync 2013 プラグイン用に最小 2GB の RAM

注: トラブルシューティングの情報については、VMware KB 2063769 と VMware KB 2053732 を参照してください。

Horizon Client と Skype for Business を使用するための要件

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、エンド ユーザーは仮想デスクトップ内で Skype for Business を実行できます。Skype で音声通話またはビデオ通話の実行中は、すべてのメディア処理が仮想デスクトップではなく、クライアント コンピュータで実行されます。

この機能を使用するには、Horizon Client for Windows のインストール時に Skype for Business 用の仮想化パックをクライアント マシンにインストールする必要があります。詳細については、章 2 「Horizon Client for Windows のインストール」を参照してください。

また、Horizon Agent のインストール時に、Horizon 管理者が VMware Virtualization Pack for Skype for Business 機能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 Agent のインストール方法については、『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。

詳しい要件については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントで「Skype for Business の設定」を参照してください。

サポートされているデスクトップのオペレーティング システム

Horizon 管理者は、ゲスト OS を実行する仮想マシンを作成して、ゲスト OS にエージェント ソフトウェアをインストールします。エンド ユーザーは、クライアント デバイスからこれらの仮想マシンにログインできます。

サポートされる Windows ゲスト OS のリストについては、『Horizon 7 のインストール』を参照してください。

View Agent 6.1.1 以降または Horizon Agent 7.0 以降の場合、いくつかの Linux ゲスト OS がサポートされます。システム要件、Linux 仮想マシンの構成、およびサポートされている機能のリストについては、『Horizon 6 for Linux デスクトップのセットアップ』または『Horizon 7 for Linux 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。

Horizon Client 向けの接続サーバの準備

エンド ユーザーがサーバに接続して、リモート デスクトップまたは公開アプリケーションにアクセスするには、Horizon 管理者が特定の接続サーバを設定する必要があります。

Unified Access Gateway とセキュリティ サーバ

- Horizon 環境に Unified Access Gateway アプライアンスがある場合は、Unified Access Gateway と連携するように接続サーバを構成します。『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。Unified Access Gateway アプライアンスは、セキュリティ サーバと同じ役割を実行します。
- Horizon 環境にセキュリティ サーバをデプロイしている場合は、接続サーバ 6.x の最新メンテナンス リリースとセキュリティ サーバ 6.x 以降のリリースを使用していることを確認します。詳細については、使用している Horizon バージョンのインストール ドキュメントを参照してください。

安全なトンネル接続

クライアント デバイスにセキュアなトンネル接続を使用し、その安全な接続を接続サーバ インスタンスまたはセキュリティ サーバの DNS ホスト名を使用して構成する場合には、クライアント デバイスがこの DNS 名を解決できることを確認します。

デスクトップおよびアプリケーション プール

- デスクトップまたはアプリケーション プールが作成済みであること、および使用する予定のユーザー アカウントにプールへのアクセス権が付与されていることを確認します。詳細については、『Horizon 7 での仮想デスクトップのセットアップ』 および 『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』 ドキュメントを参照してください。
- エンド ユーザーが高解像度ディスプレイを使用していて、高解像度モードのクライアント設定を使用して同時に全画面表示モードでリモート デスクトップを表示する場合は、Windows 7 以降のそれぞれのリモート デスクトップに十分な vRAM が割り当てられていることを確認します。vRAM の容量はエンド ユーザー用に設定したモニターの数とディスプレイの解像度に左右されます。vRAM の量を推定するには、『Horizon 7 アーキテクチャの計画』 ドキュメントを参照してください。

ユーザー認証

- Horizon Client で RSA SecurID または RADIUS 認証などの 2 要素認証を使用するには、接続サーバで 2 要素認証機能を有効にする必要があります。詳細については、『Horizon 7 の管理』 の 2 要素認証についてのトピックを参照してください。
- サーバ URL 情報や [ドメイン] ドロップダウン メニューなどの Horizon Client でセキュリティ情報を非表示にするには、接続サーバ インスタンスで [クライアントのユーザー インターフェイスでサーバ情報を非表示] および [クライアントのユーザー インターフェイスでドメイン リストを非表示] を有効にします。これらのグローバル設定は、Horizon 7 バージョン 7.1 以降で使用できます。グローバル設定については、『Horizon 7 の管理』 を参照してください。

[ドメイン] ドロップダウン メニューが表示されていない場合、**<domain>\<username>** または **<user>name@<domain>** の形式でユーザー名を [ユーザー名] テキスト ボックスに入力して、ドメイン情報を指定する必要があります。

重要: [クライアントのユーザー インターフェイスでサーバ情報を非表示] および [クライアントのユーザー インターフェイスでドメイン リストを非表示] 設定を有効にしており、接続サーバ インスタンスで 2 要素認証（RSA SecureID または RADIUS）を選択している場合、Windows ユーザー名の一致を強制しないでください。Windows ユーザー名の一致を強制すると、ユーザーは、ユーザー名のテキスト ボックスにドメイン情報を入力できなくなり、ログインが常に失敗します。詳細については、『Horizon 7 の管理』の 2 要素認証についてのトピックを参照してください。

- エンド ユーザーが認証しなくても Horizon Client で公開されたアプリケーションにアクセスできるようにするには、接続サーバ インスタンスでこの機能を有効にする必要があります。詳細については、『Horizon 7 の管理』の非認証アクセスについてのトピックを参照してください。

サーバへのログインに使用された前回のユーザー名のクリア

[クライアントのユーザー インターフェイスでドメイン リストを非表示] グローバル設定が有効になっている接続サーバにユーザーがログインすると、[ドメイン] ドロップダウン メニューが Horizon Client で非表示になり、ユーザーはドメイン情報を Horizon Client の [ユーザー名] テキスト ボックスに指定する必要があります。たとえば、ユーザーは **<domain>\<username>** または **<username>@<domain>** の形式でユーザー名を入力する必要があります。

前回のユーザー名が保存され、ユーザーが次回サーバにログインするときに [ユーザー名] テキスト ボックスに表示されるようにするかどうかは、レジストリ キーによって決定されます。[ユーザー名] テキスト ボックスに前回のユーザー名を表示せず、ドメイン情報を公開しないようにするには、Windows クライアント システムで `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\dontdisplaylastusername` レジストリ キーの値を 1 に設定する必要があります。

Horizon Client で [ドメイン] ドロップダウン メニューやサーバ URL 情報などのセキュリティ情報を非表示にする方法については、『Horizon 7 の管理』のグローバル設定に関するトピックを参照してください。

VMware Blast オプションの構成

VMware Blast 表示プロトコルを使用するリモート デスクトップ セッションと公開アプリケーション セッションに VMware Blast オプションを設定できます。

H.264 デコードと HEVC（High Efficiency Video Decoding）を許可することができます。H.264 デコードを許可するときに、色忠実度を上げることもできます。

サポートされている最大解像度と HEVC のサポートは、クライアントの画像処理装置 (GPU) の処理能力によって異なります。JPEG/PNG の 4K 解像度をサポートできる GPU であっても、H.264 の 4K 解像度をサポートしない場合があります。H.264 で解像度がサポートされていない場合、Horizon Client は JPEG/PNG を代わりに使用します。

H.264 デコードとハイカラー精度は、サーバに接続する前または後で設定できます。

注: Horizon Client の以前のバージョンでは、VMware Blast で最適なユーザー環境を提供するため、ネットワーク条件オプションを選択する必要がありました。このリリースでは、Horizon Client は、現在のネットワーク条件を検知し、1 つを以上のトランスポートを選択して、ユーザーの使用環境を自動的に最適化します。

前提条件

H.264 を使用するには、Horizon Agent 7.0 以降をインストールする必要があります。

H.264 デコードを許可するときに色忠実度を上げるには、Horizon Agent 7.4 以降をインストールする必要があります。

手順

1 メニュー バーで [オプション] ボタンをクリックして、[VMware Blast の構成] を選択します。

サーバにログインしている場合は、[設定]（歯車）アイコンをクリックし、[VMware Blast] を選択できます。

2 Horizon Client で H.264 デコードを許可するには、[H.264] チェック ボックスを選択します。

このオプションが選択されると（デフォルト設定）、エージェントが H.264 ソフトウェアまたはハードウェア エンコードをサポートしている場合に、Horizon Client は H.264 デコードを使用します。エージェントが H.264 ソフトウェアまたはハードウェア エンコードをサポートしていない場合、Horizon Client は JPG/PNG デコードを使用します。このオプションの選択を解除すると、Horizon Client は JPG/PNG デコードを使用します。

3 (オプション) Horizon Client で H.264 デコードが許可されているときに、色忠実度の向上を許可するには、[ハイカラー精度] チェック ボックスを選択します。

エージェントがハイカラー精度をサポートしている場合にのみ、このオプションを選択すると、Horizon Client がハイカラー精度を使用します。このオプションを選択すると、バッテリの消耗が早くなったり、パフォーマンスが低下する場合があります。デフォルトでは、この機能は無効になっています。

4 HEVC を許可するには、[HEVC (High Efficiency Video Decoding) を許可する] チェック ボックスを選択します。

クライアント コンピュータに HEVC デコードをサポートする GPU が搭載されている場合、このオプションを選択すると、パフォーマンスとイメージ品質が向上します。

5 [OK] をクリックして変更を保存します。

H.264 の変更は、ユーザーが次にリモート デスクトップまたは公開アプリケーションに接続して、VMware Blast 表示プロトコルを選択したときに有効になります。変更内容は、既存の VMware Blast セッションには影響しません。

Internet Explorer のプロキシ設定の使用

Horizon Client は、Internet Explorer のプロキシ設定を使用します。

プロキシ設定のバイパス

Horizon Client は、Internet Explorer のプロキシ バイパス設定を使用して、接続サーバ ホスト、セキュリティ サーバ、または Unified Access Gateway アプライアンスへの HTTPS 接続をバイパスします。

接続サーバ ホスト、セキュリティ サーバ、または Unified Access Gateway アプライアンスで安全なトンネルが有効になっている場合、トンネル接続をバイパスするアドレス リストを指定するには、Horizon Client 設定 ADM または ADMX テンプレート ファイルで **トンネル プロキシ バイパス アドレス リスト**のグループ ポリシー設定を使用する必要があります。これらのアドレスにはプロキシ サーバは使用されません。複数のエントリを区切るにはセミコロン (;) を使用します。このグループ ポリシー設定により、次のレジストリ キーが作成されます。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\TunnelProxyBypass
```

直接接続する場合、このグループ ポリシー設定は使用できません。グループ ポリシー設定を適用しても期待通りに機能しない場合、ローカル アドレスでプロキシをバイパスしてみます。詳細については、https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/ を参照してください。

プロキシ フェイル オーバー

Horizon Client では、Internet Explorer の [インターネット オプション] > [接続] > [ローカル エリア ネットワーク (LAN) の設定] にある [自動構成] の [自動構成スクリプトを使用する] 設定を使用して、プロキシのフェイル オーバーがサポートされます。この設定を使用するには、複数のプロキシ サーバを返す自動構成スクリプトを作成する必要があります。

Horizon Client データ共有の設定

Horizon 管理者がカスタマー エクスペリエンス向上プログラムへの参加を選択している場合、VMware はクライアント システムから匿名データを収集して受信し、ハードウェアとソフトウェアの互換性を優先度付けします。クライアント システムの情報を共有するかどうかを設定するには、Horizon Client の設定を有効または無効にします。

デフォルトでは、Horizon Client データ共有は有効に設定されています。データ共有の設定は、サーバに接続する前に行う必要があります。この設定は、すべてのサーバに適用されます。サーバに接続した後は、Horizon Client データ共有の設定を変更できません。

[データの共有を許可する] グループ ポリシー設定を使用すると、Horizon Client データ共有を有効または無効にしたり、Horizon Client ユーザー インターフェイスでのユーザーによる設定の変更を防ぐことができます。詳細については、「クライアント GPO の全般設定」を参照してください。

手順

1 メニュー バーで [オプション] ボタンをクリックして、[データの共有を許可する] を選択します。

2 Horizon Client データ共有を有効または無効にするには、データ共有モードを [オン] または [オフ] に設定します。

3 [OK] をクリックして変更を保存します。

VMware によって収集される Horizon Client データ

Horizon 管理者がカスタマ エクスペリエンス向上プログラムの参加を選択し、クライアント システムでデータの共有が有効になっている場合、VMware はクライアント システムに関するデータを収集します。

VMware は、クライアント システムで情報を収集し、ハードウェアとソフトウェアの互換性を優先度付けします。Horizon 管理者がカスタマ エクスペリエンス向上プログラムへの参加を決めた場合、VMware はお客様のご要望に対する対応を向上する目的で、現在ご使用の環境に関する匿名データを収集します。VMware は、組織を特定するデータを収集しません。Horizon Client の情報は、接続サーバ インスタンスに送信されてから、接続サーバ、デスクトップ プール、リモート デスクトップのデータと共に VMware に送信されます。

情報は暗号化されて、接続サーバ インスタンスに送信されます。クライアント システムの情報は、暗号化されていない状態でユーザー固有のディレクトリに記録されます。このログに個人情報は含まれません。

Horizon 管理者は、接続サーバのインストール時に VMware カスタマ エクスペリエンス向上プログラムに参加するかどうかを選択できます。インストール後に Horizon Administrator でオプションを設定することもできます。

表 1-1. カスタマー エクスペリエンス向上プログラムに関して Horizon Client で収集されるデータ

説明	このフィールドは匿名になりますか？	値の例
Horizon Client アプリケーションを開発する企業	いいえ	VMware
製品名	いいえ	VMware Horizon Client
クライアント製品のバージョン	いいえ	（形式は <x.x.x-yyyyyy> で、<x.x.x> はクライアントのバージョン番号、<yyyyyy> はビルド番号です。）
クライアントのバイナリ アーキテクチャ	いいえ	以下に例を挙げます。 ■ i386 ■ x86_64 ■ arm
クライアントのビルド名	いいえ	以下に例を挙げます。 ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
ホスト OS	いいえ	以下に例を挙げます。 ■ Windows 8.1 ■ Windows 7、64 ビット Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
ホスト OS のカーネル	いいえ	以下に例を挙げます。 ■ Windows 6.1.7601 SP1 ■ Darwin Kernel バージョン 11.0.0:Sun Apr 8 21:52:26 PDT 2012;root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ 不明（Windows ストア版）

表 1-1. カスタマー エクスペリエンス向上プログラムに関して Horizon Client で収集されるデータ (続き)

説明	このフィールドは匿名になりますか？	値の例
ホスト OS のアーキテクチャ	いいえ	以下に例を挙げます。 ■ x86_64 ■ i386 ■ armv71 ■ ARM
ホスト システムのモデル	いいえ	以下に例を挙げます。 ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision Workstation T3400 (A04 03/21/2008)
ホスト システムの CPU	いいえ	以下に例を挙げます。 ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ 不明 (iPad)
ホスト システムのプロセッサのコア数	いいえ	例： 4
ホスト システムのメモリ容量（MB）	いいえ	以下に例を挙げます。 ■ 4096 ■ 不明（Windows ストア版）
接続された USB デバイスの数	いいえ	2（USB デバイスのリダイレクトは Linux、Windows および Mac クライアントでのみサポートされています。）
同時並行する USB デバイスの最大接続数	いいえ	2
USB デバイス ベンダー ID	いいえ	以下に例を挙げます。 ■ Kingston ■ NEC ■ Nokia ■ Wacom
USB デバイス製品 ID	いいえ	以下に例を挙げます。 ■ DataTraveler ■ ゲームパッド ■ ストレージ ドライブ ■ 無線マウス
USB デバイス ファミリ	いいえ	以下に例を挙げます。 ■ セキュリティ ■ ヒューマン インターフェイス デバイス ■ イメージング
USB デバイス使用数	いいえ	（デバイスが共有された回数）

Horizon Client for Windows のインストール

2

Windows ベースの Horizon Client インストーラは、VMware Web サイト、または接続サーバで提供される Web アクセス ページから入手できます。Horizon Client をインストールした後で、エンド ユーザー向けのさまざまな起動オプションを設定できます。

この章には、次のトピックが含まれています。

Windows クライアント オペレーティング システムでの FIPS モードの有効化

連邦情報処理標準 (FIPS) 準拠の暗号を使用して Horizon Client をインストールする場合、Horizon Client インストーラを実行する前にクライアント オペレーティング システムで FIPS モードを有効にする必要があります。

クライアント オペレーティング システムで FIPS モードが有効になっている場合、FIPS-140 に準拠し、FIPS で承認されている動作モードに準拠した暗号アルゴリズムのみがアプリケーションで使用されます。ローカル セキュリティ ポリシーまたはグループ ポリシーの一部として特定のセキュリティ設定を有効にするか、Windows レジストリ キーを編集して、FIPS モードを有効にできます。

FIPS 準拠は Horizon 6 バージョン 6.2 以降で利用できます。詳細については、『Horizon 7 のインストール』を参照してください。

FIPS 構成プロパティの設定

クライアント オペレーティング システムで FIPS モードを有効にするには、Windows グループ ポリシー設定を使用したり、クライアント コンピュータの Windows レジストリ設定を使用したりできます。

- グループポリシー設定を使用するには、グループポリシー エディターを開き、**[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]** に移動し、[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] 設定を有効にします。

- Windows レジストリを使用するには、**HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled** に移動し、[有効] を 1 に設定します。

FIPS モードの詳細については、https://support.microsoft.com/en-us/kb/811833 にアクセスしてください。

重要: Horizon Client インストーラを実行する前に FIPS モードを有効にしないと、カスタム インストール中に FIPS 準拠の暗号化を使用するためのインストーラのオプションが表示されません。FIPS 準拠の暗号化は、通常のインストール時には有効になっていません。FIPS 準拠の暗号オプションを使用せずに Horizon Client をインストールし、後でこのオプションを使用することを決定する場合は、クライアントをアンインストールし、クライアント オペレーティング システムで FIPS モードを有効にして、Horizon Client インストーラをもう一度実行します。

インターネット プロトコルの自動選択の有効化

Horizon Client のカスタム インストールを実行するときに、インターネット プロトコルの自動選択を有効にできます。自動選択を有効にすると、Horizon Client は現在のネットワークを確認し、IPv4 または IPv6 経由で自動的に接続します。

自動選択を有効にすると、VMware Blast 表示プロトコルを使用する Horizon 7 バージョン 7.5 以降と Unified Access Gateway 3.3 以降で次の機能がサポートされます。

- 現在のユーザーとしてログイン
- オーディオ出力
- カスタマー エクスペリエンス向上プログラム データの収集
- 仮想印刷
- VMware 仮想印刷リダイレクト（Horizon 77.7 以降のバージョンが必要）
- HTML5 マルチメディア リダイレクト
- VMware ビデオ
- USB リダイレクト

Horizon Client for Windows のインストール

Windows ベースのインストーラ ファイルを実行して、すべての Horizon Client のコンポーネントをインストールできます。

この手順では、インタラクティブなインストール ウィザードを使用して Horizon Client をインストールする方法について説明します。コマンド ラインから Horizon Client をインストールする場合には、「コマンド ラインからの Horizon Client のインストール」を参照してください。URL コンテンツ リダイレクト機能をインストールする場合には、コマンド ラインからインストーラを実行する必要があります。

注: リモート デスクトップで View Agent 6.0 以降または Horizon Agent 7.0 以降が実行されている場合は、リモート デスクトップの仮想マシンに Horizon Client をインストールできます。エンド ユーザーが Windows シンクライアント デバイスから公開アプリケーションにアクセスする場合、このインストール方法を利用できます。

前提条件

- クライアント システムがサポートされているオペレーティング システムを使用していることを確認します。「Windows クライアント システムのシステム要件」を参照してください。
- Horizon Client インストーラを含むダウンロード ページの URL を調べておきます。この URL は、VMware のダウンロード ページ http://www.vmware.com/go/viewclients、または接続サーバ インスタンスの URL である場合があります。
- クライアント システムに管理者としてログインできることを確認します。
- ドメイン コントローラに最新のパッチが適用済みで、十分な空きディスク領域があり、互いに通信できることを検証します。それ以外の場合は、Windows 8.1 システムでインストーラを実行すると、インストーラが処理を終了するまでに通常よりも長い時間がかかることがあります。マシンのドメイン コントローラまたは階層内にある他のドメイン コントローラが応答していないか、これらのコントローラに接続できない場合に、この問題が発生します。
- FIPS 準拠の暗号を使用して Horizon Client をインストールする場合は、クライアントのオペレーティング システムで FIPS モードを有効にします。「Windows クライアント オペレーティング システムでの FIPS モードの有効化」を参照してください。
- IPv6 プロトコルを選択するか、インターネット プロトコルの自動選択を使用する場合は、IPv6 環境で利用できない機能を『Horizon 7 のインストール』ドキュメントで確認してください。
- インターネット プロトコルの自動選択を有効にする場合は、サポートされる機能を「インターネット プロトコルの自動選択の有効化」で確認してください。
- [USB リダイレクト] コンポーネントをインストールする場合には、次の操作を実行します。
  - クライアント デバイスを使用するユーザーがリモート デスクトップからローカルに接続された USB デバイスにアクセスできるようにするかどうかを決定します。アクセスが許可されていない場合は、[USB リダイレクト] コンポーネントをインストールしないか、コンポーネントをインストールしてからグループ ポリシー設定を使用して無効にします。グループ ポリシーを使用して USB リダイレクトを無効にしている場合、クライアントの USB リダイレクトを後で有効にする場合に、Horizon Client を再インストールする必要はありません。詳細については、「クライアント GPO のスクリプト定義設定」を参照してください。
  - クライアント コンピュータで Windows の自動更新機能が無効になっていないことを確認します。
- エンド ユーザーが現在ログインしているユーザーとして Horizon Client およびリモート デスクトップにログインできる機能を使用するかどうかを決定します。ユーザーがクライアント システムにログインするときに入力した認証情報が、接続サーバ インスタンスに渡され、最終的にはリモート デスクトップに渡されます。一部のクライアント OS はこの機能をサポートしていません。
- 接続サーバ インスタンスの完全修飾ドメイン名 (FQDN) をエンド ユーザーが入力する必要がないようにする場合は、インストールの間に指定できるように FQDN を決定します。

手順

1 クライアント システムに管理者としてログインします。

2 http://www.vmware.com/go/viewclients の VMware ダウンロード ページに移動します。

3 インストーラ ファイル、たとえば、**VMware-Horizon-Client-<y.y.y>-<xxxxxx>.exe** をダウンロードします。

<xxxxxx> はビルド番号、<y.y.y> はバージョン番号です。

4 インストーラ ファイルをダブルクリックしてインストールを開始します。

5 インストール タイプを選択し、画面の指示に従って操作します。

オプション	アクション
通常のインストール	[同意してインストール] をクリックします。インストーラが、IPv4 インターネット プロトコルを使用するようにクライアントを設定し、USB リダイレクト、現在のユーザーとしてログイン、Virtualization Pack for Skype for Business、HTML5 Multimedia Redirection サポート機能をインストールします。
カスタム インストール	[インストールをカスタマイズ] をクリックして、インストールする機能を選択します。 次の機能を指定するには、このオプションを選択する必要があります。 ■ デフォルト以外のインストール場所を指定します。 ■ IPv6 インターネット プロトコルを使用します。 ■ インターネット プロトコルの自動選択を有効にします。Horizon Client は現在のネットワークを確認し、IPv4 または IPv6 経由で自動的に接続します。 ■ デフォルトの接続サーバ インスタンスを構成します。 ■ デフォルトのログイン動作を設定します。 ■ FIPS 準拠の暗号を有効にします。インストーラで FIPS 準拠の暗号化を有効にするカスタム インストール オプションが使用できるのは、クライアント オペレーティング システムで FIPS モードが有効になっている場合のみです。 ■ 64 ビット マシンに 32 ビットのコア Remote Experience コンポーネントをインストールします。 注: 64 ビット クライアント マシンに製品の 64 ビット用プラグインがインストールされていない場合には、[64 ビット マシンの 32 ビット コア Remote Experience] 機能を選択します。

一部の機能では、クライアント システムの再起動が必要になります。

インストーラによって、VMware Horizon Client (**horizon_client_service**) および VMware USB Arbitration Service (**VMUSBArbService**) などの Windows サービスがインストールされます。

次のステップ

Horizon Client を起動して、正しいリモート デスクトップまたは公開アプリケーションにログインできることを確認します。「リモート デスクトップまたは公開アプリケーションへの接続」を参照してください。

コマンド ラインからの Horizon Client のインストール

コマンド ラインでインストーラのファイル名を入力し、インストール コマンドとプロパティを指定して、Horizon Client をインストールできます。

コマンド ラインから Horizon Client をインストールする場合、サイレント インストールを実行できます。サイレント インストールを使うと、大規模企業に Horizon Client を効率よく展開できます。

Horizon Client のインストール コマンド

コマンド ラインから Horizon Client をインストールするときに、特定のインストール コマンドを指定できます。

次の表に、Horizon Client インストール コマンドの説明を示します。

表 2-1. Horizon Client インストール コマンド

コマンド	説明
/? または /help	Horizon Client インストール コマンドとプロパティを一覧表示します。
/silent	Horizon Client をサイレント モードでインストールします。ウィザード プロンプトに応答する必要はありません。
/install	Horizon Client をインタラクティブにインストールします。ウィザード プロンプトに応答する必要があります。
/uninstall	Horizon Client をアンインストールします。
/repair	Horizon Client を修復します。
/norestart	インストール中に再起動プロンプトは表示されません。
/x /extract	インストーラ パッケージを %TEMP% ディレクトリに展開します。
/l または /log	インストール ログ ファイルのフォルダと名前付けパターンを指定します。 たとえば、次のコマンドを指定すると、Horizon Client インストーラは Test のプリフィックスが付いたログ ファイルを C:\Temp フォルダ配下に作成します。 `/log "C:\Temp\Test"`

Horizon Client のインストール プロパティ

コマンド ラインから Horizon Client をインストールするときに、特定のインストール プロパティを指定できます。

次の表に、Horizon Client インストール プロパティの説明を示します。

表 2-2. Horizon Client インストール プロパティ

プロパティ	説明	デフォルト
INSTALLDIR	Horizon Client がインストールされるパスおよびフォルダ。例： `INSTALLDIR=""D:\abc\my folder""` パスを囲む引用符によってインストーラにパスの有効部分としてスペースを解釈することを許可します。	%ProgramFiles %VMware\VMware Horizon View Client
VDM_IP_PROTOCOL_USAGE	Horizon Client コンポーネントが通信に使用する IP (インターネット プロトコル) バージョン。有効な値は以下のとおりです。 ■ IPv4 ■ IPv6 ■ Dual Dual を指定すると、Horizon Client は現在のネットワークを確認し、IPv4 または IPv6 経由で自動的に接続します。	IPv4

表 2-2. Horizon Client インストール プロパティ (続き)

プロパティ	説明	デフォルト
VDM_FIPS_ENABLED	FIPS 準拠の暗号を使用して Horizon Client をインストールするかどうかを決めます。 値に 1 を指定すると、FIPS 準拠の暗号化を使用して Horizon Client がインストールされます。値に 0 を指定すると、FIPS 準拠の暗号化を使用せずに Horizon Client がインストールされます。 注: このプロパティを 1 に設定する前に、Windows クライアント オペレーティング システムで FIPS モードを有効にしておく必要があります。「Windows クライアント オペレーティング システムでの FIPS モードの有効化」を参照してください。	0
VDM_SERVER	Horizon Client ユーザーがデフォルトで接続する接続サーバ インスタンスの完全修飾ドメイン名 (FQDN)。 例： VDM_Server=cs1.companydomain.com このプロパティを設定する場合、Horizon Client ユーザーがこの FQDN を入力する必要はありません。	なし
LOGINASCURRENTUSER_DISPLAY	Horizon Client のメニュー バーの [オプション] メニューに [現在のユーザーとしてログイン] を表示するかどうかを指定します。有効な値は、1（有効）または 0（無効）です。	1
LOGINASCURRENTUSER_DEFAULT	Horizon Client のメニュー バーの [オプション] メニューで、[現在のユーザーとしてログイン] がデフォルトで選択されるかどうかを指定します。有効な値は 1（有効）または 0（無効）です。 現在のユーザーとしてログインがデフォルトのログイン動作の場合、ユーザーがクライアント システムにログインするときに入力した ID と認証情報が、接続サーバ インスタンスに渡され、最終的にリモート デスクトップに渡されます。現在のユーザーとしてログインがデフォルトのログイン動作でない場合、リモート デスクトップまたはアプリケーションにアクセスする前に、ユーザーは ID と認証情報を複数回入力する必要があります。	0

表 2-2. Horizon Client インストール プロパティ (続き)

プロパティ	説明	デフォルト
ADDLOCAL	インストールする機能を指定します。有効な値は以下のとおりです。 ■ ALL - URL コンテンツ リダイレクトを除く、使用可能なすべての機能をインストールします。 ■ TSSO - 現在のユーザーとしてログイン機能をインストールします。 ■ USB - USB リダイレクト機能をインストールします。 複数の機能を指定するには、機能名のカンマ区切りのリストを入力します。名前の間にスペースを使用しないでください。 たとえば、Horizon Client と一緒に USB リダイレクト機能をインストールし、現在のユーザーとしてログイン機能をインストールしない場合には、次のコマンドを入力します。 `VMware-Horizon-Client-<y.y.y>-<xxxxxx>.exe ADDLOCAL=USB`	なし
INSTALL_32BITRMKS	64 ビット クライアント マシンに 32 ビット コア Core Remote Experience コンポーネントをインストールするかどうかを指定します。値に 1 を指定すると、32 ビット コア Remote Experience コンポーネントがインストールされます。値に 0 を指定すると、64 ビット コア Remote Experience コンポーネントがインストールされます。 64 ビット クライアント マシンに製品の 64 ビット用プラグインがインストールされていない場合には、32 ビット コア Remote Experience コンポーネントをインストールします。 このプロパティは、32 ビット クライアント マシンでは無効です。	0
INSTALL_SFB	VMware Virtualization Pack for Skype for Business 機能をインストールするかどうかを決めます。値に 1 を指定すると、この機能がインストールされます。値に 0 を指定すると、この機能はインストールされません。	1
INSTALL_HTML5MMR	HTML5 マルチメディア リダイレクト機能をインストールするかどうかを決めます。値に 1 を指定すると、この機能がインストールされます。値に 0 を指定すると、この機能はインストールされません。	1

表 2-2. Horizon Client インストール プロパティ (続き)

プロパティ	説明	デフォルト
REMOVE	インストールしない機能を指定します。有効な値は以下のとおりです。 ■ ThinPrint - 仮想印刷機能をインストールしません。 ■ Scanner - スキャナ リダイレクト機能をインストールしません。 ■ FolderRedirection - フォルダ リダイレクト機能をインストールしません。 ■ SerialPort - シリアル ポート リダイレクト機能をインストールしません。 複数の機能を指定するには、機能名のカンマ区切りのリストを入力します。名前の間にスペースを使用しないでください。 たとえば、次のコマンドでは、仮想印刷とスキャナ リダイレクト機能がインストールされません。 `VMware-Horizon-Client-<y.y.y>-<xxxxxx>.exe REMOVE=ThinPrint,Scanner`	なし
DESKTOP_SHORTCUT	Horizon Client にデスクトップ ショートカットを作成するかどうかを決めます。0 を指定すると、デスクトップ ショートカットは作成されません。1 を指定すると、デスクトップ ショートカットが作成されます。	1
STARTMENU_SHORTCUT	Horizon Client にスタート メニュー ショートカットを作成するかどうかを決めます。0 を指定すると、スタート メニュー ショートカットは作成されません。1 を指定すると、スタート メニュー ショートカットが作成されます。	1
URL_FILTERING_ENABLED	URL コンテンツ リダイレクト機能をインストールするかどうかを決めます。値に 1 を指定すると、この機能がインストールされます。値に 0 を指定すると、この機能はインストールされません。 インタラクティブ インストールでこのプロパティを 1 に設定すると、カスタム インストールのダイアログ ボックスの下に [URL コンテンツ リダイレクト] チェック ボックスが表示され、デフォルトで選択されます。このプロパティを 1 に設定しないければ、このチェック ボックスは表示されません。 注: ADDLOCAL=ALL プロパティには、URL コンテンツ リダイレクト機能が含まれていません。	0
AUTO_UPDATE_ENABLED	オンライン アップデート機能を有効にするかどうかを決めます。値に 1 を指定すると、この機能は有効になります。値に 0 を指定すると、この機能は無効になります。 詳細については、「Horizon Client オンライン更新」を参照してください。	1

コマンド ラインからの Horizon Client のインストール

コマンド ラインから Horizon Client をインストールするには、インストーラのファイル名を入力し、インストール コマンドとプロパティを指定します。コマンド ラインから Horizon Client をサイレント モードでインストールできます。

前提条件

- クライアント システムがサポートされているオペレーティング システムを使用していることを確認します。「Windows クライアント システムのシステム要件」を参照してください。
- クライアント システムに管理者としてログインできることを確認します。
- ドメイン コントローラに最新のパッチが適用済みで、十分な空きディスク領域があり、互いに通信できることを検証します。それ以外の場合は、Windows 8.1 システムでインストーラを実行すると、インストーラが処理を終了するまでに通常よりも長い時間がかかることがあります。マシンのドメイン コントローラまたは階層内にある他のドメイン コントローラが応答していないか、これらのコントローラに接続できない場合に、この問題が発生します。
- FIPS 準拠の暗号を使用して Horizon Client をインストールする場合は、クライアントのオペレーティング システムで FIPS モードを有効にします。「Windows クライアント オペレーティング システムでの FIPS モードの有効化」を参照してください。
- エンド ユーザーが現在ログインしているユーザーとして Horizon Client およびリモート デスクトップにログインできる機能を使用するかどうかを決定します。ユーザーがクライアント システムにログインするときに入力した認証情報が、接続サーバ インスタンスに渡され、最終的にはリモート デスクトップに渡されます。一部のクライアント OS はこの機能をサポートしていません。
- Horizon Client インストール コマンドについて理解しておきます。「Horizon Client のインストール コマンド」を参照してください。
- Horizon Client インストール プロパティについて理解しておきます。「Horizon Client のインストール プロパティ」を参照してください。
- エンド ユーザーがリモート デスクトップからローカルに接続された USB デバイスにアクセスできるようにするかどうかを決定します。あるいは、機能リストに **ADDLOCAL** インストール プロパティを設定し、USB 機能を除外します。詳細については、「Horizon Client のインストール プロパティ」を参照してください。
- 接続サーバ インスタンスの完全修飾ドメイン名 (FQDN) をエンド ユーザーが入力する必要がないようにする場合は、インストールの間に指定できるように FQDN を決定します。

手順

1 クライアント システムに管理者としてログインします。

2 http://www.vmware.com/go/viewclients の VMware ダウンロード ページに移動します。

3 Horizon Client インストーラ ファイル、たとえば、**VMware-Horizon-Client-<y.y.y>-<xxxxxx>.exe** をダウンロードします。

<xxxxxx> はビルド番号、<y.y.y> はバージョン番号です。

4 Windows クライアント コンピュータでコマンド プロンプトを開きます。

5 インストーラのファイル名、インストール コマンド、インストール プロパティを 1 行で入力します。

```
VMware-Horizon-Client-<y.y.y>-<xxxxxx>.exe [<commands>] [<properties>]
```

指定したインストール コマンドとプロパティに基づいて、インストーラが Horizon Client をインストールします。**/silent** インストール コマンドを指定した場合、ウィザード プロンプトは表示されません。

インストーラによって、VMware Horizon Client (**horizon_client_service**) および VMware USB Arbitration Service (**VMUSBArbService**) などの Windows サービスがインストールされます。

例：インストール コマンドの例

次のコマンドは、Horizon Client をインタラクティブにインストールし、URL コンテンツ リダイレクト機能を有効にします。

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

次のコマンドは、Horizon Client をサイレント モードでインストールします。インストール中に再起動プロンプトは表示されません。

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /norestart
```

次のステップ

Horizon Client 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した場合には、機能がインストールされていることを確認します。「URL コンテンツ リダイレクトのインストールの確認」を参照してください。

Horizon Client を起動して、正しいリモート デスクトップまたは公開アプリケーションにログインできることを確認します。「リモート デスクトップまたは公開アプリケーションへの接続」を参照してください。

URL コンテンツ リダイレクトのインストールの確認

Horizon Client 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した場合、この機能がインストールされていることを確認します。

前提条件

Horizon Client をインストールするときに、**URL_FILTERING_ENABLED=1** インストール プロパティを指定します。「コマンド ラインからの Horizon Client のインストール」を参照してください。

手順

1 クライアント マシンにログインします。

2 **vmware-url-protocol-launch-helper.exe** ファイルと **vmware-url-filtering-plugin.dll** ファイルが **%PROGRAMFILES%\VMware\VMware Horizon View Client** 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。

3 Internet Explorer に VMware Horizon View URL Filtering Plugin アドオンがインストールされ、有効になっていることを確認します。

Horizon Client オンライン更新

Horizon Client をオンラインで更新できます。

オンライン アップグレード機能を無効にするには、**Enable Horizon Client online update** グループ ポリシー設定を変更します。**URL for Horizon Client online update** グループ ポリシー設定を変更すると、更新を取得する代替 URL を指定できます。詳細については、「クライアント GPO の全般設定」を参照してください。

コマンドラインから Horizon Client をインストールする場合は、**AUTO_UPDATE_ENABLED** プロパティを 0 に設定するとオンライン　アップデート機能を無効にできます。詳細については、「Horizon Client のインストール プロパティ」を参照してください。

前提条件

- Horizon Client を更新する前に、作業を保存します。更新すると、システムが再起動される場合があります。
- クライアント システムに管理者としてログインできることを確認します。

手順

1 クライアント システムに管理者としてログインします。

2 Horizon Client を開始して、[ソフトウェアの更新] をクリックします。

オプション	アクション
サーバへの接続前	[オプション] - [ソフトウェアの更新] の順にクリックします。
サーバへの接続後	[ヘルプ] - [ソフトウェアの更新] の順にクリックします。

3 使用可能な更新を確認するには、[更新の確認] をクリックします。

Horizon Client により、利用可能な更新があるかどうかが表示されます。

[更新の通知を有効にする] チェック ボックスがオンになっている場合（デフォルト）、Horizon Client が使用可能な更新を検出します。新しい Horizon Client バージョンが使用可能であることを示すため、[オプション] メニュー（サーバとの接続前）または [ヘルプ] ボタン（サーバとの接続後）に赤色のドットが表示されます。このチェック ボックスをオフにすると、自動更新の検出を無効にできます。

4 更新が利用可能な場合に更新プロセスを開始するには、[をダウンロードとインストール] をクリックします。

5 Horizon Client が更新をダウンロードした後に更新をインストールするには、[OK] をクリックします。

Horizon Client のインタラクティブなインストール ウィザードが開きます。

エンド ユーザー向け Horizon Client の構成 3

エンド ユーザーに Horizon Client を設定するときに、Horizon Client を起動する URI、証明書確認モード、高度な TLS/SSL オプション、グループ ポリシーの使用を設定し、カスタム設定を作成できます。

この章には、次のトピックが含まれています。

一般的な設定

Horizon Client ではエンド ユーザー向けに、ログインとリモート デスクトップでの選択を簡素化し、セキュリティ ポリシーを実行するためのいくつかの構成メカニズムを提供しています。

次の表に、複数の方法で設定できる設定の一部のみを示します。

表 3-1. 一般的な設定

設定	構成メカニズム
サーバ アドレス	URI、グループ ポリシー、コマンド ライン、Windows レジストリ
Active Directory ユーザー名	URI、グループ ポリシー、コマンド ライン、Windows レジストリ
ドメイン名	URI、グループ ポリシー、コマンド ライン、Windows レジストリ
リモート デスクトップの表示名	URI、グループ ポリシー、コマンド ライン
ウィンドウ サイズ	URI、グループ ポリシー、コマンド ライン
表示プロトコル	URI、コマンド ライン
証明書確認の構成	グループ ポリシー、Windows レジストリ
TLS プロトコルと暗号化アルゴリズムの構成	グループ ポリシー、Windows レジストリ

URI を使用した Horizon Client の構成

エンドユーザーがクリックして Horizon Client を起動したり、リモート デスクトップまたは公開アプリケーションを開くことができるように、URI (Uniform resource identifier) を使用して Web ページのリンクまたは E メールのリンクを作成できます。

部分的または以下のすべての情報を提供する URI を作成することでこれらのリンクを作成すれば、エンド ユーザーは入力する必要がありません。

- サーバ アドレス
- サーバのポート番号
- Active Directory ユーザー名
- Active Directory ユーザー名と異なる場合、RADIUS または RSA SecurID ユーザー名
- ドメイン名
- リモート デスクトップまたは公開アプリケーションの表示名
- ウィンドウ サイズ
- セッションのリセット、ログアウト、開始を含むアクション
- 表示プロトコル
- USB デバイスをリダイレクトするオプション

URI を作成するには、Horizon Client 固有のパスとクエリ部分と共に `vmware-view` URI スキーマを使用します。

URI を使用して Horizon Client を起動するには、クライアント コンピュータに Horizon Client がインストールされている必要があります。

vmware-view URI を作成するための構文

URI 構文には、`vmware-view` URI スキーム、リモート デスクトップや公開アプリケーションを指定するためのパス部分、オプションでリモート デスクトップや公開アプリケーションのアクション、または構成オプションを指定するためのクエリが含まれます。

URI 仕様

以下の構文を使用して Horizon Client を起動するための URI を作成します。

```
vmware-view://[<authority-part>][/<path-part>][?<query-part>]
```

必要となる唯一の要素は URI スキーム **vmware-view** です。クライアント オペレーティング システムのバージョンによっては、スキーム名で大文字と小文字が区別されるため、**vmware-view** と入力してください。

重要: すべての部分で、非 ASCII 文字は UTF-8 [STD63] に基づいて最初にエンコードされる必要があり、次に対応する UTF-8 シーケンスの各オクテットは、URI 文字として表されるパーセントでエンコードされる必要があります。

ASCII 文字のエンコードについての詳細は、http://www.utf8-chartable.de/ の URL エンコーディング資料を参照してください。

<authority-part>

サーバ アドレス。オプションでユーザー名、デフォルト以外のポート番号、またはその両方。サーバ名ではアンダースコア (_) はサポートされません。サーバ名は、DNS 構文に一致する必要があります。

ユーザー名を指定するには、以下の構文を使用します。

```
user1@<server-address>
```

ドメインが含まれる UPN アドレスを指定できません。ドメインを指定するには、URI で **domainName** クエリ部分を使用できます。

ポート番号を指定するには、以下の構文を使用します。

```
<server-address>:<port-number>
```

<path-part>

リモート デスクトップまたは公開アプリケーション。リモート デスクトップの表示名または公開アプリケーションの表示名を使用します。この値は、デスクトップまたはアプリケーション プールの作成時に Horizon Administrator で指定した名前です。表示名にスペースが含まれている場合、**%20** エンコーディングを使用してスペースを表します。

<query-part>

使用する構成オプション。あるいは、リモート デスクトップまたは公開アプリケーションで実行するアクション。クエリは大文字と小文字の区別がありません。複数のクエリを使用するには、クエリの間にアンパサンド (&) を使用します。クエリが競合する場合、Horizon Client はリストの最後にあるクエリを使用します。次の構文を使用します。

```
<query1>=<value1>[&<query2>=<value2>...]
```

サポートされるクエリ

このタイプの Horizon Client では、次のクエリがサポートされます。デスクトップ クライアントやモバイル クライアントなど、複数のタイプのクライアントに URI を作成する場合は、対応するクライアント システムのインストールとセットアップ ガイドを参照して、サポートされるクエリを確認してください。

操作

表 3-2. アクション クエリで使用できる値

値	説明
`browse`	指定したサーバにホストされている使用可能なリモート デスクトップおよび公開アプリケーションのリストを表示します。このアクションを使用しているときに、リモート デスクトップまたは公開アプリケーションを指定する必要はありません。
`start-session`	指定されたリモート デスクトップまたは公開アプリケーションを開きます。アクション クエリが提供されず、リモート デスクトップまたは公開アプリケーション名が提供されなければ、**`start-session`** がデフォルト アクションとなります。
`reset`	指定したリモート デスクトップまたは公開アプリケーションをシャットダウンして再起動します。保存されてないデータは失われます。リモート デスクトップのリセットは、物理 PC のリセット ボタンを押すことと同じです。
`restart`	指定したリモート デスクトップをシャットダウンして再起動します。リモート デスクトップの再起動は、Windows オペレーティング システムを再起動することと同じです。オペレーティング システムでは、通常、ユーザーは再起動する前に未保存データを保存するよう求められます。
`logoff`	リモート デスクトップのゲスト OS からユーザーをログオフします。公開アプリケーションを指定すると、アクションは無視されるか、エンド ユーザーに警告メッセージ「無効な URI アクション」が表示されます。

args

公開アプリケーションの起動時に追加するコマンドライン引数を指定します。`args=`<値> の構文を使用します。<値> には文字列を指定します。次の文字についてはパーセント エンコーディングを使用します。

- コロン (:) には、**`%3A`** を使用します
- バック スラッシュ (\) には、**`%5C`** を使用します
- スペース ( ) には、**`%20`** を使用します
- 二重引用符 (") には、**`%22`** を使用します

たとえば、Notepad++ アプリケーションに `"My new file.txt"` というファイル名を指定するには、**`%22My%20new%20file.txt%22`** を使用します。

appProtocol

公開アプリケーションの場合、有効な値は **`PCOIP`** と **`BLAST`** です。たとえば、PCoIP を指定するには、***`appProtocol=PCOIP`*** 構文を使用します。

connectUSBOnInsert

USB デバイスを物理的に接続したときに、そのデバイスをフォアグラウンド リモート デスクトップまたは公開アプリケーションに接続します。リモート デスクトップに `unattended` クエリを指定すると、このクエリが暗黙的に設定されます。このクエリを使用するには、`action` クエリを **`start-session`** に設定する必要があります。さもないと、`action` クエリを持ちません。有効な値は、**`true`** および **`false`** です。構文の例は、**`connectUSBOnInsert=true`** です。

connectUSBOnStartup

クライアント システムに現在接続されているすべての USB デバイスをリモート デスクトップまたは公開アプリケーションにリダイレクトします。リモート デスクトップに `unattended` クエリを指定すると、このクエリが暗黙的に設定されます。このクエリを使用するには、`action` クエリを **`start-session`** に設定する必要があります。さもないと、`action` クエリを持ちません。有効な値は、**`true`** および **`false`** です。構文の例は、**`connectUSBOnStartup=true`** です。

desktopLayout

リモート デスクトップのウィンドウ サイズを設定します。このクエリを使用するには、`action` クエリを **`start-session`** に設定する必要があります。そうしないと、`action` クエリを使用できません。

表 3-3. desktopLayout クエリの有効値

値	説明
`fullscreen`	1 台のモニターで全画面表示。この値がデフォルトになります。
`multimonitor`	すべてのモニターで全画面表示。
`windowLarge`	大きなウィンドウ。
`windowSmall`	小さなウィンドウ。
<W>x<H>	カスタム解像度で、幅と高さをピクセルで指定します。構文の例は、**`desktopLayout=1280x800`** です。

desktopProtocol

リモート デスクトップの場合、有効な値は **RDP**、**PCOIP**、および **BLAST** です。たとえば、PCoIP を指定するには、**`desktopProtocol=PCOIP`** 構文を使用します。

domainName

リモート デスクトップや公開アプリケーションに接続しているユーザーに関連付けられている NETBIOS ドメイン名。例として、`mycompany.com` ではなく `mycompany` を使用してください。

filePath

公開アプリケーションで開くローカル システムにあるファイルへのパスを指定します。ドライブ文字を含む絶対パスを指定する必要があります。次の文字についてはパーセント エンコーディングを使用します。

- コロン (:) には、**%3A** を使用します
- バック スラッシュ (\) には、**%5C** を使用します

- スペース ( ) には、**%20** を使用します

たとえば、ファイル パス `C:\test file.txt` を表記するには、**C%3A%5Ctest%20file.txt** を使用します。

launchMinimized	Horizon Client を最小化モードで起動します。リモート デスクトップまたは公開アプリケーションが開始するまで、Horizon Client は最小化された状態のままになります。構文は、**launchMinimized=true** です。このオプションは、[unattended] クエリと一緒に使用できません。
tokenUserName	RSA または RADIUS ユーザー名を指定します。RSA または RADIUS ユーザー名が Active Directory ユーザー名と異なる場合に限ってこのクエリを使用します。このクエリを指定せず、RSA または RADIUS 認証が必要である場合、Horizon Client は Windows ユーザー名を使用します。この構文は、**tokenUserName=<name>** です。
unattended	リモート デスクトップへのサーバ接続をキオスク モードで作成します。このクエリを使用する場合に、クライアント デバイスの MAC アドレスからアカウント名を生成したときには、ユーザー情報を指定しないでください。「custom-」で始まる名前など、カスタム アカウント名を ADAM で作成した場合、アカウント情報を指定する必要があります。
useExisting	このオプションが **true** に設定されている場合、実行できる Horizon Client インスタンスは 1 つのみです。ユーザーが 2 番目のサーバへの接続を試みる場合、ユーザーは 1 番目のサーバからログアウトし、リモート デスクトップおよび公開アプリケーションのセッションを切断する必要があります。このオプションが **false** に設定されている場合は、複数の Horizon Client インスタンスを実行でき、ユーザーが同時に複数のサーバに接続できます。デフォルトは **true** です。構文の例は、**useExisting=false** です。
unauthenticatedAccessEnabled	このオプションが **true** に設定されている場合、非認証アクセス機能は、デフォルトで有効になります。[認証されていないアクセスを使用して匿名ログイン] オプションがユーザー インターフェイスに表示され選択されます。このオプションが **false** に設定されている場合、非認証アクセス機能は無効になります。[認証されていないアクセスを使用して匿名ログイン] 設定は表示されず無効になります。このオプションが **""** に設定されている場合、非認証アクセス機能は無効になり、[認証されていないアクセスを使用して匿名ログイン] 設定がユーザー インターフェイスに表示されず、無効になります。構文の例は、**unauthenticatedAccessEnabled=true** です。
unauthenticatedAccessAccount	非認証アクセス機能が有効になっている場合、使用するアカウントを設定します。非認証アクセス機能が無効な場合、このクエリは無視されます。**anonymous1** ユーザー アカウントを使用する場合、**unauthenticatedAccessAccount=anonymous1** のように構文を指定します。

vmware-view URI の例

vmware-view URI スキームを使用してハイパー テキスト リンクまたはボタンを作成し、これらのリンクを E メールまたは Web ページで使用できます。たとえば、エンドユーザーが URI リンクをクリックすると、指定した起動オプションでリモート デスクトップが起動します。

URI 構文の例

各 URI の例に続いて、URI リンクをクリック後にエンド ユーザーに表示される事柄について説明します。

1
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session
```

Horizon Client が起動し、**view.mycompany.com** サーバに接続します。ログインのダイアログ ボックスが表示され、ユーザー名、ドメイン名、パスワードの入力が要求されます。ログインに成功すると、表示名が **Primary Desktop** のリモート デスクトップにクライアントが接続します。ユーザーはゲスト OS にログインされます。

注: この例では、デフォルトの表示プロトコルとウィンドウ サイズが使用されます。デフォルトの表示プロトコルは PCoIP で、デフォルトのウィンドウ サイズは全画面表示です。

2
```
vmware-view://view.mycompany.com:7555/Primary%20Desktop
```

この URI は前の例と同じ効果がありますが、接続サーバ インスタンスに 7555 の非デフォルト ポートを使用するところが異なります。(デフォルトのポートは 443 です)。リモート デスクトップ ID が提供されるので、**start-session** アクションが URI に含まれていない場合であっても、リモート デスクトップが開きます。

3
```
vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP
```

Horizon Client が起動し、**view.mycompany.com** サーバに接続します。ログイン ダイアログ ボックスで、[ユーザー名] テキスト ボックスに **fred** が挿入されます。ユーザーはドメイン名とパスワードを入力する必要があります。ログインに成功すると、表示名が **Finance Desktop** のリモート デスクトップにクライアントが接続します。ユーザーはゲスト OS にログインされます。PCoIP 表示プロトコルを使用して接続します。

4
```
vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST
```

Horizon Client が起動し、**view.mycompany.com** サーバに接続します。ユーザーは、ログイン ダイアログ ボックスにユーザー名、ドメイン名、パスワードを入力する必要があります。ログインに成功すると、クライアントは **Calculator** という表示名の公開アプリケーションに接続します。VMware Blast 表示プロトコルを使用して接続します。

5
```
vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany
```

Horizon Client が起動し、**view.mycompany.com** サーバに接続します。ログイン ダイアログ ボックスで、[ユーザー名] テキスト ボックスに **fred** が挿入され、[ドメイン] テキスト ボックスに **mycompany** が挿入されます。ユーザーはパスワードを入力する必要があるだけです。ログインに成功すると、表示名が **Finance Desktop** のリモート デスクトップにクライアントが接続します。ユーザーはゲスト OS にログインされます。

6
```
vmware-view://view.mycompany.com/
```

Horizon Client が起動し、ユーザーは、**view.mycompany.com** サーバに接続するためにログインを求められます。

7
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=reset
```

Horizon Client が起動し、**view.mycompany.com** サーバに接続します。ログインのダイアログ ボックスが表示され、ユーザー名、ドメイン名、パスワードの入力が要求されます。ログインに成功すると Horizon Client はダイアログ ボックスを表示し、**Primary Desktop** のリセット操作をユーザーに確認します。

注: Horizon 管理者がリモート デスクトップのリセット機能を有効にしている場合にのみ、このアクションを実行できます。

8
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=restart
```

Horizon Client が起動し、**view.mycompany.com** サーバに接続します。ログインのダイアログ ボックスが表示され、ユーザー名、ドメイン名、パスワードの入力が要求されます。ログインに成功すると Horizon Client はダイアログ ボックスを表示し、**Primary Desktop** の再起動をユーザーに確認します。

注: Horizon 管理者がリモート デスクトップの再起動機能を有効にしている場合にのみ、このアクションを実行できます。

9
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=start-
session&connectUSBOnStartup=true
```

この URI は最初の例と同じ効果があり、クライアント システムに接続しているすべての USB 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。

10
```
vmware-view://
```

Horizon Client が実行されていない場合、起動します。Horizon Client が実行されている場合、フォアグラウンドで実行されます。

11
```
vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22
```

Notepad++ をサーバ 10.10.10.10 で起動して、引数 `My new file.txt` を公開アプリケーションの起動コマンドに渡します。スペース文字と二重引用符では、パーセントのエスケープ文字が使用されます。ファイル名にはスペース文字が含まれるため、二重引用符で囲まれています。

次の構文を使用して、Windows コマンド ライン プロンプトでこのコマンドを入力することもできます。

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""
```

この例では、二重引用符は、\" の文字を使用してエスケープされます。

12

```
vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt
```

Notepad++ 12 をサーバ 10.10.10.10 で起動して、引数 `a.text b.txt` をアプリケーションの起動コマンドに渡します。引数は引用符で囲まれていないため、スペース文字によってファイル名が分割され、2 つのファイルが Notepad++ で別々に開きます。

注: 公開アプリケーションによって、コマンドラインの引数を使用する方法が異なる場合があります。たとえば、引数 `a.txt b.txt` をワードパッドに渡すと、ワードパッドは `a.txt` の 1 ファイルのみを開きます。

13

```
vmware-view://view.mycompany.com/Notepad?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1
```

Horizon Client が起動すると、**`anonymous1`** というユーザー アカウントを使用して、`view.mycompany.com` サーバに接続します。Notepad アプリケーションは、ユーザーにログイン認証情報の指定を求めずに起動します。

HTML コードの例

URI を使用してハイパー リンクおよびボタンを作成し、E メールまたは Web ページに含めることができます。以下の例では、[Test Link（テスト リンク）] というラベルのハイパー リンクと [TestButton] というラベルのボタンのコードを記述するために、最初の URI のサンプルの URI を使用しています。

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test
Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Horizon Client の証明書検証モードの設定

Horizon Client とサーバ間の接続でサーバ証明書が確認されます。証明書は、デジタル形式の識別情報で、パスポートや運転免許証のような役割を果たします。

エンドユーザーは、Horizon Client で、サーバ証明書の確認に失敗した場合に Horizon Client との接続を拒否するかどうかを設定できます。

デフォルトの証明書確認モードを設定すると、エンド ユーザーによる Horizon Client での変更を防ぐことができます。詳細については、「エンド ユーザーの証明書確認モードの設定」を参照してください。

サーバ証明書の確認では、以下のことが確認されます。

- 証明書は失効しているか。
- 証明書の目的は、送信側の ID 検証やサーバ通信の暗号化以外にあるか。つまり、証明書のタイプは正しいか。
- 証明書は期限切れになっているか、また有効なのは未来のみか。つまり、証明書はコンピュータの時刻に応じて有効になっているか。
- 証明書上の共通名は、それを送信するサーバのホスト名と一致しているか。ロード バランサが Horizon Client を、Horizon Client で入力したホスト名と一致しない証明書を持つサーバにリダイレクトした場合、不一致が発生する可能性があります。クライアントにホスト名ではなく IP アドレスを入力した場合でも、不一致の原因となる可能性があります。
- 不明なまたは信頼されていない証明機関（CA）によって署名された証明書か。自己署名された証明書は、信頼されていない CA の証明書タイプの 1 つです。

  チェックをパスするには、証明書のトラスト チェーンが、デバイスのローカル証明書ストアでルートになっている必要があります。

ドメイン内のすべての Windows クライアント システムに自己署名付ルート証明書を配布する情報については、『Horizon 7 のインストール』ドキュメントの「信用されるルート証明書機関を追加」を参照してください。

証明書検証モードを設定するには、Horizon Client を起動し、Horizon Client メニューの [オプション] メニューで、[SSL を構成] を選択します。選択肢は次の 3 つです。

- [信頼が確認されていないサーバには絶対に接続しない]。この設定は、証明書の確認に失敗した場合にサーバに接続できないことを意味します。失敗したチェックは、エラー メッセージに一覧表示されます。
- [信頼されていないサーバに接続する前に警告する]。この設定は、サーバが自己署名証明書を使用しているために証明書の確認に失敗したときに、[続行] をクリックして警告を無視できることを意味します。自己署名証明書の場合、Horizon Client に入力したサーバ名と証明書名が一致する必要はありません。

  証明書が期限切れの場合でも、警告を受信します。
- [サーバ ID 証明書を検証しない]。この設定は、証明書確認が実行されないことを示します。

後で管理者が信頼される認証局からのセキュリティ証明書をインストールし、接続時のすべての証明書チェックにパスするようになると、この信頼された接続はその特定のサーバに対して記録されます。その後、このサーバが自己署名証明書を再び提示すると、接続は失敗します。特定のサーバが完全に検証可能な証明書を提示した後は、必ずその処理が行われます。

重要: 過去に SSL Cipher Suite Order グループ ポリシーを設定するなどして、社内のクライアント システムを構成し、特定の暗号を使用するようにした場合、Horizon Client グループ ポリシーのセキュリティ設定を使用する必要があります。「クライアント GPO のセキュリティ設定」を参照してください。または、クライアント システムの `SSLCipherList` レジストリ設定を使用できます。「Windows レジストリを使用した Horizon Client の構成」を参照してください。

エンド ユーザーの証明書確認モードの設定

エンド ユーザーの証明書確認モードを設定できます。たとえば、完全な検証を常に実行するように設定できます。証明書確認は、サーバと Horizon Client 間の TLS 接続に対して実行されます。

エンド ユーザーに、次のいずれかの証明書確認方法を設定できます。

- Horizon Client で、証明書確認モードの選択をエンド ユーザーに許可できます。
- （検証なし）証明書確認は実行されません。
- （警告）サーバに自己署名証明書がある場合、エンド ユーザーに警告が表示されます。ユーザーは、このタイプの接続を許可するかどうかを選択できます。
- （フル セキュリティ）フル検証が実行され、フル検証をパスしない接続は拒否されます。

実行可能な証明書確認の種類については、「Horizon Client の証明書検証モードの設定」を参照してください。

Horizon Client 設定 ADMX テンプレート ファイル (`vdm_client.admx`) を使用して、証明書確認モードを設定できます。グループ ポリシー設定用のすべての ADMX ファイルは、`VMware-Horizon-Extras-Bundle-<x.x.x>-<yyyyyyy>.zip` に含まれています。<x.x.x> はバージョン番号で、<yyyyyyy> はビルド番号です。この ZIP ファイルは、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。このテンプレートを使用してグループ ポリシー設定を制御する方法については、「グループ ポリシーによる Horizon Client の設定」を参照してください。

また、Horizon Client 設定 ADMX テンプレート ファイルを使用することで、暗号化 TLS 接続を確立する前に特定の暗号化アルゴリズムとプロトコルの使用を制限することもできます。詳細については、「クライアント GPO のセキュリティ設定」を参照してください。

証明書確認モードをグループ ポリシーとして設定しない場合は、クライアント コンピュータ上の次のレジストリ キーのいずれかに `CertCheckMode` 値の名前を追加することで、証明書の確認を有効にできます。

- 32 ビット Windows の場合：`HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- 64 ビット Windows の場合: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

レジストリ キーでは次の値を使用します。

- `0` は、 `Do not verify server identity certificates` を実装します。
- `1` は、 `Warn before connecting to untrusted servers` を実装します。
- `2` は、 `Never connect to untrusted servers` を実装します。

グループ ポリシー設定とレジストリ キーの `CertCheckMode` 設定の両方を構成すると、グループ ポリシー設定の方がレジストリ キーでの設定よりも優先されます。

注: Horizon Client の今後のバージョンでは、Windows レジストリでの設定がサポートされなくなる可能性があります。グループ ポリシー設定を使用してください。

TLS 詳細オプションの設定

Horizon Client とサーバ間、または Horizon Client とリモート デスクトップのエージェント間の通信を暗号化するために使用するセキュリティ プロトコルと暗号化アルゴリズムを選択できます。

これらのセキュリティ オプションは、USB チャネルの暗号化にも使用されます。

デフォルトの設定では、暗号化スイートは 128 ビットまたは 256 ビット AES を使用し、匿名 DH アルゴリズムを削除して、現在の暗号リストを暗号化アルゴリズムのキー長の順にソートします。

デフォルトでは、TLS v1.1 と TLS v1.2 が有効になっています SSL v2.0、SSL v3.0、TLS v1.0 はサポートされていません。

クライアントの接続先であるサーバで有効になっていないセキュリティ プロトコルを Horizon Client に対して構成すると、TLS エラーが発生して接続に失敗します。

重要: Horizon Client で有効にするプロトコルの 1 つがリモート デスクトップで有効になっている必要があります。有効になっていないと、USB デバイスがリモート デスクトップにリダイレクトされません。

クライアント システム上でグループ ポリシー設定または Windows レジストリ設定のいずれかを使用して、デフォルトの暗号化およびプロトコルを変更できます。グループ ポリシー設定の使用方法については、「クライアント GPO のセキュリティ設定」で [SSL プロトコルと暗号化アルゴリズムの構成] を参照してください。Windows レジストリの SSLCipherList 設定の使用方法については、「Windows レジストリを使用した Horizon Client の構成」 を参照してください。

グループ ポリシーによる Horizon Client の設定

Horizon Client には、Horizon Client 機能と動作の設定に使用できるグループ ポリシーの ADMX テンプレート ファイルが含まれています。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 デスクトップと公開アプリケーションの接続を最適化し、保護することができます。

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、ホストのクライアントを誰が実行しているかに関係なく、Horizon Client に適用するポリシーを設定します。
- ユーザーの構成ポリシーは、Horizon Client を実行している全ユーザー、ならびに RDP 接続設定に適用する Horizon Client ポリシーを設定します。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。

Horizon Client は、リモート デスクトップおよび公開アプリケーション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 Client 設定 ADMX テンプレート ファイル (**vdm_client.admx**)、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** 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 ZIP ファイルは、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。このファイルを Active Directory サーバにコピーし、グループ ポリシー管理エディタを使用して管理テンプレートを追加する必要があります。手順については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。

クライアント GPO のスクリプト定義設定

リモート デスクトップのウィンドウ サイズ、ログイン ユーザー名、ログイン ドメイン名など、コマンド ラインから Horizon Client を実行する場合と同じ設定をグループ ポリシーに設定できます。

次の表では、VMware Horizon Client の設定 ADMX テンプレート ファイルにおけるスクリプト定義設定について説明します。このテンプレート ファイルには、各スクリプト定義の設定についてコンピュータ構成のバージョンとユーザー設定のバージョンが用意されています。ユーザーの設定は、対応するコンピュータの設定より優先されます。設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [スクリプト定義] フォルダの順に移動します。

表 3-4. VMware Horizon Client 構成テンプレート：スクリプトの定義

設定	説明
Automatically connect if only one launch item is entitled	使用資格のあるリモート デスクトップが 1 つしかない場合は、そのリモートにユーザーを接続します。この設定により、リモート デスクトップを 1 台だけ含んだリストからリモート デスクトップを選択する必要がなくなります。
Connect all USB devices to the desktop or remote application on launch	リモート デスクトップまたは公開アプリケーションの起動時に、クライアント システムのすべての USB デバイスを、リモート デスクトップまたは公開アプリケーションに接続するかどうかを指定します。
Connect USB devices to the desktop or remote application when they are plugged in	USB デバイスがクライアント システムに差し込まれた場合、その USB デバイスをリモート デスクトップまたは公開アプリケーションに接続するかどうかを指定します。
DesktopLayout	ユーザーがリモート デスクトップにログインするときに表示される Horizon Client ウィンドウのレイアウトを指定します。次から選択できます。 ■ Full Screen ■ Multimonitor ■ Window – Large ■ Window – Small この設定は、**DesktopName to select setting** 設定も設定されている場合にのみ利用可能です。
DesktopName to select	Horizon Client がログイン時に使用するデフォルトのリモート デスクトップを指定します。
Disable 3rd-party Terminal Services plugins	標準 RDP プラグインとしてインストールされているサードパーティ製ターミナル サービス プラグインを Horizon Client でチェックするかどうかを指定します。この設定を構成しない場合、サードパーティ製プラグインは Horizon Client によってデフォルトでチェックされます。この設定は、USB リダイレクトなどの Horizon 固有のプラグインには適用されません。

表 3-4. VMware Horizon Client 構成テンプレート：スクリプトの定義 (続き)

設定	説明
Locked Guest Size	1 台のモニターでディスプレイを使用している場合は、リモート デスクトップの画面解像度を指定します。リモート デスクトップのディスプレイを [すべてのモニター] に設定している場合、この設定は機能しません。 この設定を有効にすると、リモート デスクトップの自動調整機能が無効になります。最小画面サイズは 640x480 です。最大画面サイズは 4096x4096 です。この設定は、PCoIP 接続にのみ適用されます。 重要: ベスト プラクティスとして、解像度はリモート デスクトップでサポートされている最大解像度より高い解像度に設定しないでください。最大解像度は、Horizon Administrator で次のように設定されています。 ■ 3D が有効な場合は、最大 1920x1200 の解像度で 2 台までのモニターがサポートされています。 ■ 3D が無効な場合は、最大 2560x1600 の解像度で 4 台までのモニターがサポートされています。 実際には、クライアント側のこの設定で、リモート デスクトップで指定可能な値より高い解像度、リモート デスクトップの所定のオペレーティング システム バージョン、vRAM の量、および色深度が設定されている場合は無視されます。たとえば、Horizon Administrator でリモート デスクトップの解像度が 1920x1200 に設定されている場合、リモート デスクトップの機能によっては、クライアントに表示される解像度が 1920x1200 より高くならない場合があります。
Logon DomainName	Horizon Client がログイン時に使用する NetBIOS ドメインを指定します。
Logon Password	Horizon Client がログイン時に使用するパスワードを指定します。このパスワードは、Active Directory によってテキスト形式で格納されます。セキュリティ向上のため、この設定を指定しないでください。ユーザーはパスワードをインタラクティブに入力できます。
Logon UserName	Horizon Client がログイン時に使用するパスワードを指定します。このパスワードは、Active Directory によってテキスト形式で格納されます。
Server URL	Horizon Client がログイン時に使用する URL（`https://view1.example.com` など）を指定します。
Suppress error messages (when fully scripted only)	ログイン時に Horizon Client によるエラー メッセージを非表示にするかどうかを指定します。 この設定は、ログイン プロセスが完全にスクリプト化されている場合、たとえば、必須のログイン情報がすべてグループ ポリシーによって事前に設定されている場合にのみ適用されます。 不正なログイン情報のためログインに失敗した場合は、ユーザーに通知されず、Horizon Client のプロセスが終了します。
Disconnected application session resumption behavior	ユーザーがサーバに再接続したときの公開アプリケーションの動作方法を決定します。次から選択できます。 ■ 再接続を要求し、アプリケーションを開く ■ 自動的に再接続し、アプリケーションを開く ■ 再接続も自動再接続も要求しない この設定を有効にすると、エンド ユーザーは Horizon Client で再接続時における公開アプリケーションの動作を設定できません。 この設定を無効にすると、エンド ユーザーは Horizon Client で再接続時における公開アプリケーションの動作を設定できます。デフォルトでは、この設定は無効になっています。

表 3-4. VMware Horizon Client 構成テンプレート：スクリプトの定義 (続き)

設定	説明
Enable Unauthenticated Access to the server	Horizon Client を使用している場合、アプリケーションにアクセスするときに認証情報の入力をユーザーに求めるかどうかを決定します。 この設定が有効な場合、[認証されていないアクセスを使用して匿名ログイン] 設定が Horizon Client に表示され、無効になり、選択されます。非認証アクセスが使用できない場合、クライアントは別の認証方法に戻って選択する場合があります。 この設定を無効にすると、ユーザーが公開アプリケーションにログインしてアクセスするときには必ず認証情報を入力するように要求されます。Horizon Client で、[認証されていないアクセスを使用して匿名ログイン] 設定は表示されず選択解除されます。 デフォルトでは、ユーザーは Horizon Client での非認証アクセスを有効にできます。[認証されていないアクセスを使用して匿名ログイン] 設定が表示され、有効にされて、選択解除されます。
Account to use for Unauthenticated Access	Enable Unauthenticated Access to the server グループ ポリシー設定が有効な場合、また、ユーザーが Horizon Client で [認証されていないアクセスを使用して匿名ログイン] を選択して非認証アクセスを有効にしている場合、Horizon Client がサーバに匿名でログインするときに使用する非認証アクセス ユーザー アカウントを指定します。 サーバへの特定の接続で非認証アクセスが使用されない場合、この設定は無視されます。デフォルトでは、ユーザーはアカウントを選択できます。

クライアント GPO のセキュリティ設定

セキュリティ設定には、証明書、ログイン認証情報、シングル サインオン機能のグループ ポリシーが含まれます。

次の表では、Horizon Client の設定 ADMX テンプレート ファイルにおけるセキュリティ設定について説明します。この表では、設定に含まれているのがコンピュータ構成とユーザー設定の両方か、コンピュータ構成だけかを示しています。両タイプの設定を含むセキュリティ設定の場合、ユーザー設定の方が、同等のコンピュータ設定よりも優先されます。設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [セキュリティ設定] フォルダの順に移動します。

表 3-5. Horizon Client の構成テンプレート：セキュリティ設定

設定	コンピュータ	ユーザー	説明
Allow command line credentials	X		Horizon Client のコマンドライン オプションでユーザー認証情報を指定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、ユーザーがコマンド ラインから Horizon Client を実行するときに smartCardPIN および password オプションは使用できません。 デフォルトでは、この設定は有効になっています。 これに相当する Windows レジストリの値は AllowCmdLineCredentials です。
Servers Trusted For Delegation	X		ユーザーが Horizon Client のメニュー バーの [オプション] メニューで [現在のユーザーとしてログイン] を選択したときに、入力されたユーザー ID と認証情報を受け入れる接続サーバ インスタンスを指定します。接続サーバ インスタンスを指定しない場合は、すべての接続サーバ インスタンスがこの情報を受け付けます。 接続サーバ インスタンスを追加するには、次のいずれかの形式を使用します。 ■ **domain\system$** ■ **system$@domain.com** ■ 接続サーバ サービスのサービス プリンシパル名（SPN） これに相当する Windows レジストリの値は BrokersTrustedForDelegation です。

表 3-5. Horizon Client の構成テンプレート：セキュリティ設定 (続き)

設定	コンピュータ	ユーザー	説明
Certificate verification mode	X		Horizon Client が実行する証明書確認のレベルを設定します。次のいずれかのモードを選択できます。 ■ No Security。証明書の確認は行われません。 ■ Warn But Allow。サーバが自己署名証明書を使用するために証明書の確認に失敗した場合、ユーザーに警告が表示されますが、この警告は無視してかまいません。自己署名証明書の場合、Horizon Client に入力したサーバ名と証明書名が一致する必要はありません。 他の証明書エラーが発生した場合、Horizon Client はエラーを表示し、ユーザーはサーバに接続できません。 Warn But Allow はデフォルト値です。 ■ Full Security。証明書に関する何らかのエラーが発生すると、ユーザーはサーバに接続できなくなります。Horizon Client で証明書エラーが表示されます。 このグループ ポリシー設定が構成されると、ユーザーは選択した証明書確認モードを Horizon Client で確認できますが、設定を構成することはできません。証明書確認モードのダイアログ ボックスが表示され、管理者が設定をロックしていることをユーザーに通知します。 この設定を無効にすると、Horizon Client ユーザーは証明書確認モードを選択できるようになります。デフォルトでは、この設定は無効になっています。 サーバが Horizon Client から提供された証明書の確認を実行できるようにするには、クライアントが接続サーバまたはセキュリティ サーバ ホストに対して HTTPS 接続を行う必要があります。接続サーバまたはセキュリティ サーバ ホストに対する HTTP 接続を確立する中間デバイスに TLS をオフロードした場合、証明書確認はサポートされません。 この設定をグループ ポリシーとして構成したくないときは、クライアント コンピュータの次のレジストリ キーのいずれかに、CertCheckMode 値の名前を追加することにより、証明書検証を有効にできます。 ■ 32 ビット Windows の場合：HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security ■ 64 ビット Windows の場合: HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security レジストリ キーでは次の値を使用します。 ■ 0 は、No Security を実装します。 ■ 1 は、Warn But Allow を実装します。 ■ 2 は、Full Security を実装します。 グループ ポリシー設定と Windows レジストリ キーの CertCheckMode 設定の両方を構成すると、グループ ポリシー設定の方がレジストリ キーでの設定よりも優先されます。 注: Horizon Client の今後のリリースでは、Windows レジストリでの設定がサポートされなくなる可能性があります。グループ ポリシー設定を使用してください。

表 3-5. Horizon Client の構成テンプレート：セキュリティ設定 (続き)

設定	コンピュータ	ユーザー	説明
`Default value of the 'Log in as current user' checkbox`	X	X	Horizon Client のメニュー バーの [オプション] メニューで、[現在のユーザーとしてログイン] のデフォルト値を指定します。 この設定により、Horizon Client インストール中に指定したデフォルトの値が上書きされます。 ユーザーがコマンド ラインから Horizon Client を実行し、`logInAsCurrentUser` オプションを指定すると、この設定はその値によって上書きされます。 [オプション] メニューで [現在のユーザーとしてログイン] が選択されると、ユーザーがクライアント システムにログインするときに入力した ID と認証情報が接続サーバ インスタンスに渡され、最終的にリモート デスクトップまたは公開アプリケーションに渡されます。[現在のユーザーとしてログイン] が選択されていない場合、リモート デスクトップまたは公開アプリケーションにアクセスする前に、ユーザーが ID と認証情報を複数回入力する必要があります。 デフォルトでは、この設定は無効になっています。 これに相当する Windows レジストリの値は `LogInAsCurrentUser` です。
`Display option to Log in as current user`	X	X	[現在のユーザーとしてログイン] を Horizon Client のメニュー バーの [オプション] メニューに表示するかどうかを指定します。 [現在のユーザーとしてログイン] が表示される場合、ユーザーはこのオプションを選択または選択解除し、デフォルト値をオーバーライドできます。[現在のユーザーとしてログイン] が表示されない場合、ユーザーは Horizon Client の [オプション] メニューからデフォルト値をオーバーライドできません。 `Default value of the 'Log in as current user' checkbox` のポリシー設定を使用することで、[現在のユーザーとしてログイン] のデフォルト値を指定できます。 デフォルトでは、この設定は有効になっています。 これに相当する Windows レジストリの値は `LogInAsCurrentUser_Display` です。
`Enable jump list integration`	X		Windows 7 以降のシステムのタスクバーにある Horizon Client アイコンにジャンプ リストを表示するかどうかを決定します。ジャンプ リストを使用すると、最近使用したサーバ、リモート デスクトップまたは公開アプリケーションに接続できます。 Horizon Client が共有されている場合、最近使用したデスクトップおよび公開アプリケーションの名前を他のユーザーに見られたくないことがあります。この設定を無効にすると、ジャンプ リストを非表示にできます。 デフォルトでは、この設定は有効になっています。 これに相当する Windows レジストリの値は `EnableJumplist` です。

表 3-5. Horizon Client の構成テンプレート：セキュリティ設定 (続き)

設定	コンピュータ	ユーザー	説明
Enable SSL encrypted framework channel	X	X	View 5.0 以前のリモート デスクトップで TLS を有効にするかどうかを決めます。View 5.0 以前では、ポート TCP 32111 経由でリモート デスクトップに送信されるデータが暗号化されませんでした。 ■ [有効化] : TLS を有効にしますが、リモート デスクトップで TLS がサポートされていない場合は、非暗号化接続に戻ることを許可します。たとえば、View 5.0 以前のリモート デスクトップでは TLS がサポートされていません。[有効化] はデフォルトの設定です。 ■ [無効化] : TLS を無効にします。デバッグを行う場合や、チャネルがトンネリングされず、WAN アクセラレータ製品によって最適化される可能性がある場合、この設定が役立つことがあります。 ■ [強制] : TLS を有効にします。TLS をサポートしていないリモート デスクトップへの接続は拒否されます。 これに相当する Windows レジストリの値は EnableTicketSSLAuth です。
Configures SSL protocols and cryptographic algorithms	X	X	TLS 暗号化接続を確立する前に、特定の暗号化アルゴリズムとプロトコルの使用を制限する暗号リストを構成します。暗号リストは、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。暗号文字列では、大文字と小文字が区別されます。 デフォルト値は、[TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES] になります。 この暗号文字列は、TLS v1.1 と TLS v1.2 が有効で、SSL v.2.0、SSL v3.0、TLS v1.0 が無効になっていることを意味します。SSL v2.0、SSL v3.0、TLS v1.0 は、承認プロトコルではなくなりました。今後は無効になります。 暗号化スイートは、128 ビットまたは 256 ビット AES を使用して、ECDHE、ECDH、RSA を使用します。GCM モードをおすすめします。 詳細については、http://www.openssl.org/docs/apps/ciphers.html を参照してください。 これに相当する Windows レジストリの値は SSLCipherList です。
Enable Single Sign-On for smart card authentication	X		スマート カード認証に対してシングル サインオンを有効にするかどうかを指定します。シングル サインオンを有効にすると、Horizon Client は、スマート カードの暗号化された PIN を、一時的なメモリに格納してから接続サーバに送信します。シングル サインオンを無効にすると、Horizon Client でカスタム PIN ダイアログ ボックスは表示されません。 これに相当する Windows レジストリの値は EnableSmartCardSSO です。
Ignore certificate revocation problems	X	X	失効したサーバ証明書に関連するエラーを無視するかどうかを指定します。 サーバが送信する証明書が失効するか、クライアントが証明書の失効ステータスを確認できない場合、エラーが表示されます。 デフォルトでは、この設定は無効になっています。
Unlock remote sessions when the client machine is unlocked	X	X	再帰的なロック解除機能を有効にするかどうかを指定します。再帰的なロック解除機能を使用すると、クライアント マシンのロックが解除された後で、すべてのリモート セッションのロックを解除できます。この機能が適用されるのは、ユーザーが「現在のユーザーとしてログイン」機能を使用してサーバにログインした後です。 デフォルトでは、この設定は有効になっています。

クライアント GPO の RDP 設定

Microsoft RDP 表示プロトコルを使用すると、オーディオ、プリンタ、ポート、その他のデバイスなどのリダイレクトといったオプションに対してグループ ポリシーを設定できます。

次の表では、Horizon Client の設定 ADMX テンプレート ファイルにおけるリモート デスクトップ プロトコル (RDP) 設定について説明します。RDP の設定はすべてユーザーの設定です。設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [RDP の設定] フォルダの順に移動します。

表 3-6. Horizon Client 構成管理テンプレート：RDP 設定

設定	説明
Audio redirection	リモート デスクトップで再生されるオーディオ情報をリダイレクトするかどうかを指定します。次のいずれかの設定を選択します。 ■ [オーディオの無効化]：オーディオが無効になります。 ■ [仮想マシンで再生（VoIP USB のサポートが必要）]：オーディオはリモート デスクトップ内で再生されます。この設定で、クライアントでサウンドを再生するには、共有 USB オーディオ デバイスが必要です。 ■ [クライアントにリダイレクト]：オーディオはクライアントにリダイレクトされます。この設定はデフォルトのモードです。 この設定は RDP オーディオにのみ適用されます。MMR 経由でリダイレクトされたオーディオがクライアントで再生されます。
Enable audio capture redirection	デフォルトのオーディオ入力デバイスをクライアントからリモート セッションにリダイレクトするかどうかを指定します。この設定を有効にすると、クライアント上のオーディオ録音デバイスがリモート デスクトップに表示され、オーディオ入力を録音できるようになります。 デフォルトでは、この設定は無効になっています。
Bitmap cache file size in <unit> for <number> bpp bitmaps	特定の bpp ビットマップ カラー設定で使用するビットマップ キャッシュのサイズを KB または MB 単位で指定します。 次の単位と bpp の組み合わせで、この設定の異なるバージョンが提供されています。 ■ MB/8 bpp ■ MB/16 bpp ■ MB/24 bpp ■ MB/32 bpp
In-memory bitmap cache size in KB for 8bpp bitmaps	8 bpp の色設定に使用する RAM ビットマップ キャッシュのサイズを KB 単位で指定します。ScaleBitmapCachesByBPP が true（デフォルト）の場合、このキャッシュ サイズに bpp を掛けた値から実際の RAM を決定します。 この設定が有効になっている場合には、サイズを KB 単位で入力します。
Bitmap caching/cache persistence active	通常のビットマップ キャッシュを使用するかどうかを指定します（アクティブ）。通常のビットマップ キャッシュを使用するとパフォーマンスが向上する可能性がありますが、追加のディスク領域が必要になります。

表 3-6. Horizon Client 構成管理テンプレート：RDP 設定 (続き)

設定	説明
Color depth	リモート デスクトップの色の深度を指定します。次のいずれかの設定を選択します。 ■ 8 ビット ■ 15 ビット ■ 16 ビット ■ 24 ビット ■ 32 ビット 24 ビットの Windows XP システムの場合、[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] - [ターミナル サービス] の順に移動して、最大色深度を制限するポリシーを有効にし、24 ビットに設定する必要があります。
Cursor shadow	リモート デスクトップでポインタの下にシャドウを表示するかどうかを指定します。
Desktop background	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、デスクトップの背景を表示するかどうかを指定します。
Desktop composition	(Windows Vista 以降) リモート デスクトップでデスクトップ コンポジションを有効にするかどうかを指定します。 デスクトップ コンポジションを有効にすると、従来のバージョンの Microsoft Windows とは異なる描画方法が採用され、各ウィンドウ上のコンテンツは直接画面やプライマリ ディスプレイ デバイスに描画されません。その代わりに、描画はビデオ メモリのオフスクリーン サーフェスにリダイレクトされ、その後、デスクトップ イメージにレンダリングされ、ディスプレイに表示されます。
Enable compression	RDP データを圧縮するかどうかを指定します。デフォルトでは、この設定は有効になっています。
Enable RDP Auto-Reconnect	RDP プロトコル接続が失敗した後に RDP クライアント コンポーネントがリモート デスクトップへの再接続を試みるかどうかを指定します。この設定は、Horizon Administrator で [デスクトップへのアクセスに安全なトンネル接続を使用する] オプションが有効になっている場合は無効です。デフォルトでは、この設定は無効になっています。
Font smoothing	(Windows Vista 以降) リモート デスクトップでフォントにアンチエイリアシングを適用するかどうかを指定します。
Menu and window animation	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、メニューとウィンドウのアニメーションを有効にするかどうかを指定します。
Redirect clipboard	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、ローカル クリップボード情報をリダイレクトするかどうかを指定します。
Redirect drives	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、ローカル ディスク ドライブをリダイレクトするかどうかを指定します。デフォルトでは、ローカル ドライブはリダイレクトされます。 この設定を有効にするか、または未構成のままにしておくと、リモート デスクトップ上のリダイレクトされたドライブ上のデータはクライアント コンピュータ上のドライブにコピーできます。リモート デスクトップからユーザーのクライアント コンピュータへのデータの受け渡しを許可することが潜在的なセキュリティ リスクとなる展開では、この設定を無効にします。別のアプローチとして、Microsoft Windows グループ ポリシー設定の Do not allow drive redirection を有効にすることによってリモート デスクトップ仮想マシンのフォルダ リダイレクトを無効にできます。 Redirect drives 設定は RDP にのみ適用されます。
Redirect printers	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、ローカル プリンタをリダイレクトするかどうかを指定します。
Redirect serial ports	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、ローカル COM ポートをリダイレクトするかどうかを指定します。

表 3-6. Horizon Client 構成管理テンプレート：RDP 設定 (続き)

設定	説明
Redirect smart cards	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、ローカル スマート カードをリダイレクトするかどうかを指定します。 注: この設定は RDP 接続と PCoIP 接続の両方に適用されます。
Redirect supported plug-and-play devices	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、ローカル プラグアンドプレイおよび POS（販売時点情報管理）デバイスをリダイレクトするかどうかを指定します。この動作は、エージェントの USB リダイレクト コンポーネントが管理するリダイレクトとは異なります。
Shadow bitmaps	ビットマップにシャドウを表示するかどうかを指定します。この設定は、全画面表示モードでは無効です。
Show contents of window while dragging	ユーザーがフォルダを新しい場所までドラッグしたときに、フォルダの内容を表示するかどうかを指定します。
Themes	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、テーマを表示するかどうかを指定します。
Windows key combination redirection	Windows キーの組み合わせを適用する場所を指定します。 この設定により、リモート仮想マシンにキーの組み合わせを送信したり、キーの組み合わせをローカルに適用することができます。 デフォルトでは、キーの組み合わせはローカルに適用されます。
Enable Credential Security Service Provider	リモート デスクトップ接続がネットワーク レベル認証（NLA）を使用するかどうかを指定します。Windows Vista では、リモート デスクトップ接続にはデフォルトで NLA が必要です。ゲスト OS でリモート デスクトップ接続に NLA が必要な場合は、この設定を有効にする必要があります。有効にしないと、Horizon Client はリモート デスクトップに接続できません。この設定を有効にするだけでなく、次の条件が満たされていることも確認する必要があります。 ■ クライアントとゲスト OS が両方とも NLA をサポートしている。 ■ 接続サーバ インスタンスで直接クライアント接続が有効になっている。トンネル接続は NLA ではサポートされていません。

クライアント GPO の全般設定

全般設定には、プロキシ オプション、タイムゾーンの転送、マルチメディアのアクセラレーションおよびその他の表示設定が含まれます。

全般設定

次の表では、Horizon Client の設定 ADMX テンプレート ファイルにおける全般設定について説明します。全般設定には、コンピュータの構成とユーザーの構成の両方の設定があります。ユーザーの設定は、対応するコンピュータの設定より優先されます。設定は、グループ ポリシー管理エディタの [VMware Horizon Client の設定] フォルダにあります。

表 3-7. Horizon Client の構成テンプレート：全般設定

設定	コンピュータ	ユーザー	説明
Allow data sharing	X		この設定を有効にすると、Horizon Client ユーザー インターフェイスのデータ共有モードの設定がオンに設定されます。エンド ユーザーはこの設定を変更できません。 この設定を無効にすると、Horizon Client ユーザー インターフェイスのデータ共有モードの設定がオフに設定されます。エンド ユーザーはこの設定を変更できません。 この設定が構成されていない場合（デフォルト）、エンド ユーザーは、Horizon Client ユーザー インターフェイスでデータ共有モードの設定を変更できます。
Allow display scaling	X	X	この設定を有効にすると、すべてのリモート デスクトップと公開アプリケーションでディスプレイのスケーリング機能が有効になります。 この設定を無効にすると、すべてのリモート デスクトップと公開アプリケーションでディスプレイのスケーリング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（デフォルト設定）、エンド ユーザーは Horizon Client ユーザー インターフェイスでディスプレイのスケーリングを有効または無効にできます。 Horizon Client ユーザー インターフェイスで [ロックしたゲストのサイズ] グループ ポリシー設定を有効にして、ディスプレイのスケーリング設定を非表示にできます。詳細については、「クライアント GPO のスクリプト定義設定」を参照してください。
Always on top		X	Horizon Client ウィンドウを常に最前面のウィンドウにするかどうかを決定します。この設定を有効にすると、全画面表示の Horizon Client ウィンドウが Windows タスクバーによって隠れることがなくなります。デフォルトでは、この設定は無効になっています。
Default value of the "Hide the selector after launching an item" check box	X	X	[アイテムの起動後にセレクタを非表示] チェック ボックスをデフォルトで選択するかどうかを設定します。デフォルトでは、この設定は無効になっています。
Disable time zone forwarding	X		リモート デスクトップおよび接続されたクライアント間のタイム ゾーンの同期を無効にするかどうかを指定します。
Disable toast notifications	X	X	Horizon Client からのトースト通知を無効にするかどうかを決定します。 画面の端にトースト通知を表示しないようにするには、この設定を有効にします。 注: この設定を有効にすると、セッション タイムアウト機能がアクティブになったときに 5 分間の警告がユーザーに表示されません。
Disallow passing through client information in a nested session	X		Horizon Client で、クライアント情報がネストされたセッションを通過しないようにするかを指定します。有効にした場合は、Horizon Client がリモート セッションの内部で実行されていれば、仮想マシンのデバイス情報ではなく実際の物理クライアント情報を送信します。この設定は、クライアント情報（デバイス名とドメイン、クライアント タイプ、IP アドレス、および MAC アドレス）に適用されます。この設定はデフォルトで無効になっており、クライアント情報がネストされたセッションを通過することを許可します。

表 3-7. Horizon Client の構成テンプレート：全般設定 (続き)

設定	コンピュータ	ユーザー	説明
Display modifier function key	X	X	ユーザーが使用できるスイッチ修飾子とファンクション キーの組み合わせを指定します。ユーザーがこのキーの組み合わせを押すと、PCoIP または VMware Blast リモート デスクトップ セッションで入力が有効になったときに、クライアント コンピュータの表示設定が変更されます。 この設定が構成されていない場合（デフォルト）、エンド ユーザーは、マウスを使用してリモート デスクトップを解放し、Windows ロゴ キー + P を押してプレゼンテーションの表示モードを選択する必要があります。 この設定は、公開アプリケーションのセッションに適用されません。
Don't check monitor alignment on spanning		X	デフォルトでは、画面を組み合わせたときに正確な長方形にならない場合、クライアント デスクトップは複数のモニターをスパンしません。この設定を有効にすると、デフォルトが上書きされます。デフォルトでは、この設定は無効になっています。
Enable multi-media acceleration		X	クライアントでマルチメディア リダイレクト（MMR）を有効にするかどうかを指定します。 Horizon Client のビデオ ディスプレイ ハードウェアでオーバーレイがサポートされていない場合は、MMR が正しく機能しません。
Enable relative mouse	X	X	PCoIP 表示プロトコルを使用する場合に、相対マウスを有効にします。相対マウスモードにより、特定のグラフィックス アプリケーションやゲームでマウスの動作が改善されます。リモート デスクトップで相対マウスがサポートされていない場合、この設定は使用されません。デフォルトでは、この設定は無効になっています。
Enable the shade		X	Horizon Client ウィンドウの最上部にあるシェード メニュー バーを表示するかどうかを指定します。デフォルトでは、この設定は有効になっています。 注: キオスク モードでは、シェード メニュー バーがデフォルトで無効にされます。
Enable Horizon Client online update	X		オンライン アップデート機能を有効にします。デフォルトでは、この設定は有効になっています。 注: コマンドラインから Horizon Client をインストールする場合は、AUTO_UPDATE_ENABLED プロパティを 0 に設定するとオンライン アップデート機能を無効にできます。詳細については、「Horizon Client のインストール プロパティ」を参照してください。
Tunnel proxy bypass address list	X		トンネル アドレスのリストを指定します。これらのアドレスにはプロキシ サーバは使用されません。複数のエントリを区切るにはセミコロン（;）を使用します。
URL for Horizon Client online help	X		Horizon Client がヘルプ ページを取得できる代替 URL を指定します。この設定は、インターネットにアクセスできないためにリモートでホストされているヘルプ システムを取得できない環境で使用するためのものです。
URL for Horizon Client online update	X		Horizon Client がアップデートを取得できる代替 URL を指定します。この設定は、独自のプライベート/個人のアップデート センターを定義する環境で使用するためのものです。有効でない場合、VMware の公式アップデート サーバが使用されます。
Pin the shade		X	Horizon Client ウィンドウの最上部にあるシェードの固定を有効にして、メニューバーの自動非表示が行われないようにするかどうかを指定します。シェードが無効になっている場合、この設定の効果はありません。デフォルトでは、この設定は有効になっています。

表 3-7. Horizon Client の構成テンプレート：全般設定 (続き)

設定	コンピュータ	ユーザー	説明
Disable desktop disconnect messages	X	X	通常、リモート デスクトップの切断時に表示されるメッセージを無効にするかどうかを指定します。これらのメッセージはデフォルトで表示されます。
Disable sharing files and folders		X	クライアント ドライブのリダイレクト機能を Horizon Client で使用できるようにするかどうかを指定します。 この設定を有効にすると、公開アプリケーションでローカル ファイルを開く機能を含め、Horizon Client のクライアント ドライブ リダイレクト機能がすべて無効になります。また、次の要素が Horizon Client のユーザー インターフェイスに表示されなくなります。 ■ [設定] ダイアログ ボックスの [共有する] パネル。 ■ リモート デスクトップの [オプション] メニューにある [フォルダを共有] 項目 ■ システム トレイの Horizon Client にある [共有する] 項目 ■ サーバへの接続後、初めてリモート デスクトップまたはアプリケーションに接続すると表示される [共有する] ダイアログ ボックス この設定を [無効] にすると、クライアント ドライブのリダイレクト機能が完全に機能します。デフォルトでは、この設定は無効になっています。
Always hide the remote floating language (IME) bar for Hosted Apps	X	X	アプリケーション セッションでフロート表示言語バーをオフに強制します。この設定を有効にすると、ローカルで IME 機能が有効かどうかにかかわらず、公開アプリケーション セッションでフローティング言語バーが必ず非表示になります。この設定を無効にすると、ローカルで IME 機能が無効になっている場合にのみ、フロート表示言語バーが表示されます。デフォルトでは、この設定は無効になっています。
Disable opening local files in hosted applications		X	ホスト型アプリケーションがサポートするファイル拡張子のローカル ハンドラを Horizon Client が登録するかどうかを指定します。 この設定を [有効] に設定すると、Horizon Client は、ファイル拡張子ハンドラを登録せず、ユーザーが設定をオーバーライドすることを許可しません。 この設定を [無効] に設定すると、Horizon Client はファイル拡張子ハンドラを常に登録します。デフォルトでは、ファイル拡張子ハンドラは登録されますが、ユーザーは、[設定] ダイアログ ボックスの [共有] パネルにある [ローカル ファイル システムからリモート アプリケーションを使用してローカル ファイルを開く機能を有効にする] 設定を使用して、Horizon Client ユーザー インターフェイスでこの機能を無効にできます。詳細については、「クライアント ドライブのリダイレクトによるローカル フォルダおよびドライブへのアクセス共有」を参照してください。 デフォルトでは、この設定は無効になっています。
Automatically install shortcuts when configured on the Horizon server		X	Connection Server インスタンスに公開アプリケーションおよびリモート デスクトップのショートカットが設定されている場合、この設定は、ユーザーがサーバに接続したときにクライアント マシンにショートカットがインストールされるかどうかを指定します。また、インストールの方法も指定します。 この設定を有効すると、クライアント マシンにショートカットがインストールされます。ショートカットのインストールを確認するプロンプトは表示されません。 この設定を無効にすると、クライアント マシンにショートカットがインストールされません。ショートカットのインストールを確認するプロンプトは表示されません。 デフォルトでは、ショートカットはインストールされます。

表 3-7. Horizon Client の構成テンプレート：全般設定 (続き)

設定	コンピュータ	ユーザー	説明
Block multiple Horizon Client instances per Windows session	X		Windows セッションで、複数の Horizon Client インスタンスを起動できないようにします。 この設定を有効にすると、Horizon Client は単一インスタンス モードで動作するため、Windows セッションでは複数の Horizon Client インスタンスを起動できなくなります。 この設定を無効にすると、Windows セッションで複数の Horizon Client インスタンスを起動できるようになります。デフォルトでは、この設定は無効になっています。
Display only smart card certificates during login	X		ユーザーとシステムのストアからすべての証明書のリストを表示するのか、スマート カード証明書のみを表示するのかを指定します。 [有効] に設定すると、証明書の選択ダイアログ ボックスにスマート カードの証明書のみが表示されます。 [無効] に設定すると、証明書選択ダイアログ ボックスにすべてのタイプの証明書が表示されます。 デフォルトでは、この設定は無効になっています。

クライアント GPO の USB 設定

Horizon Agent と Horizon Client で USB ポリシー設定を定義できます。接続すると、Horizon Client が Horizon Agent から USB ポリシーの設定と Horizon Client USB ポリシーの設定をダウンロードし、ホスト マシンからのリダイレクトに使用可能なデバイスを特定します。

複合 USB デバイスを分割するポリシー設定

次の表で、Horizon Client 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。設定はコンピュータ レベルで適用されます。コンピュータ レベルでの GPO の設定は、レジストリの **HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB** よりも優先されます。設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。

USB リダイレクトを制御するポリシーの使用方法については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。

表 3-8. Horizon Client 構成テンプレート：USB 分割設定

設定	プロパティ
`Allow Auto Device Splitting`	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`	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： `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： **`vid-0781_pid-55**`** デフォルト値は定義されていません。
`Split Vid/Pid Device`	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： `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： **`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は、Horizon 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。 デフォルト値は定義されていません。

USB デバイスをフィルタリングするポリシー設定

次の表では、USB デバイスのフィルリングに使用する Horizon Client の設定 ADMX テンプレート ファイルのポリシー設定について説明します。設定はコンピュータ レベルで適用されます。コンピュータ レベルでの GPO の設定は、レジストリの `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB` よりも優先されます。

USB リダイレクトにフィルター ポリシーの設定方法については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。

表 3-9. Horizon Client 構成テンプレート：USB フィルタリング設定

設定	プロパティ
`Allow Audio Input Devices`	オーディオ入力デバイスのリダイレクトを許可します。 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。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。
`Allow Audio Output Devices`	オーディオ出力デバイスのリダイレクトを許可します。 デフォルト値は未定義で、**`false`** と同じです。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。

表 3-9. Horizon Client 構成テンプレート：USB フィルタリング設定 (続き)

設定	プロパティ
Allow HID-Bootable	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（起動可能なデバイス）のリダイレクトを許可します。 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。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。
Allow Device Descriptor Failsafe Behavior	Horizon Client で構成/デバイスの記述子を取得できない場合でも、デバイスのリダイレクトを許可します。config/desc が失敗してもデバイスを許可するには、**IncludeVidPid** または **IncludePath** などの Include フィルタにそれを含みます。 デフォルト値は未定義で、**false** と同じです。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] - [エージェントで構成できない設定] フォルダの順に移動します。
Allow Other Input Devices	HID 起動可能なデバイスや統合型ポインティング デバイス付きキーボード以外の入力デバイスのリダイレクトを許可します。 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。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。
Allow Keyboard and Mouse Devices	統合型ポインティング デバイス（マウス、トラックボール、タッチ パッドなど）付きキーボードのリダイレクトを許可します。 デフォルト値は未定義で、**false** と同じです。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。
Allow Smart Cards	スマート カード デバイスのリダイレクトを許可します。 デフォルト値は未定義で、**false** と同じです。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。
Allow Video Devices	ビデオ デバイスのリダイレクトを許可します。 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。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。
Disable Remote Configuration	USB デバイスのフィルタリングを実行するときは、エージェント設定の使用を無効にします。 デフォルト値は未定義で、**false** と同じです。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] - [エージェントで構成できない設定] フォルダの順に移動します。
Exclude All Devices	リダイレクト対象からすべての 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 ファミリがリダイレクト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 ファミリがリダイレクトされるのを防止できます。 エージェントで **Exclude All Devices** の値を **true** に設定し、この設定が Horizon Client に渡されると、エージェントの設定によって Horizon Client の設定はオーバーライドされます。 デフォルト値は未定義で、**false** と同じです。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。

表 3-9. Horizon Client 構成テンプレート：USB フィルタリング設定 (続き)

設定	プロパティ
Exclude Device Family	リダイレクト対象からデバイス ファミリを除外します。設定の形式：<family_name_1>[;<family_name_2>]... 例： **bluetooth;smart-card** 自動デバイス分割を有効にした場合、Horizon は複合 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判断します。自動デバイス分割を無効にした場合、Horizon は複合 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。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。
Exclude Vid/Pid Device	指定したベンダーとプロダクト ID のデバイスを、リダイレクト対象から除外します。設定の形式： **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： **vid-0781_pid-****;vid-0561_pid-554c** デフォルト値は定義されていません。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。
Exclude Path	特定のハブまたはポートのパスにあるデバイスをリダイレクト対象から除外します。設定の形式： **bus-**<x1>[/<y1>]...**/port-**<z1>[**;bus-**<x2>[/<y2>].../**port-**<z2>]... バスやポート番号は 16 進数で指定する必要があります。パスにワイルドカード文字を使用することはできません。 例： **bus-1/2/3_port-02;bus-1/1/1/4_port-ff** デフォルト値は定義されていません。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] - [エージェントで構成できない設定] フォルダの順に移動します。
Include Device Family	デバイス ファミリをリダイレクト対象に含めます。設定の形式： <family_name_1>[;<family_name_2>]... 例： **storage** デフォルト値は定義されていません。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。

表 3-9. Horizon Client 構成テンプレート：USB フィルタリング設定 (続き)

設定	プロパティ
Include Path	特定のハブやポートのパスにあるデバイスをリダイレクト対象に含めます。設定の形式： bus-<x1>[/<y1>]…/port-<z1>[;bus-<x2>[/<y2>]…/port-<z2>]… パスやポート番号は 16 進数で指定する必要があります。パスにワイルドカード文字を使用することはできません。 例： **bus-1/2_port-02;bus-1/7/1/4_port-0f** デフォルト値は定義されていません。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] - [エージェントで構成できない設定] フォルダの順に移動します。
Include Vid/Pid Device	特定のベンダー ID とプロダクト ID を持ち、リダイレクト可能な USB デバイスを指定します。設定の形式：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： **vid-0561_pid-554c** デフォルト値は定義されていません。 設定を確認するには、グループ ポリシー管理エディタで [VMware Horizon Client の設定] - [View の USB 構成] フォルダの順に移動します。

ネストされたセッションに関する考慮事項

ネスト モードまたはダブルホップ シナリオの場合、ユーザーは物理クライアント システムからリモート デスクトップに接続して、リモート デスクトップ（ネストされたセッション）内で Horizon Client を起動し、別のリモート デスクトップに接続します。ネストされたセッションでデバイスを期待どおり動作あせるには、物理的なクライアント マシンとネストされたセッションの両方で、USB ポリシーを設定する必要があります。

PCoIP クライアントのセッション変数 ADMX テンプレートの設定

PCoIP クライアントのセッション変数 ADMX テンプレート ファイル (**pcoip.client.admx**) 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。管理者がオーバーライドできるコンピュータのデフォルト値を設定できます。あるいは、管理者がオーバーライドできないユーザー設定を行うこともできます。オーバーライドできる設定を確認するには、グループ ポリシー管理エディタで [PCoIP クライアントのセッション変数] - [上書き可能な管理者デフォルト] フォルダの順に移動します。オーバーライドできない設定を確認するには、グループ ポリシー管理エディタで [PCoIP クライアントのセッション変数] - [上書き不可の管理者設定] フォルダの順に移動します。

ADMX ファイルは、**VMware-Horizon-Extras-Bundle-<x.x.x>-<yyyyyyy>.zip** に含まれています。このファイルは、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 ファイルが含まれます。

表 3-10. PCoIP クライアントのセッション変数

設定	説明
`Configure PCoIP client image cache size policy`	PCoIP クライアントのイメージ キャッシュのサイズを制御します。クライアントは、イメージ キャッシュを使用して以前に送信された表示の一部を保存します。イメージ キャッシュにより、再送されるデータ量が削減されます。 この設定を無効にすると、PCoIP はクライアント イメージ キャッシュのデフォルト サイズ、250MB を使用します。 この設定を有効にすると、クライアントのイメージ キャッシュサイズを最小 50MB から最大 300MB まで構成できます。デフォルト値は 250 MB です。 デフォルトでは、この設定は無効になっています。
`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。この設定が構成されている場合、サイズ（MB 単位）でログ ファイルのクリーンアップが制御されます。たとえば、<m> がゼロ以外に設定されている場合は、サイズが <m> MB より大きいログ ファイルが自動的に削除されます。0 に設定されている場合、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。この設定を無効にすると、サイズ (MB) 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 になります。デフォルトでは、この設定は無効になっています。
`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。この設定が構成されている場合、日数でログ ファイルのクリーンアップが制御されます。たとえば、<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。このポリシーを無効にすると、時間（日数）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 7 になります。デフォルトでは、この設定は無効になっています。 ログ ファイルのクリーンアップは、セッションの開始時に 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場合、冗長性のレベルを 0 から 3 の範囲で設定できます。設定を無効にすると、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。デフォルトでは、この設定は無効になっています。 この設定をアクティブ 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 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 ボックスを選択すると、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 承認モードが有効であると、AES-128-GCM 暗号化と AES-256-GCM 暗号化の両方が無効である場合に、[AES-128-GCM 暗号化を無効にする] の値がオーバーライドされます。 `Configure SSL Connections` 設定を無効にすると、このエンドポイントによるネゴシエーションに Salsa20-256round12 と AES-128-GCM の両方のアルゴリズムを使用できます。デフォルトでは、この設定は無効になっています。 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。

表 3-10. PCoIP クライアントのセッション変数 (続き)

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 の仮想チャネル許可文字列は、**`mksvchan|vdp_rdpvcbridge`** 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 SSL cipher list`	TLS/SSL 暗号化接続を確立する前に、暗号の使用を制限する TLS/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。 この設定を使用した場合、`Configure SSL connections to satisfy Security Tools` 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。
`Configure SSL connections to satisfy Security Tools`	TLS 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 スキャナなどのセキュリティ ツールの要件を満たすには、この設定を有効にして、次の操作を行います。 1 信頼されたルート証明書ストアに、PCoIP で使用するサーバ証明書に署名した認証局の証明書を保存します。 2 証明書ストアから証明書を読み込むようにエージェントを設定します。ローカル マシンの個人用ストアを使用する場合、手順 1 で別の場所を使用していなければ、CA 証明書ストアの名前 (ROOT) を変更せず、そのまま使用します。 この設定を無効にすると、AES-128 暗号化スイートは使用できなくなるため、エンドポイントはマシン アカウントの MY ストアにある認証局の証明書、および ROOT ストアにある認証局の証明書を使用します。デフォルトでは、この設定は無効になっています。
`Configure SSL protocols`	TLS 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。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。 この設定がクライアントとエージェントの両方に指定されている場合、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。

表 3-10. PCoIP クライアントのセッション変数 (続き)

設定	説明
Configure the Client PCoIP UDP port	ソフトウェア PCoIP クライアントによって使用される UDP クライアント ポートを指定します。UDP ポートの値によって、使用されるベース UDP ポートが指定されます。ベース ポートが使用できない場合、UDP ポート範囲の値により、試行する追加ポートの数が決まります。 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 50002 でポート範囲が 64 の場合、範囲は 50002 から 50066 までになります。 この設定はクライアントにのみ適用されます。 デフォルトでは、ベース ポートは 50002、ポート範囲は 64 です。
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。 この設定をエンドポイントで無効にすると、エンドポイントはバンド幅を制限しなくなります。この設定を有効にすると、その設定値が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。 デフォルト値は 900000 キロビット/秒です。 この設定はエージェント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と、最小バンド幅は予約されません。デフォルトでは、この設定は無効になっています。 この設定はエージェント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 は、標準の MTU 検出メカニズムを使用して MTU を設定します。この設定の影響はありません。 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。 この設定はエージェント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、クライアントではエージェントとのネゴシエーションにデフォルト値が使用されます。

表 3-10. PCoIP クライアントのセッション変数 (続き)

設定	説明
`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 転送ヘッダーは、すべての PCoIP UDP パケットに追加される 32 ビット ヘッダーです（転送ヘッダーが有効にされ、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] PCoIP エージェントとクライアントは、転送セッション優先度の値をネゴシエートします。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。
`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。オーディオはデフォルトで有効です。

コマンド ラインからの Horizon Client の実行

Horizon Client をコマンド ラインまたはスクリプトから実行できます。エンド ユーザーにリモート デスクトップ アプリケーションへのアクセスを許可するキオスク ベースのアプリケーションを実装する場合などは、Horizon Client をコマンドラインから実行します。

Horizon Client をコマンドラインから実行するには、`vmware-view.exe` コマンドを使用します。`vmware-view.exe` コマンドには、Horizon Client の動作を変更するために指定できるオプションが含まれます。

Horizon Client コマンドの使用

`vmware-view` コマンドの構文によって、Horizon Client の動作が制御されます。

Windows コマンド プロンプトで、次の形式の `vmware-view` コマンドを使用します。

```
vmware-view [<command_line_option> [<argument>]] ...
```

`vmware-view` コマンドの実行ファイルへのデフォルト パスは、クライアント システムによって異なります。このパスは、クライアント システムの <PATH> 環境変数に追加できます。

- 32 ビット システム：`C:\Program Files\VMware\VMware Horizon View Client\`
- 64 ビット システム：`C:\Program Files (x86)\VMware\VMware Horizon View Client\`

次の表に、`vmware-view` コマンドと併用できるコマンド ライン オプションを示します。

表 3-11. Horizon Client のコマンド ライン オプション

オプション	説明
/?	コマンド オプションの一覧を表示します。
-appName <application_name>	デスクトップおよびアプリケーションの選択ウィンドウに表示された公開アプリケーションの名前を指定します。この名前は、プール作成ウィザードでアプリケーション プールに対して指定した表示名です。
-appProtocol <protocol>	使用可能であれば、公開アプリケーションの表示プロトコルを指定します。有効なプロトコルは次のとおりです。 ■ **VMware Blast** ■ **PCoIP**
-appSessionReconnectionBehavior <引数>	再接続時における公開アプリケーションの動作の設定を指定します。有効な引数は次のとおりです。 **always** [自動的に再接続し、アプリケーションを開く] 設定を実装します。 **never** [再接続も自動再接続も要求しない] が設定されます。 **ask** [再接続を要求し、アプリケーションを開く] が設定されます。 このオプションを使用すると、Horizon Client で公開アプリケーションの再接続設定が無効になります。
-args <引数>	公開アプリケーションの起動時に追加するコマンドライン引数を指定します。例： `vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""`
-connectUSBOnStartup	**true** に設定すると、ホストに接続されているすべての USB デバイスをリモート デスクトップまたは公開アプリケーションにリダイレクトします。リモート デスクトップに -unattended オプションを指定すると、このオプションが暗黙のうちに設定されます。デフォルトは、**false** です。
-connectUSBOnInsert	**true** に設定すると、USB デバイスを差し込んだときに、そのデバイスを前面のリモート デスクトップまたは公開アプリケーションに接続します。リモート デスクトップに -unattended オプションを指定すると、このオプションが暗黙のうちに設定されます。デフォルトは、**false** です。
-desktopLayout <window_size>	リモート デスクトップのウィンドウを表示する方法を指定します。有効なウィンドウ サイズの値は次のとおりです。 **fullscreen** 全画面表示。 **multimonitor** 複数のモニター表示 **windowLarge** 大きなウィンドウ。 **windowSmall** 小さなウィンドウ。 **length X width** カスタム サイズ。たとえば、800 x 600。

表 3-11. Horizon Client のコマンド ライン オプション (続き)

オプション	説明
–desktopName <desktop_name>	デスクトップおよびアプリケーションの選択ウィンドウに表示されたリモート デスクトップの名前を指定します。この名前は、プール作成ウィザードでプールに指定した表示名です。 重要: キオスク モードではクライアントにこのオプションを指定しないでください。リモート デスクトップがキオスク モードで実行されている場合、このオプションは効果がありません。キオスク モードでは、資格を付与されたリモート デスクトップのリストの最初のリモート デスクトップに接続が確立されます。
–desktopProtocol <protocol>	使用する表示プロトコル (デスクトップおよびアプリケーションの選択ウィンドウに表示されたプロトコル) を指定します。有効な表示プロトコルは次のとおりです。 ■ **Blast** ■ **PCoIP** ■ **RDP**
–domainName <domain_name>	エンド ユーザーが Horizon Client にログインするために使用する NETBIOS ドメインを指定します。たとえば、**mycompany.com** ではなく **mycompany** を使用してください。
–file <file_path>	追加のコマンド オプションおよび引数を記述した構成ファイルのパスを指定します。「Horizon Client 構成ファイル」を参照してください。
–h	ヘルプ オプションを表示します。
–hideClientAfterLaunchSession	[**true**] に設定すると、リモート セッションの起動後に、デスクトップおよびアプリケーションの選択ウィンドウと [VMware Horizon Client を表示] メニューが非表示になります。[**false**] に設定すると、リモート セッションの起動後に、デスクトップおよびアプリケーションの選択ウィンドウと [VMware Horizon Client を表示] メニューが表示されます。デフォルトは、**true** です。
–languageId <Locale_ID>	Horizon Client をさまざまな言語で使用するための各国語化サポートを提供します。リソース ライブラリが利用可能な場合は、使用するロケール ID（LCID）を指定します。英語（米国）の場合は、値 0x409 を入力します。
–launchMinimized	Horizon Client を最小化モードで起動します。 **–appName** または **–desktopName** オプションを指定した場合、指定した公開アプリケーションまたはリモート デスクトップが開始するまで、Horizon Client は最小化されたままになります。 このオプションは、**–unattended** または **–nonInteractive** オプションと一緒に使用できません。

–listMonitors	接続されているモニターのインデックス値と表示レイアウトの情報を表示します。例：
	`1: (0, 0, 1920, 1200)`
	`2: (1920, 0, 3840, 1200)`
	`3: (-900, -410, 0, 1190)`
	これらのインデックス値は **–monitors** オプションで使用します。

–logInAsCurrentUser	**true** に設定している場合、クライアント システムにログインするときにエンド ユーザーが入力する認証情報を使用してサーバにログインし、最終的にリモート デスクトップにログインします。デフォルトは、**false** です。

表 3-11. Horizon Client のコマンド ライン オプション (続き)

オプション	説明
`–monitors "<n>[,<n>,<n>,<n>]"`	複数のモニター環境で使用するモニター数を指定します。 <n> は、モニターのインデックス値です。`–listMonitors` オプションを使用して、接続されているモニターのインデックス値を判別できます。カンマで区切りで最大 4 つのインデックス値を指定できます。例： `–monitors "1,2"` `–desktopLayout` が `multimonitor` に設定されていない限り、このオプションは効果がありません。
`–nonInteractive`	Horizon Client をスクリプトから起動するときにエラー メッセージ ボックスを非表示にします。`–unattended` オプションを指定すると、このオプションが暗黙のうちに設定されます。 注: インタラクティブ モードでないサーバにログインする場合、[スタート] メニューのショートカット（使用可能な場合）のインストールを求めるプロンプトは表示されず、ショートカットはデフォルトでインストールされます。
`–noVMwareAddins`	仮想印刷など、VMware 固有の仮想チャネルのロードを防止します。
`–password` <password>	エンド ユーザーが Horizon Client にログインするために使用するパスワードを指定します。このパスワードはコマンドコンソール、またはスクリプト ツールによって、テキスト形式で処理されます。パスワードを自動生成する場合は、キオスク モードのクライアントにこのオプションを指定する必要はありません。セキュリティ向上のため、このオプションを指定しないでください。ユーザーはパスワードをインタラクティブに入力できます。
`–printEnvironmentInfo`	クライアント デバイスの IP アドレス、MAC アドレス、およびマシン名を表示します。
`–serverURL` <connection_server>	サーバの URL、IP アドレス、または FQDN を指定します。
`–shutdown`	すべてのリモート デスクトップと公開アプリケーションをシャットダウンします。関連するユーザー インターフェイス コンポーネントもシャットダウンされます。
`–singleAutoConnect`	ユーザーが使用資格を持つリモート デスクトップまたは公開アプリケーションが 1 つだけの場合、ユーザーがサーバで認証を行った後に、そのリモート デスクトップまたは公開アプリケーションに接続します。この設定を行うと、1 項目しかないリストからリモート デスクトップまたは公開アプリケーションを選択する必要がなくなります。
`–smartCardPIN` <PIN>	エンド ユーザーがスマート カードを挿入してログインするときの PIN を指定します。
`–usernameHint` <user_name>	ユーザー名のヒントとして使用するアカウント名を指定します。
`–standalone`	同じまたは異なるサーバに接続できる Horizon Client の 2 つ目のインスタンスを起動します。後方互換性のため、このオプションがサポートされています。これは、クライアントのデフォルトの動作のため、`–standalone` を指定する必要はありません。 同じサーバまたは異なるサーバへの複数のリモート デスクトップの接続では、セキュアなトンネルの使用はサポートされます。 注: 2 番目のリモート デスクトップ接続では、USB デバイス、スマート カード、プリンタ、およびマルチモニタなどのローカル ハードウェアへのアクセスはできません。
`–supportText` <file_name>	テキスト ファイルのフルパスを指定します。ファイルのコンテンツは、[サポート情報] ダイアログ ボックスに表示されます。

表 3-11. Horizon Client のコマンド ライン オプション (続き)

オプション	説明
–unattended	キオスク モードのクライアントに適した非対話式モードで Horizon Client を起動します。次の情報も指定する必要があります。 ■ クライアント デバイスの MAC アドレスからアカウント名を生成しなかった場合は、クライアントのアカウント名。名前は、文字列「custom-」、または ADAM で定義した別のプリフィックス文字列で始まる必要があります。 ■ パスワードを自動生成しないようにクライアントのアカウントを設定した場合は、クライアントのパスワード。 –unattended オプションを指定すると、–nonInteractive、–connectUSBOnStartup、–connectUSBOnInsert、および –desktopLayout multimonitor の各オプションも暗黙のうちに設定されます。
–unauthenticatedAccessAccount	非認証アクセスが有効な場合に、サーバに匿名でログインするために使用する非認証アクセス ユーザー アカウントを指定します。非認証アクセスが無効な場合、このオプションは無視されます。 例： `vmware–view.exe –serverURL view.mycompany.com –unauthenticatedAccessEnabled true –unauthenticatedAccessAccount anonymous1`
–unauthenticatedAccessEnabled	true に設定されている場合、非認証アクセスが有効になります。非認証アクセスが使用できない場合、クライアントは別の認証方法を選択できます。[認証されていないアクセスを使用して匿名ログイン] 設定が Horizon Client に表示され、無効にされて、選択されます。 false に設定されている場合、認証情報を入力してログインし、アプリケーションにアクセスするようにユーザーに求めます。[認証されていないアクセスを使用して匿名ログイン] 設定が、Horizon Client に表示されず選択解除されます。 このオプションを指定しない場合、Horizon Client で非認証アクセスを有効にできます。[認証されていないアクセスを使用して匿名ログイン] 設定が表示され、有効にされて、選択解除されます。

表 3-11. Horizon Client のコマンド ライン オプション (続き)

オプション	説明

–useExisting	1 つの Horizon Client セッションから複数のリモート デスクトップと公開アプリケーションを起動できるようになります。
	このオプションを指定すると、Horizon Client は、同じユーザー名、ドメイン、およびサーバ URL があるセッションが存在していないかどうかが確認され、存在している場合には、セッションを作成する代わりにそのセッションを再利用します。
	たとえば、次のコマンドでは user-1 が電卓アプリケーションを起動し、新しいセッションが作成されます。
	`vmware-view.exe –userName user-1 –password secret –domainName domain –appName Calculator –serverURL view.mycompany.com –useExisting`
	次のコマンドでは、user1 がペイント アプリケーションを同じユーザー名、ドメイン、およびサーバ URL を使用して起動しており、同じセッションが使用されます。
	`vmware-view.exe –userName user-1 –password secret –domainName domain –appName Paint –serverURL view.mycompany.com –useExisting`

–userName <user_name>	エンド ユーザーが Horizon Client にログインするために使用するアカウント名を指定します。クライアント デバイスの MAC アドレスからアカウント名を生成する場合、キオスク モードのクライアントにこのオプションを指定する必要はありません。

–file、–languageId、–printEnvironmentInfo、–smartCardPIN、および –unattended を除くすべてのオプションを Active Directory グループ ポリシーによって指定できます。

注: コマンドラインで指定する設定より、グループ ポリシーの設定が優先されます。

Horizon Client 構成ファイル

構成ファイルから Horizon Client のコマンド ライン オプションを読み取ることができます。

vmware-view コマンドの –file <file_path> オプションに引数として構成ファイルのパスを指定できます。ファイルは Unicode (UTF-16) または ASCII テキスト ファイルである必要があります。

例：非対話的アプリケーション用の構成ファイルの例

以下の例は、非対話的アプリケーション用の構成ファイルの内容を示します。

```
–serverURL https://view.yourcompany.com
–userName autouser
–password auto123
–domainName companydomain
–desktopName autodesktop
–nonInteractive
```

例：キオスク モードのクライアントの構成ファイルの例

以下の例は、アカウント名がクライアントの MAC アドレスに基づくキオスク モードのクライアントを示しています。クライアントは自動的に生成されたパスワードを持ちます。

```
–serverURL 145.124.24.100
–unattended
```

Windows レジストリを使用した Horizon Client の構成

Horizon Client のデフォルト設定をコマンド ラインで指定する代わりに、Windows レジストリで定義することができます。グループ ポリシー設定は、Windows レジストリ設定に優先します。また、Windows レジストリ設定はコマンド ラインより優先されます。

注: Horizon Client の今後のバージョンでは、Windows レジストリの設定がサポートされなくなる可能性があります。グループ ポリシー設定を使用してください。

次の表に、Horizon Client へのログインで使用されるレジストリの設定を示します。これらの設定はレジストリの `HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\` の下に置かれます。この場所は、ユーザーごとに異なります。次の表にある `HKEY_LOCAL_MACHINE` の設定は、コンピュータ全体の設定で、Windows ドメイン環境でコンピュータにログインできるすべてのローカル ユーザーとドメイン ユーザーに適用されます。

表 3-12. Horizon Client の認証情報のレジストリ設定

レジストリ設定	説明
`Password`	デフォルト パスワード。
`UserName`	デフォルトのユーザー名。

次の表に、ログイン認証情報が含まれていない Horizon Client のレジストリ設定を示します。次のように、これらの設定の場所はシステムのタイプによって異なります。

- 32 ビット Windows の場合：`HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
- 64 ビット Windows の場合：`HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\`

表 3-13. Horizon Client のレジストリ設定

レジストリ設定	説明
`DomainName`	デフォルトの NETBIOS ドメイン名。例として、`mycompany.com` ではなく `mycompany` を使用してください。
`EnableShade`	Horizon Client ウィンドウ上部のメニュー バー（網掛け）を有効にするかどうかを決めます。キオスク モードのクライアントを除き、メニュー バーはデフォルトで有効です。この値を **`false`** にするとメニュー バーが無効になります。 注: この設定は、表示レイアウトを [すべてのモニター] または [全画面表示] に設定している場合にのみ適用されます。

表 3-13. Horizon Client のレジストリ設定 (続き)

レジストリ設定	説明
ServerURL	デフォルトの接続サーバ インスタンスの URL、IP アドレス、または FQDN。
EnableSoftKeypad	**true** に設定すると、Horizon Client ウィンドウにフォーカスがある場合、マウスまたはオンスクリーン キーボードが Horizon Client ウィンドウの外にあっても、物理キーボード、オンスクリーン キーボード、マウス、手書きパッドのイベントがリモート デスクトップまたは公開アプリケーションに送信されます。デフォルトは **false** です。

次の表に、追加可能なセキュリティ設定を示します。次のように、これらの設定の場所はシステムのタイプによって異なります。

- 32 ビット Windows の場合：HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security
- 64 ビット Windows の場合: HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security

表 3-14. セキュリティ設定

レジストリ設定	説明および有効な値
CertCheckMode	証明書確認モード。有効な値は以下のとおりです。 ■ **0** は、 Do not verify server identity certificates を実装します。 ■ **1** は、 Warn before connecting to untrusted servers を実装します。 ■ **2** は、 Never connect to untrusted servers を実装します。
SSLCipherList	TLS 暗号化接続を確立する前に、特定の暗号化アルゴリズムとプロトコルの使用を制限する暗号リストを構成します。暗号リストは、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では、大文字と小文字が区別されます。 デフォルト値は、[TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES] になります。 デフォルト値は、TLS v1.1 と TLS v1.2 が有効で、SSL v.2.0、SSL v3.0、TLS v1.0 が無効であることを意味します。SSL v2.0、SSL v3.0、TLS v1.0 は、承認プロトコルではなくなりました。今後は無効になります。 暗号化スイートは 128 ビットまたは 256 ビット AES を使用し、匿名 DH アルゴリズムを削除して、現在の暗号リストを暗号化アルゴリズムのキー長の順にソートします。 構成のリファレンス情報については、http://www.openssl.org/docs/apps/ciphers.html を参照してください。

リモート デスクトップ/公開アプリケーションとの接続の管理

4

エンドユーザーは、Horizon Client を使用してサーバに接続し、リモート デスクトップにログインまたはログアウトしたり、公開アプリケーションを使用できます。トラブルシューティングを目的として、エンド ユーザーは公開デスクトップやアプリケーションを再起動したり、リセットすることができます。

ポリシーの設定方法によっては、エンド ユーザーはリモート デスクトップや公開アプリケーションで多くの操作を実行できるようになります。

この章には、次のトピックが含まれています。

リモート デスクトップまたは公開アプリケーションへの接続

リモート デスクトップまたは公開アプリケーションに接続するには、サーバ名を指定し、ユーザー アカウントの認証情報を入力する必要があります。

エンド ユーザーがリモート デスクトップおよび公開アプリケーションにアクセスする前に、クライアント デバイスからリモート デスクトップまたは公開アプリケーションに接続できることをテストします。サーバを指定し、ユーザー アカウントの認証情報を入力する必要がある場合があります。

前提条件

- ユーザー名とパスワード、RSA SecurID ユーザー名とパスコード、RADIUS 認証ユーザー名とパスコード、スマート カード個人識別番号 (PIN) などのログイン認証情報を取得します。
- ログイン用の NETBIOS ドメイン名を取得します。例として、**mycompany.com** ではなく **mycompany** を使用してください。
- 管理タスクの実行については、「Horizon Client 向けの接続サーバの準備」で説明しています。
- 企業のネットワークの外部から VPN 接続でリモート デスクトップおよび公開アプリケーションにアクセスする必要がある場合には、クライアント デバイスが VPN 接続を使用するように設定され、その接続が有効になっていることを確認します。
- リモート デスクトップまたは公開アプリケーションへのアクセスを提供するサーバの完全修飾ドメイン名 (FQDN) があることを確認します。サーバ名ではアンダースコア (_) はサポートされません。ポートが 443 でない場合、ポート番号も必要です。
- RDP 表示プロトコルを使用してリモート デスクトップに接続する予定である場合は、AllowDirectRDP エージェント グループ ポリシーが有効になっていることを確認します。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。
- サーバによって示された証明書に証明書確認モードを設定します。使用するモードを決定するには、「Horizon Client の証明書検証モードの設定」を参照してください。

手順

1 VPN 接続が必要な場合、VPN をオンにしてください。

2 Horizon Client を開始します。

3 (オプション) 現在ログインしている Windows ドメイン ユーザーとしてログインするには、メニュー バーの [オプション] ボタンをクリックし、[現在のユーザーとしてログイン] を選択します。

この設定は、クライアント システムに [現在のユーザーとしてログイン] 機能がインストールされている場合にのみ使用できます。

4 サーバに接続します。

オプション	アクション
新規サーバに接続	[+ サーバの追加] ボタンをダブルクリックするか、メニュー バーの [+ 新規サーバ] ボタンをクリックして、サーバの名前を入力して[接続] をクリックします。
既存サーバに接続	サーバのアイコンをダブルクリックするか、サーバ アイコンを右クリックして [接続] を選択します。

Horizon Client とサーバ間の接続には常に TLS が使用されます。TLS 接続のデフォルト ポートは 443 です。サーバがデフォルト ポートを使用するように構成されていない場合、**<servername>:<port>** の形式を使用します。たとえば、**view.company.com:1443** とします。

ログイン ダイアログ ボックスが表示される前に、確認する必要があることを知らせるメッセージが表示されます。

5 RSA SecurID の認証情報または RADIUS の認証証明書の入力を求められた場合、ユーザー名とパスコードを入力して [続行] をクリックします。

6 少なくとも 1 つのリモート デスクトップまたは公開アプリケーションを使用する資格を付与されたユーザーの認証情報を入力し、ドメインを選択して [ログイン] をクリックします。

username@domain の形式でユーザー名を入力すると、Horizon Client はこれをユーザー プリンシパル名 (UPN) として扱います。この場合、[ドメイン] ドロップダウン メニューは使用できなくなります。

[ドメイン] ドロップダウン メニューが表示されていない場合、**<username>@<domain>** または **<domain>\<username>** の形式でユーザー名を入力する必要があります。

7 Windows の [スタート] メニューに公開アプリケーションまたはリモート デスクトップをインストールするように Horizon Client から指示された場合、[はい] または [いいえ] をクリックします。

このプロンプトは、公開アプリケーションまたはリモート デスクトップにショートカットが設定されているサーバに初めて接続したときに表示されます。[はい] をクリックすると、ユーザーに使用資格がある場合、クライアント システムに公開アプリケーションまたはリモート デスクトップの [スタート] メニューのショートカットがインストールされます。[いいえ] をクリックすると、[スタート] メニュー ショートカットはインストールされません。

Horizon 管理者は、[Horizon Server の構成時にショートカットを自動的にインストールする] グループ ポリシーで、「エンド ユーザーにショートカットをインストールするように指示する」(デフォルト)、「ショートカットを自動的にインストールする」または「ショートカットをインストールしない」を設定できます。

8 (オプション) リモート デスクトップの表示設定を行うには、リモート デスクトップのアイコンを右クリックして [設定] を選択します。

オプション	アクション
表示プロトコルの選択	Horizon 管理者が許可している場合、[接続方法] ドロップダウン メニューから表示プロトコルを選択できます。 VMware Blast を使用するには、Horizon Agent 7.0 以降をインストールする必要があります。
表示レイアウトの選択	[表示] ドロップダウン メニューを使用して、ウィンドウ サイズを選択するか複数のモニターを使用します。

9 リモート デスクトップまたは公開アプリケーションに接続するには、デスクトップまたはアプリケーションの選択ウィンドウでリモート デスクトップまたは公開アプリケーションのアイコンをダブルクリックします。

公開デスクトップに接続するときに、公開デスクトップが別の表示プロトコルを使用するようにすでに設定されている場合、すぐには接続できません。Horizon Client がプロンプトを表示し、既定のプロトコルを使用するか、ログアウトするか確認されます。ログアウトすると、Horizon Client が別の表示プロトコルで接続できるようになります。

接続すると、リモート デスクトップまたは公開アプリケーションが開きます。

サーバで使用資格のあるリモート デスクトップまたは公開アプリケーションが複数ある場合は、デスクトップとアプリケーションの選択ウィンドウが開いたままになります。このウィンドウで、別のリモート デスクトップまたは公開アプリケーションに接続できます。

クライアント ドライブ リダイレクト機能が有効になっている場合、[共有] ダイアログ ボックスが表示され、ローカル ファイル システムのファイルに対するアクセスを許可または拒否できます。詳細については、「クライアント ドライブのリダイレクトによるローカル フォルダおよびドライブへのアクセス共有」を参照してください。

サーバに最初に接続したときに、Horizon Client はサーバのショートカットを Horizon Client ホーム ウィンドウに保存します。次にサーバに接続するときに、このサーバのショートカットをダブルクリックできます。

サーバへの認証に失敗した場合、またはクライアントがリモート デスクトップまたは公開アプリケーションに接続できない場合は、以下の手順を実行します。

- サーバの証明書が正常に動作していることを確認します。正常に動作していない場合は、Horizon Administrator で、リモート デスクトップのエージェントが接続不能になる場合もあります。これらは、証明書の問題によって発生する二次的な接続の問題の現象です。
- 接続サーバ インスタンスで設定されているタグがこのユーザーからの接続を許可していることを確認します。『Horizon 7 の管理』ドキュメントを参照してください。
- ユーザーがこのリモート デスクトップまたは公開アプリケーションにアクセスする資格を付与されていることを確認します。『Horizon 7 での仮想デスクトップのセットアップ』または『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。
- RDP 表示プロトコルを使用してリモート デスクトップに接続する場合は、リモート デスクトップのオペレーティング システムでリモート デスクトップ接続が許可されていることを確認します。

次のステップ

起動設定を行います。エンド ユーザーがサーバのホスト名を指定する必要がないようにする場合、または他の起動設定を行う場合は、コマンドライン オプションを使用してリモート デスクトップのショートカットを作成します。「コマンド ラインからの Horizon Client の実行」を参照してください。

公開アプリケーションへの接続に非認証のアクセスを使用する

Horizon 管理者は、非認証アクセスのユーザーを作成して、特定のサーバの公開アプリケーションの使用資格を付与できます。非認証アクセスのユーザーは、サーバに匿名でログインして、公開アプリケーションに接続することができます。

非認証アクセス機能でエンドユーザーを公開アプリケーションにアクセスさせる前に、クライアント デバイスから公開アプリケーションに接続できるかテストしてください。サーバを指定し、ユーザー アカウントの認証情報を入力する必要がある場合があります。

デフォルトでは、ユーザーは [オプション] メニューの [認証されていないアクセスを使用して匿名ログイン] 設定を選択し、匿名でログインするユーザー アカウントを選択します。Horizon 管理者は、グループ ポリシーを設定して [認証されていないアクセスを使用して匿名ログイン] の設定と特定の非認証アクセス ユーザー アカウントのログイン ユーザーを事前に選択できます。

前提条件

- 管理タスクの実行については、「Horizon Client 向けの接続サーバの準備」で説明しています。
- 接続サーバ インスタンスで非認証アクセス ユーザーを設定します。詳細については、『Horizon 7 の管理』の「公開アプリケーションでの非認証アクセスの提供」を参照してください。
- 企業のネットワークの外部にいる場合は、クライアント デバイスが VPN 接続を使用し、その接続がオンに設定されていることを確認します。

- 公開アプリケーションへのアクセスを提供するサーバの完全修飾ドメイン名（FQDN）が手元にあることを確認します。サーバ名ではアンダースコア (_) はサポートされません。ポートが 443 でない場合、ポート番号も必要です。
- Horizon Client で、サーバによって示された証明書に証明書確認モードを設定します。使用するモードを決定するには、「Horizon Client の証明書検証モードの設定」を参照してください。
- （オプション）[非認証アクセスに使用するアカウント] および [認証されていないアクセスを使用して匿名ログイン] グループ ポリシー設定を構成して、デフォルトの非認証アクセスの動作を変更します。詳細については、「クライアント GPO のスクリプト定義設定」を参照してください。

手順

1 VPN 接続が必要な場合、VPN をオンにしてください。

2 Horizon Client を開始します。

3 メニュー バーの [オプション] ボタンをクリックして、[認証されていないアクセスを使用して匿名ログイン] を選択します。

クライアント システムの構成によっては、この設定はすでに選択されている場合があります。

4 公開アプリケーションへの非認証アクセスを許可しているサーバに接続します。

オプション	アクション
新規サーバに接続	[+ サーバの追加] ボタンをダブルクリックするか、メニュー バーの [+ 新規サーバ] ボタンをクリックして、サーバの名前を入力して[接続] をクリックします。
既存サーバに接続	Horizon Client のホーム ウィンドウでサーバのアイコンをダブルクリックします。

Horizon Client とサーバ間の接続には常に TLS が使用されます。TLS 接続のデフォルト ポートは 443 です。サーバがデフォルト ポートを使用するように構成されていない場合、以下の例にある形式を使用します。**`view.company.com:1443`**。

ログイン ダイアログ ボックスが表示される前に、確認する必要があることを知らせるメッセージが表示されます。

5 ログイン ダイアログ ボックスが表示されたら、必要に応じて、[ユーザー アカウント] ドロップダウン メニューからユーザー アカウントを選択します。

利用可能なユーザー アカウントが 1 つしかない場合、ドロップダウン メニューは無効になり、このユーザー アカウントが選択されます。

6 (オプション) [常にこのアカウントを使用] チェック ボックスが利用可能な場合、このオプションを選択すると、サーバに次回接続するときにログイン ダイアログ ボックスをバイパスします。

サーバに次回接続する前にこの設定をオフにするには、Horizon Client のホーム ウィンドウのサーバ アイコンを右クリックして、[保存されている認証されていないアクセス アカウントの削除] を選択します。

7 [ログイン] をクリックしてサーバにログインします。

アプリケーション選択ウィンドウが表示されます。

8 公開アプリケーションを起動するには、公開アプリケーションのアイコンをダブルクリックします。

デスクトップとアプリケーションの選択の使用のヒント

Horizon Client のデスクトップとアプリケーションの選択ウィンドウで、アイコンを並べ替えたり、アイコンの数を減らすことができます。

特定サーバへの接続後、使用を許可されているすべてのリモート デスクトップおよび公開アプリケーションのアイコンを含むウィンドウが表示されます。頻繁に使用するリモート デスクトップおよび公開アプリケーションを開くには、次の提案を試してみてください。

- 名前の最初の数文字を入力します。たとえば、Paint、PowerPoint、および Publisher のアイコンがある場合、***pa*** と入力して Paint 公開アプリケーションを選択できます。

  入力した文字と一致するアイテムが複数ある場合は、F4 を押して、一致する次のアイテムにジャンプできます。最後のアイテムに到達したら、F4 を押して、一致する最初のアイテムに戻ることができます。

- アイコンを右クリックし、コンテキスト メニューから [お気に入りとしてマーク] を選択することで、アイコンをお気に入りとしてマークすることができます。お気に入りを選択したら、[[お気に入り] ビューを表示] ボタン（星アイコン）をクリックして、お気に入りでないすべてのアイコンを削除できます。

- [お気に入り] ビューでアイコンの順序を変更するには、アイコンを選択して新しい場所にドラッグします。[お気に入り] ビュー以外では、リモート デスクトップのアイコンが最初に表示され、その後に公開アプリケーションのアイコンが英字順に表示されます。アイコンの位置を変更するには、アイコンを新しい場所にドラッグします。

  サーバから切断したとき、あるいは公開アプリケーションまたはリモート デスクトップを開いたときに、Horizon Client は新しいアイコンの順序をサーバに保存します。サーバから手動で切断したり、公開アプリケーションまたはリモート デスクトップを手動で開いた場合、変更は保存されません。

- クライアント システムで、選択ウィンドウを表示せずにリモート デスクトップまたは公開アプリケーションを開くには、アイコンを右クリックし、コンテキスト メニューから [ショートカットを作成] を選択します。

- 選択ウィンドウを表示せずに、ローカルのスタート メニューからリモート デスクトップまたは公開アプリケーションを開くにはリモート デスクトップまたは公開アプリケーションのアイコンを右クリックし、コンテキスト メニューから [[スタート] メニューに追加] を選択します。

注: Windows 7 以降のクライアント システムの場合、Horizon Client を開き、Windows タスクバーの Horizon Client アイコンを右クリックして、最近使用したサーバ、リモート デスクトップまたは公開アプリケーションを選択します。最大 10 個のアイテムがリストに表示されます。アイテムを削除するには、アイテムを右クリックして [このリストから削除] を選択します。

タスクバーの Horizon Client アイコンを右クリックしてジャンプ リストが表示されない場合には、タスクバーを右クリックして [プロパティ] を選択し、[スタート メニュー] タブをクリックします。[プライバシー] セクションで [最近開いたアイテムを [スタート メニュー] およびタスクバーに保存および表示] チェック ボックスをオンにして [OK] をクリックします。

位置情報の共有

リモート デスクトップまたは公開アプリケーションで位置情報リダイレクト機能を有効にすると、クライアント システムの位置情報をリモート デスクトップまたは公開アプリケーションと共有できます。

クライアント システムの位置情報を共有するには、Horizon Client で設定を行う必要があります。

前提条件

Horizon 管理者は、リモート デスクトップまたは公開アプリケーションに位置情報リダイレクト機能を設定する必要があります。

たとえば、Horizon Agent をインストールするときに、位置情報リダイレクト機能を有効にします。また、位置情報リダイレクト機能のグループ ポリシーを設定し、VMware Horizon 位置情報リダイレクト IE プラグインを有効にします。詳しい要件については、「位置情報リダイレクトのシステム要件」を参照してください。

手順

1 サーバに接続します。

2 [設定] ダイアログ ボックスを開いて、左ペインで [位置情報] を選択します。

- デスクトップとアプリケーションの選択ウィンドウの右上隅で、[設定]（歯車のアイコン）をクリックします。
- デスクトップとアプリケーションの選択ウィンドウでリモート デスクトップまたは公開デスクトップを右クリックして、[設定] を選択します。

3 位置情報を設定します。

オプション	アクション
クライアント システムの位置情報をリモート デスクトップまたは公開アプリケーションと共有する	[位置情報を共有] チェック ボックスを選択します。
リモート デスクトップまたは公開アプリケーションへの接続時に [位置情報] ダイアログ ボックスを表示しない	[デスクトップやアプリケーションに接続するときにダイアログを表示しない] チェック ボックスをオンにします。[位置情報] ダイアログ ボックスで、リモート デスクトップまたは公開アプリケーションと位置情報を共有するかどうか確認されます。 このチェック ボックスをオフにすると、リモート デスクトップや公開アプリケーションに最初に接続したときに [位置情報] ダイアログ ボックスが表示されます。たとえば、サーバにログインしてリモート デスクトップに接続すると、[位置情報] ダイアログ ボックスが表示されます。さらに、別のリモート デスクトップまたは公開アプリケーションに接続すると、ダイアログ ボックスは表示されなくなります。もう一度ダイアログ ボックスを表示するには、サーバから切断して再度ログインする必要があります。

4 変更内容を保存するには、[適用] をクリックします。

5 ダイアログ ボックスを閉じるには、[OK] をクリックします。

VMware Horizon Client ウィンドウを非表示にする

VMware Horizon Client ウィンドウは、リモート デスクトップまたは公開アプリケーションを開いた後に非表示にできます。

グループ ポリシー設定を使用して、リモート デスクトップまたは公開アプリケーションを開いた後に常にウィンドウを非表示にするかどうかを設定できます。詳細については、「クライアント GPO の全般設定」を参照してください。

手順

- リモート デスクトップまたは公開アプリケーションを開いた後に VMware Horizon Client ウィンドウを非表示にするには、VMware Horizon Client ウィンドウの隅にある [閉じる] ボタンをクリックします。
- リモート デスクトップまたは公開アプリケーションを開いた後に VMware Horizon Client ウィンドウを常に非表示にするように設定するには、サーバに接続する前に、メニュー バーで [オプション] ボタンをクリックし、[アイテムの起動後にセレクタを非表示] を選択します。
- 非表示にした後で VMware Horizon Client ウィンドウを表示するには、システム トレイの VMware Horizon Client アイコンを右クリックし、[VMware Horizon Client] を選択するか、またはリモート デスクトップにログインしている場合は、メニュー バーの [オプション] ボタンをクリックして [他のデスクトップに切り替え] を選択します。

リモート デスクトップまたは公開アプリケーションへの再接続

セキュリティ上の理由から、Horizon 管理者はタイムアウトを設定し、非アクティブ状態が一定の時間が経過したときにユーザーをサーバからログアウトし、公開アプリケーションをロックすることができます。

デフォルトでは、Horizon Client が特定のサーバに 10 時間以上接続している場合、再度ログインする必要があります。このタイムアウトは、リモート デスクトップと公開アプリケーションの両方の接続に適用されます。

公開アプリケーションが自動的にロックされる 30 秒前に警告のプロンプトが表示されます。ユーザーが応答しない場合、公開アプリケーションがロックされます。デフォルトでは、非アクティブな状態が 15 分間続くとタイムアウトになりますが、このタイムアウトは Horizon 管理者側で変更可能です。

たとえば、1 つ以上の公開アプリケーションを実行しているときにコンピュータから離れ、1 時間後に戻ってきたときに、公開アプリケーションのウィンドウが開いていません。代わりに、公開アプリケーションのウィンドウを再表示するために [OK] ボタンをクリックするよう求めるダイアログ ボックスが表示されます。

これらのタイムアウトを設定するには、Horizon Administrator で [グローバル設定] に移動し、一般的な設定を編集します。

Windows クライアント デスクトップまたはスタート メニューでのショートカットの作成

リモート デスクトップまたは公開アプリケーションのショートカットを作成できます。作成したショートカットは、ローカルにインストールされたアプリケーションのショートカットと同様にクライアント システムのデスクトップ上に表示されます。Windows スタート メニューのショートカットも作成できます。

手順

1 Horizon Client を起動し、サーバにログインします。

2 デスクトップとアプリケーションの選択ウィンドウで、リモート デスクトップまたは公開アプリケーションを右クリックして、コンテキスト メニューから [デスクトップへのショートカットを作成] または [[スタート] メニューに追加] を選択します。

選択したコマンドに応じて、Horizon Client は、クライアント システムのデスクトップまたは Windows のスタート メニューにショートカットを作成します。

次のステップ

このショートカットについては、ローカルにインストールされたアプリケーションのショートカットに対して行うことができるあらゆる操作（名前変更、削除、実行など）を実行できます。ショートカットを使用するときに、サーバにまだログインしていない場合、Horizon Client は、リモート デスクトップまたは公開アプリケーションのウィンドウの起動前にプロンプトを表示し、ユーザーにログインするように指示します。

サーバによって作成されたショートカットの使用

Horizon 管理者は、リモート デスクトップまたは公開アプリケーションのスタート メニューまたはデスクトップのショートカットを設定できます。

スタート メニューのショートカットは、Horizon 7 バージョン 7.3 以降のサーバでサポートされます。デスクトップのショートカットは、Horizon 7 バージョン 7.5 以降のサーバでサポートされます。

ショートカットのあるリモート デスクトップまたは公開アプリケーションの使用資格がある場合、サーバに接続すると、Horizon Client がクライアント システムのスタート メニュー、デスクトップまたはその両方にショートカットを配置します。

Windows 7 システムでスタート メニューのショートカットを使用する場合、Horizon Client は、スタート メニューの VMware アプリケーション フォルダにショートカットを配置します。Windows 8 および Windows 10 システムの場合、Horizon Client はショートカットをアプリケーション リストに配置します。Horizon 管理者がショートカットのカテゴリ フォルダを作成している場合、VMware アプリケーション フォルダの下にカテゴリ フォルダが表示されます。または、アプリケーション リストのカテゴリとして表示されます。

グループ ポリシー設定を使用して、Horizon Client がショートカットを自動的にインストールするのか、ショートカットのインストール前にエンドユーザーにプロンプトを表示するのか、あるいはショートカットをインストールしないのかを設定できます。詳細については、「クライアント GPO の全般設定」で [Horizon Server の構成時にショートカットを自動的にインストールする] グループ ポリシー設定を参照してください。

サーバが作成したショートカットをクリックしたときにサーバにログインしていない場合、Horizon Client は、リモート デスクトップまたは公開アプリケーションのウィンドウを開く前にプロンプトを表示し、ユーザーにログインするように指示します。

Horizon 管理者がサーバでリモート デスクトップや公開アプリケーションのショートカットを変更すると、デフォルトでは、ユーザーが次にサーバに接続したときにクライアント システムのショートカットが更新されます。デフォルトのショートカットの更新動作は、Horizon Client で変更できます。詳細については、「ショートカット更新動作の設定」を参照してください。

サーバで作成されたショートカットをクライアント システムから削除するには、Horizon Client サーバの選択ウィンドウからサーバを削除するか、Horizon Client をアンインストールします。

注: キオスク モードのクライアントの場合、サーバが作成したショートカットをインストールするように指示されず、ショートカットも作成されません。

ショートカット更新動作の設定

サーバ上でリモート デスクトップまたは公開アプリケーションのショートカットに行った変更をサーバ接続時にクライアント システムに適用するかどうかを設定します。

前提条件

サーバからショートカットをインストールした場合を除き、ショートカットの更新設定を変更することはできません。

手順

1 Horizon Client で [設定] ダイアログ ボックスを開き、[ショートカット] を選択します。

- デスクトップとアプリケーションの選択ウィンドウの右上隅で、[設定]（歯車のアイコン）をクリックします。
- リモート デスクトップまたは公開アプリケーションのアイコンを右クリックして、[設定] を選択します。

2 [アプリケーションとデスクトップ ショートカットのリストを自動的に更新する] チェック ボックスを選択または選択解除します。

3 変更内容を保存するには、[OK] をクリックします。

リモート デスクトップまたは公開アプリケーションの切り替え

リモート デスクトップに接続している場合は、別のリモート デスクトップに切り替えることができます。また、リモート デスクトップに接続している間は、公開アプリケーションに接続することもできます。

手順

◆ 同じサーバまたは異なるサーバからリモート デスクトップまたは公開アプリケーションを選択します。

オプション	アクション
同じサーバの別のリモート デスクトップまたは公開アプリケーションを選択する	次のいずれかのアクションを実行します。 ■ リモート デスクトップにログインしている場合は、Horizon Client メニュー バーから、[オプション] - [他のデスクトップに切り替え] の順に選択し、別のリモート デスクトップまたは公開アプリケーションを選択します。 ■ 公開アプリケーションにログインしている場合は、システム トレイで [VMware Horizon Client] アイコンを右クリックし、[VMware Horizon Client] を選択してデスクトップとアプリケーションの選択ウィンドウを表示し、別のリモート デスクトップまたは公開アプリケーションのアイコンをダブルクリックします。 ■ デスクトップとアプリケーションの選択ウィンドウで、他のリモート デスクトップや公開アプリケーションを表すアイコンをダブルクリックします。新しいウィンドウでリモート デスクトップまたは公開アプリケーションを開きます。複数のウィンドウが表示された場合は、ウィンドウの切り替えを行うことができます。
異なるサーバの別のリモート デスクトップまたは公開アプリケーションを選択する	次のいずれかのアクションを実行します。 ■ 現在のリモート デスクトップまたは公開アプリケーションを開いたまま、別のサーバのリモート デスクトップまたは公開アプリケーションに接続する場合は、Horizon Client の新しいインスタンスを開始して、別のリモート デスクトップや公開アプリケーションに接続します。 ■ 現在のリモート デスクトップを終了して別のサーバのリモート デスクトップに接続する場合は、デスクトップとアプリケーションの選択ウィンドウに移動し、ウィンドウの左上隅にある [切断] アイコンをクリックして、サーバからログオフします。現在のサーバと開いているリモート デスクトップ セッションから切断され、別のサーバに接続できるようになります。

リモート デスクトップの自動接続機能の設定

サーバに接続したときに特定のリモート デスクトップが自動的に開くようにサーバを構成できます。特定の公開アプリケーションが自動的に開くようにサーバを構成することはできません。

前提条件

ユーザー名とパスワード、RSA SecurID ユーザー名とパスコード、RADIUS 認証ユーザー名とパスコード、スマート カード個人識別番号 (PIN) など、サーバに接続するための認証情報を取得します。

手順

1 Horizon Client を起動し、サーバにログインします。

2 デスクトップおよびアプリケーションの選択ウィンドウで、リモート デスクトップを右クリックし、[このデスクトップに自動接続] を選択します。

3 変更内容を保存するには、[適用] をクリックします。

4 ダイアログ ボックスを終了するには、[OK] をクリックします。

5 サーバから切断します。

6 サーバに再接続します。

Horizon Client がリモート デスクトップを自動的に起動します。

7 (オプション) リモート デスクトップの自動接続機能を無効にするには、リモート デスクトップのメニュー バーで [オプション] ドロップダウン メニューをクリックし、[このデスクトップに自動接続] オプションを選択解除します。

ログオフまたは切断

ログオフせずにリモート デスクトップから切断すると、リモート デスクトップ内のアプリケーションは開いたままになります。サーバから切断し、公開アプリケーションを実行したままにすることもできます。

リモート デスクトップを開いていなくても、リモート デスクトップのオペレーティング システムからログオフできます。この機能は、リモート デスクトップに Ctrl + Alt + Del を送信してから [ログオフ] をクリックするのと同じ結果になります。

注: Windows のキーの組み合わせ Ctrl+Alt+Del は、リモート デスクトップでサポートされていません。代わりに、メニュー バーで [Ctrl + Alt + Delete を送信] ボタンをクリックします。あるいは、Ctrl + Alt + Insert キーを押します。

手順

- ログオフせずにリモート デスクトップから切断します。

オプション	アクション
リモート デスクトップ ウィンドウから	次のいずれかのアクションを実行します。 ■ リモート デスクトップ ウィンドウの隅の [閉じる] ボタンをクリックします。 ■ リモート デスクトップ ウィンドウのメニュー バーから [オプション] - [切断] の順に選択します。
デスクトップとアプリケーションの選択ウィンドウから	デスクトップとアプリケーションの選択ウィンドウの左上隅の [このサーバから切断] アイコンをクリックし、警告ダイアログ ボックスの [OK] をクリックします。 サーバで複数のリモート デスクトップまたは公開アプリケーションに対する資格がある場合、デスクトップとアプリケーションの選択ウィンドウが開きます。

  注: Horizon 管理者は、切断時にログオフするようにリモート デスクトップを設定できます。その場合、リモート デスクトップで開いているアプリケーションは終了します。

- リモート デスクトップからログオフして切断する。

オプション	アクション
リモート デスクトップから	Windows の[スタート]メニューを使用してログオフします。
メニュー バーから	[オプション] - [切断してログオフ] を選択します。 この手順を使用すると、リモート デスクトップで開いているファイルが保存されずに終了します。

- 公開アプリケーションとの接続を切断します。

オプション	アクション
サーバではなく公開アプリケーションから切断	通常の方法で公開アプリケーションを終了します。たとえば、アプリケーション ウィンドウの隅の [閉じる] ボタンをクリックします。
公開アプリケーションとサーバから切断	アプリケーションの選択ウィンドウの左上隅の [このサーバから切断] アイコンをクリックし、警告ダイアログ ボックスの [OK] をクリックします。
アプリケーション選択ウィンドウを閉じ、公開アプリケーションは実行したままにする	[閉じる] ボタンをクリックします。アプリケーションの選択ウィンドウが閉じます。

- リモート デスクトップが開いていないときにログオフします。

  この手順を使用すると、リモート デスクトップで開いているファイルが保存されずに終了します。

  a Horizon Client を起動し、リモート デスクトップへのアクセスを提供するサーバに接続し、認証情報を入力します。

  b リモート デスクトップ アイコンを右クリックし、[ログアウト] を選択します。

サーバからの切断

リモート デスクトップまたは公開アプリケーションの使用が完了したら、サーバから切断できます。

サーバから切断するには、Horizon Client ウィンドウの左上隅にある [このサーバから切断] アイコンをクリックするか、Alt + D キーを押します。

リモート デスクトップまたは公開アプリケーションの操作

5

Horizon Client for Windows は、使い慣れた個人用のデスクトップとアプリケーション環境を提供します。エンドユーザーは、ローカルの Windows コンピュータに接続された USB デバイスやその他のデバイスへのアクセス、ローカル コンピュータで検出できる任意のプリンタへのドキュメント送信、スマート カード認証、複数のディスプレイ モニターの使用が可能です。

この章には、次のトピックが含まれています。

Windows クライアントの機能サポート一覧

エンド ユーザーにどの表示プロトコルと機能を使用できるようにするかを計画する場合、以下の情報を使用して、どのゲスト OS がこの機能をサポートするかを判断します。

表 5-1. Windows 仮想デスクトップでサポートされる機能

機能	Windows XP デスクトップ（View Agent 6.0.2 以前）	Windows Vista デスクトップ（View Agent 6.0.2 以前）	Windows 7 デスクトップ	Windows 8.x デスクトップ	Windows 10 デスクトップ	Windows Server 2008/2012 R2、Windows Server 2016 または Windows Server 2019 デスクトップ
USB リダイレクト	制限あり	制限あり	X	X	X	X
クライアント ドライブのリダイレクト			X	X	X	X
リアルタイム オーディオビデオ (RTAV)	制限あり	制限あり	X	X	X	X
スキャナ リダイレクト		制限あり	X	X	X	X
シリアル ポート リダイレクト			X	X	X	X
VMware Blast 表示プロトコル			X	X	X	X
RDP 表示プロトコル	制限あり	制限あり	X	X	X	X
PCoIP 表示プロトコル	制限あり	制限あり	X	X	X	X
個人設定管理	制限あり	制限あり	X	X		
Wyse MMR	制限あり	制限あり				
Windows Media MMR			X	X	X	
ロケーション ベースの印刷	制限あり	制限あり	X	X	X	X
仮想印刷	制限あり	制限あり	X	X	X	X
VMware 仮想印刷リダイレクト			X	X	X	X
スマート カード	制限あり	制限あり	X	X	X	X
RSA SecurID または RADIUS	制限あり	制限あり	X	X	X	X
シングル サインオン	制限あり	制限あり	X	X	X	X
複数のモニター	制限あり	制限あり	X	X	X	X

Windows 10 リモート デスクトップには、View Agent 6.2 以降、または Horizon Agent 7.0 以降が必要です。Windows Server 2008 R2 と Windows Server 2012 R2 のリモート デスクトップには、View Agent 6.1 以降、または Horizon Agent 7.0 以降が必要です。Windows Server 2016 リモート デスクトップでは、Horizon Agent 7.0.2 以降が必要です。Windows Server 2019 リモート デスクトップでは、Horizon Agent 7.7 以降が必要です。

重要: View Agent 6.1 以降のリリースでは、Windows XP および Windows Vista リモート デスクトップはサポートされていません。これらのゲスト OS をサポートしている最後の View リリースは View Agent 6.0.2 です。Windows XP および Vista に関して Microsoft と拡張サポート契約を行っているお客様、およびこれらのゲスト OS システムに関して VMware と拡張サポート契約を行っているお客様は、接続サーバ 6.1 を使用して Windows XP および Vista リモート デスクトップの View Agent 6.0.2 バージョンを展開できます。

各クライアント オペレーティング システムでサポートされるエディションについては、『「Windows クライアント システムのシステム要件」』を参照してください。

RDS ホストで公開されたデスクトップの機能サポート

RDS ホストは、Windows リモート デスクトップ サービスと View Agent または Horizon Agent がインストールされたサーバ コンピュータです。RDS ホスト上のリモート デスクトップ セッションは複数のユーザーによる同時利用が可能です。RDS ホストには物理マシンまたは仮想マシンのいずれかを使用できます。

注: 次の表には、サポートされている機能のみが記載されています。View Agent の最小バージョンを指定するテキストがある場合、「以降」というテキストは、Horizon Agent7.0.x 以降を含むことを示します。

表 5-2. View Agent 6.0.x 以降、または Horizon Agent 7.0.x 以降がインストールされた RDS ホストでサポートされている機能

機能	Windows Server 2008 R2 RDS ホスト	Windows Server 2012 R2 RDS ホスト	Windows Server 2016 RDS ホスト	Windows Server 2019 RDS ホスト
RSA SecurID または RADIUS	X	X	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
スマート カード	View Agent 6.1 以降	View Agent 6.1 以降	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
シングル サインオン	X	X	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
RDP 表示プロトコル	X	X	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
PCoIP 表示プロトコル	X	X	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
VMware Blast 表示プロトコル	Horizon Agent 7.0 以降	Horizon Agent 7.0 以降	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
HTML Access	View Agent 6.0.2 以降 (仮想マシンのみ)	View Agent 6.0.2 以降 (仮想マシンのみ)	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
Windows Media MMR	View Agent 6.1.1 以降	View Agent 6.1.1 以降	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
USB リダイレクト		View Agent 6.1 以降	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
クライアント ドライブのリダイレクト	View Agent 6.1.1 以降	View Agent 6.1.1 以降	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降

表 5-2. View Agent 6.0.x 以降、または Horizon Agent 7.0.x 以降がインストールされた RDS ホストでサポートされている機能 (続き)

機能	Windows Server 2008 R2 RDS ホスト	Windows Server 2012 R2 RDS ホスト	Windows Server 2016 RDS ホスト	Windows Server 2019 RDS ホスト
仮想印刷	View Agent 6.0.1 から Horizon Agent 7.6（仮想マシンのみ） Horizon Agent 7.7 以降（仮想マシンと物理マシン）	View Agent 6.0.1 から Horizon Agent 7.6（仮想マシンのみ） Horizon Agent 7.7 以降（仮想マシンと物理マシン）	Horizon Agent 7.0.2 から Horizon Agent 7.6（仮想マシンのみ） Horizon Agent 7.7 以降（仮想マシンと物理マシン）	Horizon Agent 7.7 以降
VMware 仮想印刷リダイレクト	Horizon Agent 7.7 以降	Horizon Agent 7.7 以降	Horizon Agent 7.7 以降	Horizon Agent 7.7 以降
スキャナ リダイレクト	View Agent 6.0.2 以降	View Agent 6.0.2 以降	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
ロケーション ベースの印刷	View Agent 6.0.1 から Horizon Agent 7.6（仮想マシンのみ） Horizon Agent 7.7 以降（仮想マシンと物理マシン）	View Agent 6.0.1 から Horizon Agent 7.6（仮想マシンのみ） Horizon Agent 7.7 以降（仮想マシンと物理マシン）	Horizon Agent 7.0.2 から Horizon Agent 7.6（仮想マシンのみ） Horizon Agent 7.7 以降（仮想マシンと物理マシン）	Horizon Agent 7.7 以降
複数のモニター	X	X	Horizon Agent 7.0.2 以降	Horizon Agent 7.7 以降
リアルタイム オーディオ ビデオ (RTAV)	Horizon Agent 7.0.2 以降	Horizon Agent 7.0.2 以降	Horizon Agent 7.0.3 以降	Horizon Agent 7.7 以降

各ゲスト OS でサポートされるエディションについては、『Horizon 7 のインストール』を参照してください。

固有機能の制限事項

Windows ベースのクライアントでサポートされている機能には、以下の制限があります。

表 5-3. 固有機能の要件

機能	要件
Windows Media MMR	View Agent 6.0.2 以降が必要です。Windows Media MMR 機能を公開デスクトップで使用するには、View Agent 6.1.1 以降または Horizon Agent 7.0 以降が必要です。 VMware Blast 表示プロトコルを使用するには、Horizon Agent 7.0 またはそれ以降が必要です。
シリアル ポート リダイレクト	View Agent 6.1.1 以降が必要です。Windows 10 には、View Agent 6.2 またはそれ以降、または Horizon Agent 7.0 またはそれ以降が必要です。 VMware Blast 表示プロトコルを使用するには、Horizon Agent 7.0 またはそれ以降が必要です。
公開デスクトップと公開アプリケーションでの仮想印刷（ロケーション ベースの印刷を含む）	Windows Server 2008 R2 と Windows Server 2012 の RDS ホストの場合、View Agent 6.0.1 以降が必要です。 Windows Server 2016 RDS ホストの場合、Horizon Agent 7.0.2 以降が必要です。 Windows Server 2019 RDS ホストの場合、Horizon Agent 7.7 以降が必要です。 Horizon Agent 7.7 以降では、仮想マシンと物理マシンの両方の RDS ホストがサポートされます。Horizon Agent 7.6 以前では、仮想マシンの RDS ホストのみがサポートされます。 VMware Blast 表示プロトコルを使用するには、Horizon Agent 7.0 またはそれ以降が必要です。
VMware 仮想印刷リダイレクト	Horizon Agent 7.7 以降が必要です。

表 5-3. 固有機能の要件 (続き)

機能	要件
スキャナ リダイレクト	View Agent 6.0.2 以降が必要です。PCoIP 表示プロトコルが必要です。Windows 10 には、View Agent 6.2 またはそれ以降、または Horizon Agent 7.0 またはそれ以降が必要です。 VMware Blast 表示プロトコルを使用するには、Horizon Agent 7.0 またはそれ以降が必要です。
クライアント ドライブのリダイレクト	シングルユーザー仮想マシン デスクトップと公開デスクトップの場合は、View Agent 6.1.1 またはそれ以降、または Horizon Agent 7.0 またはそれ以降が必要です。 VMware Blast 表示プロトコルを使用するには、Horizon Agent 7.0 またはそれ以降が必要です。

上記の機能の詳細および制限事項については、『Horizon 7 アーキテクチャ プランニング ガイド』を参照してください。

Linux デスクトップでサポートされる機能

View Agent 6.1.1 以降または Horizon Agent 7.0 以降の場合、いくつかの Linux ゲスト OS がサポートされます。

サポートされている Linux オペレーティング システムのリストおよびサポートされている機能の情報については、『Horizon 6 for Linux デスクトップのセットアップ』、または『Horizon 7 での仮想デスクトップのセットアップ』を参照してください。

ネスト モードでサポートされる機能

このモードは、ゼロ クライアントまたはシン クライアント向けに使用されることがあります。エンドユーザーがゼロ クライアントにログインすると、Horizon Client が自動的に起動して、リモート デスクトップに接続します。ユーザーは、このリモート デスクトップ セッションから公開アプリケーションを起動します。リモート デスクトップは、仮想デスクトップまたは公開デスクトップになります。

公開アプリケーションを提供するには、リモート デスクトップに Horizon Client がインストールされている必要があります。このセットアップは、Horizon Client がインストールされているリモート デスクトップに Horizon Client が接続するため、ネスト モードといいます。

Horizon Client と Horizon Agent の両方がインストールされているリモート デスクトップは、第 1 レベルのリモート デスクトップになります。Horizon Client のみがインストールされているマシンは、ホストといいます。

Horizon Client をネスト モードで実行する場合、次のオペレーティング システムがサポートされています。

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 7 Enterprise SP1
- Horizon Client がサポートしているすべての Windows 10 オペレーティング システムのバージョン。「Windows クライアント システムのシステム要件」を参照してください。

ユーザーが Horizon Client をネスト モードで使用する場合、次の機能がサポートされます。

- VMware Blast、PCoIP、および RDP 表示プロトコル
- ロケーション ベースの印刷
- 仮想印刷（VMware 仮想印刷リダイレクトではありません）

- シングル サインオン（スマート カードを使用しない）
- クリップボード リダイレクト
- URL コンテンツ リダイレクト
- 現在のユーザーとしてログイン
- USB リダイレクト
- 公開アプリケーションでローカル ファイルを開く

ネスト モードでは、次の機能に特定の制限があります。

- USB リダイレクト機能をネスト モードで実行するには、第 1 レベルのリモート デスクトップを仮想デスクトップにする必要があります。公開デスクトップはサポートされていません。
- ネスト モードで USB リダイレクトを使用する場合、サポートされる USB デバイスは、TOPAZ 署名パッド、Olympus ディクテーション用フット ペダル、Wacom 署名パッド、USB ディスク ストレージのみです。
- ネスト モードで公開アプリケーションのローカル ファイルを開く場合は、第 2 レベルの公開アプリケーションで第 1 レベルのリモート デスクトップのファイルを開くことができます。第 2 レベルの公開アプリケーションで、ホスト上のファイルを開くことはできません。

国際化

ユーザー インターフェイスとドキュメントは、英語、日本語、フランス語、ドイツ語、簡体字中国語、繁体字中国語、韓国語、およびスペイン語で利用可能です。

オンスクリーン キーボードのサポートの有効化

マウスまたはオンスクリーン キーボードが Horizon Client ウィンドウの外にあっても、Horizon Client が物理キーボード、オンスクリーン キーボード、マウス、手書きパッドのイベントをリモート デスクトップや公開アプリケーションに送信するようにクライアント システムを設定できます。Horizon Client ウィンドウにフォーカスを移す必要があります。この機能は、特に Surface Pro などの x86 ベースの Windows タブレットを使用している場合に便利です。

この機能を使用するには、クライアント コンピュータで Windows レジストリを編集し、`EnableSoftKeypad` 値を `true` に設定します。タイプは REG_SZ です。この値の場所はシステムのタイプによって異なります。

システムのタイプ	レジストリの場所
32 ビット Windows	`HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
64 ビット Windows	`HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\`

デフォルトでは、この機能は無効になっています。

リモート デスクトップ ウィンドウのサイズ変更

リモート デスクトップ ウィンドウの隅をドラッグしてサイズを変更すると、ウィンドウの右下隅に画面解像度がヒントとして表示されます。

VMware Blast 表示プロトコルや PCoIP 表示プロトコルを使用している場合、リモート デスクトップ ウィンドウのサイズを変更すると、ヒントの情報が変更され、変更された画面解像度が表示されます。リモート デスクトップのサイズを特定の解像度に変更する必要がある場合に、この情報が役立ちます。

Horizon 管理者がゲストのサイズをロックしている場合、または RDP 表示プロトコルを使用している場合は、リモート デスクトップ ウィンドウの解像度を変更できません。このような場合、解像度のヒントには最初の解像度が表示されます。

マルチモニタがある場合は、リモート デスクトップのウィンドウを表示するモニターを選択できます。詳細については、「リモート デスクトップを表示する特定のモニターの選択」を参照してください。1 台のモニターで表示されるように、リモート デスクトップのウィンドウを設定することもできます。詳細については、「複数モニター環境の 1 台のモニターでのリモート デスクトップの表示」を参照してください。

モニターおよび画面解像度

リモート デスクトップや公開アプリケーションを複数のモニターに拡張できます。高解像度モニターを使用している場合は、リモート デスクトップまたは公開アプリケーションを高解像度で表示できます。

サポートされる複数のモニター構成

Horizon Client は、以下の複数のモニター構成をサポートします。

- 2 台のモニターを使用する場合、同じモードにする必要はありません。たとえば、外部モニター接続されているノートパソコンを使用している場合、外部モニターはポートレート モードまたはランドスケープ モードにできます。
- 2 台のモニターを使用している場合に限り、モニターは、並べるか 2 つずつ重ねることができます。合計の高さが 4096 ピクセル未満の場合に限り、縦に重ねることができます。
- 複数のモニター環境でモニター選択機能を使用するには、VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用する必要があります。詳細については、「リモート デスクトップを表示する特定のモニターの選択」を参照してください。
- vSGA 3D レンダリング機能を使用するには、VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用する必要があります。最大 1920 x 1200 の解像度で最大 2 台のモニターを使用できます。4K (3840 x 2160) の解像度の場合、1 台のモニターのみがサポートされます。
- vGPU または他の GPU パススルー モードの場合、ベンダーのハードウェアとドライバにより、モニター数と最大解像度が決まります。詳細については、NVIDIA GRID 仮想 GPU ユーザー ガイドまたはベンダーの Web サイトを参照してください。
- インスタント クローン デスクトップ プールを Horizon 7 バージョン 7.1 以前で使用する場合は、リモート デスクトップの表示に使用できるモニターの最大数は 2 台になります。解像度は最大で 2560 x 1600 です。

- VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルでは、リモート デスクトップの 4K (3840 x 2160) の画面解像度がサポートされます。サポートされる 4K ディスプレイの数は、デスクトップ仮想マシンのハードウェア バージョンと Windows のバージョンによって異なります。

ハードウェア バージョン	Windows バージョン	サポートされる 4K ディスプレイの数
10（ESXi 5.5.x 互換）	7、8、8.x、10	1
11（ESXi 6.0 互換）	7 （3D レンダリング機能が無効で、Windows Aero が無効の場合）	3
11	7 （3D レンダリング機能が有効の場合）	1
11	8、8.x、10	1
13	8、8.x、10	4

  リモート デスクトップには、View Agent 6.2 以降、または Horizon Agent7.0 以降がインストールされている必要があります。最高のパフォーマンスを得るために、2 GB の RAM と 2 個の vCPU がある仮想マシンを推奨します。この機能では、ネットワーク遅延が小さく、パッケージ損失率が低く、1000 Mbps のバンド幅が確保されるような良好なネットワーク環境が求められる場合があります。

  注: リモート デスクトップの画面解像度が 3840 x 2160 (4K) に設定されると、画面上の項目が小さく表示される場合があり、リモート デスクトップの [画面の解像度] ダイアログ ボックスを使用してテキストやその他の項目を大きくできない場合があります。この場合、クライアント マシンの DPI を適切に設定し、DPI 同期機能を有効にして、クライアント マシンの DPI 設定をリモート デスクトップにリダイレクトできます。

- Microsoft RDP 7 を使用する場合、リモート デスクトップの表示に使用できるモニターは最大 16 台です。
- Microsoft RDP 表示プロトコルを使用する場合は、Microsoft リモート デスクトップ接続 (RDC) 6.0 以降がリモート デスクトップにインストールされている必要があります。

リモート デスクトップを表示する特定のモニターの選択

複数のモニターがある場合は、リモート デスクトップのウィンドウを表示するモニターを選択できます。たとえば、3 台のモニターがある場合、リモート デスクトップ ウィンドウを 2 台のモニターにのみ表示するように指定できます。

最大で 4 台のモニターを並べて選択できます。モニターは、1 列に並べることも、2 台ずつ積み重ねることも、縦に積み重ねることもできます。最大 2 台のモニターを縦に積み重ねることができます。

前提条件

複数のモニターが必要です。

手順

1 Horizon Client を起動し、サーバにログインします。

2 デスクトップおよびアプリケーションの選択ウィンドウで、リモート デスクトップを右クリックし、[設定] を選択します。

3 [接続方法] ドロップダウン メニューから、[PCoIP] または [VMware Blast] を選択します。

[接続方法] ドロップダウン メニューは、Horizon 管理者がこのメニューを有効にしている場合にのみ表示されます。VMware Blast を使用するには、Horizon Agent 7.0 以降をインストールする必要があります。

4 [表示] ドロップダウン メニューから、[すべてのモニター] を選択します。

クライアント システムに現在接続されているモニターのサムネイルが、[表示設定] に表示されます。表示トポロジは、クライアント システムの表示設定と一致します。

5 リモート デスクトップ ウィンドウを表示するモニターを選択するか、選択解除するには、サムネイルをクリックします。

モニターを選択すると、サムネイルの色が変わります。ディスプレイの選択ルールに違反すると、警告メッセージが表示されます。

6 変更内容を保存するには、[適用] をクリックします。

7 ダイアログ ボックスを閉じるには、[OK] をクリックします。

8 リモート デスクトップに接続します。

リモート デスクトップに接続すると、変更はすぐに反映されます。Horizon Client から終了すると、Horizon Client がリモート デスクトップの環境設定ファイルに表示設定を保存します。

複数モニター環境の 1 台のモニターでのリモート デスクトップの表示

複数のモニターがある環境でも 1 台のモニターにのみリモート デスクトップ ウィンドウを表示する場合、1 台のモニターで開くようにリモート デスクトップ ウィンドウを設定できます。

前提条件

複数のモニターが必要です。

手順

1 Horizon Client を起動し、サーバにログインします。

2 デスクトップおよびアプリケーションの選択ウィンドウで、リモート デスクトップを右クリックし、[設定] を選択します。

3 [接続方法] ドロップダウン メニューから、[PCoIP] または [VMware Blast] を選択します。

[接続方法] ドロップダウン メニューは、Horizon 管理者がこのメニューを有効にしている場合にのみ表示されます。VMware Blast を使用するには、Horizon Agent 7.0 以降をインストールする必要があります。

4 [表示] ドロップダウン メニューで、[ウィンドウ - 大]、[ウィンドウ - 小]、または [カスタム] を選択します。

[ウィンドウ - 大] を選択すると、ウィンドウ サイズが 1904 x 978 ピクセルに設定されます。[ウィンドウ - 小] を選択すると、ウィンドウ サイズが 640 x 480 ピクセルに設定されます。[カスタム] を選択する場合、特定のウィンドウ サイズを選択できます。

5 変更内容を保存するには、[適用] をクリックします。

6 ダイアログ ボックスを閉じるには、[OK] をクリックします。

デフォルトでは、プライマリ モニターリモート デスクトップ ウィンドウが開きます。リモート デスクトップ ウィンドウをプライマリではないモニターにドラッグできます。リモート デスクトップを次回開くときに、リモート デスクトップ ウィンドウは同じモニターに表示されます。ウィンドウが開き、モニターの中央に表示されます。サイズ変更するためにウィンドウをドラッグして作成したサイズではなく、表示モードでユーザーが選択したウィンドウ サイズが使用されます。

公開アプリケーションを表示する特定のモニターの選択

3 台以上のモニターを使用している場合、公開アプリケーションのウィンドウを表示するモニターを選択できます。たとえば、3 台のモニターがある場合、公開アプリケーション ウィンドウを 2 台のモニターにのみ表示するように指定できます。

最大で 4 台のモニターを並べて選択できます。モニターは、1 列に並べることも、2 台ずつ積み重ねることも、縦に積み重ねることもできます。最大 2 台のモニターを縦に積み重ねることができます。

前提条件

3 台以上のモニターが必要です。

手順

1 Horizon Client を起動し、サーバにログインします。

2 デスクトップとアプリケーションの選択ウィンドウの右上隅で、[設定]（歯車）アイコンをクリックし、左側のペインで [アプリケーション] を選択します。

3 [表示設定] で、公開済アプリケーション ウィンドウを表示するモニターを選択または選択解除します。

   モニターを選択すると、サムネイルの色が変わります。ディスプレイの選択ルールに違反すると、警告メッセージが表示されます。

4 変更内容を保存するには、[適用] をクリックします。

5 ダイアログ ボックスを閉じるには、[OK] をクリックします。

ディスプレイのスケーリング機能の使用

視覚障害者向けの画面や 4K モニターなどの高解像度画面を使用しているユーザーは、通常、クライアント システムで 100% より大きい DPI (Dots Per Inch) を設定してスケーリングを有効にしています。DPI の設定では、テキスト、アプリケーション、アイコンのサイズを制御します。DPI を低く設定すると小さく表示され、高く設定すると大きく表示されます。リモート デスクトップと公開アプリケーションは、ディスプレイ スケーリング機能によってクライアント マシンのスケーリング設定に対応し、通常サイズで表示されます。

Horizon Client は、各リモート デスクトップのディスプレイのスケーリング設定を個別に保存します。公開アプリケーションの場合、現在ログインしているユーザーが使用できるすべての公開アプリケーションにディスプレイのスケーリング設定が適用されます。DPI の設定がクライアント システムで 100% であっても、ディスプレイのスケーリング設定が表示されます。

Horizon Client で [ロックしたゲストのサイズ] グループ ポリシー設定を有効にして、ディスプレイのスケーリング設定を非表示にできます。[Locked Guest Size] グループ ポリシー設定を有効にしても、DPI 同期機能は無効になりません。DPI 同期機能を無効にするには、Horizon 管理者が [DPI 同期] グループ ポリシー設定を無効にする必要があります。詳細については、「DPI 同期の使用」を参照してください。

すべてのリモート デスクトップと公開アプリケーションでディスプレイのスケーリングを有効または無効にするには、[ディスプレイのスケーリングを許可する] グループ ポリシー設定を使用します。詳細については、「クライアント GPO の全般設定」を参照してください。

複数のモニターがある環境で、画面スケーリング機能を使用しても、Horizon Client がサポートするモニター数や最大解像度は影響を受けません。画面スケーリングが許可され使用されている場合、プライマリ モニターの DPI 設定を基準にスケーリングされます。

この手順では、リモート デスクトップまたは公開アプリケーションに接続する前にディスプレイのスケーリング機能を有効にする方法について説明します。リモート デスクトップに接続した後に、Horizon Client メニュー バーから [オプション] - [ディスプレイのスケーリングを許可する] の順に選択して、ディスプレイのスケーリング機能を有効にできます。

手順

1 Horizon Client を起動し、サーバに接続します。

2 リモート デスクトップおよび公開アプリケーションの選択ウィンドウで、リモート デスクトップまたはアプリケーションを右クリックし、[設定] を選択します。

3 [ディスプレイのスケーリングを許可する] チェック ボックスを選択します。

管理者がディスプレイのスケーリングを事前に設定している場合、このチェック ボックスはグレーアウトされます。管理者がディスプレイのスケーリング設定を非表示にしている場合、このチェック ボックスは表示されません。

4 変更内容を保存するには、[適用] をクリックします。

5 ダイアログ ボックスを閉じるには、[OK] をクリックします。

DPI 同期の使用

DPI 同期機能により、リモート デスクトップまたは公開アプリケーションの DPI 設定とクライアント システムの DPI 設定が確実に一致します。新しいリモート セッションを開始すると、Horizon Agent によりリモート セッションの DPI 値とクライアント システムの DPI 値とが一致するよう設定されます。

DPI 同期機能によって、アクティブなリモート セッションの DPI 設定を変更することはできません。既存のリモート セッションに再接続する場合、ディスプレイのスケーリング機能によって、リモート デスクトップや公開アプリケーションが適切にスケーリングされます。

DPI 同期機能は、デフォルトで有効になっています。Horizon 管理者は、[DPI 同期] エージェント グループ ポリシー設定を無効にして DPI 同期機能を無効にできます。構成の変更を有効にするには、ログアウトしてからもう一度ログインする必要があります。[DPI 同期] グループ ポリシーの設定については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。

DPI 同期機能とディスプレイのスケーリング機能の両方が有効になっている場合、一度に有効になるのはいずれかの機能だけです。DPI 同期がまだ有効になっていない場合にのみ（つまり、リモート デスクトップの DPI 設定とクライアント システムの DPI 設定が一致する前）、ディスプレイのスケーリングは実行され、DPI 設定が一致するとディスプレイのスケーリングは実行されなくなります。

仮想デスクトップの場合、DPI 同期機能は次のゲスト OS に対応します。

- 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
- デスクトップとして構成されている Windows Server 2019

公開デスクトップおよびアプリケーションでは、DPI 同期機能は次の RDS ホストでサポートされます。

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

DPI 同期機能では、Horizon Agent 7.0.2 以降および Horizon Client 4.2 以降が必要です。

注: Horizon Client 4.2 を Horizon Agent 7.0 や 7.0.1 と一緒に、また、Horizon Client 4.0 や 4.1 を Horizon Agent 7.0.2 以降と一緒に使用している場合には、DPI 同期機能は使用できません。ディスプレイのスケーリング機能は、これらのシナリオでのみ使用できます。

DPI 同期機能を使用するときのヒントを、次に説明します。

- クライアント システムで DPI 設定を変更する場合、Horizon Client にクライアント システムの新しい DPI 設定を認識させるため、ログアウトしてからもう一度ログインする必要があります。クライアント システムで Windows 10 が実行されている場合でも、この要件は適用されます。
- DPI 設定が 100 パーセント以上になっているクライアント システムでリモート セッションを開始してから、100 パーセント以上の異なる DPI 設定になっている別のクライアント システムで同じセッションを使用する場合、2 番目のクライアント システムで DPI を同期するには、2 番目のクライアント システムでログアウトしてから再度ログインしてリモート セッションに戻る必要があります。
- Windows 10 と Windows 8.x システムでは異なるモニターで異なる DPI 設定がサポートされますが、DPI 同期機能では、クライアント システムのプライマリ モニターで設定されている DPI 値のみが使用されます。また、リモート デスクトップのすべてのモニターで、クライアント システムのプライマリ モニターと同じ DPI 設定が使用されます。Horizon Client は、異なるモニターで異なる DPI 設定をサポートしません。
- Horizon 管理者が、Horizon Agent の [DPI 同期] グループ ポリシー設定の値を変更する場合、新しい設定を有効にするためにログアウトしてからもう一度ログインする必要があります。

- 異なるモニターで異なる DPI 設定をサポートするラップトップを外部モニターに接続し、外部モニターをプライマリ モニターに設定する場合、Windows は、外部モニターを接続または再接続するときに毎回プライマリ モニターとプライマリ モニターの DPI 設定をに変更します。この場合、Horizon Client にプライマリ モニターの変更を認識させるため、クライアント システムからログアウトしてからもう一度ログインする必要があり、クライアント システムとリモート デスクトップや公開アプリケーション間で DPI 設定を一致させるために、リモート デスクトップや公開アプリケーションからログアウトしてから一度ログインする必要があります。
- Windows 10 クライアント システムでは、デスクトップを右クリックして、[表示設定] - [ディスプレイの詳細設定] - [テキストやその他の項目のサイズ調整] の順に選択して、[カスタムの拡大率を設定] リンクをクリックし、再ログインして、新しい DPI 設定を有効にします。

リモート デスクトップの表示モードの変更

リモート デスクトップに接続する前または後に、表示モードを変更できます。たとえば、[すべてのモニター] から [全画面表示] に切り替えることができます。この機能は、公開アプリケーションではサポートされません。

手順

1 Horizon Client を起動し、サーバにログインします。

2 リモート デスクトップに接続します。あるいは、デスクトップとアプリケーションの選択ウィンドウでリモート デスクトップを右クリックして、[設定] を選択します。

3 [表示] ドロップダウン メニューから表示モードを選択します。

オプション	説明
すべてのモニター	リモート デスクトップのウィンドウをマルチモニタに表示します。リモート デスクトップ ウィンドウは、デフォルトですべてのモニターに表示されます。
全画面表示	リモート デスクトップのウィンドウを全画面で表示します。
ウィンドウ - 大	リモート デスクトップのウィンドウ サイズを 1904 x 978 ピクセルに設定します。
ウィンドウ - 小	リモート デスクトップのウィンドウ サイズを 640 x 480 ピクセルに設定します。
カスタム	リモート デスクトップのカスタム ウィンドウ サイズを設定するスライダーが表示されます。

4 変更内容を保存するには、[適用] をクリックします。

5 ダイアログ ボックスを閉じるには、[OK] をクリックします。

リモート デスクトップに接続している場合、変更はすぐに適用されます。まだ接続していない場合は、リモート デスクトップに接続したときに変更が適用されます。Horizon Client から終了すると、Horizon Client がリモート デスクトップの環境設定ファイルに表示設定を保存します。

[すべてのモニター] モードを使用しているときに、[最小化] ボタンをクリックしてからウィンドウを最大化すると、ウィンドウは [すべてのモニター] モードに戻ります。同様に、[全画面表示] モードを使用しているときに、ウィンドウを最小化してから最大化すると、ウィンドウは 1 台のモニターで [全画面表示] モードに戻ります。

注: Horizon Client がすべてのモニターを使用しているときに、公開アプリケーションのウィンドウを最大化すると、アプリケーションが表示されているモニターだけでウィンドウが全画面表示に拡大します。

USB デバイスの接続に USB リダイレクトを使用する

USB リダイレクト機能を使用すると、小型のフラッシュ ドライブなど、ローカルで接続された USB デバイスをリモート デスクトップまたは公開アプリケーションで使用できます。

USB リダイレクト機能を使用すると、ローカルのクライアント システムに接続されているほとんどの USB デバイスが Horizon Client のメニューで使用できるようになります。このメニューを使用して、デバイスを接続したり接続解除したりします。

View Agent 6.1 以降、または Horizon Agent 7.0 以降では、ローカルで接続された小型の USB フラッシュ ドライブやハード ディスクをリダイレクトして、公開デスクトップやアプリケーションで使用きます。Horizon Agent 7.0.2 以降では、公開されたデスクトップおよびアプリケーションは、TOPAZ 署名パッド、Olympus ディクテーション用フット ペダル、Wacom 署名パッドなどの一般的な USB デバイスをサポートできます。セキュリティ ストレージ ドライブや USB CD-ROM ドライブなど、他の種類の USB デバイスは公開デスクトップおよびアプリケーションではサポートされていません。

リモート デスクトップや公開アプリケーションへの USB デバイスの接続は、手動でも自動でも行うことができます。

この手順では、Horizon Client を使用してリモート デスクトップまたは公開アプリケーションに USB デバイスを自動接続する方法について説明しています。また、自動接続は Horizon Client のコマンドライン インターフェイスを使用するか、グループ ポリシーを作成して構成することもできます。

コマンドライン インターフェイスの詳細については、「コマンド ラインからの Horizon Client の実行」 を参照してください。グループ ポリシーの設定については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。

前提条件

- リモート デスクトップや公開アプリケーションで USB デバイスを使用するには、Horizon 管理者側で USB リダイレクト機能を有効にしておく必要があります。

  このタスクには、Horizon Agent の USB リダイレクト コンポーネントのインストールが含まれ、USB リダイレクトに関するポリシー設定が含まれる場合もあります。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』のドキュメントおよび『「クライアント GPO の USB 設定」』を参照してください。

- USB リダイレクト コンポーネントを Horizon Client にインストールする必要があります。このコンポーネントをインストールに含めていなかった場合、Horizon Client をアンインストールして、もう一度インストーラを実行し、USB リダイレクト コンポーネントを追加します。

  インストール方法については、『VMware Horizon Client for Windows のインストールとセットアップ ガイド』を参照してください。

- 「USB リダイレクトの制限事項」 を確認してください。

手順

- 手動で USB デバイスをリモート デスクトップに接続します。
  a USB デバイスをローカルのクライアント システムに接続します。
  b リモート デスクトップの VMware Horizon Client メニュー バーから [USB デバイスを接続] をクリックします。
  c USB デバイスを選択します。

  デバイスは手動でローカル システムからリモート デスクトップにリダイレクトされます。
- USB デバイスを公開アプリケーションに接続します。
  a USB デバイスをローカルのクライアント システムに接続します。
  b Horizon Client を起動し、公開アプリケーションに接続します。
  c デスクトップとアプリケーションの選択ウィンドウの右上にある [設定]（歯車）アイコンをクリックして、[USB デバイス] をクリックします。
  d 右側のペインで、USB デバイスを選択して [接続] をクリックし、公開アプリケーションを選択、[OK] をクリックします。

  Horizon Client により、選択した公開アプリケーションに USB デバイスが接続されます。この USB デバイスは、選択したアプリケーションと同じファーム内の他のアプリケーションでも使用できます。
  e (オプション) Horizon Client の設定で、公開アプリケーションの起動時に、USB デバイスを公開アプリケーションに自動的に接続するには、[起動時に自動接続] チェック ボックスをオンにします。
  f (オプション) Horizon Client の設定で、USB デバイスをローカルのシステムに挿入したときに、その USB デバイスを公開アプリケーションに自動的に接続するには、[挿入時に自動接続] チェック ボックスをオンにします。

  この動作を反映させるには、公開アプリケーションをアクティブにして、前面に移動しておく必要があります。
  g [設定] ダイアログ ボックスを閉じるには、[OK] をクリックします。
  h 公開アプリケーションを使い終わったら、[設定] ダイアログ ボックスを再度開き、[USB デバイス] を選択して [切断] を選択します。

  ローカル システムで USB デバイスにアクセスできるよう USB デバイスを解除してください。

- ローカル システムに USB デバイスを接続したときに、その USB デバイスをリモート デスクトップに自動的に接続するよう Horizon Client を設定します。

  Android ベースの Samsung スマートフォンおよびタブレットなど、MTP ドライバを使用するデバイスを接続するには、自動接続機能を使用します。

  a USB デバイスを接続する前に、Horizon Client を起動してリモート デスクトップに接続します。

  b リモート デスクトップの VMware Horizon Client メニュー バーから、[USB デバイスを接続] - [挿入時に自動接続] の順に選択します。

  c USB デバイスを接続します。

  Horizon Client を起動した後にローカル システムに接続する USB 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。

- Horizon Client の起動時に、USB デバイスをリモート デスクトップに自動的に接続するよう Horizon Client を設定します。

  a リモート デスクトップの VMware Horizon Client メニュー バーから、[USB デバイスを接続] - [起動時に自動接続] の順に選択します。

  b USB デバイスを挿入し、Horizon Client を再起動します。

  Horizon Client の起動時にローカル クライアント システムに接続される USB 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。

USB デバイスがリモート デスクトップや公開アプリケーションに表示されます。USB デバイスがリモート デスクトップや公開アプリケーションに表示されるまで、20 秒ほどかかる場合があります。初めてデバイスをリモート デスクトップに接続する場合は、ドライバのインストールが求められる場合があります。

数分経過しても、USB デバイスがリモート デスクトップまたは公開アプリケーションに表示されない場合は、デバイスを一度クライアント コンピュータから取り外し、再度、挿入してみてください。

次のステップ

USB のリダイレクトで問題がある場合、『Horizon 7 でのリモート デスクトップ機能の構成』の USB リダイレクトのトラブルシューティングについてのトピックを参照してください。

USB リダイレクトの制限事項

USB リダイレクト機能には、特定の制限があります。

- Horizon Client のメニューから USB デバイスにアクセスして、リモート デスクトップでそのデバイスを使用しているとき、ローカル コンピュータ上ではそのデバイスにアクセスできません。
- 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 デバイスを含め、メニューには表示されないが、リモート デスクトップには表示される USB デバイス。リモート デスクトップとローカル コンピュータは、これらのデバイスを同時に使用します。これらのデバイスとのやりとりは、ネットワーク遅延のため低速になる場合があります。
- 大容量 USB ディスク ドライブは、リモート 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 デバイスによっては特定のドライバが必要になります。必要なドライバがまだリモート デスクトップにインストールされていない場合、USB デバイスをリモート デスクトップに接続するとドライバのインストールを求められます。
- Android ベースの Samsung 製スマート フォンやタブレットなどの MTP ドライバを使用する USB デバイスを接続する場合には、USB デバイスをリモート デスクトップに自動接続するように Horizon Client を設定する必要があります。そうしないと、メニュー項目を使用して USB デバイスを手動でリダイレクトしようとしても、デバイスを取り外して接続し直さない限りリダイレクトできません。
- [USB デバイスを接続] メニューを使用してスキャナを接続しないでください。スキャナ デバイスを使用するには、スキャナ リダイレクト機能を使用します。View Agent 6.0.2 以降または Horizon Agent 7.0 以降と併用すれば、Horizon Client でこの機能を使用できます。「スキャナの使用」を参照してください。
- 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。オーディオ入力デバイスと出力デバイスは、リアルタイム オーディオビデオ機能で適切に動作します。これらのデバイスに対する USB リダイレクトを使用する必要はありません。
- 管理者ユーザーとして接続する場合を除き、公開デスクトップでは、リダイレクトされた USB ドライブをフォーマットできません。
- 起動時および挿入時の公開アプリケーションの自動接続機能は、グローバルのアプリケーション資格では動作しません。

注: USB イーサネット デバイス、タッチ画面デバイスなどの USB デバイスをリモート デスクトップや公開アプリケーションにリダイレクトしないでください。USB イーサネット デバイスをリダイレクトすると、クライアント システムはネットワーク接続を失います。タッチ画面デバイスをリダイレクトすると、リモート デスクトップまたは公開アプリケーションではタッチ入力は受け付けますが、キーボード入力は受け付けません。リモート デスクトップや公開アプリケーションを USB デバイスと自動接続する設定を行っている場合は、特定のデバイスを除外するポリシーを設定できます。

USB デバイス再起動時に再接続するためのクライアント構成

USB デバイスをリモート デスクトップに自動接続するように Horizon Client を構成していない場合、時々再起動する特定のデバイスに再接続するように Horizon Client を構成できます。このように構成しない場合、アップグレード中にデバイスが再起動すると、デバイスはリモート デスクトップではなくローカル システムに接続します。

オペレーティング システムのアップグレード中に自動的に再起動するスマート フォンやタブレットなどの USB デバイスを接続する予定の場合は、特定のデバイスをリモート デスクトップに再接続するように Horizon Client を設定できます。このタスクを実行するには、クライアント システムの構成ファイルを編集します。

Horizon Client の [挿入時に自動接続] オプションを使用すると、クライアント システムに接続するすべてのデバイスがリモート デスクトップにリダイレクトされます。一部のデバイスを接続しないようにする場合は、以下の手順に従って Horizon Client を構成すると、特定の USB デバイスだけが再接続されます。

前提条件

デバイスのベンダ ID (VID) および製品 ID (PID) の 16 進数フォーマットを決定します。詳細については、http://kb.vmware.com/kb/1011600 の VMware KB の記事を参照してください。

手順

1 クライアント システムで、テキスト エディタを起動し、config.ini ファイルを開きます。

オペレーティング システム	ファイル パス
Windows 7、8.x、または Windows 10	C:\ProgramData\VMware\VMware USB Arbitration Service\config.ini
Windows XP	C:\Documents and Settings\All Users\Application Data\VMware\VMware USB Arbitration Service\config.ini

2 特定のデバイスの slow-reconnect プロパティを設定します。

```
usb.quirks.device0 = "<vid>:<pid> slow-reconnect"
```

<vid>:<pid> は、デバイスのベンダー ID および製品 ID を 16 進数で表します。たとえば、以下の行は 2 台の USB デバイスにこのプロパティを設定します:

```
usb.quirks.device0 = "0x0529:0x0001 slow-reconnect"
usb.quirks.device1 = "0x0601:0x0009 slow-reconnect"
```

usb.quirks.device<N> デバイス プロパティを 0 から始まる順序で指定します。たとえば、行 usb.quirks.device0 の後ろに usb.quirks.device1 ではなく、usb.quirks.device2 が続く場合、最初の行だけが読み込まれます。

スマート フォンおよびタブレットなどのデバイスのファームウェアまたはオペレーティング システムがアップグレードされると、デバイスは再起動され、それを管理するリモート デスクトップに接続するので、アップグレードが成功します。

Web カメラとマイクでリアルタイム オーディオ ビデオ機能を使用

リアルタイム オーディオビデオ機能を使用すれば、リモート デスクトップまたは公開アプリケーションでローカル クライアント システムの Web カメラまたはマイクを使用できます。リアルタイム オーディオビデオは、標準の会議アプリケーションやブラウザ ベースのビデオ アプリケーションと互換性があります。標準の Web カメラ、オーディオ USB デバイス、アナログ オーディオ入力をサポートします。

リアルタイム オーディオビデオ機能のセットアップ、およびエージェント マシンのフレーム レートとイメージの解像度の設定については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。クライアント システムでのこれらの設定については、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。

リアルタイム オーディオ ビデオ機能の適切なインストールと操作を検証するテスト アプリケーションをダウンロードするには、http://labs.vmware.com/flings/real-time-audio-video-test-application にアクセスしてください。このテスト アプリケーションは VMware Flings で提供されるため、テクニカル サポートは利用できません。

Webcam を使用できる場合

Horizon 管理者がリアルタイム オーディオ ビデオ機能を構成していて、ユーザーが 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場合は、内蔵またはローカル クライアント コンピュータに接続された Web カメラをリモート デスクトップまたは公開アプリケーションで使用できます。Skype、Webex、または Google ハングアウトなどの会議アプリケーションで Web カメラを使用できます。

Skype、Webex、または Google ハングアウトなどのアプリケーションをリモート デスクトップで設定するときに、アプリケーションのメニューから入力および出力デバイスを選択できます。仮想デスクトップの場合は、VMware 仮想マイクと VMware 仮想 Web カメラを選択できます。公開されたデスクトップとアプリケーションの場合には、リモート オーディオ デバイスと VMware 仮想 Web カメラを選択できます。

多くのアプリケーションでは、入力デバイスを選択する必要はありません。

ローカル クライアント コンピュータが Web カメラを使用している場合、リモート セッションでは同時に使用できません。また、リモート セッションで Web カメラを使用している場合、ローカル クライアント コンピュータで同時に使用できません。

重要: USB Web カメラ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。この操作を行うと、USB リダイレクトでデバイスがルーティングされるため、パフォーマンスが低下してビデオ チャットが困難になります。

複数の Web カメラがローカル クライアント コンピュータに接続されている場合、リモート セッションで優先的に使用する Web カメラを設定できます。

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が接続されている場合、リモート デスクトップまたは公開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 ビデオ機能を設定して、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。

使用可能な場合、優先 web カメラまたはマイクがリモート デスクトップまたは公開アプリケーションで使用されます。優先 Web カメラまたはマイクが使用できない場合は、他の Web カメラまたはマイクが使用されます。

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 Web カメラや USB マイクまたは他のタイプのマイク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 デスクトップや公開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。
   - デスクトップとアプリケーションの選択ウィンドウの右上隅で、[設定]（歯車のアイコン）をクリックします。
   - デスクトップとアプリケーションの選択ウィンドウでリモート デスクトップまたは公開デスクトップを右クリックして、[設定] を選択します。
2 優先 Web カメラを選択するには、[優先 Web カメラ] ドロップダウン メニューから、Web カメラを選択します。

   メニューには、クライアント システムで使用可能な Web カメラが表示されます。
3 優先マイクを選択するには、[優先マイク] ドロップダウン メニューから、マイクを選択します。

   メニューには、クライアント システムで使用可能なマイクが表示されます。
4 変更内容を保存するには、[OK] または [適用] をクリックします。

リモート デスクトップや公開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 カメラやマイクが、リモート セッションにリダイレクトされます。

セッション共同作業機能の使用

セッション共同作業機能を使用すると、他のユーザーを既存のリモート デスクトップ セッションに招待できます。

リモート デスクトップ セッションに参加するユーザーの招待

リモート デスクトップでセッション共同作業機能を有効にすると、他のユーザーを既存のリモート デスクトップ セッションに招待できます。

デフォルトでは、セッション共同作業の招待状を E メールまたはインスタント メッセージで送信できます（Windows リモート デスクトップの場合のみ）。また、リンクをクリップボードにコピーして、ユーザーに転送することもできます。招待状を E メールで送信するには、E メール アプリケーションがインストールされている必要があります。Windows リモート デスクトップでの招待方法として IM を選択する場合は、Skype for Business をインストールして設定する必要があります。招待できるのは、サーバで認証可能なドメインのユーザーだけです。デフォルトでは、最大 5 人のユーザーを招待できます。

セッション共同作業機能には次の制限があります。

- 複数のモニターを使用している場合、プライマリ モニターにのみセッション共同作業者が表示されます。
- リモート デスクトップ セッションを作成するときに、VMware Blast 表示プロトコルを選択する必要があります。セッション共同作業機能は、PCoIP または RDP セッションに対応していません。
- H.264 ハードウェア エンコードに対応していません。セッション オーナーがハードウェア エンコードを使用しているときに、共同作業者がセッションに参加すると、両方ともソフトウェア エンコードに戻ります。

- 匿名で共同作業を行うことはできません。セッション共同作業者は、Horizon がサポートする認証メカニズムで識別可能でなければなりません。
- セッション共同作業者が Horizon Client 4.7 for Windows、Mac、または Linux をインストールしているか、HTML Access 4.7 以降を使用する必要があります。
- セッション共同作業者がサポート対象外の Horizon Client バージョンを使用している場合、共同作業のリンクをクリックすると、エラー メッセージが表示されます。
- セッション共同作業機能を使用して、公開されたアプリケーション セッションを共有できません。

前提条件

リモート デスクトップ セッションに参加するユーザーを招待するには、Horizon 管理者がセッション共同作業機能を有効にする必要があります。

Windows デスクトップの場合、これにより、デスクトップ プールまたはファーム レベルでセッション共同作業機能を有効にします。また、グループ ポリシーを使用して、使用可能な招待方法などのセッション共同作業機能を設定することもできます。詳しい要件については、「セッション共同作業機能の要件」を参照してください。

Windows デスクトップでセッション共同作業機能を有効にする方法については、『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。ファームでセッション共同作業機能を有効にする方法については、『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』ドキュメントを参照してください。グループ ポリシー設定を使用してセッション共同作業機能を設定する方法については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントを参照してください。

Linux デスクトップでセッション共同作業機能を有効にする方法については、『Horizon 7 for Linux 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。

手順

1 セッション共同作業機能が有効になっているリモート デスクトップに接続します。

VMware Blast 表示プロトコルを使用する必要があります。

2 リモート デスクトップのシステム トレイで、[VMware Horizon Collaboration] のアイコン（たとえば、  ）をクリックします。

共同作業のアイコンは、オペレーティング システムのバージョンによって異なる場合があります。

3 VMware Horizon Collaboration のダイアログ ボックスが開いたら、リモート デスクトップ セッションに参加するユーザーのユーザー名（たとえば、**testuser**、**domain\testuser**）またはメール アドレスを入力します。

特定のユーザーのユーザー名またはメール アドレスを初めて入力する場合には、[「<user>」の検索]をクリックしてカンマを入力するか、[Enter] キーを押してユーザーを検証する必要があります。ユーザー名またはメール アドレスを次に入力したときに、セッション共同作業機能がユーザーを記憶します。

デフォルトでは、最大 5 人のユーザーを招待できます。Horizon 管理者は、招待できるユーザーの最大数を変更できます。

4 招待方法を選択します。

すべての招待方法が使用できるとは限りません。

オプション	アクション
E メール	共同作業の招待状をクリップボードにコピーし、デフォルトのメール アプリケーションで新しいメール メッセージを開きます。この方法で招待する場合には、メール アプリケーションがインストールされている必要があります。
IM	(Windows リモート デスクトップの場合のみ) 共同作業の招待状をクリップボードにコピーし、Skype for Business で新しいウィンドウを開きます。Ctrl + V キーを押し、Skype for Business のウィンドウにリンクを貼り付けます。この方法で招待するには、Skype for Business がインストールされ、設定されている必要があります。
リンクのコピー	共同作業の招待状をクリップボードにコピーします。メモ帳などの別のアプリケーションを手動で開き、Ctrl + V キーを押して招待状を貼り付ける必要があります。

招待状の送信後、VMware Horizon Collaboration のアイコンがデスクトップに表示され、共同作業セッションのユーザー インターフェイスがダッシュボードに変わり、共同作業セッションの現在の状態が表示されます。ここで、特定のアクションを実行できます。

セッション共同作業者が招待を受け入れ、Windows リモート デスクトップのセッションに参加すると、システム トレイの VMware Horizon Collaboration のアイコンが赤いドットで表示され、ユーザーの参加が通知されます。Linux リモート デスクトップのセッションでは、この機能を使用できません。

次のステップ

VMware Horizon Collaboration のダイアログ ボックスで、共同作業セッションを管理します。「共同作業セッションの管理」を参照してください。

共同作業セッションの管理

招待状の送信後、共同作業セッションのユーザー インターフェイスがダッシュボードに変わり、共同作業セッションの現在の状態が表示されます。ここで、特定のアクションを実行できます。

前提条件

共同作業セッションを開始します。「リモート デスクトップ セッションに参加するユーザーの招待」を参照してください。

手順

1 リモート デスクトップで、システム トレイの [VMware Horizon Collaboration] アイコンをクリックします。

[名前] 列に、すべてのセッション共同作業者の名前が表示され、[ステータス] 列に共同作業者の状態が表示されます。

2 VMware Horizon セッション共同作業のダッシュボードを使用して、共同作業セッションを管理します。

オプション	アクション
招待を取り消すか、共同作業者を削除する	[ステータス] 列で [削除] をクリックします。
別のセッション共同作業者にコントロールを渡す	セッション共同作業者がセッションに参加した後、[コントロール] 列のスイッチを [オン] に切り替えます。 セッションの制御を再開するには、ダブルクリックするか、任意のキーを押します。セッション共同作業者は、[コントロール] 列のスイッチを [オフ] に切り替えるか、[コントロールを返す] ボタンをクリックすると、コントロールを返すことができます。
共同作業者を追加する	[共同作業者を追加] をクリックします。
共同作業セッションを終了する	[共同作業を終了] をクリックします。アクティブな共同作業者がすべて切断されます。 Windows リモート デスクトップでは、[VMware Horizon セッション共同作業] アイコンの横にある [停止] ボタンでも共同作業セッションを終了できます。Linux リモート デスクトップの場合、[停止] ボタンは使用できません。

共同作業セッションへの参加

共同作業セッションに参加するには、共同作業の招待状のリンクをクリックします。このリンクは、E メールやインスタント メッセージで提供される場合も、セッション オーナーから転送された文書に含まれている場合もあります。また、サーバにログインして、リモート デスクトップとアプリケーションの選択ウィンドウで共同作業セッションのアイコンをダブルクリックすることもできます。

ここでは、共同作業の招待状から共同作業セッションに参加する方法について説明します。

注: クラウド ポッド アーキテクチャ環境では、セッション オーナーのポッドにログインする場合を除き、サーバにログインして共同作業セッションに参加することはできません。

共同作業セッションで次のリモート デスクトップ機能を使用することはできません。

- USB リダイレクト
- リアルタイム オーディオビデオ (RTAV)
- マルチメディア リダイレクト
- クライアント ドライブのリダイレクト
- スマート カード リダイレクト
- 仮想印刷
- VMware 仮想印刷リダイレクト
- Microsoft Lync リダイレクト
- ファイルのリダイレクトと「Dock に追加」機能
- クリップボード リダイレクト

共同作業セッションでは、リモート デスクトップの解像度を変更できません。

前提条件

共同作業セッションに参加するには、クライアント システムに Horizon Client 4.7 for Windows、Mac、または Linux がインストールされているか、HTML Access 4.7 以降を使用する必要があります。

手順

1 共同作業の招待状にあるリンクをクリックします。

クライアント システムで Horizon Client が開きます。

2 認証情報を入力して、Horizon Client にログインします。

認証に成功すると、共同作業セッションが開始し、セッション オーナーのリモート デスクトップが表示されます。セッション オーナーからマウスとキーボードのコントロールが渡されると、リモート デスクトップが使用できるようになります。

3 マウスとキーボードのコントロールをセッション オーナーに返すには、システム トレイにある [VMware Horizon Collaboration] アイコンをクリックします。[コントロール] 列のスイッチを [オフ] に切り替えるか、[コントロールを返す] ボタンをクリックします。

4 共同作業セッションを終了するには、[オプション] - [切断] の順にクリックします。

クライアント ドライブのリダイレクトによるローカル フォルダおよびドライブへのアクセス共有

クライアント ドライブ リダイレクト機能を使用すると、ローカル クライアント システムのフォルダとドライブをリモート デスクトップや公開アプリケーションと共有できます。

共有ドライブには、マッピングされたドライブおよび USB ストレージ デバイスを含めることができます。マッピングされたドライブには、UNC（汎用命名規則）パスを設定できます。

Windows リモート デスクトップで、共有フォルダおよびドライブは、Windows オペレーティング システムのバージョンに応じて [PC] フォルダまたは [コンピュータ] フォルダに表示されます。Notepad などの公開アプリケーションでは、共有フォルダまたはドライブ内のファイルを参照したり開いたりすることができます。

ローカルのファイル システムにあるローカルのファイルを、公開アプリケーションで直接開く機能もオンにできます。この機能が有効な場合、ローカル ファイルを右クリックすると、クライアント システムの [プログラムから開く] メニューに、使用可能な公開アプリケーションの一覧が表示されます。

また、ファイルをダブルクリックすることで、そのファイルが公開アプリケーションで自動的に開くよう設定することもできます。この機能を有効にすると、特定の拡張子を持つローカル ファイル システムのすべてのファイルが、ユーザーがログインしているサーバに登録されます。たとえば、サーバで Microsoft Word が公開アプリケーションになっている場合、ローカルのファイル システムで **.docx** ファイルを右クリックすると、Microsoft Word の公開アプリケーションでファイルを開くことができます。

この機能では、Horizon 6 バージョン 6.2 以降のサーバとエージェントが必要となります。

クライアント ドライブ リダイレクトの設定は、すべてのリモート デスクトップと公開アプリケーションに適用されます。

前提条件

フォルダおよびドライブをリモート デスクトップまたは公開アプリケーションと共有するには、Horizon 管理者がクライアント ドライブのリダイレクト機能を有効にする必要があります。このタスクには、View Agent 6.1.1 以降または Horizon Agent 7.0 以降をインストールすることと、エージェントの [クライアント ドライブ リダイレクト] オプションを有効にすることが含まれます。ポリシーの設定を行って、クライアント ドライブ リダイレクトの動作を制御することも含まれる場合があります。UNC パス サポートでは、Horizon Agent 7.3 以降が必要です。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』 を参照してください。

グループ ポリシー設定を有効にして、Horizon Client でクライアント ドライブのリダイレクト機能を非表示にできます。詳細については、「クライアント GPO の全般設定」の[ファイルとフォルダの共有を無効にする]を参照してください。

接続サーバ インスタンスでセキュアなトンネルが有効の場合、プロキシ サーバを使用するようにクライアント システムのブラウザを設定すると、クライアント ドライブ リダイレクトのパフォーマンスが低下する可能性があります。クライアント ドライブ リダイレクトの最高のパフォーマンスを得るには、プロキシ サーバを使用しないか、LAN 設定を自動的に検出するようブラウザを構成します。

手順

1 [設定] ダイアログ ボックスを開き、[共有する] パネルを表示します。

オプション	説明
デスクトップとアプリケーションの選択ウィンドウから	リモート デスクトップまたは公開アプリケーションのアイコンを右クリックし、[設定] を選択して、表示されるウィンドウの左側のパネルで [共有する] を選択します。
リモート デスクトップまたは公開アプリケーションに接続したときに表示される [共有する] ダイアログ ボックスから	ダイアログ ボックスで、[設定] - [共有する] リンクをクリックします。
リモート デスクトップから	メニュー バーから [オプション] - [フォルダを共有] を選択します。

2 クライアント ドライブ リダイレクト設定を構成します。

オプション	アクション
特定のフォルダまたはドライブを、リモート デスクトップおよび公開アプリケーションと共有する	[追加] ボタンをクリックし、共有するフォルダまたはドライブを参照して選択し、[OK] をクリックします。 注: USB リダイレクト機能で USB デバイスがリモート デスクトップまたは公開アプリケーションにすでに接続している場合、この USB デバイスでフォルダを共有することはできません。 また、USB リダイレクト機能は、起動時またはデバイスの挿入時に USB デバイスを自動的に接続するため、この機能はオンにしないでください。オンにすると、次に Horizon Client を開始するか、USB デバイスを挿入したときに、クライアント ドライブのリダイレクト機能ではなく、USB リダイレクト機能でデバイスが接続されます。
特定のフォルダまたはドライブの共有を停止する	フォルダ リストでフォルダまたはドライブを選択し、[削除] ボタンをクリックします。
リモート デスクトップおよび公開アプリケーションからローカル ユーザー ディレクトリのファイルへのアクセスを許可する	[ローカル ファイルを共有<ユーザー名>] チェック ボックスをオンにします。

オプション	アクション
リモート デスクトップと公開アプリケーションで USB ストレージ デバイスを共有する	[リムーバブル ストレージへのアクセスを許可] チェック ボックスをオンにします。クライアント ドライブ リダイレクト機能により、クライアント システムに挿入されているすべての USB ストレージ デバイス、および FireWire と Thunderbolt で接続されているすべての外部ドライブが自動的に共有されます。共有する特定のデバイスを選択する必要はありません。 注: リモート デスクトップまたは公開アプリケーションに USB リダイレクト機能ですでに接続されている USB ストレージ デバイスは共有されません。 このチェック ボックスがオフの場合、USB リダイレクト機能を使用して、USB ストレージ デバイスをリモート デスクトップや公開アプリケーションに接続できます。
公開アプリケーションを使用してローカルのファイル システムからローカル ファイルを開く機能をオンする	[ホスト型アプリケーションでローカル ファイルを開く] チェック ボックスを選択します。このオプションを使用すると、ローカル ファイル システムにあるファイルを右クリックして選択し、公開アプリケーションでファイルを開くよう選択することができます。 また、ファイルをダブルクリックしたときなど、特定のファイル拡張子を持つすべてのファイルが公開アプリケーションによってデフォルトで開くように、ファイルのプロパティを変更することもできます。たとえば、ファイルを右クリックして、[プロパティ] を選択し、[変更] をクリックして、そのタイプのファイルを開く公開アプリケーションを選択します。 Horizon 管理者は、この機能を無効にできます。
リモート デスクトップまたは公開アプリケーションへの接続時に [共有する] ダイアログ ボックスを表示しない	[デスクトップやアプリケーションに接続するときにダイアログを表示しない] チェック ボックスをオンにします。 このチェック ボックスをオフにすると、リモート デスクトップや公開アプリケーションに最初に接続したときに [共有する] ダイアログ ボックスが表示されます。たとえば、サーバにログインしてリモート デスクトップに接続すると、[共有する] ダイアログ ボックスが表示されます。さらに、別のリモート デスクトップまたは公開アプリケーションに接続すると、ダイアログ ボックスは表示されなくなります。もう一度ダイアログ ボックスを表示するには、サーバから切断して再度ログインする必要があります。

次のステップ

リモート デスクトップまたは公開アプリケーションで共有フォルダを表示できることを確認してください。

- Windows オペレーティング システムのバージョンに応じて、Windows リモート デスクトップでエクスプローラーを開いて [PC] フォルダを検索するか、Windows エクスプローラーを開いて [コンピューター] フォルダを検索します。
- 公開アプリケーションで、[ファイル] - [開く] の順に選択するか、[ファイル] - [名前を付けて保存] の順に選択してフォルダまたはドライブに移動します。

共有に選択したフォルダとドライブには、次のような命名規則が使用されます。

命名規則	例
`<desktop-name> の <folder-name>`	`JSMITH-W03 の jsmith`
`<folder-name> (<drive-number>:)`	`jsmith (Z:)`
`<desktoptop-name> (<drive-number>:) の <folder-name>`	`JSMITH-W03 (Z:) の jsmith`

Horizon Agent のバージョンによっては、リダイレクトされたフォルダに 2 つのエントリがあります。たとえば、Windows 10 では、[デバイスとドライブ] と [ネットワークの場所] の 2 つがあります。両方のエントリが同時に表示される場合もあります。すべてのボリューム ラベル（A: から Z: まで）が使用済みの場合、リダイレクトされたフォルダのエントリは 1 つだけになります。

コピーとペースト

デフォルトでは、ローカル クライアント システムからリモート デスクトップまたは公開アプリケーションにコピー アンド ペーストを行うことができます。リモート デスクトップや公開アプリケーションからクライアント システムにコピー アンド ペーストを行うこともできます。また、2 つのリモート デスクトップまたは公開アプリケーション間でもコピー アンド ペーストが可能です。ただし、Horizon 管理者がこれらの機能を有効にしている必要があります。

テキストやイメージをコピーして貼り付けることができます。次のファイル フォーマットがサポートされています。

- CF_BITMAP
- CF_DIB
- CF_HDROP（ファイル タイプ）
- CF_UNICODETEXT
- Biff12
- Art::GVML ClipFormat
- HTML 形式
- RTF (Rich Text Format)

たとえば、クライアント システムにテキストをコピーするには、テキストを選択して Ctrl + C キーを押します。リモート デスクトップにテキストを貼り付けるには、リモート デスクトップで Ctrl + V キーを押します。

VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用する場合、Horizon 管理者は、コピー アンド ペースト操作をクライアント システムからリモート デスクトップまたは公開アプリケーションに対してのみ、リモート デスクトップまたは公開アプリケーションからクライアント システムに対してのみ、あるいは双方向で許可または禁止するように、この機能を設定できます。

Horizon 管理者は、エージェント グループのポリシーでコピー アンド ペースト機能を設定します。Horizon Server と Horizon Agent のバージョンによっては、Horizon 管理者は、グループ ポリシーを使用して、コピー アンド ペースト操作でクリップボードがサポートするフォーマットを制限したり、スマート ポリシーを使用してリモート デスクトップでのコピー アンド ペースト操作を制御ことができます。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。

Horizon 7 バージョン 7.0 以前のサーバに接続している場合、コピー/貼り付け操作でクリップボードに 1 MB のデータを格納できます。Horizon 7 バージョン 7.0.1 以降のサーバに接続している場合、サーバとクライアントの両方でクリップボードのメモリ サイズを設定できます。PCoIP または VMware Blast セッションが確立されると、サーバはクライアント システムにクリップボード メモリ サイズを送信します。有効なクリップボード メモリ サイズは、サーバとクライアントのクリップボード メモリ サイズの値の小さい方となります。

コピー アンド ペースト機能には、次の制限があります。

- リモート デスクトップとローカル クライアント コンピュータのファイル システム間では、ファイルのコピーおよび貼り付けを行うことができません。

- フォーマットされたテキストをコピーする場合、データの一部がテキストで、一部のデータはフォーマットされた情報となります。大容量のフォーマットされたテキスト、またはテキストとイメージをコピーする場合、テキストとイメージをペーストする時は、プレーン テキストの一部またはすべてを見ることができますが、フォーマットまたはイメージを見ることができないケースがあります。その理由は、3 種類のデータが分割されて保存される場合があるためです。たとえば、コピーされるドキュメントのタイプによっては、イメージはイメージまたは RTF データとして保存される場合があります。
- テキストと RTF データを合わせたサイズが最大クリップボード サイズより小さければ、フォーマットされたテキストが貼り付けられます。RTF データは多くの場合に分割できないため、テキストとフォーマットのサイズが最大クリップボード サイズより大きい場合は、RTF データが破棄されてプレーン テキストが貼り付けられます。
- 1 回の操作で選択したフォーマットされたテキストとイメージすべてをペーストできない場合、1 回の操作でコピー アンド ペーストするデータ量を少なくする必要があります。

クライアントのクリップボードのメモリ サイズの構成

Horizon 7 バージョン 7.0.1 以降および Horizon Client 4.1 以降では、サーバとクライアントの両方についてクリップボード メモリ サイズを構成できます。

PCoIP または VMware Blast セッションが確立されると、サーバはクライアントにクリップボード メモリ サイズを送信します。有効なクリップボード メモリ サイズは、サーバとクライアントのクリップボード メモリ サイズの値の小さい方となります。

クライアントのクリップボードのメモリ サイズを設定するには、Windows レジストリの値 `HKLM\Software\VMware, Inc.\VMware VDPService\Plugins\MKSVchan\ClientClipboardSize` を修正します。値のデータ型は、REG_DWORD です。値は、KB で指定されます。0 を指定する場合、または値を指定しない場合、クライアントのクリップボードのメモリ サイズは、デフォルトで 8192 KB (8 MB) になります。

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。

コピー アンド ペースト アクティビティの記録

クリップボード監査機能を有効にすると、Horizon Agent は、コピーアンドペースト アクティビティに関する情報をエージェント マシンのイベント ログに記録します。デフォルトでは、クリップボード監査機能は無効になっています。

クリップボード監査機能を有効にするには、VMware Blast または PCoIP の [クリップボード監査の設定] グループポリシー設定を使用する必要があります。

エージェント マシンに Horizon Agent 7.6 がインストールされている場合、エージェント マシンからクライアント コンピュータにコピーされたクリップボード データの情報だけがイベント ログに記録されます。エージェント マシンに Horizon Agent7.7 以降がインストールされている場合、クリップボード監査機能がクライアント コンピュータからエージェント マシンにコピーされたデータの情報のみを記録するのか、エージェント マシンからクライアント コンピュータにコピーされたデータの情報のみを記録するのか、あるいはその両方を記録するのかを構成できます。

オプションで、VMware Blast または PCoIP に [クライアントが監査をサポートしていないときに、クライアント側へのクリップボードのリダイレクトをブロックするかどうかを設定します] グループ ポリシー設定を使用して、クリップボード監査機能をサポートしていないクライアントでクリップボード リダイレクトをブロックするかどうか指定できます。

これらのグループ ポリシー設定の詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』で「VMware Blast ポリシー設定」と「PCoIP クリップボード設定」を参照してください。

コピーアンドペースト アクティビティの情報が記録されるイベント ログの名前は VMware Horizon RX Audit です。エージェント マシンでイベント ログを表示するには、Windows イベント ビューアを使用します。イベント ログを一元的に表示するには、VMware Log Insight または Windows Event Collector を設定します。Log Insight の詳細については、https://docs.vmware.com/jp/vRealize-Log-Insight/index.html を参照してください。Windows Event Collector の詳細については、Microsoft のドキュメントを参照してください。

ファイルとフォルダのドラッグ アンド ドロップ

ドラッグ アンド ドロップ操作により、クライアント システムとリモート デスクトップまたは公開アプリケーションの間でファイルやフォルダを移動できます。同時に複数のファイルとフォルダをドラッグ アンド ドロップできます。進行状況バーにドラッグ アンド ドロップ操作のステータスが表示されます。

クライアント システムとリモート デスクトップの間でファイルまたはフォルダをドラッグ アンド ドロップ ファイルすると、移動先のシステムのファイル システムにファイルまたはフォルダが表示されます。ファイルをドラッグし、メモ帳などの開いているアプリケーションにドロップすると、アプリケーション内にテキストが表示されます。新しい E メール メッセージをファイルをドラッグすると、ファイルが E メール メッセージに添付されます。

デフォルトでは、クライアント システムからリモート デスクトップまたは公開アプリケーションへのドラッグ アンド ドロップが有効になっています。リモート デスクトップまたは公開アプリケーションからクライアント システムへのドラッグ アンド ドロップは無効になっています。Horizon 管理者は、VMware Blast と PCoIP の [ドラッグ アンド ドロップの方向を設定] グループ ポリシー設定を使用して、ドラッグ アンド ドロップの動作を制御できます。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントの「VMware Blast ポリシー設定」と「PCoIP クリップボード設定」を参照してください。

この機能には次の要件と制限があります。

- Horizon 管理者が、エージェント マシンでクライアント ドライブのリダイレクト機能を有効にする必要があります。これには、Horizon Agent 7.7 以降をインストールして、[クライアント ドライブのリダイレクト] オプションを有効にする作業も含まれます。ドラッグ アンド ドロップの動作を制御するグループ ポリシーも設定できます。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。
- クライアント システムでクライアント ドライブのリダイレクト機能を有効にする必要があります。Horizon Client[ファイルとフォルダの共有の無効化] 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が Horizon Client で使用可能かどうかが決まります。詳細については、「クライアント GPO の全般設定」を参照してください。
- VMware Blast または PCoIP 表示プロトコルを使用する必要があります。
- 相対マウス機能が有効になっている場合 ([オプション] - [相対マウスを有効化])、クライアント システムから仮想デスクトップにのみドラッグ アンド ドロップを行うことができます。

- クライアント システムからファイルをドラッグして、公開アプリケーションにドロップした場合、[名前を付けて保存] をクリックして、クライアント システムに別のファイルとしてコピーを作成することはできません。クライアント システム内の既存のファイルに上書きするには、[保存] をクリックします。
- クライアント システムからリモート デスクトップのアプリケーションにファイルをドラッグすると、ファイルがリモート デスクトップにコピーされます。このファイルのコピーが編集可能になります。
- ドラッグ アンド ドロップ操作の進行中は、実行中のドラッグ アンド ドロップ操作が完了するまで、新しいドラッグ アンド ドロップを開始することはできません。
- ドラッグ アンド ドロップ機能をネスト モードで実行することはできません。
- ドラッグ アンド ドロップを行う場合は、マウスの主ボタン（デフォルトでは左ボタン）を使用する必要があります。マウスの副ボタン（デフォルトでは右ボタン）を使用している場合、Ctrl、Shift、Alt を押しながらマウスの主ボタンを押すことはできません。
- リモート デスクトップの間ドラッグ アンド ドロップを行うことはできません。
- 公開アプリケーションの間でドラッグ アンド ドロップは使用できません。

公開アプリケーションの使用

公開アプリケーションは、ローカルのクライアント システムにインストールされたアプリケーションと同じように表示され、動作します。

公開アプリケーションを使用する場合、次のことに注意してください。

- 公開アプリケーションの最小化および最大化はその公開アプリケーションを使って行うことができます。公開アプリケーションを最小化すると、アプリケーションはクライアント システムのタスクバーに表示されます。また、タスクバーにある公開アプリケーションのアイコンをクリックしても最小化や最大化を行うことができます。
- 公開アプリケーションを終了する場合は、公開アプリケーションを直接閉じるか、タスクバーのアイコンを右クリックして閉じます。
- 開いている複数の公開アプリケーションの切り替えは Alt+Tab キーを押して行います。
- 公開アプリケーションで Windows システム トレイのアイテムを作成すると、そのアイテムはユーザー自身のクライアント システムのシステム トレイにも表示されます。デフォルトでは、システム トレイ アイコンは通知を表示する場合にのみ表示されます。この設定は、ネイティブでインストールされているアプリケーションと同じ方法でカスタマイズできます。

  注: コントロール パネルを開いて、通知領域アイコンをカスタマイズすると、公開アプリケーションのアイコンの名前は VMware Horizon Client - <application name> と表示されます。

公開アプリケーションへのドキュメントの保存

Microsoft Word、WordPad などの特定の公開アプリケーションを使ってドキュメントを作成したり保存したりできます。これらドキュメントの保存場所は、企業のネットワーク環境によります。たとえば、ドキュメントがローカルのコンピュータにマウントされたホーム共有に保存される場合があります。

Horizon 管理者は、[リモート デスクトップ サービス ユーザー ホーム ディレクトリの設定] という RDS プロファイル グループ ポリシー設定を使用して、ドキュメントの保存先を指定できます。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。

再接続時における公開アプリケーションの動作の設定

Horizon Client でサーバの接続を切断した後も、実行中の公開アプリケーションを開いた状態にしておくこともできます。Horizon Client がサーバに再接続した際の実行中の公開アプリケーションの動作を設定できます。

再接続時における公開アプリケーションの Horizon Client での動作の設定をコマンド ラインやグループ ポリシー設定で無効にできます。グループ ポリシーの設定は、コマンドラインの設定よりも優先されます。詳細については、「Horizon Client コマンドの使用」の `-appSessionReconnectionBehavior` オプションまたは「クライアント GPO のスクリプト定義設定」の [切断されたアプリケーション セッションを再開するときの動作] グループ ポリシーを参照してください。

手順

1 Horizon Client のデスクトップとアプリケーションの選択ウィンドウで、公開アプリケーションを右クリックして [設定] を選択します。

2 [リモートアプリケーション] ペインで、再接続時におけるアプリケーションの動作の設定を選択します。

オプション	説明
再接続を要求し、公開アプリケーションを開く	Horizon Client は、サーバに再接続するときに、1 つまたは複数の公開アプリケーションが実行されていることを通知します。[アプリケーションに再接続] をクリックして、公開アプリケーションのウィンドウを再度開くか、[今はしない] をクリックして、公開アプリケーションのウィンドウを再度開かないようにすることができます。
自動的に再接続し、公開アプリケーションを開く	サーバに再接続すると、実行中の公開アプリケーションのウィンドウが自動的に開きます。
再接続も自動再接続も要求しない	Horizon Client は、実行中の公開アプリケーションを再度開くように求めるよう画面を表示せず、実行中の公開アプリケーションのウィンドウはサーバに再接続しても、再度開きません。

3 変更内容を保存するには、[OK] をクリックします。

変更は、Horizon Client が次にサーバに接続したときに有効になります。

公開アプリケーションの複数セッション モードの有効化

公開アプリケーションの複数セッション モードを有効にすると、異なるクライアント デバイスからサーバにログインしたときに、同じ公開アプリケーションの複数のセッションを使用できます。

たとえば、クライアント A で公開アプリケーションを複数セッション モードで開き、同じ公開アプリケーションをクライアント B で開くと、クライアント A で公開アプリケーションが開いたまま、クライアント B で公開アプリケーションの新しいセッションが開きます。複数セッション モードが無効になっている場合（単一セッション モードの場合）は、クライアント A の公開アプリケーションのセッションが切断され、クライアント B で再接続されます。

複数セッション モード機能には次の制限があります。

- Skype for Business など、複数のインスタンスをサポートしていないアプリケーションの場合、複数セッション モードは機能しません。
- 複数セッション モードで公開アプリケーションを使用しているときにアプリケーション セッションが切断されると、自動的にログアウトされ、未保存のデータは失われます。

前提条件

Horizon 管理者は、アプリケーション プールの複数セッション モードを有効にする必要があります。Horizon 管理者が許可しない限り、ユーザーは公開アプリケーションの複数セッション モードを変更できません。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 を参照してください。この機能には、Horizon 7 のバージョン 7.7 以降が必要です。

手順

1 サーバに接続します。

2 [設定] ダイアログ ボックスを開いて、左ペインで [マルチ起動] を選択します。

   - デスクトップとアプリケーションの選択ウィンドウの右上隅で、[設定]（歯車のアイコン）をクリックします。
   - デスクトップとアプリケーションの選択ウィンドウでリモート デスクトップまたは公開デスクトップを右クリックして、[設定] を選択します。

   複数セッション モードで使用できる公開アプリケーションがない場合、[マルチ起動] 設定は表示されません。

3 複数セッション モードで使用する公開アプリケーションを選択して、[OK] をクリックします。

   Horizon 管理者が公開アプリケーションに複数セッション モードを適用している場合、この設定を変更することはできません。

公開アプリケーションでのローカル IME の使用

英語以外のキーボードとロケールを使用している場合、ローカル クライアント システムにインストールされている IME (Input Method Editor) を使用して、英語以外の文字を公開アプリケーションに送信できます。

ローカル クライアント システムの通知領域（システム トレイ）のアイコンやホット キーを使用して、別の IME に切り替えることもできます。公開アプリケーションをホストするサーバに IME をインストールする必要はありません。

この機能を有効にすると、ローカル IME が使用されます。公開アプリケーションをホストするサーバに IME がインストールされ、設定されている場合、そのリモート IME は無視されます。

デフォルトでは、この機能は無効になっています。この機能を有効または無効にした場合、サーバから切断して再度ログインしないと、変更が適用されません。

前提条件

- クライアント システムに 1 つ以上の IME がインストールされていることを確認します。
- ローカル クライアント システムの入力言語が IME で使用している言語と一致することを確認します。
- リモート デスクトップに View Agent 6.0.2 または Horizon Agent 7.0 以降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 のデスクトップとアプリケーションの選択ウィンドウで、公開アプリケーションを右クリックして [設定] を選択します。

2 [リモート アプリケーション] ペインで、[ローカル IME をホスト型アプリケーションに拡張する] チェック ボックスをオンにして [OK] をクリックします。

3 セッションを再起動します。

オプション	アクション
サーバからログオフ	サーバから切断して再度ログインし、公開アプリケーションに再接続します。切断されても閉じられていない公開アプリケーションとリモート デスクトップを再開できます。
アプリケーションをリセット	公開アプリケーションのアイコンを右クリックし、[設定] を選択して [リセット] をクリックします。このオプションを使用すると、開いているリモート デスクトップは切断されませんが、すべての公開アプリケーションは閉じられ、再起動が必要になります。

この設定を有効にするには、セッションを再起動する必要があります。この設定は、サーバ上のすべての公開アプリケーションに適用されます。

4 ローカルにインストールされたアプリケーションで使用できる場合は、ローカル IME を使用します。

ローカル クライアント システムの通知領域（システム トレイ）に言語の指定と IME のアイコンが表示されます。ホット キーを使用して別の言語または IME に切り替えることができます。テキストを切り取るための Ctrl+X キーや別のタブに移動するための Alt+ 右矢印キーなど、特定の操作を実行するキーの組み合わせが正しく機能します。

注: Windows 7 および 8.x システムでは、[コントロール パネル] - [地域と言語] - [キーボードと言語] - [キーボードの変更] - [テキスト サービスと入力言語] - [詳細なキー設定] の順に移動すると表示される、**[テキスト サービスと入力言語]** ダイアログ ボックスを使用して、IME のホット キーを指定できます。

リモート デスクトップまたは公開アプリケーションからの印刷

リモート デスクトップまたは公開アプリケーションから、ローカルのクライアント コンピュータに接続している USB プリンタや仮想プリンタへの印刷が可能です。

Horizon Agent で有効になっている機能に応じて、仮想印刷機能または VMware 仮想印刷リダイレクト機能を使用できます。

仮想印刷と VMware 仮想印刷リダイレクトをサポートしているリモート デスクトップのタイプについては、「Windows クライアントの機能サポート一覧」を参照してください。

仮想印刷機能の印刷設定を行う

リモート デスクトップで仮想印刷機能の印刷設定を行うことができます。仮想印刷機能を使用すると、リモート デスクトップに追加のプリンタ ドライバをインストールすることなく、リモート デスクトップからローカルまたはネットワーク プリンタを使用できます。この機能で使用可能なプリンタごとに、データ圧縮、印刷品質、両面印刷、カラーなどの環境設定を行うことができます。

ローカル クライアント コンピュータにプリンタを追加すると、Horizon Client がこのプリンタをリモート デスクトップで使用可能なプリンタのリストに追加します。何も構成する必要はありません。管理者権限があれば、仮想印刷コンポーネントと競合することなく、リモート デスクトップにプリンタ ドライバをインストールできます。

重要: この機能は次の種類のプリンタには使用できません。

- USB リダイレクト機能を使用してリモート デスクトップの仮想 USB ポートに接続する USB プリンタ。

  リモート デスクトップで仮想印刷機能を使用するには、リモート デスクトップから USB プリンタを切断する必要があります。

- ファイルに出力するための Windows 機能。

  Print（印刷） ダイアログ ボックスで [Print to file（ファイルへ出力）] を選択しても動作しません。ファイルを作成するプリンタ ドライバを使用すると動作します。たとえば、PDF ライターを使用すると PDF ファイルに出力できます。

前提条件

仮想印刷を使用するには、Horizon 管理者がリモート デスクトップの仮想印刷機能を有効にする必要があります。このタスクには、エージェントのインストーラーで [仮想印刷] の設定オプションを有効にすることが含まれます。仮想印刷の動作を制御するポリシーの設定が含まれる場合もあります。Horizon Agent のインストール方法については、『Horizon 7 での仮想デスクトップのセットアップ』または『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』ドキュメントを参照してください。ポリシーの設定については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。

リモート デスクトップで仮想印刷機能がインストールされているかどうかを確認するには、リモート デスクトップのファイル システムに `C:\Program Files\Common Files\ThinPrint` フォルダが存在することを確認します。

手順

1 Windows リモート デスクトップで、[コントロール パネル] - [ハードウェアとサウンド] - [デバイスとプリンタ] の順に移動します。

2 **[デバイスとプリンタ]** ウィンドウで仮想プリンタを右クリックし、コンテキスト メニューから [プリンタ プロパティ] を選択します。

  シングル ユーザー仮想マシン デスクトップの場合、仮想プリンタは <<printer_name>> と表示されます。公開デスクトップに View Agent 6.2 以降または Horizon Agent7.0 以降がインストールされている場合、仮想プリンタは <<printer_name>(s<session_ID>)> として表示されます。View Agent 6.1 以前がリモート デスクトップにインストールされている場合、仮想プリンタは <<printer_name>#:<number>> として表示されます。

3 [全般] タブで、[環境設定] をクリックします。

4 [印刷設定] ダイアログ ボックスで、異なるタブを選択して使用する設定を指定します。

5 変更内容を保存するには、[OK] をクリックします。

6 カスタムの用紙フォームを使用するには、クライアント システムでフォームを定義します。

   a [コントロール パネル] - [ハードウェアとサウンド] - [デバイスとプリンタ] をクリックします。

   b プリンタを選択し、画面上部の [プリント サーバ プロパティ] をクリックします。

   c [フォーム] タブで、設定を指定して [フォームを保存] をクリックします。

   このフォームがリモート デスクトップで使えるようになります。

VMware 仮想印刷リダイレクト機能の印刷設定

リモート デスクトップで VMware 仮想印刷リダイレクト機能の印刷設定を行うことができます。VMware 仮想印刷リダイレクト機能を使用すると、Windows リモート デスクトップに追加のプリンタ ドライバをインストールすることなく、リモート デスクトップからローカルまたはネットワーク プリンタを使用できます。この機能で使用可能なプリンタごとに、データ圧縮、印刷品質、両面印刷、カラーなどの環境設定を行うことができます。

前提条件

VMware 仮想印刷リダイレクトを使用するには、Horizon 管理者がリモート デスクトップの VMware 仮想印刷リダイレクト機能を有効にする必要があります。これには、Horizon Agent インストーラで [VMware 仮想印刷] オプションを有効にして、仮想印刷の動作を制御するポリシーを設定する作業も含まれます。Horizon Agent のインストール方法については、『Horizon 7 での仮想デスクトップのセットアップ』または『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』ドキュメントを参照してください。ポリシーの設定については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。

リモート デスクトップに VMware 仮想印刷リダイレクト機能がインストールされているかどうかを確認するには、リモート デスクトップのファイル システムに `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-server.exe` ファイルと `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe` ファイルが存在することを確認します。

この機能には、Horizon Agent 7.7 以降が必要です。

手順

1 Windows リモート デスクトップで、[コントロール パネル] - [ハードウェアとサウンド] - [デバイスとプリンタ] の順に移動します。

2 **[デバイスとプリンタ]** ウィンドウで仮想プリンタを右クリックし、コンテキスト メニューから [プリンタ プロパティ] を選択します。

   リモート デスクトップで仮想プリンタは <<printer_name>(v<session_ID>)> と表示されます。

3 [全般] タブで、[環境設定] をクリックします。

4 [印刷設定] ダイアログ ボックスで、異なるタブを選択して使用する設定を指定します。

5 変更内容を保存するには、[OK] をクリックします。

USB プリンタの使用

USB プリンタは、ローカル クライアント システムの USB ポートに接続されるプリンタです。ローカル クライアント システムに接続された USB プリンタにリモート デスクトップから印刷ジョブを送信できます。

- 必要なドライバがリモート デスクトップにもインストールされていれば、USB リダイレクト機能を使用して USB プリンタをリモート デスクトップの仮想 USB ポートに接続できます。

  USB リダイレクト機能を使用すると、プリンタは論理的にはクライアントの物理 USB ポートに接続されなくなるので、ローカル クライアント コンピュータのローカル プリンタのリストには表示されません。リモート デスクトップから USB プリンタに印刷できますが、ローカル クライアント コンピュータから USB プリンタに印刷することはできません。リモート デスクトップで、リダイレクトされた USB プリンタは <<printer_name>> のように表示されます。

  USB プリンタの接続方法の詳細は、「USB デバイスの接続に USB リダイレクトを使用する」を参照してください。

- Windows クライアント システムでは、仮想印刷機能または VMware 仮想印刷リダイレクト機能を使用して USB プリンタに印刷ジョブを送信することもできます。リモート デスクトップとクライアント システムの両方から USB プリンタに印刷でき、リモート デスクトップにプリンタ ドライバをインストールする必要はありません。

仮想プリンタおよびリダイレクトされた USB プリンタは競合することなく共に動作します。

Adobe Flash の表示の制御

Horizon 管理者は、リモート デスクトップに表示する Adobe Flash コンテンツについて、コンピューティング リソースを消費しすぎないように設計されたレベルに設定できます。これらの設定により、再生品質が低下する場合があります。Adobe Flash コンテンツにマウス ポインタを移動し、Horizon 管理者が指定した Adobe Flash 設定を上書きすることができます。

Adobe Flash の表示制御機能は、Windows 上の Internet Explorer セッションと Adobe Flash バージョン 9、10 でのみ利用できます。Adobe Flash の表示品質を制御するには、Adobe Flash が全画面表示モードで実行されていてはなりません。

手順

1 リモート デスクトップの Internet Explorer で、関連する Adobe Flash コンテンツを参照し、必要に応じて開始します。

  Horizon 管理者が構成した Adobe Flash 設定によっては、フレームが欠けたり、再生品質が低下したりすることがあります。

2 再生中に、マウス ポインタを Adobe Flash コンテンツに移動します。

  ポインタが Adobe Flash コンテンツ内に残っている場合、表示の品質が向上します。

3 品質の向上を保つには、Adobe Flash コンテンツの中でダブルクリックします。

Horizon Client の外部で開く URL リンクのクリック

Horizon 管理者は、リモート デスクトップまたは公開アプリケーションの内部でクリックした URL リンクをローカル クライアント システムのデフォルト ブラウザで開くように設定できます。URL のリンク先は、Web ページ、電話番号、メール アドレスなどである場合があります。この機能は、URL コンテンツ リダイレクトと呼ばれます。

また、Horizon 管理者は、ローカル クライアント システムのブラウザやアプリケーション内でクリックした URL リンクをリモート デスクトップや公開で開くように設定することもできます。Horizon Client が開いていない場合、URL リンクをクリックすると、ログインが求められます。

Horizon 管理者は、セキュリティ上の目的で URL コンテンツ リダイレクト機能を設定することもできます。たとえば、職場にいるユーザーがネットワークの外部にある URL にアクセスするリンクをクリックする場合、公開アプリケーションでこのリンクを開くほうが安全な場合があります。管理者は、リンクを開く公開アプリケーションを構成できます。

Chrome での URL コンテンツ リダイレクトの使用

クライアントの Chrome ブラウザで URL が最初にリダイレクトされるときに、URL を Horizon Client で開くかどうか確認されます。[URL:VMware Hori...lient Protocol リンクの選択内容を保存] チェック ボックス（推奨）を選択して [URL:VMware Hori...lient Protocol を開く] をクリックすると、このプロンプトは再度表示されません。

リモート デスクトップでの相対マウス機能の有効化

3D アプリケーションがリモート デスクトップで使用されている時に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用する場合、相対マウス機能を有効にするとマウスのパフォーマンスが向上します。

ほとんどの状況で、3D レンダリングを必要としないアプリケーションを使用している場合は、Horizon Client は絶対座標を使用してマウス ポインタの移動に関する情報を転送します。絶対座標を使用すれば、クライアントはマウスの移動をローカルで描画し、これはパフォーマンスが改善され、特に企業ネットワークの外にいる場合は顕著です。

AutoCAD や 3D のビデオ ゲームの再生などのグラフィックスを多用するアプリケーションを使用する必要がある業務では、絶対座標ではなく相対座標を使用する相対マウス機能を有効にしてマウスのパフォーマンスを改善できます。

相対マウス機能を有効にすると、企業ネットワークの外 (WAN) ではパフォーマンスが遅くなることがあります。

前提条件

Horizon 管理者は、デスクトップ プールで 3D レンダリングをオンにする必要があります。プールの設定および 3D レンダリングで使用できるオプションの詳細については、『Horizon 7 での仮想デスクトップのセットアップ』または『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。

手順

1 Horizon Client を起動し、サーバにログインします。

2 リモート デスクトップを右クリックして、[VMware Blast] または [PCoIP] を選択します。

3 リモート デスクトップに接続します。

4 Horizon Client メニュー バーから [オプション] - [相対マウスを有効化] の順に選択します。

オプションが切り替わります。相対マウス機能を無効にするには、もう一度 [オプション] - [相対マウスを有効化] の順に選択します。

注: 全画面表示モードではなくウィンドウ モードで Horizon Client を使用して相対マウス機能を有効にすると、マウス ポインタを Horizon Client メニュー オプションに移動したり、Horizon Client ウィンドウの外にポインタを移動できなくなることがあります。この状態を解決するには、<Ctrl>+<Alt> を押します。

スキャナの使用

スキャナ リダイレクト機能を使用すると、ローカル クライアント システムに接続されているスキャナを使用して、リモート デスクトップおよび公開アプリケーションの情報をスキャンできます。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スキャン データをリダイレクトします。

スキャナ リダイレクトでは、TWAIN 形式および WIA (Windows Image Acquisition) 形式と互換性がある標準のスキャン デバイスがサポートされます。ローカル クライアント システムにはスキャナ デバイス ドライバをインストールしておく必要がありますが、エージェントをインストールするリモート 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 管理者がスキャナ リダイレクト機能を構成していて、ユーザーが 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場合は、ローカル システムに接続されたスキャナをリモート デスクトップまたは公開アプリケーションで使用できます。

重要: Horizon Client の [USB デバイスを接続] メニューから、スキャナを接続しないでください。パフォーマンスが不安定になります。

スキャン データがリモート デスクトップまたは公開アプリケーションにリダイレクトされているとき、ローカル コンピュータ上ではスキャナにアクセスできません。逆に言えば、スキャナがローカル コンピュータで使用中であれば、リモート デスクトップまたは公開アプリケーションでそのスキャナにアクセスできません。

スキャナ リダイレクト機能の使用のヒント

- システム トレイまたはリモート デスクトップの通知領域にあるスキャナ アイコンをクリックして（  ）、デフォルト以外のスキャナを選択したり、設定を変更したりします。公開アプリケーションでは、システム トレイ アイコンはローカルのクライアント コンピュータにリダイレクトされます。

  このアイコンをクリックしたときに表示されるメニューを使用する必要はありません。スキャナ 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 メニューを使用すると、複数のデバイスがローカル 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。

  注: 表示されるメニューにスキャナが一覧表示されない場合は、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ます。スキャナ アイコンがない場合は、リモート デスクトップでスキャナ リダイレクト機能が無効になっているか、インストールされていません。この機能をサポートしていないクライアント システムにはスキャナ アイコンも表示されません。

- メニューの [環境設定] オプションをクリックすると、イメージの圧縮をコントロールするオプション、スキャナ リダイレクト メニューで Web カメラを非表示にするオプション、およびデフォルト スキャナの選択方法を決定するオプションを選択できます。

  VMware が推奨するように、リアルタイム オーディオビデオ機能を使用して Web カメラをリダイレクトする場合は、Web カメラを非表示にするオプションを選択できます。スキャナ リダイレクトと Web カメラを併用すると、自分の写真を撮ってスキャンすることができます。

  注: Horizon 管理者が特定のスキャナを使用するようにスキャナ リダイレクトを設定していて、そのスキャナを使用できない場合、スキャナ リダイレクトは機能しません。

- ほとんどの TWAIN スキャナではスキャナ設定ダイアログ ボックスがデフォルトで表示されますが、表示されないスキャナもあります。設定オプションを表示しないスキャナでは、スキャナ アイコン メニューの [環境設定] オプションを使用して、[[スキャナ設定] ダイアログを常に表示] オプションを選択できます。
- サイズが大きすぎるイメージのスキャンや解像度が高すぎるスキャンは機能しない場合があります。この場合は、スキャンの進行状況のインジケータがフリーズしたり、スキャナ アプリケーションが予期せず終了したりすることがあります。リモート デスクトップを最小化すると、解像度が高すぎることを通知するエラー メッセージがローカル クライアント システムに表示される場合があります。この問題を解決するには、解像度を下げるかイメージをより小さいサイズにトリミングしてから、スキャンをやり直します。

シリアル ポート リダイレクトの使用

シリアル ポート リダイレクトを使用すると、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。

Horizon 管理者がシリアル ポート リダイレクト機能を設定しており、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場合、それ以上構成しなくても、リモート デスクトップでシリアル ポート リダイレクトが動作します。たとえば、ローカル クライアント システムの COM1 は、リモート デスクトップの COM1 にリダイレクトされます。COM2 は COM2 にリダイレクトされます。COM ポートがすでに使用されている場合は、競合を回避するためにマッピングされます。たとえば、COM1 と COM2 がリモート デスクトップに存在している場合、クライアント システムの COM1 は、デフォルトで COM3 にマッピングされます。

ローカル クライアント システムにはデバイス ドライバがインストールされている必要がありますが、リモート デスクトップにデバイス ドライバをインストールする必要はありません。たとえば、ローカル クライアント システムで動作させるために特定のデバイス ドライバが必要となる USB シリアル変換アダプタを使用する場合、クライアント システムのみにこれらのドライバをインストールする必要があります。

重要: USB シリアル変換アダプタに接続するデバイスを使用している場合、Horizon Client の [USB デバイスを接続] メニューからデバイスを接続しないでください。これにより、USB リダイレクトでデバイスがルーティングされ、シリアル ポート リダイレクト機能がバイパスされます。

シリアル ポート リダイレクト機能の使用のヒント

- システム トレイまたはリモート デスクトップの通知領域にあるシリアル ポート アイコンをクリックして ()、マッピングされた COM ポートを接続、切断、およびカスタマイズします。

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] コンテキスト メニューが表示されます。管理者が設定をロックしている場合、コンテキスト メニューの項目がグレーアウトされます。Horizon 管理者がシリアル ポート リダイレクト機能を設定し、すべての要件を満たしている場合にのみ、アイコンが表示されます。詳細については、「シリアル ポート リダイレクトのシステム要件」を参照してください。

- コンテキスト メニューで、ポートは [「<ポート>」が「<ポート>]」にマップされましたと表示されます。たとえば、[/dev/ttyS0 が COM1 にマッピングされました] と表示されます。最初のポート（この例では COM1）は、物理ポートまたはローカル クライアント システムの USB シリアル変換アダプタです。2 番目のポート（この例では COM3）は、リモート デスクトップで使用されるポートです。
- [Port Properties] コマンドを選択するには、COM ポートを右クリックします。

  [COM プロパティ] ダイアログ ボックスで、リモート デスクトップ セッションが開始したときに自動的に接続するポートを構成できます。また、いくつかのモデムおよびその他のデバイスで必要となる DSR（データセットレディー信号）を無視できます。

  また、リモート デスクトップで使用するポート番号を変更できます。たとえば、クライアント システムの COM1 ポートがリモート デスクトップの COM3 にマッピングされているものの、使用しているアプリケーションでは COM1 が必要となる場合には、ポート番号を COM1 に変更できます。COM1 がリモート デスクトップに存在する場合、[COM1（重複）] と表示される場合があります。この重複したポートはそのまま使用できます。リモート デスクトップは、サーバのポートおよびクライアント システムのポートからもシリアル データを受信できます。
- ポートにアクセスする必要があるアプリケーションを起動しようとする前に、マッピングされた COM ポートに接続します。たとえば、COM ポートを右クリックして、[接続] を選択して、リモート デスクトップでポートを使用します。アプリケーションを起動すると、アプリケーションがシリアル ポートを開きます。

  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。
- リモート デスクトップで、Windows デバイス マネージャの [ポートの設定] タブを使用して、特定の COM ポートのデフォルトのボー レートを設定します。クライアント システムで Windows デバイス マネージャと同じ設定を使用します。アプリケーションでポート設定が指定されていない場合にのみ、このタブの設定が使用されます。
- 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。次に、[切断] コマンドを使用して切断して、クライアント コンピュータでこの物理 COM ポートを利用可能にできます。
- シリアル ポートを自動接続するようにしている場合に、シリアル ポートを開くアプリケーションを起動してから、リモート デスクトップ セッションを切断して再接続すると、自動接続機能が動作しません。また、シリアル ポートのシステム トレイ アイコンのメニュー オプションを使用して接続することもできません。ほとんどの場合、アプリケーションがシリアル ポートを使用できなくなります。問題を解決するには、アプリケーションを停止し、デスクトップ セッションを切断してから、再接続する必要があります。

キーボード ショートカット

メニュー コマンドおよび共通の操作にキーボード ショートカットを使用できます。

共通のキーボード ショートカット

Horizon Client でのキーボード ショートカットの動作は、アプリケーションで使用した場合と同じになります。

表 5-4. 共通のキーボード ショートカット

アクション	キーまたはキーの組み合わせ
ダイアログボックスでハイライト表示されたボタンをクリックする	Enter キーを押します。
コンテキスト メニューを開く	Shift+F10 キーを押します。
ダイアログボックスで [キャンセル] ボタンをクリックする	ESC キーを押します。
サーバ選択ウィンドウ、またはデスクトップおよびアプリケーション選択ウィンドウのアイテム間を移動する	矢印キーを使用して、矢印の方向に移動します。右に移動するには、Tab キーを押します。左に移動するには、Shift + Tab キーを押します。
サーバ選択ウィンドウ、またはデスクトップおよびアプリケーション選択ウィンドウからアイテムを削除する	Delete キーを押します。
Windows 8.x で、**[スタート]** 画面とリモート デスクトップ ウィンドウ間を移動する	Windows キーを押します。

サーバ選択ウィンドウでのキーの組み合わせ

Horizon Client のサーバ選択ウィンドウで、これらのキーの組み合わせを使用できます。

表 5-5. サーバ選択でのキーの組み合わせ

メニュー コマンドまたは操作	キーの組み合わせ
ブラウザ ウィンドウでオンライン ヘルプを開く	Alt+O+H、Ctrl+H
[新規サーバ] コマンド	Alt+N
[サポート情報] ウィンドウを開く	Alt+O+S
[Horizon Client のバージョン情報] ウィンドウを開く	Alt+O+V
[SSL の構成] コマンド	Alt+O+O
[アイテムの起動後にセレクタを非表示] コマンド	Alt+O+I

デスクトップおよびアプリケーション セレクタのキーボード ショートカット

Horizon Client でリモート デスクトップと公開アプリケーションを選択するときに、これらのキーボード ショートカットを使用できます。

表 5-6. デスクトップおよびアプリケーション セレクタのキーボード ショートカット

メニュー コマンドまたは操作	キーの組み合わせ
ブラウザ ウィンドウでオンライン ヘルプを開く	Alt+O+H、Ctrl+H
[オプション] メニューを開く	Alt+O
[サポート情報] ウィンドウを開く	Alt+O+S
[Horizon Client のバージョン情報] ウィンドウを開く	Alt+O+V
リモート デスクトップからログオフする	Shift+F10+O

表 5-6. デスクトップおよびアプリケーション セレクタのキーボード ショートカット (続き)

メニュー コマンドまたは操作	キーの組み合わせ
サーバを切断してログオフする	Alt+D
[お気に入りを表示] と [すべて表示] 間を切り替える	Alt+F
お気に入りの表示中に、公開アプリケーションまたはリモート デスクトップ名の最初の数文字を入力したら、検索に一致する次のアイテムに移動する	F4
お気に入りの表示中に、検索に一致する前のアイテムに移動する	Shift+F4
お気に入りとしてマークするか、お気に入りの指定を解除する	Shift+F10+F
[設定] メニューを開く	Alt+S、または Shift+F10+S
選択したアイテムを起動する	Enter、または Shift+F10+L
リモート デスクトップまたは公開アプリケーションのショートカットをクライアント システムの [スタート] メニュー（Windows 7 以前のバージョン）または [スタート] ウィンドウ（Windows 8.x 以降）に固定します。	Shift+F10+A
選択したリモート デスクトップの [表示設定] コンテキスト メニューを開く	Shift+F10+D
PCoIP 表示プロトコルを使用して、選択したリモート デスクトップに接続する	Shift+F10+P
RDP 表示プロトコルを使用して、選択したリモート デスクトップに接続する	Shift+F10+M
選択したアイテムのリモート デスクトップ ショートカットを選択する	Shift+F10+C
選択したアイテムを [スタート] メニューまたは [スタート] ウィンドウに追加する	Shift+F10+A
選択したリモート デスクトップをリセットする（管理者がリセットを許可している場合）	Shift+F10+R
リモート デスクトップと公開アプリケーションのリストを更新します。	F5

デスクトップ ウィンドウのショートカット

これらのショートカットを使用するには、最初に Ctrl+Alt キーを押すか、リモート デスクトップ内ではなく、Horizon Client のメニュー バーをクリックしてからキーを押す必要があります。これらのショートカットは、VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用する場合にのみ機能します。

表 5-7. リモート デスクトップ ウィンドウのショートカット

メニュー コマンドまたは操作	キーの組み合わせ
リモート デスクトップ内から移動できるように、マウス ポインタをリリースする	Ctrl+Alt
[オプション] メニューを開く	Alt+O
[サポート情報] ウィンドウを開く	Alt+O+M
[Horizon Client のバージョン情報] ウィンドウを開く	Alt+O+V
[共有フォルダの設定] ダイアログ ボックスを開く	Alt+O+F

表 5-7. リモート デスクトップ ウィンドウのショートカット (続き)

メニュー コマンドまたは操作	キーの組み合わせ
[ディスプレイの拡張を有効にする] を切り替える	Alt+O+N
[他のデスクトップに切り替え] コマンド	Alt+O+S
[このデスクトップに自動接続] コマンド	Alt+O+A
[相対マウスを有効化] コマンド	Alt+O+E
[Ctrl+Alt+Del の送信] コマンド	Alt+O+C
[切断] コマンド	Alt+O+D
[切断およびログオフ] コマンド	Alt+O+L
[USB デバイスの接続] コマンド	Alt+U

Horizon Client のトラブルシューティング

6

Horizon Client の大部分の問題は、リモート デスクトップや公開アプリケーションをリセットするか、Horizon Client を再インストールすると解決できます。

この章には、次のトピックが含まれています。

リモート デスクトップの再起動

リモート デスクトップのオペレーティング システムが応答しない場合、リモート デスクトップの再起動が必要になることがあります。リモート デスクトップの再起動は、Windows オペレーティング システムの再起動コマンドと似ています。通常、リモート デスクトップのオペレーティング システムは、再起動の前に未保存データを保存するように求めます。

Horizon 管理者がリモート デスクトップの再起動機能を有効にしている場合にのみ、リモート デスクトップを再起動できます。

デスクトップの再起動機能を有効する操作の詳細については、『Horizon 7 での仮想デスクトップのセットアップ』または『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。

前提条件

ユーザー名とパスワード、RSA SecurID ユーザー名とパスワード、RADIUS 認証ユーザー名とパスワード、スマートカード個人識別番号 (PIN) などのログイン認証情報を取得します。

手順

- [デスクトップの再起動] コマンドを使用します。

オプション	アクション
リモート デスクトップから	メニュー バーから [オプション] - [デスクトップの再起動] を選択します。
デスクトップ選択ウィンドウから	リモート デスクトップのアイコンを右クリックし、[デスクトップの再起動] を選択します。

  Horizon Client から、再起動を確認するように求められます。

リモート デスクトップのオペレーティング システムが再起動し、Horizon Client がリモート デスクトップから切断され、ログオフされます。

次のステップ

システムが完全に再起動するまで待機してから、リモート デスクトップへの再接続します。

リモート デスクトップを再起動しても問題が解決しない場合、リモート デスクトップをリセットする必要がある場合があります。「リモート デスクトップまたは公開アプリケーションのリセット」を参照してください。

リモート デスクトップまたは公開アプリケーションのリセット

デスクトップ オペレーティング システムが応答を停止し、リモート デスクトップを再起動しても問題が解決しない場合は、リモート デスクトップをリセットする必要がある場合があります。公開アプリケーションをリセットすると、開いているすべてのアプリケーションが終了します。

リモート デスクトップをリセットする操作は、物理的な PC を強制的に再起動するときに PC のリセット ボタンを押す操作と同じです。リモート デスクトップで開いているすべてのファイルが閉じられますが、保存されません。

公開アプリケーションをリセットすると、未保存のデータを保存せずにアプリケーションを終了します。複数の RDS サーバ ファームから提供されているアプリケーションであっても、開いているリモート アプリケーションはすべて閉じられます。

Horizon 管理者がリモート デスクトップのリセット機能を有効にしている場合にのみ、リモート デスクトップをリセットできます。

デスクトップのリセット機能を有効する操作の詳細については、『Horizon 7 での仮想デスクトップのセットアップ』または『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。

手順

1 リモート デスクトップをリセットするには、[デスクトップのリセット] コマンドを使用します。

オプション	アクション
リモート デスクトップから	メニュー バーから [オプション] - [デスクトップのリセット] を選択します。
デスクトップとアプリケーションの選択ウィンドウから	リモート デスクトップのアイコンを右クリックし、[デスクトップのリセット] を選択します。

2 公開アプリケーションをリセットするには、デスクトップとアプリケーションの選択ウィンドウの [リセット] ボタンを使用します。

a メニュー バーの [設定] ボタン（歯車のアイコン）をクリックします。

b 左ペインの [アプリケーション] をクリックし、右ペインの [リセット] ボタンをクリックして、[OK] をクリックします。

リモート デスクトップをリセットすると、リモート デスクトップのオペレーティング システムが再起動し、Horizon Client がリモート デスクトップから切断され、ログオフされます。公開アプリケーションをリセットすると、そのアプリケーションは終了します。

次のステップ

システムが完全に再起動するまで待機してから、リモート デスクトップや公開アプリケーションに再接続します。

Horizon Client for Windows の修復

Horizon Client を修復すると、Horizon Client に関する問題を解決できる場合があります。

前提条件

- クライアント システムに管理者としてログインできることを確認します。
- Horizon Client インストーラがあることを確認します。インストーラがないと、Horizon Client を修復できません。

手順

- Horizon Client をインタラクティブに修復するには、次のいずれかのタスクを実行します。
  - Horizon Client インストーラをダブルクリックして、[修復] をクリックします。
  - コマンドラインから Horizon Client インストーラを実行して、`/repair` コマンドを入力します。

    たとえば、コマンド プロンプトで次のコマンドを入力します。

    ```
    VMware-Horizon-Client-<y.y.y>-<xxxxxx>.exe /repair
    ```

    <y.y.y> はバージョン番号、<xxxxxx> はビルド番号です。
- Horizon Client をサイレント モードで修復するには、コマンド ラインから Horizon Client インストーラを実行し、`/silent` と `/repair` コマンドを入力します。

  たとえば、コマンド ラインで次のコマンドを入力します：

  ```
  VMware-Horizon-Client-<y.y.y>-<xxxxxx>.exe /silent /repair
  ```

  <y.y.y> はバージョン番号、<xxxxxx> はビルド番号です。

Horizon Client for Windows のアンインストール

Horizon Client を修復しても問題が解決しない場合は、Horizon Client のアンインストールと再インストールが必要になる場合があります。

ここでは、Horizon Client インストーラを使用して Horizon Client をアンインストールする方法を説明します。

Horizon Client インストーラがない場合には、Windows システムの他のアプリケーションと同じ方法で Horizon Client をアンインストールできます。たとえば、Windows 10 システムでは、Windows オペレーティング システムのプログラムのアンインストールまたは機能変更を使用できます（[コントロール パネル] - [プログラムと機能] - [プログラムのアンインストールまたは変更] の順に選択します）。

前提条件

クライアント システムに管理者としてログインできることを確認します。

手順

- Horizon Client をインタラクティブにアンインストールするには、次のいずれかのタスクを実行します。
  - Horizon Client インストーラをダブルクリックして、[削除] をクリックします。
  - コマンドラインから Horizon Client インストーラを実行して、`/uninstall` コマンドを入力します。

    たとえば、コマンド プロンプトで次のコマンドを入力します。

    ```
    VMware-Horizon-Client-<y.y.y>-<xxxxxx.>exe /uninstall
    ```

    <y.y.y> はバージョン番号、<xxxxxx> はビルド番号です。
- Horizon Client をサイレント モードでアンインストールするには、コマンド ラインで Horizon Client インストーラを実行し、`/silent` と `/uninstall` コマンドを入力します。

  たとえば、コマンド プロンプトで次のコマンドを入力します。

  ```
  VMware-Horizon-Client-<y.y.y>-<xxxxxx>.exe /silent /uninstall
  ```

  <y.y.y> はバージョン番号、<xxxxxx> はビルド番号です。

次のステップ

Horizon Client を再インストールします。章 2 「Horizon Client for Windows のインストール」を参照してください。

キーボード入力の問題

リモート デスクトップや公開アプリケーションに入力するときに、キー入力が機能しません。

問題

リモート デスクトップまたは公開アプリケーションへの接続中、入力した文字が表示されない。1 つのキーが何回も繰り返される現象が発生することもある。

原因

Norton 360 トータル セキュリティなどの一部のセキュリティ ソフトウェアには、キーロガーを検出してキーストロークの記録をブロックする機能があります。このセキュリティ機能は、パスワードやクレジットカード番号を盗み取るスパイウェアからシステムを保護するためのものです。このようなセキュリティ ソフトウェアによって、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キーストロークを送信できなくなることがあります。

ソリューション

- クライアント システムで、ウィルス対策ソフトウェアまたはセキュリティ ソフトウェアのキーロガー検出機能をオフにします。

Horizon Client が予期せずに終了する場合の対処

ユーザーが終わらせたわけではないのに Horizon Client が終了します。

問題

Horizon Client が予期せずに終了します。サーバの構成によっては、「**View 接続サーバへの安全な接続がありません**」のようなメッセージが表示される場合があります。メッセージが表示されない場合もあります。

原因

この問題は、サーバへの接続が失われると発生します。

ソリューション

- Horizon Client を再起動します。サーバの再起動後、正常に接続できます。接続の問題が解決しない場合は、システム管理者へお問い合わせください。

Workspace ONE モードでのサーバへの接続

Horizon Client から直接サーバに接続することはできません。また、リモート デスクトップまたは公開アプリケーションに対する資格は Horizon Client に表示されません。

問題

- Horizon Client からサーバに直接接続すると、Horizon Client が Workspace ONE ポータルにリダイレクトします。
- URI またはショートカットでリモート デスクトップまたは公開アプリケーションを開くか、ファイルの関連付けからローカル ファイルを開くと、Workspace ONE ポータルにリダイレクトされ、認証が実行されます。
- Workspace ONE からリモート デスクトップまたは公開アプリケーションを開き、Horizon Client を開始すると、資格のある他のリモート デスクトップまたは公開アプリケーションを Horizon Client で表示したり、開いたりすることができなくなります。

原因

Horizon 7 バージョン 7.2 以降では、Horizon 管理者が接続サーバ インスタンスで Workspace ONE モードを有効にできます。接続サーバ インスタンスで Workspace ONE モードが有効になっている場合、この動作は正常です。

ソリューション

Workspace ONE を使用して、Workspace ONE が有効になっているサーバに接続し、リモート デスクトップと公開アプリケーションにアクセスしてください。