VMware Horizon View Feature Pack のインストールと管理ガイド

Horizon View 5.3
Horizon View Feature Pack 6

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各製品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、http://www.vmware.com/jp/support/pubs を参照してください。

JA-001301-01

vmware®

最新の技術ドキュメントは VMware の Web サイト（http://www.vmware.com/jp/support/）にあります
VMware の Web サイトでは最新の製品アップデートも提供されています。
このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

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

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

目次

VMware Horizon View 機能パック インストールおよび管理

以下の『VMware Horizon View Feature Pack のインストールと管理ガイド』は、VMware® Horizon View™ Feature Pack コンポーネントのインストールと構成についての情報を提供します。

この文書の情報には、Horizon View デスクトップに Remote Experience Agent、そして View 接続サーバ インスタンスに HTML Access インストーラをインストールするためのシステム要件と手順が含まれています。インストール以降の構成作業についても説明されています。

対象者

この文書は、Horizon View の展開で Feature Pack をインストールおよび構成する管理者を対象としています。これらの情報は、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記述されています。Horizon View に慣れていないユーザーである場合、『VMware Horizon View インストール』および『VMware Horizon View 管理ガイド』のステップを追った基本手順の参照が必要な場合があります。

VMware Horizon View 機能パック コンポーネント

VMware Horizon View 機能パック には、Horizon View 環境に Feature Pack コンポーネントを提供する 2 つのインストーラが含まれます。Remote Experience Agent インストーラは、 Horizon View デスクトップでそれらのコンポーネントを構成します。HTML Access インストーラは、HTML Access を介してデスクトップにアクセスを提供するために View 接続サーバを構成します。

Remote Experience Agent インストーラ

Remote Experience Agent は Horizon View デスクトップに Feature Pack コンポーネントをインストールし、View Agent 5.3 によって提供されるリモート デスクトップ エクスペリエンスを強化します。このプログラムは以下のコンポーネントをインストールします。

- HTML Access Agent
- フラッシュ URL リダイレクト
- リアルタイム オーディオ-ビデオ
- Unity Touch
- Windows 7 マルチメディア リダイレクト (MMR)

Feature Pack のコンポーネントによって、ユーザーが多くの新しいデスクトップ機能を利用できるようになります。

HTML Access Agent

HTML Access Agent によってユーザーは HTML Access を使用して Horizon View デスクトップに接続できます。HTML Access Agent は、デスクトップで HTML Access を有効にするためにそのデスクトップで実行する必要があります。

したがって、HTML Access を使用するには、HTML Access 機能と共に Remote Experience Agent をインストールする必要があります。

フラッシュ URL リダイレクト

Flash URL リダイレクトは、ShockWave Flash (SWF) ファイルをインターセプトし、リモート デスクトップからクライアント エンドポイントにリダイレクトします。この機能がないと、マルチキャストまたはユニキャストのビデオ データは Adobe Media Server から ESXi ホストで実行されている仮想デスクトップにストリームされます。データは、それぞれの仮想デスクトップからそれぞれのクライアント エンドポイントに個々の PCoIP セッションで再送信されます。

Flash URL リダイレクトによって、Adobe Media Server から Flash コンテンツをクライアント エンドポイントに直接ストリームでき、仮想デスクトップ インフラストラクチャをバイパスします。そして、Flash コンテンツは、クライアントのローカル Flash メディア プレーヤーを使用して表示されます。

Adobe Media Server からクライアント エンドポイントに Flash コンテンツを直接ストリーミングするとデータセンター ESXi ホストへの負荷が軽減され、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 Flash コンテンツを同時にストリームするために必要となる帯域幅が削減されます。

リアルタイム オーディオ-ビデオ

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

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

この機能は、VMware Virtual Webcam および VMware Virtual Microphone をデスクトップ オペレーティング システムにインストールします。会議アプリケーションが起動すると、これらの VMware 仮想デバイスを表示および使用し、これらはクライアントでローカル接続されたデバイスからオーディオ ビデオ リダイレクトを処理します。VMware Virtual Microphone は、デスクトップ オペレーティング システムのデバイス マネージャにも表示されます。

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

リアルタイム オーディオ ビデオは、ローカル モード デスクトップでサポートされません。

この機能は、Active Directory または個々のデスクトップにリアルタイム オーディオ ビデオ グループ ポリシ設定をインストールできる ADM テンプレート ファイルを提供します。これらの設定によって、webcam のデフォルトの最大フレーム レートおよび画像解像度を変更でき、機能をまとめて無効または有効にできます。

Unity Touch

Unity Touch を使用すれば、タブレットおよびスマートフォン ユーザーは Windows アプリケーションやファイルの参照、検索、およびオープンを簡単に行ったり、お気に入りのアプリケーションやファイルを選択したり、スタート メニューまたはタスクバーを使用せずに実行しているアプリケーションを切り替えることができます。iOS および Android デバイス向けの VMware Horizon View Client ドキュメントには、Unity Touch で提供されるエンド ユーザー機能についての詳細が記載されています。

Windows 7 マルチメディア リダイレクト (MMR)

この機能は、MMR を Windows 7 デスクトップおよびクライアントに拡張します。

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

HTML Access インストーラ

このインストーラは、View 接続サーバ インスタンスを構成してユーザーが HTML Access を選択してデスクトップに接続できるようにします。HTML Access インストーラを実行すると、View Portal は、View Client アイコンに加えて HTML Access アイコンを表示します。

HTML Access を使用して Horizon View 展開でデスクトップに接続する場合は、このインストーラを実行する必要があります。ユーザーが Horizon Workspace から移動し、HTML Access を選択してデスクトップに接続する場合、このインストーラの実行も必要です。

セットアップとインストール

Horizon View 機能パック をセットアップするには、Horizon View デスクトップに Remote Experience Agent　そして View 接続サーバ インスタンスに HTML Access インストーラをインストールします。

Horizon View 機能パック のシステム要件

Horizon View デスクトップおよび View 接続サーバ インスタンスは、Feature Pack コンポーネントをサポートするために特定のソフトウェア要件を満たす必要があります。

View 接続サーバ

View 接続サーバ 5.3

インストール手順は、『VMware Horizon View インストール ガイド』で提供されています。

Horizon View デスクトップ

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

- オペレーティング システム:Windows XP SP3 (32 ビット)、Windows Vista (32 ビット)、Windows 7 (32 ビットまたは 64 ビット)、Windows 8 (32 ビットまたは 64 ビット)、Windows 8.1 (32 ビットまたは 64 ビット)、または Windows Server 2008 R2

  注意　Feature Pack の一部の個別のコンポーネントは、サポートされているデスクトップ オペレーティング システムの一部でのみサポートされています。表 1 を参照してください。

- View Agent 5.3

  インストール手順は、『VMware Horizon View 管理ガイド』に記載されています。

表 1 に、それぞれの Feature Pack コンポーネントがサポートされているデスクトップ オペレーティング システムを記載します。

表 1. Feature Pack の個々のコンポーネントに対する Horizon View デスクトップ オペレーティング システムのサポート

Feature Pack のコンポーネント	Windows XP SP3 (32 ビット)	Windows Vista (32 ビット)	Windows 7 (32 または 64 ビット)	Windows 8 または Windows 8.1 (32 または 64 ビット)	Windows Server 2008 R2
HTML Access Agent	はい	はい	はい	はい (技術プレビュー)	はい
フラッシュ URL リダイレクト	いいえ	いいえ	はい	いいえ	いいえ
リアルタイム オーディオ-ビデオ	はい	はい	はい	はい	はい
Unity Touch	はい	はい	はい	はい	はい
Windows 7 MMR	いいえ	いいえ	はい	いいえ	いいえ

サポートされる Feature Pack コンポーネントは、Remote Experience Agent インストーラの実行時にデフォルトでインストールされます。インストール時に選択をオフにすることで、コンポーネントをインストールしないように選択できます。

個々の Feature Pack コンポーネントをサポートするには、Horizon View の展開が追加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。

のシステム要件 HTML Access

HTML Access を使用すれば、クライアント システムでは、サポートされるブラウザ以外のソフトウェアは必要ありません。以下の Horizon View の導入では、特定のソフトウェア要件を満たす必要があります。

クライアント システムのブラウザ

以下の Web ブラウザがサポートされます:

- Chrome 28 以降
- Internet Explorer 9 以降
- Safari 6 以降
- iOS 6 以降が実行されている iOS デバイスの Mobile Safari
- Firefox 21 以降

クライアント オペレーティング システム

- Windows XP SP3 (32 ビット)
- Windows 7 SP1 または SP (32 または 64 ビット)
- Windows 8 Desktop (32 または 64 ビット)
- Windows Vista SP1 または SP2 (32 ビット)
- Mac OS X Snow Leopard (10.6.8)
- Mac OS X Lion (10.7)
- Mac OS X Mountain Lion (10.8)
- iOS 6.0 以降の iPad (したがって、iPad 1 はサポートされていません)
- Chrome OS 28.<x> 以降

View デスクトップ

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

- オペレーティング システム:Windows XP SP3 (32 ビット)、Windows Vista (32 ビット)、Windows 7 (32 ビットまたは 64 ビット)、または Windows Server 2008 R2。

  さらに、HTML Access は Windows 8 (32 ビットまたは 64 ビット) または Windows 8.1 (32 ビットまたは 64 ビット) で技術プレビューとして利用可能です。Windows 8 または Windows 8.1 デスクトップで HTML Access を試用できますが、サポートは提供されません。

- View Agent 5.3

  インストール手順は、『VMware Horizon View 管理ガイド』に記載されています。

プール設定

HTML Access では、View Administrator で以下のプール設定が必要です:

- [1 台のモニタの最大解像度] 設定は [1920x1200] 以上が必要なので、View デスクトップは少なくとも 17.58MB のビデオ RAM が必要です。
- [HTML Access] 設定は有効にする必要があります。

構成手順は、『VMware Horizon View HTML Access の使用』の「HTML Access 用に View デスクトップとプールを準備」を参照してください。

View 接続サーバ

以下のソフトウェアを View 接続サーバをホストするサーバにインストールする必要があります:

- View 接続サーバ 5.3

  インストール手順は、『VMware Horizon View インストール ガイド』で提供されています。

- HTML Access

  インストール手順は、「View 接続サーバに HTML Access ソフトウェアをインストール (P. 21)」を参照してください。

HTML Access をインストールする場合、ファイアウォールはインバウンド トラフィックを TCP ポート 8443 に許可するために自動的に構成されます。

セキュリティ サーバ

Windows Firewall サービスまたは他のソフトウェア ファイアウォールは、インバウンド トラフィックを TCP ポート 8443 に許可するために構成する必要があります。

企業のファイアウォールの外部からクライアント システムが接続する場合には、セキュリティ サーバを使用することを推奨します。セキュリティ サーバでは、クライアント システムで VPN 接続が必要にはなりません。

注意　1 つセキュリティ サーバは、最大で 350 個の Web クライアントへの接続を同時にサポートできます。

サードパーティ ファイア ウォール

以下のトラフィックを許可するための規則を追加します:

- View サーバ（セキュリティ サーバ、View 接続サーバ インスタンス、および複製サーバを含む）:TCP ポート 8443 へのインバウンド トラフィック。

- View デスクトップ:TCP ポート 22443 へのインバウンド トラフィック（View サーバから）。

Horizon View 用の表示プロトコル

Blast

Web ブラウザを使用して View デスクトップにアクセスする場合、PCoIP または Microsoft RDP ではなく Blast プロトコルが使用されます。Blast は HTTPS (HTTP over SSL/TLS) を使用します。

注意　HTML Access を VMware Horizon Workspace と一緒に使用すると、ユーザーが HTML5 ブラウザから自分のデスクトップに接続できます。Horizon Workspace のインストールおよび View 接続サーバで使用するための構成についての詳細は、Horizon Workspace のマニュアルを参照してください。View 接続サーバを SAML 認証サーバとペアにする詳細については、『VMware Horizon View 管理』ガイドを参照してください。

Flash URL リダイレクトのシステム要件

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

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

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

Horizon View デスクトップ

- デスクトップは、64 ビットまたは 32 ビットの Windows 7 オペレーティング システムで実行する必要があります。
- デスクトップには View Agent 5.3 をインストールする必要があります。
- サポートされているデスクトップ ブラウザには、Internet Explorer 8、9、および 10、Chrome 29.<x>、および Firefox 20.<x> が含まれます。

Horizon View Client ソフトウェア

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

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

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

- Linux 版 Horizon View Client 2.0 または 2.1
- Windows 版 Horizon View Client 5.4

View Client コンピュータまたはクライアント アクセス デバイス

- Flash URL リダイレクトは、x86 シン クライアント デバイスで Linux 版 Horizon View Client を実行するすべてのオペレーティング システムでサポートされます。この機能は ARM プロセッサではサポートされません。
- Flash URL リダイレクトは、Windows 版 Horizon View Client 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 版 VMware Horizon View Client の使用』を参照してください。
- Windows クライアント デバイスでは、Internet Explorer 用の Adobe Flash Player 10.1 以降をインストールする必要があります。

- Linux シン クライアント デバイスでは、**libexpat.so.0** と **libflashplayer.so** ファイルをインストールする必要があります。「Flash URL リダイレクト用のクライアント デバイスの設定 (P. 31)」を参照してください。

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

リアルタイム オーディオ ビデオのシステム要件

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

Horizon View デスクトップ

デスクトップには View Agent 5.3 をインストールする必要があります。リアルタイム オーディオ ビデオは、View Agent 5.3 をサポートするすべての Windows ゲスト OS でサポートされます。

Horizon View Client ソフトウェア

Horizon View Client 5.4 (Windows 版)

Horizon View Client 2.2 以降のリリース (Windows 版)

注意　Windows 版 Horizon View Client 2.2 は Windows 版 Horizon View Client 5.4 より後のリリースです。Windows 版のリリース番号は、他のオペレーティング システムおよびデバイスの Horizon View Client リリースと整合性が取れています。

Linux 版 Horizon View Client 2.2 以降のリリース。この機能は、サードパーティ ベンダーによって提供される Linux 版 Horizon View Client だけで使用できるので注意してください。

View 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、Windows 版 Horizon View Client 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 版 VMware Horizon View Client の使用』を参照してください。
- リアルタイム オーディオ ビデオは、x86 デバイスで Linux 版 Horizon View Client を実行するすべてのオペレーティング システムでサポートされます。この機能は ARM プロセッサではサポートされません。詳細については、『Linux 版 VMware Horizon View Client の使用』を参照してください。
- webcam およびオーディオ デバイス ドライバをインストールする必要があり、webcam およびオーディオ デバイスがクライアント コンピュータで操作可能である必要があります。リアルタイム オーディオ ビデオをサポートするために、View Agent がインストールされているデスクトップ オペレーティング システムにデバイス ドライバをインストールする必要はありません。

Horizon View 用の表示プロトコル

PCoIP

リアルタイム オーディオ ビデオは、RDP デスクトップ セッションでサポートされません。

Unity Touch のシステム要件

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

Horizon View Client ソフトウェア

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

- iOS 版 Horizon View Client 2.0 以降
- Android 版 Horizon View Client 2.0 以降

モバイル デバイス オペレーティング システム

Unity Touch は以下のモバイル デバイス オペレーティング システムでサポートされます:

- iOS 5.0 以降
- Android 3（Honeycomb）、Android 4（Ice Cream Sandwich）、および Android 4.1/4.2（Jelly Bean）。

Horizon View デスクトップ

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

- オペレーティング システム:Windows XP SP3 (32 ビット)、Windows Vista (32 ビット)、Windows 7 (32 ビットまたは 64 ビット)、Windows 8 (32 ビットまたは 64 ビット)、Windows 8.1 (32 ビットまたは 64 ビット)、または Windows Server 2008 R2
- View Agent 5.3

  インストール手順は、『VMware Horizon View 管理ガイド』に記載されています。

Windows 7 マルチメディア リダイレクトのシステム要件

Windows 7 Multimedia Redirection (MMR) をサポートするには、Horizon View の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

Horizon View デスクトップ

- デスクトップは、64 ビットまたは 32 ビットの Windows 7 オペレーティング システムで実行する必要があります。
- [3D レンダリング] はデスクトップ プールで有効にする必要があります。
- デスクトップ仮想マシンは、仮想ハードウェア バージョン 8 以降でなければなりません。
- ユーザーは Windows Media Player 12 以降でビデオを再生する必要があります。

Horizon View Client ソフトウェア

Windows 版 Horizon View Client 2.2 または以降のリリース

View Client コンピュータまたはクライアント アクセス デバイス

- クライアントは、64 ビットまたは 32 ビットの Windows 7 または Windows 8 オペレーティング システムで実行する必要があります。
- クライアントは、選択したビデオをデコードできる DirectX Video Acceleration (DXVA) 互換のビデオ カードが必要です。

- Windows Media Player 12 以降をクライアントにインストールして、ローカル ハードウェアにリダイレクトできるようにする必要があります。

サポートされるメディア フォーマット

メディア フォーマットは、H.264 ビデオ圧縮規格に準拠する必要があります。M4V、MP4、および MOV ファイル フォーマットがサポートされます。仮想デスクトップは、これらのファイル フォーマットのいずれかを使用する必要があり、これらのフォーマットのローカル デコーダがクライアント システムに存在する必要があります。

View ポリシー

View Administrator で、[マルチメディア リダイレクト (MMR)] ポリシーがデフォルト値である [許可] に設定されていることを確認します。

バックエンド ファイア ウォール

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

Windows 7 マルチメディア リダイレクト (MMR) コンポーネントと Windows XP および Windows Vista のデスクトップで動作する Wyse MMR との比較については、「デスクトップ オペレーティング システムでのマルチメディア リダイレクトのサポート (P. 13)」を参照してください。

デスクトップ オペレーティング システムでのマルチメディア リダイレクトのサポート

Windows 7 マルチメディア リダイレクト (MMR) は、Remote Experience Agent でインストールされる Feature Pack コンポーネントです。Wyse MMR コンポーネントは View Agent とともにインストールされ、Windows XP および Windows Vista デスクトップで動作します。Windows 7 MMR は Wyse MMR コンポーネントとは特徴および要件が少し異なります。

表 2. Horizon View マルチメディア リダイレクトのデスクトップ オペレーティング システム サポート

デスクトップ オペレーティング システム	デスクトップ仮想マシン要件	サポートされるメディア フォーマット	サポートされるクライアント	オーディオ リダイレクト
Windows XP、Windows Vista	Windows Media Player 10 以降をインストールする必要があります。	多くのフォーマットがサポートされます。例： MPEG2-1、MPEG2、MPEG-4 Part 2、WMV 7、8、および 9、WMA、AVI、ACE、MPT3、WAV	Windows XP、Windows Vista、Windows 7 Windows Media Player 10 以降をインストールする必要があります。	オーディオ ストリームがクライアント システムにリダイレクトされます。
Windows 7	デスクトップは、仮想ハードウェア バージョン 8 以降でなければなりません。 [3D レンダリング] を有効にする必要があります。 Windows Media Player 12 以降をインストールする必要があります。	M4V、MP4、または MOV フォーマットの H.264 圧縮規格。	Windows 7、Windows 8 クライアントは、選択したビデオをデコードできる DirectX Video Acceleration (DXVA) 互換のビデオ カードが必要です。 Windows Media Player 12 以降をインストールする必要があります。	オーディオ ストリームはリダイレクトされません。オーディオは、リモート デスクトップからクライアント システムに PCoIP で配信されます。
Windows 8	サポートされません	サポートされません	サポートされません	サポートされません

Horizon View クライアントの MMR システム要件についての詳細は、『Windows 版 VMware Horizon View Client の使用』を参照してください。

Horizon View デスクトップに Remote Experience Agent をインストールおよび展開

Remote Experience Agent インストーラを実行して Horizon View デスクトップに Freature Pack コンポーネントをインストールします。対話的な Remote Experience Agent インストーラを使用するか、コマンド ラインからサイレントにインストーラを実行できます。

新しいデスクトップ プールを作成したい場合は、親仮想マシンに Remote Experience Agent をインストールします。スナップショットを撮るか仮想マシンからテンプレートを作成し、デスクトップ プールを作成します。

既存のデスクトップ プールに Feature Pack コンポーネントをインストールする場合は、デスクトップ プールのタイプによってアプローチが異なります。たとえば、流動割り当てがあるリンク クローン プールでは、親仮想マシンで Remote Experience Agent インストーラを実行して、リンク クローンを再構成することができます。フル クローン プールまたは再構成しないプールでは、Remote Experience Agent をデスクトップにサイレントでインストールできます。独自のスクリプトまたはソフトウェア配布ツールを使用して、配布されたインストールを実行できる場合もあります。

Remote Experience Agent のアップグレード

Remote Experience Agent の以前のリリースがデスクトップにインストールされている場合、現在のリリースをインストールして、Feature Pack コンポーネントの最新バージョンを入手します。

Horizon View 5.3 Feature Pack 1 で提供される Remote Experience Agent をインストールする前に、View Agent 5.3 をデスクトップにインストールする必要があります。View Agent 5.3 をインストールすると、以前の Remote Experience Agent リリースおよび関連する Feature Pack コンポーネントは削除されます。これで Remote Experience Agent の現在のリリースをインストールでき、Feature Pack コンポーネントの新しいインストールが実行されます。

Remote Experience Agent を対話的にインストール

Remote Experience Agent をインストールして Horizon View デスクトップに Freature Pack コンポーネントを構成します。

HTML Access Agent component では HTML Access が必要です。Horizon View デスクトップおよび HTML Access のプールの設定についての詳細は、『VMware Horizon View Client ドキュメント』ページに置かれている『VMware Horizon View HTML Access の使用』の「HTML Access 用に View デスクトップとプールを準備」を参照してください。

重要　View Client または HTML Access によって確立された View デスクトップ セッション内から Remote Experience Agent をインストールまたはアンインストールしないでください。仮想マシンでインストーラを直接実行してください。たとえば、vSphere Web Client または vSphere Client の仮想マシンでコンソールを開くことができます。

開始する前に

- View Agent 5.3 が仮想マシンにインストールされていることを確認します。
- 仮想マシンに対して管理者権限を持っていることを確認します。
- Windows Firewall サービスが仮想マシンで実行されていることを確認します。Windows Firewall サービスが起動および実行されていなければ、Remote Experience Agent のインストールを完了できません。
- Remote Experience Agent によってインストール可能な機能を理解してください。「Remote Experience Agent のインストール オプション (P. 15)」を参照してください。
- http://www.vmware.com/jp/products/ の VMware 製品ページの Remote Experience Agent インストーラ ファイルにアクセスしていることを確認します。

手順

1 VMware 製品ページから Remote Experience Agent インストーラ ファイルをダウンロードします。

適切なインストーラ ファイルを選択します。<y.y> は Feature Pack のバージョン番号で、<xxxxxx> はビルド番号です。

オプション	説明
32 ビット インストーラ	VMware-Horizon-View-5.3-Remote-Experience-Agent-<y.y>-<xxxxxx>.exe
64 ビット インストーラ	VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-<xxxxxx>.exe

2 インストーラ ファイルをダブルクリックして Remote Experience Agent インストール プログラムを起動します。

3 VMware 使用許諾契約書を承諾します。

4 インストール オプションを選択します。

個別の機能に対してドロップダウン メニューを使用して、インストールする機能を選択または選択解除します。

5 [インストール] をクリックします。

インストールが完了すると、インストーラは以下のメッセージを表示します。**VMware Horizon View 5.3 Remote Experience Agent が正しくインストールされました。**

6 [終了] をクリックします。

HTML Access Agent が仮想マシンにインストールされると、TCP ポート 22443 が Windows ファイアウォールでオープンになります。「HTML Access のファイアウォール ルール (P. 22)」を参照してください。

次に進む前に

親仮想マシンに Remote Experience Agent をインストールした場合、スナップショットを撮るかテンプレートを作成し、Horizon View デスクトップ プールを作成するか、既存のプールを再構成します。

Remote Experience Agent のインストール オプション

仮想マシンに Remote Experience Agent をインストールするときにインストール オプションを選択できます。

オプション	説明
HTML Access	ユーザーは HTML Access を使用して Horizon View デスクトップに接続できます。HTML Access Agent は Horizon View デスクトップにインストールする必要があり、これによってユーザーは HTML Access に接続できます。 この機能はデフォルトでインストールされます。
フラッシュ URL リダイレクト	Flash URL マルチキャストまたはユニキャストのストリーミング データを仮想デスクトップからクライアント デバイスにリダイレクトします。この機能によって、ビデオはマルチキャストまたはユニキャストの Web ソースからクライアント ハードウェアに直接ストリームしてクライアントのローカル Flash メディア プレーヤーで表示できます。 この機能はデフォルトでインストールされます。
リアルタイム オーディオ-ビデオ	クライアント システムに接続される webcam およびオーディオ デバイスをリダイレクトするので、それらをリモート デスクトップで使用できます。 この機能はデフォルトでインストールされます。
Unity Touch	タブレットおよびスマートフォンのユーザーは、便利なサイドバーをタッチすることによって、Windows アプリケーションやファイルの参照、検索、開閉、実行しているアプリケーションの切り替えを行えます。 この機能はデフォルトでインストールされます。
Win7 マルチメディア リダイレクト	Windows 7 デスクトップおよびクライアントにマルチメディア リダイレクトを拡張します。この機能は、クライアント コンピュータに直接マルチメディア ストリームを配信し、これによってリモート ESXi ホストの代わりにクライアント ハードウェアでマルチメディア ストリームを処理できます。 この機能はデフォルトでインストールされます。

Remote Experience Agent をサイレントにインストール

Microsoft Windows インストーラ（MSI）のサイレント インストール機能を使用して、複数の Windows 仮想マシンに Remote Experience Agent をインストールできます。サイレント インストールではコマンド ラインを使用するので、ウィザードのプロンプトに応答する必要はありません。

Remote Experience Agent インストーラは、Horizon View デスクトップに Freature Pack コンポーネントを構成します。

重要　View Client または HTML Access によって確立された View デスクトップ セッション内から Remote Experience Agent をインストールまたはアンインストールしないでください。仮想マシンでインストール コマンドを直接実行してください。たとえば、vSphere Web Client または vSphere Client の仮想マシンでコンソールを開くことができます。

開始する前に

- View Agent 5.3 が仮想マシンにインストールされていることを確認します。
- 仮想マシンに対して管理者権限を持っていることを確認します。
- Windows Firewall サービスが仮想マシンで実行されていることを確認します。Windows Firewall サービスが起動および実行されていなければ、Remote Experience Agent のインストールを完了できません。
- http://www.vmware.com/jp/products/ の VMware 製品ページの Remote Experience Agent インストーラ ファイルにアクセスしていることを確認します。
- Remote Experience Agent で使用できるサイレント インストール プロパティを理解してください。「Remote Experience Agent のサイレント インストール プロパティ (P. 17)」を参照してください。
- MSI インストーラのコマンド ライン オプションを理解します。「Remote Experience Agent インストーラの MSI コマンド ライン オプション (P. 17)」を参照してください。

手順

1 VMware 製品ページから Remote Experience Agent インストーラ ファイルをダウンロードします。

適切なインストーラ ファイルを選択します。<y.y> は Feature Pack のバージョン番号で、<xxxxxx> はビルド番号です。

オプション	説明
32 ビット インストーラ	`VMware-Horizon-View-5.3-Remote-Experience-Agent-<y.y>-<xxxxxx>.exe`
64 ビット インストーラ	`VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-<xxxxxx>.exe`

2 Windows 仮想マシンで Windows コマンド プロンプトを開きます。

3 インストール コマンドを 1 行で入力します。

この例は、仮想マシンに Remote Experience Agent をインストールします。インストーラは、すべての Remote Experience Agent インストール オプションを構成し、ログを `install.log` ファイルに書き込みます。

```
VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-
<xxxxxx>.exe /s /v"/qn /l*v ""C:\myfolder\install.log"""
```

注意　先行の例は、公開されているすべての使用可能な機能をインストールします。選択した機能をインストールするには、`ADDLOCAL=` オプションを使用し、コンマで区切ったリストでサイレント インストール プロパティをリストします。例：`ADDLOCAL=Core,HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR`。`Core` プロパティは、`ADDLOCAL=` を使用して選択した機能を指定する場合に必要です。

HTML Access Agent が仮想マシンにインストールされると、TCP ポート 22443 が Windows ファイアウォールでオープンになります。「HTML Access のファイアウォール ルール (P. 22)」を参照してください。

次に進む前に

親仮想マシンに Remote Experience Agent をインストールした場合、スナップショットを撮るかテンプレートを作成し、Horizon View デスクトップ プールを作成するか、既存のプールを再構成します。

Remote Experience Agent のサイレント インストール プロパティ

サイレント インストール コマンドでは、MSI プロパティ **ADDLOCAL=** を使用して、Remote Experience Agent インストーラが構成する Feature Pack 機能を指定できます。各サイレント インストール機能は、対話的なインストール中にユーザーが選択または選択解除できるインストール オプションに対応します。

これらの機能についての詳細は、「Remote Experience Agent のインストール オプション (P. 15)」を参照してください。

表 3. Remote Experience Agent のサイレント インストール機能と対話的インストール オプション

サイレント インストール機能	対話的インストールのインストール オプション
HTML Access	HTML Access Agent
Flash URL リダイレクト	Flash URL リダイレクト
RTAV	リアルタイム オーディオ ビデオ
ユニティ タッチ	ユニティ タッチ
MMR	Win7 マルチメディア リダイレクト (MMR)

Remote Experience Agent インストーラの MSI コマンド ライン オプション

Remote Experience Agent をサイレントにインストールするには、Microsoft Windows Installer (MSI) コマンド ライン オプションおよびプロパティを使用する必要があります。このインストーラは MSI プログラムで、標準の MSI 機能を使用します。

MSI の詳細については、Microsoft の Web サイトを参照してください。MSI コマンド ライン オプションについては、Microsoft Developer Network (MSDN) ライブラリの Web サイトを参照して、MSI コマンド ライン オプションを検索してください。MSI コマンド ラインの使用方法を確認するには、インストールを実行している仮想マシンでコマンド プロンプトを開いて **`msiexec /?`** と入力できます。

注意　**`INSTALLDIR`** オプションは、Remote Experience Agent インストーラで使用できません。インストール ディレクトリを変更できません。

インストーラをサイレントで実行するには、インストーラを一時ディレクトリに展開するブートストラップ プログラムの消音から始め、対話的なインストールを開始します。

コマンド ラインで、インストーラのブートストラップ プログラムを制御するコマンド ライン オプションを入力する必要があります。

表 4. インストーラのブートストラップ プログラムのコマンド ライン オプション

オプション	説明
/s	ブートストラップのスプラッシュ画面と抽出ダイアログを無効にします。これによって、対話的なダイアログは表示されません。 例：VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-<xxxxxx>.exe /s /s オプションがサイレント インストールを実行するために必要です。
/v"<MSI_command_line_options>"	コマンド ラインで入力する二重引用符で囲んだ文字列を MSI のオプションのセットとして解釈するようにインストーラに指示します。二重引用符でコマンド ライン入力を囲む必要があります。/v の後とコマンド ラインの最後に二重引用符を配置します。 例：VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-<xxxxxx>.exe /s /v"<command_line_options>" /v"<command_line_options>" オプションがサイレント インストールを実行するために必要です。

コマンド ライン オプションおよび MSI プロパティ値を MSI インストーラ msiexec.exe に渡すことによってサイレント インストールの残りを制御します。MSI インストーラはコマンド ラインに入力する値およびオプションを使用して、Remote Experience Agent インストーラに固有のインストール オプションを解釈します。

表 5. MSI コマンド ライン オプションおよび MSI プロパティ

MSI オプションまたはプロパティ	説明
/qn	MSI インストーラにインストーラ ウィザード ページを表示しないように指示します。 たとえば、Remote Experience Agent をサイレントでインストールして、デフォルトのセットアップ オプションと機能だけを使用したい場合があります。 VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-<xxxxxx>.exe /s /v"/qn" その代わりに、/qb オプションを使用して、非対話的にウィザード ページを表示する自動インストールができます。インストールが進むとウィザード ページが表示されますが、それらに応答はできません。 /qn または /qb オプションがサイレント インストールを実行するために必要です。
/x	Remote Experience Agent をアンインストールします。例： VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-<xxxxxx>.exe /s /v"/qb /x" Remote Experience Agent のアンインストールおよび Horizon View デスクトップをインストール前の状態に戻す手順については、「Remote Experience Agent のアンインストール (P. 19)」を参照してください。
UNITY_DEFAULT_APPS	モバイル デバイスのユニティ タッチ サイドバーに表示されるデフォルトのお気に入りのアプリケーションのリストを指定します。このプロパティは、ユニティ タッチ コンポーネントをサポートするために作成されました。これは一般的な MSI プロパティではありません。 お気に入りのアプリケーションのデフォルト リストの構成およびこのプロパティで使用するための構文とフォーマットについての詳細は、「Unity Touch で表示されるお気に入りアプリケーションの構成 (P. 27)」を参照してください。 UNITY_DEFAULT_APPS プロパティはオプションです。

表 5. MSI コマンド ライン オプションおよび MSI プロパティ (続き)

MSI オプションまたはプロパティ	説明
ADDLOCAL	インストールするコンポーネント固有の機能を決定します。対話的なインストールでは、インストーラは選択するインストール オプションを表示します。ADDLOCAL プロパティによって、コマンド ラインでこれらのオプションを指定できます。 ADDLOCAL プロパティを使用しなければ、デフォルト オプションがインストールされます。 個々のインストール オプションを指定するには、オプション名のコンマで区切られた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。ADDLOCAL=<value,value,value...> というフォーマットを使用してください。オプション名は大文字と小文字を区別します。使用できるインストール オプションのリストについては、「Remote Experience Agent のサイレント インストール プロパティ (P. 17)」を参照してください。 以下は HTML Access Agent、ユニティ タッチ、Flash URL リダイレクト、およびリアルタイム オーディオ ビデオをインストールする例です。 `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-<xxxxxx>.exe /s /v"/qn ADDLOCAL=Core,HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR"` Core コンポーネントは、インストール オプションを指定するために ADDLOCAL プロパティを使用するときに必要です。 ADDLOCAL プロパティはオプションです。
REBOOT	REBOOT=ReallySuppress オプションを使用して、システム構成作業をシステムが再起動する前に完了することができます。 この MSI プロパティはオプションです。
REMOVE	Remote Experience Agent インストーラでインストールされた特定の Feature Pack コンポーネント (インストール オプション) を削除します。 個々のインストール オプションを削除するには、オプション名のコンマで区切られた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。REMOVE=<value,value,value...> というフォーマットを使用してください。オプション名は大文字と小文字を区別します。使用できるインストール オプションのリストについては、「Remote Experience Agent のサイレント インストール プロパティ (P. 17)」を参照してください。 以下は HTML Access Agent、ユニティ タッチ、Flash URL リダイレクト、およびリアルタイム オーディオ ビデオを削除する例です。 `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-<xxxxxx>.exe /s /v"/qn REMOVE=HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR"` REMOVE プロパティはオプションです。
/l*v <log_file>	ログ情報を詳細出力で指定したログ ファイルに書き込みます。 例：`/l*v ""%TEMP%\vmmsi.log""` この例は、対話的なインストール中に生成されたログに類似する詳細なログ ファイルを生成します。 このオプションを使用して、インストールで一意的に適用するカスタム機能を記録できます。記録された情報を使用して、将来のサイレント インストールでインストール機能を指定できます。 /l*v オプションはオプションです。

Remote Experience Agent のアンインストール

他の Windows ソフトウェアを削除するために使用するのと同じ方法で Horizon View デスクトップから Remote Experience Agent を削除できます。

Remote Experience Agent は、View Agent 5.3 でインストールされる特定のファイルに影響します。Remote Experience Agent をアンインストールして View Agent 仮想マシンをインストール前の状態に戻す場合、View Agent をアンインストールして再インストールするか、View Agent を修復する必要があります。

手順

1 Remote Experience Agent がインストールされている仮想マシンで、Windows [コントロール パネル] の [プログラムの追加と削除] を開きます。

2 [VMware Horizon View 5.3 Remote Experience Agent] を選択して [アンインストール] をクリックします。

3 View Agent をアンインストールして再インストールするか、修復します。

オプション	説明
アンインストールと再インストール	a Windows の [プログラムのアンインストール] で [VMware View Agent] を選択し、[アンインストール] をクリックします。 b VMware View Agent 5.3 インストール ファイルを起動してソフトウェアを再インストールします。
修復	VMware View Agent 5.3 インストール ファイルを起動して [修復] オプションを選択します。

4 (オプション) 仮想マシンの Windows ファイアウォールで、TCP ポート 22443 がインバウンド トラフィックを許可しないことを確認します。

次に進む前に

適用可能であれば、社内のファイアウォールのルールを変更して、デスクトップ仮想マシンの TCP ポート 22443 に対するインバウンド トラフィックを不許可にします。

View 接続サーバに HTML Access ソフトウェアをインストール

HTML Access インストーラは、View 接続サーバの View Portal ページを構成し、ユーザーがデスクトップに接続するときに HTML Access を選択できるようにします。View 接続サーバ インスタンスおよび複製グループのすべてのインスタンスでインストーラを実行します。

デフォルトでは、ブラウザを開いて View 接続サーバ インスタンスの URL を入力すると、View Client をダウンロードするための VMware へのリンクが付けられている View Portal ページが表示されます。

HTML Access インストーラを実行後、View Portal ページは View Client アイコンに加えて HTML Access アイコンを表示し、これによってユーザーは HTML Access からデスクトップに接続できます。デスクトップに接続するためにユーザーは View Client をインストールする必要はありません。

View Client をダウンロードするためのアイコンを無効にする場合は View Portal ページをカスタマイズでき、HTML Access から接続するためのアイコンを無効にするか、View Client をダウンロードするための Web ページの URL を変更します。「VMware Horizon View Client ドキュメント」ページに置かれている『VMware Horizon View HTML Access の使用』の「エンド ユーザー用に HTML Access ページを構成」を参照してください。

重要 Horizon View に含まれていた View Portal ページ、または Horizon View 5.2 Feature Pack 1 に含まれていた HTML Access Portal ページを以前に編集したことがある場合、HTML Access の新しいバージョンにアップグレードすると、それらのカスタマイズは失われます。アップグレード後に、このページを再びカスタマイズできます。Horizon View 5.2 Feature Pack 2 以降に含まれていた HTML Access Portal ページを以前に編集したことがある場合、カスタマイズは保持されます。

HTML Access に View 接続サーバをセットアップする概要については、『VMware Horizon View Client ドキュメント』ページに置かれている『VMware Horizon View HTML Access の使用』の「HTML Access 用に View 接続サーバおよびセキュリティ サーバを準備」を参照してください。

HTML Access ソフトウェアのアップグレード

現在の HTML Access リリースをインストールして、最新のアップデートおよび機能向上を入手してください。

Horizon View 5.3 Feature Pack 1 リリースで提供される HTML Access ソフトウェアをインストールする前に、お使いの View 接続サーバを Horizon View 5.3 にアップグレードする必要があります。

アップグレードするには、複製されたグループの View 接続サーバ インスタンスで HTML Access ソフトウェアの最新バージョンを実行します。

HTML Access のアップグレードを完了するには、適切な親仮想マシンまたはデスクトップ プール用の仮想マシン テンプレートで Remote Experience Agent インストーラの最新バージョンを実行する必要もあります。「Remote Experience Agent のアップグレード (P. 14)」を参照してください。

View 接続サーバに HTML Access ソフトウェアをインストール

エンド ユーザーに HTML Access アイコンを表示するために View Portal ページを構成するには、複製されたグループの View 接続サーバ インスタンスで HTML Access インストーラを実行します。

開始する前に

- View 接続サーバが Horizon View 5.3 であることを確認します。
- http://www.vmware.com/jp/products/ の VMware 製品ページの HTML Access インストーラにアクセスしていることを確認します。

手順

1 VMware 製品ページから HTML Access インストーラ ファイルをダウンロードします。

このインストーラの名前は以下のとおりです。 **VMware-Horizon-View-HTML-Access_X64-<y.y.y>-<xxxxxx>.exe**。<y.y.y> はバージョン番号で、<xxxxxx> はビルド番号です。

2 インストーラ ファイルをダブルクリックして HTML Access インストール プログラムを起動します。

3 VMware 使用許諾契約書を承諾します。

4 インストール先フォルダを受け入れるか、変更します。

5 [インストール] をクリックします。

6 [終了] をクリックします。

次に進む前に

セキュリティ サーバへの接続を許可するために HTML Access によって使用されるポートが Windows ファイアウォールで開かれていることを確認します。「セキュリティ サーバで HTML Access を使用してポートを開く (P. 21)」を参照してください。

View Client アイコンまたは HTML Access アイコンをユーザーに非表示にすることで View Portal ページを変更できます。「VMware Horizon View Client ドキュメント」ページに置かれている『VMware Horizon View HTML Access の使用』の「エンド ユーザー用に HTML Access ページを構成」を参照してください。

セキュリティ サーバで HTML Access を使用してポートを開く

View 接続サーバまたはセキュリティ サーバをインストールする場合、View サーバ インストーラはクライアント接続用の HTML Access によって使用されるポートの Windows ファイアウォール ルールを作成しますが、インストーラは実際に必要となるまでこのルールを無効にします。View 接続サーバ インスタンスで HTML Access を後でインストールする場合、HTML Access インストーラは、このポートへの通信を許可するためのルールを自動的に有効にします。ただし、セキュリティ サーバでは、Windows ファイアウォールのルールを手動で有効にしてポートへの通信を許可する必要があります。

デフォルトでは、HTML Access は、Blast Secure Gateway へのクライアント接続用に TCP ポート 8443 を使用します。

手順

- View 接続サーバ コンピュータで HTML Access によって使用されるポートを開くには、そのコンピュータに HTML Access をインストールします。

  HTML Access インストーラは、Windows ファイアウォールの [VMware View 接続サーバ (Blast-In)] ルールを有効にします。

- セキュリティ サーバで HTML Access 用のポートを開くには、Windows ファイアウォールの [VMware View 接続サーバ (Blast-In)] ルールを手動で有効にします。

View 接続サーバから HTML Access をアンインストール

他の Windows ソフトウェアを削除するために使用するのと同じ方法で HTML Access を削除できます。

手順

1 HTML Access がインストールされている View 接続サーバのホストで、Windows [コントロール パネル] の [プログラムの追加と削除] を開きます。

2 HTML Access を選択して、[アンインストール] をクリックします。

3 (オプション) そのホストの Windows ファイアウォールで、TCP ポート 8443 がインバウンド トラフィックを許可しないことを確認します。

次に進む前に

ペアのセキュリティ サーバの Windows ファイアウォールの TCP ポート 8443 に対するインバウンド トラフィックを非許可にします。適用可能な場合は、サードパーティ ファイアウォールで規則を変更して、すべてのペアのセキュリティ サーバおよびこの View 接続サーバのホストで TCP ポート 8443 に対するインバウンド トラフィックを非許可にします。

HTML Access のファイアウォール ルール

セキュリティ サーバ、View 接続サーバ インスタンス、および Horizon View デスクトップに接続するために HTML Access を使用することをクライアント Web ブラウザに許可するため、ファイアウォールは特定の TCP ポートの受信トラフィックを許可する必要があります。

HTML Access 接続は HTTPS を使用する必要があります。HTTP 接続は許可されません。

HTML Access で使用される TCP ポートにトラフィックが許可されるようにセキュリティ サーバの Windows ファイアウォールで確実に構成するには、「セキュリティ サーバで HTML Access を使用してポートを開く (P. 21)」を参照してください。

表 6. HTML Access のファイアウォール ルール

送信元	デフォルトの送信元ポート	プロトコル	送信先	デフォルトの送信先ポート	備考
クライアント Web ブラウザ	すべての TCP	HTTPS	セキュリティ サーバまたは View 接続サーバ インスタンス	TCP 443	Horizon View に最初に接続するために、クライアント デバイスの Web ブラウザは、TCP ポート 443 でセキュリティ サーバまたは View 接続サーバ インスタンスに接続します。
クライアント Web ブラウザ	すべての TCP	HTTPS	Blast Secure Gateway	TCP 8443	Horizon View への最初の接続が行われた後、クライアント デバイスの Web ブラウザは、TCP ポート 8443 で Blast Secure Gateway に接続します。Blast Secure Gateway をセキュリティ サーバまたは View 接続サーバ インスタンスで有効にして、この第 2 の接続が行われることを許可します。 注意 Blast Secure Gateway は、Horizon View 5.2 以降のリリースの View 接続サーバでインストールされます。
Blast Secure Gateway	すべての TCP	HTTPS	HTML Access Agent	TCP 22443	Blast Secure Gateway が有効にされ、ユーザーが Horizon View デスクトップを選択すれば、Blast Secure Gateway はデスクトップの TCP ポート 22443 で HTML Access Agent に接続します。
クライアント Web ブラウザ	すべての TCP	HTTPS	HTML Access Agent	TCP 22443	Blast Secure Gateway が有効にされおらず、ユーザーが Horizon View デスクトップを選択すると、クライアント デバイスの Web ブラウザはデスクトップの TCP ポート 22443 で HTML Access Agent に直接接続します。

HTML Access Agent を構成して新しい SSL 証明書を使用

業界またはセキュリティの規定に準拠するため、HTML Access Agent で生成されるデフォルトの SSL 証明書を Certificate Authority (CA) によって署名される証明書に置き換えることができます。

Horizon View デスクトップに HTML Access Agent をインストールすると、HTML Access Agent サービスがデフォルトの自己署名の証明書を作成します。このサービスは、デフォルトの証明書を Horizon View に接続するために HTML Access を使用するブラウザに示します。

注意　デスクトップ仮想マシンのゲスト OS で、このサービスは VMware Blast サービスと呼ばれます。

デフォルトの証明書を CA から取得する署名された証明書に置き換えるには、証明書を各 Horizon View デスクトップの Windows ローカル コンピュータ証明書ストアにインポートする必要があります。各デスクトップでレジストリ値を設定する必要もあり、これによって HTML Access Agent は新しい証明書を使用することができます。

デフォルトの HTML Access Agent 証明書を CA が署名した証明書に置き換える場合、VMware は各デスクトップで一意の証明書を構成することを推奨しています。親仮想マシンまたはデスクトップ プールを作成するために使用するテンプレートに CA が署名した証明書を構成しないでください。これを行うと、多くのデスクトップが同一の証明書を持つ結果となります。

手順

1 Horizon View デスクトップで証明書のスナップインを MMC に追加する (P. 23)

Windows ローカル コンピュータ証明書ストアに証明書を追加できる前に、HTML Access Agent がインストールされる Horizon View デスクトップで Microsoft Management Console (MMC) に証明書のスナップインを追加する必要があります。

2 HTML Access Agent の証明書を Windows 証明書ストアにインポート (P. 24)

デフォルトの HTML Access Agent 証明書を CA によって署名された証明書に置き換えるには、Windows ローカル コンピュータ証明書ストアに CA によって署名された証明書をインポートする必要があります。HTML Access Agent がインストールされている各デスクトップでこの手順を実行します。

3 HTML Access Agent のルート証明書と中間証明書のインポート (P. 25)

証明書チェーンのルート証明書と中間証明書が、HTML Access Agent にインポートした SSL 証明書と共にインポートされていない場合、Windows ローカル コンピュータ証明書ストアにこれらの証明書をインポートする必要があります。

4 Windows レジストリで証明書の拇印を設定 (P. 25)

HTML Access Agent に Windows 証明書ストアにインポートされた CA によって署名された証明書を使用することを許可するには、Windows レジストリ キーに証明書の拇印を構成する必要があります。デフォルトの証明書を CA によって署名された証明書に置き換える各デスクトップで、この手順を行う必要があります。

Horizon View デスクトップで証明書のスナップインを MMC に追加する

Windows ローカル コンピュータ証明書ストアに証明書を追加できる前に、HTML Access Agent がインストールされる Horizon View デスクトップで Microsoft Management Console (MMC) に証明書のスナップインを追加する必要があります。

開始する前に

MMC および証明書のスナップインが、HTML Access Agent がインストールされている Windows ゲスト OS で使用できることを確認します。

手順

1 Horizon View デスクトップで、[Start（スタート）] をクリックして **`mmc.exe`** を入力します。

2 [MMC] ウィンドウで、[File（ファイル）] - [Add/Remove Snap-in（スナップインの追加と削除）] を選択します。

3 [スナップインの追加と削除] ウィンドウで、[Certificates（証明書）] を選択して [Add（追加）] をクリックします。

4 [証明書のスナップイン] ウィンドウで、[Computer account（コンピュータ アカウント）] を選択し、[Next（次へ）] をクリックして [Local computer（ローカル コンピュータ）] を選択し、次に [Finish（完了）] をクリックします。

5 [スナップインの追加と削除] ウィンドウで、[OK] をクリックします。

次に進む前に

SSL 証明書を Windows ローカル コンピュータ証明書ストアにインポートします。「HTML Access Agent の証明書を Windows 証明書ストアにインポート (P. 24)」を参照してください。

HTML Access Agent の証明書を Windows 証明書ストアにインポート

デフォルトの HTML Access Agent 証明書を CA によって署名された証明書に置き換えるには、Windows ローカル コンピュータ証明書ストアに CA によって署名された証明書をインポートする必要があります。HTML Access Agent がインストールされている各デスクトップでこの手順を実行します。

開始する前に

- Horizon View デスクトップで HTML Access Agent がインストールされていることを確認します。
- CA によって署名された証明書がデスクトップにコピーされたことを確認します。
- 証明書のスナップインが MMC に追加されたことを確認します。「Horizon View デスクトップで証明書のスナップインを MMC に追加する (P. 23)」を参照してください。

手順

1 Horizon View デスクトップの MMC ウィンドウで、[Certificates (Local Computer)証明書 (ローカル コンピュータ)] ノードを展開して [Personal（個人）] フォルダを選択します。

2 Actions（操作） ペインで、[More Actions（その他の操作）] - [All Tasks（すべてのタスク）] - [Import（インポート）] に移動します。

3 [Certificate Import（証明書のインポート）] ウィザードで、[Next（次へ）] をクリックして証明書が保存されている場所を参照します。

4 証明書ファイルを選択し、[Open（開く）] をクリックします。

証明書のファイル タイプを表示するには、[File name（ファイル名）] ドロップダウン メニューからファイル フォーマットを選択できます。

5 証明書ファイルに含まれるプライベート キーのパスワードを入力します。

6 [Mark this key as exportable（このキーをエクスポート可能にマーク）] を選択します。

7 [Include all extendable properties（すべての拡張可能なプロパティを含む）] を選択します。

8 [Next（次へ）] をクリックし、[Finish（完了）] をクリックします。

新しい証明書は、[Certificates (Local Computer)証明書 (ローカル コンピュータ)] - [Personal（個人）] - [Certificates（証明書）] フォルダに表示されます。

9 新しい証明書にプライベート キーが含まれることを確認します。

a [Certificates (Local Computer) (ローカル コンピュータ)] - [Personal（個人）] - [Certificates（証明書）] フォルダで、新しい証明書をダブルクリックします。

b Certificate Information（証明書情報） ダイアログ ボックスの General（一般） タブに以下の文が表示されることを確認します。**この証明書に対応するプライベート キーがあります。**

次に進む前に

必要に応じて、ルート証明書と中間証明書を Windows 証明書ストアにインポートします。「HTML Access Agent のルート証明書と中間証明書のインポート (P. 25)」を参照してください。

適切なレジストリ キーを証明書の拇印で構成します。「Windows レジストリで証明書の拇印を設定 (P. 25)」を参照してください。

HTML Access Agent のルート証明書と中間証明書のインポート

証明書チェーンのルート証明書と中間証明書が、HTML Access Agent にインポートした SSL 証明書と共にインポートされていない場合、Windows ローカル コンピュータ証明書ストアにこれらの証明書をインポートする必要があります。

手順

1 Horizon View デスクトップの MMC ウィンドウで、[Certificates (Local Computer)証明書 (ローカル コンピュータ)] ノードを展開して [Trusted Root Certification Authorities（信頼されたルート証明機関）] - [Certificates（証明書）] フォルダに移動します。

- ルート証明書がこのフォルダにあり、証明書チェーンに中間証明書がなければ、この手順をスキップします。
- ルート証明書がこのフォルダになければ、手順 2 に進みます。

2 [Trusted Root Certification Authorities（信頼されたルート証明機関）] - [Certificates（証明書）] フォルダを右クリックし、[All Tasks（すべてのタスク）] - [Import（インポート）] をクリックします。

3 [Certificate Import（証明書のインポート）] ウィザードで、[Next（次へ）] をクリックしてルート CA 証明書が保存されている場所を参照します。

4 ルート CA 証明書ファイルを選択し、[Open（開く）] をクリックします。

5 [Next（次へ）] をクリックし、[Next（次へ）] をクリックし、そして [Finish（完了）] をクリックします。

6 サーバ証明書が中間 CA によって署名されていた場合、証明書チェーンのすべての中間証明書を Windows ローカル コンピュータ証明書ストアにインポートします。

a [Certificates (Local Computer)証明書 (ローカル コンピュータ)] - [Intermediate Certification Authorities（中間証明機関）] - [Certificates（証明書）] フォルダに移動します。

b インポートする必要がある各中間証明書で手順 3 から 6 を繰り返します。

次に進む前に

適切なレジストリ キーを証明書の拇印で構成します。「Windows レジストリで証明書の拇印を設定 (P. 25)」を参照してください。

Windows レジストリで証明書の拇印を設定

HTML Access Agent に Windows 証明書ストアにインポートされた CA によって署名された証明書を使用することを許可するには、Windows レジストリ キーに証明書の拇印を構成する必要があります。デフォルトの証明書を CA によって署名された証明書に置き換える各デスクトップで、この手順を行う必要があります。

開始する前に

CA によって署名された証明書が Windows 証明書ストアにインポートされることを確認します。「HTML Access Agent の証明書を Windows 証明書ストアにインポート (P. 24)」を参照してください。

手順

1 HTML Access Agent がインストールされる Horizon View デスクトップの MMC ウィンドウで、[Certificates (Local Computer)（証明書（ローカル コンピュータ））] - [Personal（個人）] - [Certificates（証明書）] フォルダに移動します。

2 Windows 証明書ストアにインポートした CA によって署名された証明書をダブルクリックします。

3 Certificates（証明書）ダイアログ ボックスで、Details（詳細）タブをクリックしてスクロールダウンし、[Thumbprint（拇印）] アイコンを選択します。

4 選択した拇印をテキスト ファイルにコピーします。

例： `31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e`

注意　拇印をコピーする場合、先行するスペースを含めないでください。先行するスペースを拇印とともにレジストリ キーに不注意にペーストすると（手順 7）、証明書が正しく構成できない場合があります。この問題は、先行するスペースがレジストリ値テキスト ボックスに表示されない場合であっても発生します。

5 HTML Access Agent がインストールされたデスクトップで Windows Registry Editor を起動します。

6 `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` レジストリ キーに移動します。

7 `SslHash` 値を変更し、証明書の拇印をテキスト ボックスにペーストします。

8 VMware Blast サービスを再起動して変更を有効にします。

Windows ゲスト OS では、HTML Access Agent のサービスは、VMware Blast と呼ばれます。

ユーザーが HTML Access からデスクトップに接続すると、HTML Access Agent は、CA によって署名された証明書をユーザーのブラウザに示します。

HTML Access Agent のセキュリティ プロトコルと暗号化スイートの構成

Feature Pack 5 (FP5) からは、Windows レジストリを編集して、HTML Access Agent によって使用されるセキュリティ プロトコルと暗号化スイートを構成できます。 グループ ポリシー オブジェクト (GPO) で構成を指定することもできます。

デフォルトでは、FP5 HTML Access Agent で TLS 1.0、TLS 1.1 と TLS 1.2 のみが使用されます。許可されるプロトコルは、低いものから高いものの順序で、TLS 1.0、TLS 1.1、TLS 1.2 です。SSLv3 以前のような古いプロトコルは許可されません。レジストリ値 `SslProtocolLow` と `SslProtocolHigh` により、HTML Access Agent によって承認されるプロトコルの範囲が決まります。 たとえば、`SslProtocolLow=tls_1.0` と `SslProtocolHigh=tls_1.2` を設定すると、HTML Access Agent は、TLS 1.0、TLS 1.1、TLS 1.2 を承認します。デフォルト設定は `SslProtocolLow=tls_1.0` と `SslProtocolHigh=tls_1.2` です。

暗号化方式のリストは、http://openssl.org/docs/manmaster/apps/ciphers.html の「CIPHER LIST FORMAT」で定義されている形式で指定する必要があります。 デフォルトの暗号化方式リストを次に示します。

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

手順

1 Windows レジストリ エディタを開始します。

2 `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` レジストリ キーに移動します。

3 2 つの新しい文字列 (REG_SZ) 値、`SslProtocolLow` と `SslProtocolHigh` を追加して、プロトコルの範囲を指定します。

レジストリ値のデータは、`tls_1.0`、`tls_1.1`、`tls_1.2` のいずれかにする必要があります。 プロトコルを 1 つのみ有効にするには、両方のレジストリ値に同じプロトコルを指定します。 2 つのレジストリ値のいずれかが存在しないか、データが 3 つのうちのいずれかのプロトコルに設定されていない場合は、デフォルトのプロトコルが使用されます。

4 新しい文字列 (REG_SZ) 値、`SslCiphers` を追加して、暗号化スイートのリストを指定します。

レジストリ値のデータ フィールドに暗号化スイートのリストを入力するか貼り付けます。 次に例を示します。

```
ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

5 Windows サービスの VMware Blast を再起動します。

デフォルトの暗号化リストを使用するように戻すには、**SslCiphers** レジストリ値を削除して、Windows サービスの VMware Blast を再起動します。 値のデータ部分を単に削除しないでください。データ部分を削除すると、HTML Access Agent は、OpenSSL 暗号化リスト形式の定義に従って、すべての暗号化を許可しなくなります。

HTML Access Agent が起動すると、ログ ファイルにプロトコルと暗号化の情報が書き込まれます。 ログ ファイルを調べると、有効になっている値を判断できます。

デフォルトのプロトコルと暗号化スイートは、VMware でネットワーク セキュリティのベスト プラクティスが進展することに伴い、今後変更されることがあります。

ユニティ タッチを構成

ユニティ タッチ スライドバーに表示されるお気に入りのアプリケーションのデフォルト リストを構成して、インストール後にユニティ タッチ機能を無効または有効にすることができます。

Unity Touch で表示されるお気に入りアプリケーションの構成

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

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

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

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

たとえば、Microsoft Office 2010 および Microsoft Visio が 1 つの仮想マシンにインストールされ、Windows Powershell および VMware vSphere Client が第 2 の仮想マシンにインストールされている場合、すべての 4 つのアプリケーションを含む 1 つのリストを作成できます。インストールされたアプリケーションだけが、それぞれのデスクトップにデフォルトのお気に入りのアプリケーションとして表示されます。

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

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

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

開始する前に

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

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

手順

- (オプション) Windows レジストリに値を追加してお気に入りのアプリケーションのデフォルト リストを作成します。

  a `regedit` を開き、`HKLM\Software\VMware, Inc.\VMware Unity` レジストリ設定に移動します。

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

  b `FavAppList` と呼ばれる文字列値を作成します。

  c デフォルトのお気に入りのアプリケーションを指定します。

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

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

  例：

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

- (オプション) Remote Experience Agent インストーラから管理インストール パッケージを作成してお気に入りのアプリケーションのデフォルト リストを作成します。

  a コマンド ラインから、以下のフォーマットを使用して管理インストール パッケージを作成します。

  ```
  VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-
  <xxxxxx>.exe /s /a /v"/qn TARGETDIR=""<a network share to store the admin
  install package>"" UNITY_DEFAULT_APPS=""<the list of default favorite apps that
  should be set in the registry>"""
  ```

  例：

  ```
  VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-
  <xxxxxx>.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-share\ViewFeaturePack\""
  UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of Access.lnk|
  Programs/Accessories/System Tools/Character Map.lnk|
  Programs/Accessories/Windows PowerShell/Windows PowerShell.lnk|
  Programs/Internet Explorer (64-bit).lnk|Programs/Google Chrome/Google
  Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft
  SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|
  Programs/Skype/Skype.lnk|Programs/WebEx/Productivity Tools/WebEx
  Settings.lnk|"""
  ```

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

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

  次のフォーマットを使用します。

  ```
  VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-<y.y>-<xxxxxx>.exe /s /v"/qn
  UNITY_DEFAULT_APPS=""<the list of default favorite apps that should be set in the
  registry>"""
  ```

  注意　先行コマンドは、Remote Experience Agent のインストールとお気に入りのアプリケーションのデフォルト リストの指定を結合します。このコマンドを実行する前に Remote Experience Agent をインストールする必要はありません。

次に進む前に

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

ユニティ タッチを無効または有効

Remote Experience Agent をインストールする場合、ユニティ タッチのインストール オプションがデフォルトで選択され、機能が有効になります。それらのデスクトップの Windows レジストリ キーの設定値によって、選択した仮想デスクトップでユニティ タッチ機能を無効または有効にすることができます。

ユニティ タッチが Remote Experience Agent インストーラでインストールされ、レジストリで無効にされた場合に限って、レジストリを使用してユニティ タッチを有効にできます。ユニティ タッチが 1 度もインストールされていなければ、つまり Remote Experience Agent をインストールした時にオプションを選択しなかった場合、レジストリ値を設定してユニティ タッチを有効にしても特定のユニティ タッチ機能は正しく動作しません。

手順

1　仮想デスクトップで Windows Registry Editor を起動します。

2　ユニティ タッチを制御する Windows レジストリ キーを指定します。

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

3　値を設定してユニティ タッチを無効または有効にします。

オプション	値
無効	0
有効	1

デフォルトでは、この値は 1 です。

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

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

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

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

手順

1 Flash URL リダイレクト機能がインストールされていることの確認 (P. 30)

この機能を使用する前に、Flash URL リダイレクト オプションとともに Remote Experience Agent がインストールされ、仮想デスクトップで実行されていることを確認します。

2 マルチキャストまたはユニキャストのストリームを提供する Web ページを設定 (P. 31)

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

3 Flash URL リダイレクト用のクライアント デバイスの設定 (P. 31)

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

4 Flash URL リダイレクトを無効または有効 (P. 32)

Remote Experience Agent をインストールして Flash URL リダイレクトのインストール オプションを選択すると、この機能が有効になります。それらのデスクトップの Windows レジストリ キーの設定値によって、選択した仮想デスクトップで Flash URL リダイレクト機能を無効または有効にすることができます。

Flash URL リダイレクト機能がインストールされていることの確認

この機能を使用する前に、Flash URL リダイレクト オプションとともに Remote Experience Agent がインストールされ、仮想デスクトップで実行されていることを確認します。

Flash URL リダイレクト機能は、マルチキャストまたはユニキャストのリダイレクトを使用するすべてのデスクトップにインストールしておく必要があります。Remote Experience Agent のインストール手順については、「Horizon View デスクトップに Remote Experience Agent をインストールおよび展開 (P. 14)」を参照してください。

手順

1 PCoIP を使用する仮想デスクトップ セッションを開始します。

2 タスク マネージャを開きます。

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

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

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

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

開始する前に

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

手順

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

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

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

例：`"var vmwareScriptErroMessage=<localized error message>"`

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

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

Flash URL リダイレクト用のクライアント デバイスの設定

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

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

手順

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

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

Flash URL リダイレクトを無効または有効

Remote Experience Agent をインストールして Flash URL リダイレクトのインストール オプションを選択すると、この機能が有効になります。それらのデスクトップの Windows レジストリ キーの設定値によって、選択した仮想デスクトップで Flash URL リダイレクト機能を無効または有効にすることができます。

手順

1 仮想デスクトップで Windows Registry Editor を起動します。

2 Flash URL リダイレクトを制御する Windows レジストリ キーを指定します。

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

3 値を設定して Flash URL リダイレクトを無効または有効にします。

オプション	値
無効	`0`
有効	`1`

デフォルトでは、この値は `1` です。

リアルタイム オーディオ ビデオの構成

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

グループ ポリシ設定を構成して、これらのデフォルト値を変更して、特定のアプリケーション、webcam、または環境に適応することができます。「リアルタイム オーディオ ビデオ グループ ポリシ設定の構成 (P. 38)」を参照してください。

クライアント コンピュータに内蔵または接続されている複数の webcam およびオーディオ入力デバイスがある場合、デスクトップにリダイレクトされる優先される webcam およびオーディオ入力デバイスを構成できます。「優先される Webcam とマイクロフォンの選択 (P. 33)」を参照してください。

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

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

リアルタイム オーディオ ビデオは、ローカル モード デスクトップでサポートされません。

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

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

リアルタイム オーディオ ビデオは、会議アプリケーションで使用するための webcam およびオーディオ入力リダイレクトをサポートします。View Agent でインストールできる USB リダイレクト機能は、webcam リダイレクトをサポートしません。USB リダイレクトからオーディオ入力デバイスをリダイレクトすると、オーディオ ストリームはリアルタイム オーディオ ビデオ セッション中にビデオを適切に同期せず、ネットワーク帯域幅の要求を削減するメリットが失われます。手順を踏んで webcam およびオーディオ入力デバイスが、USB リダイレクトではなくリアルタイム オーディオ ビデオからデスクトップにリダイレクトされることを確認できます。

デスクトップが USB リダイレクトで構成されると、エンド ユーザーは VMware Horizon View Client メニュー バーの [USB デバイスを接続] オプションを選択して、ローカルで接続された USB デバイスに接続および表示できます。

エンド ユーザーが [USB デバイスを接続] リストから USB デバイスを選択すると、そのデバイスはビデオまたはオーディオ会議で使用できなくなります。たとえば、Skype で電話をかけると、ビデオ画像は表示されず、オーディオ ストリームも品質が低下します。エンド ユーザーが会議セッション中にデバイスを選択すると、webcam またはオーディオ リダイレクトが中断されます。

これらのデバイスをエンド ユーザーに非表示にして中断を防止するには、USB リダイレクト ポリシ設定を構成して、VMware Horizon View Client での webcam とオーディオ入力デバイスの表示を無効にします。

特に、Horizon View Agent で USB リダイレクト フィルタリング ルールを作成して **`audio-in`** および **`video`** デバイス ファミリ名を無効に指定できます。グループ ポリシの設定および USB リダイレクトのフィルタリング ルールの指定についての詳細は、『VMware Horizon View 管理者ガイド』の「USB リダイレクトを制御するためのポリシの使用」を参照してください。

注意　USB デバイス ファミリを無効にするために USB リダイレクト フィルタリング ルールを設定しない場合、VMware Horizon View Client メニューの [USB デバイスを接続] リストから webcam またはオーディオ デバイスを選択できないことをエンド ユーザーに通知してください。

優先される Webcam とマイクロフォンの選択

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

Windows クライアント コンピュータでは、レジストリ キー値を設定することで、優先する webcam を選択します。Linux クライアント コンピュータでは、構成ファイルを編集することで、優先する webcam またはマイクロフォンを指定できます。リアルタイム オーディオ ビデオは、優先される webcam が使用できればそれをリダイレクトします。使用できない場合、リアルタイム オーディオ ビデオはシステム列挙によって提供される最初の webcam を使用します。

デフォルトのマイクロフォンを選択するには、クライアント コンピュータの Windows または Linux オペレーティング システムでサウンド コントロールを構成します。

Windows クライアント システムでの優先 webcam の選択

リアルタイム オーディオ ビデオ機能があり、クライアント システムに複数の webcam がある場合、1 台だけが View デスクトップで使用されます。どの webcam を優先するかを指定するために、レジストリ キー値を設定できます。

優先される webcam は、使用できる場合は View デスクトップで使用され、使用できない場合は他の webcam が使用されます。

開始する前に

- USB webcam がインストールされ、クライアント システムで動作できる状態であることを確認します。
- View デスクトップで PCoIP 表示プロトコルを使用していることを確認します。

手順

1 使用する webcam を接続します。

2 呼び出しを開始し、そして呼び出しを停止します。

このプロセスでログ ファイルが作成されます。

3 テキスト エディタでデバッグ ログ ファイルを開きます。

オペレーティング システム	ログ ファイルの場所
Windows XP	`C:\Documents and Settings\username\Local Settings\Application Data\VMware\VDM\Logs\debug-20<YY-MM-DD-XXXXXX>.txt`
Windows 7 または Windows 8	`C:\Users\%username%\AppData\Local\VMware\VDM\Logs\debug-20<YY-MM-DD-XXXXXX>.txt`

ログファイルのフォーマットは、`debug-20<YY-MM-DD-XXXXXX>.txt` で、20<YY> は年、<MM> は月、<DD> は日で、<XXXXXX> は数値です。

4 `[ViewMMDevRedir] VideoInputBase::LogDevEnum` のログ ファイルを検索し、接続される webcam を参照するログ ファイル エントリを探します。

以下は Microsoft Lifecam HD-5000 webcam を識別するログ ファイルの抜粋です:

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum - 2 Device(s) found

[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=0 Name=Integrated Webcam
UserId=vid_1bcf&pid_2b83&mi_00#7&1b2e878b&0&0000
SystemId=\\?\usb#vid_1bcf&pid_2b83&mi_00#

[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=1 Name=Microsoft LifeCam
HD-5000  UserId=vid_045e&pid_076d&mi_00#8&11811f49&0&0000
SystemId=\\?\usb#vid_045e&pid_076d&mi_00#
```

5 優先される webcam のユーザー ID をコピーします。

たとえば、`vid_045e&pid_076d&mi_00#8&11811f49&0&0000` をコピーして、デフォルトの webcam として Microsoft LifeCam HD-5000 を設定します。

6 Registry Editor (`regedit.exe`) を起動し、`HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RTAV` に移動します。

7 REG_SZ 値の [srcWCamId] に文字列の ID 部分を貼り付けます。

たとえば、`vid_045e&pid_076d&mi_00#8&11811f49&0&0000` を [srcWCamId] に貼り付けます。

8 変更を保存してレジストリを終了します。

9 新しい呼び出しを開始します。

Linux クライアント システムでの優先する webcam またはマイクロフォンの選択

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

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

リアルタイム オーディオ ビデオ機能を使用すれば、webcam、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帯域幅量は大幅に削減されます。アナログ オーディオ入力デバイスもサポートされます。

`/etc/vmware/config` ファイルにプロパティを設定し、優先するデバイスを指定するには、デバイス ID を確定する必要があります。

- webcam の場合、この後の手順の説明にしたがって、`rtav.srcWCamId` プロパティをログ ファイルに出力されている webcam の記述の値に設定します。
- オーディオ デバイスの場合、`rtav.srcAudioInId` プロパティを Pulse Audio `device.description` フィールドの値に設定します。

  このフィールドの値を探すには、この後の手順の説明にしたがって、ログ ファイルを検索します。

開始する前に

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

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

手順

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

   a 使用する webcam またはオーディオ デバイスを接続します。

   b `vmware-view` コマンドを使用して View Client を開始します。

   c 呼び出しを開始し、そして呼び出しを停止します。

      このプロセスでログ ファイルが作成されます。

2 webcam または microphone というログのエントリを探します。

a テキスト エディタでデバッグ ログ ファイルを開きます。

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

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

webcam を抽出する例を以下に示します。

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

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

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

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

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

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

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

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

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

webcam の場合には、たとえば Microsoft webcam を優先する webcam として指定するために `Microsoft® LifeCam HD-6000 for Notebooks` をコピーし、プロパティを次のように設定します。

```
rtav.srcWCamId="Microsoft® LifeCam HD-6000 for Notebooks"
```

この例では、プロパティを `rtav.srcWCamId="Microsoft"` に設定することもできます。

オーディオ デバイスの場合には、たとえば Logitech ヘッドセットを優先オーディオ デバイスとして指定するために `Logitech USB Headset Analog Mono` をコピーし、プロパティを次のように設定します。

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

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

5 新しい呼び出しを開始します。

Windows クライアント システムでのデフォルトのマイクロフォンの選択

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

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

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

開始する前に

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

手順

1 電話中の場合は電話を切ってください。

2 システム トレイのスピーカー アイコンを右クリックし、[デバイスのレコーディング] を選択します。

その代わりに、[コントロール パネル] から [サウンド] コントロールを開いて [レコーディング] タブをクリックできます。

3 [サウンド] ダイアログ ボックスの [レコーディング] タブで使用するマイクロフォンを右クリックします。

4 [デフォルト デバイスとして設定] を選択して [OK] をクリックします。

5 View デスクトップから新たに電話をかけます。

Linux クライアント システムでのデフォルトのマイクロフォンの選択

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

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

この手順では、クライアント システムのユーザー インターフェイスからデフォルトのマイクロフォンを選択する方法について説明します。管理者が構成ファイルを編集して、優先するマイクロフォンを構成することもできます。「Linux クライアント システムでの優先する webcam またはマイクロフォンの選択 (P. 35)」を参照してください。

開始する前に

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

手順

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

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

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

3 優先するデバイスを選択して [閉じる] をクリックします。

リアルタイム オーディオ ビデオ グループ ポリシ設定の構成

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

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

リアルタイム オーディオ ビデオ中に使用する帯域幅の例については、「リアルタイム オーディオ ビデオの帯域幅 (P. 40)」を参照してください。

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

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

アクティブ ディレクトリに RTAV ADM テンプレートを追加した設定の構成

Horizon View は、VMware 製品ダウンロード ページの RTAV ADM ファイル **`vdm_agent_rtav.adm`** を提供します。この ADM ファイルのポリシ設定を Active Directory のグループ ポリシ オブジェクト（GPO）に追加し、Group Policy Object Editor の設定を構成することができます。

利便性のため、RTAV ADM ファイルは、すべての他の Horizon View ADM ファイルとともに zip ファイルでバンドルされます。

RTAV ADM ファイルは、この Feature Pack リリースで初めてです。他の ADM ファイルは、**<install_directory>\VMware\VMware View\Server\extras\GroupPolicyFiles** ディレクトリの View 接続サーバの Horizon View 5.3 でインストールされるバージョンと同じです。Horizon View 5.3 をインストールまたはアップグレードしたときに、Active Directroy に既に追加されている場合は、他の ADM ファイルを再インストールする必要はありません。

開始する前に

- RTAV オプションで Remote Experience Agent がデスクトップにインストールされていることを確認します。この設定は RTAV がインストールされなければ効果がありません。「Horizon View デスクトップに Remote Experience Agent をインストールおよび展開 (P. 14)」を参照してください。
- Active Directory GPO が RTAV グループ ポリシ設定で作成されることを確認します。GPO は、デスクトップを含む OU にリンクする必要があります。Active Directory で Horizon View グループ ポリシ設定を行う一般情報については、『VMware Horizon View 管理ガイド』の「ポリシの構成」を参照してください。
- Microsoft MMC およびグループ ポリシ オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。
- RTAV グループ ポリシ設定をよく理解してください。「リアルタイム オーディオ ビデオ グループ ポリシ設定 (P. 39)」を参照してください。

手順

1 VMware 製品ページからバンドルされた Horizon View ADM zip ファイルをダウンロードします。

zip ファイルの名前は **VMware-Horizon-View-GPO-Bundle-<y.y.y>-<xxxxxx>.zip** です。<y.y.y> はバージョン番号で、<xxxxxx> はビルド番号です。

2 zip ファイルを展開して RTAV ADM ファイル **vdm_agent_rtav.adm** を Active Directory サーバにコピーします。

3 Active Directory サーバで、[スタート] - [管理ツール] - [グループ ポリシ管理] を選択し、その GPO を右クリックし、[編集] を選択して GPO を編集します。

4 グループ ポリシ オブジェクト エディタで、 [コンピュータの構成] - [管理テンプレート] フォルダを右クリックして、[テンプレートの追加と削除] を選択します。

5 [追加] をクリックして **vdm_agent_rtav.adm** ファイルを参照し、[開く] をクリックします。

6 [閉じる] をクリックして ADM ファイルのポリシ設定を GPO に適用します。

設定は、[コンピュータの構成] - [管理テンプレート] - [従来の管理用テンプレート] - [VMware View Agent の構成] - [RTAV 構成を表示] フォルダに格納されています。

7 RTAV グループ ポリシ設定を構成します。

リアルタイム オーディオ ビデオ グループ ポリシ設定

リアルタイム オーディオ ビデオ (RTAV) グループ ポリシ設定は、仮想 webcam の最大フレーム レートおよび最大画像解像度を制御します。追加設定によって RTAV 機能を無効または有効にできます。これらのポリシ設定は、物理デバイスが接続されているクライアント システムではなく、Horizon View デスクトップに影響します。

RTAV グループ ポリシ設定を構成しなければ、RTAV はクライアント システムに設定された値を使用します。クライアント システムでは、デフォルトの webcam フレーム レートは毎秒 15 フレームです。デフォルトの webcam 画像解像度は 320x240 ピクセルです。

RTAV グループ ポリシ設定は、使用可能な最大値を決定します。クライアント システムに設定されるフレーム レートと解像度は絶対値です。たとえば、最大画像解像度の RTAV 設定を 640x480 ピクセルに構成すると、webcam は最大 640x480 ピクセルに設定された解像度を表示します。クライアントの画像解像度を 640x480 ピクセルよりも大きい値に設定すると、クライアント解像度は 640x480 ピクセルに制限されます。

すべての構成が、毎秒 25 フレームで 1920x1080 の解像度の最大グループ ポリシ設定を達成できるわけではありません。構成が指定した解像度で達成できる最大フレーム レートは、使用される webcam、クライアント システムのハードウェア、View Agent 仮想ハードウェア、および使用できる帯域幅によって異なります。

グループ ポリシ設定	説明
RTAV を無効にする	この設定を有効にすると、リアルタイム オーディオ ビデオ機能は無効になります。 この設定を構成しないか無効にすると、リアルタイム オーディオ ビデオは有効になります。 この設定は [RTAV 構成を表示] フォルダにあります。
毎秒の最大フレーム	webcam がフレームをキャプチャできる毎秒の最大レートを決定します。この設定を使用して、低い帯域幅のネットワーク環境で webcam のフレーム レートを制限することができます。 最小値は毎秒 1 フレームです。最大値は毎秒 25 フレームです。 この設定を構成しないか無効にすると、最大フレーム レートは設定されません。リアルタイム オーディオ ビデオは、クライアント システムで webcam に対して選択されるフレーム レートを使用します。 デフォルトでは、クライアント webcam のフレーム レートは毎秒 15 フレームです。クライアント システムで設定しないか、[毎秒の最大フレーム] 設定を構成しないか無効にすると、webcam は毎秒 15 フレームをキャプチャします。 この設定は [RTAV 構成を表示] - [RTAV Webcam 設定を表示] フォルダにあります。
解像度 - 最大画像幅（ピクセル）	webcam によってキャプチャされる画像フレームの最大幅をピクセルで決定します。低い最大画像幅を設定することによって、キャプチャされるフレームの解像度を低くすることができ、低い帯域幅のネットワーク環境での画像エクスペリエンスを改善できます。 この設定を構成しないか無効にすると、最大画像幅は設定されません。RTAV は、クライアント システムで設定される画像幅を使用します。クライアント システムの webcam 画像のデフォルト幅は 320 ピクセルです。 任意の webcam 画像の上限は 1920x1080 ピクセルです。1920 ピクセルより大きい値にこの設定を構成すると、有効最大画像幅は 1920 ピクセルになります。 この設定は [RTAV 構成を表示] - [RTAV Webcam 設定を表示] フォルダにあります。
解像度 - 最大画像高（ピクセル）	webcam によってキャプチャされる画像フレームの最大高をピクセルで決定します。低い最大画像高を設定することによって、キャプチャされるフレームの解像度を低くすることができ、低い帯域高のネットワーク環境での画像エクスペリエンスを改善できます。 この設定を構成しないか無効にすると、最大画像高は設定されません。RTAV は、クライアント システムで設定される画像高を使用します。クライアント システムの webcam 画像のデフォルト高は 240 ピクセルです。 任意の webcam 画像の上限は 1920x1080 ピクセルです。1080 ピクセルより大きい値にこの設定を構成すると、有効最大画像高は 1080 ピクセルになります。 この設定は [RTAV 構成を表示] - [RTAV Webcam 設定を表示] フォルダにあります。

リアルタイム オーディオ ビデオの帯域幅

リアルタイム オーディオ ビデオの帯域幅は、webcam の画像解像度とフレーム レート、そしてキャプチャされる画像とオーディオ データによって異なります。

表 7 で示すサンプル テストは、標準の webcam およびオーディオ入力デバイスがある Horizon View 環境でリアルタイム オーディオ ビデオが使用する帯域幅を測定します。このテストは、Horizon View Client から Horizon View Agent にビデオとオーディオ データの両方を送信するための帯域幅を測定します。View Client からデスクトップ セッションを実行する必要がある帯域幅合計は、これらの数値より大きくなる場合があります。これらのテストでは、webcam は各画像の解像度で毎秒 15 フレームで画像をキャプチャします。

表 7. Horizon View Client から Horizon View Agent にリアルタイム オーディオ ビデオ データを送信するためのサンプル帯域幅の結果

画像の解像度 (幅 x 高)	使用される帯域幅 (Kbps)
160 x 120	225
320 x 240	320
640 x 480	600

Windows 7 マルチメディア リダイレクトへのアクセスの管理

以下の手順で、適切なリソースがあり、セキュア ネットワークの Horizon View に接続されている View Client システムだけに Windows 7 マルチメディア リダイレクト (MMR) がアクセスできるようにすることができます。

MMR データはアプリケーション ベースの暗号化なしにネットワーク経由で送信されますが、リダイレクトされるコンテンツによっては、機密データが含まれていることもあります。このデータをネットワーク上で監視できないようにするには、MMR をセキュア ネットワークだけで使用します。

クライアント システムにローカルでのマルチメディア デコードを処理できるリソースが足りない、あるいは、MMR へのアクセスをセキュア ネットワークのクライアント システムだけに制限したいという理由で、MMR を無効にしたいこともあるでしょう。View Administrator のポリシを構成して、 [Multimedia redirection (MMR)] によってクライアント システムの MMR を無効または有効にすることができます。固有のデスクトップ プールまたは固有のユーザーに対してポリシをグローバルに設定できます。このポリシはデフォルトでは有効にされています。このポリシは、Windows 7、Windows XP、および Windows Vista デスクトップの MMR に影響します。詳細については、『VMware Horizon View 管理ガイド』の「ポリシの構成」を参照してください。

クライアントから Windows 7 MMR を開始できるようにする

Windows 7 MMR は Horizon View Client システムとデスクトップの間のハンドシェイクを使用して、マルチメディア リダイレクトの要求を検証します。ネットワークの状態によっては、このハンドシェイクの完了に時間がかかり、MMR が開始しなくなることがあります。Windows 7 MMR を確実に開始できるようにするには、デスクトップの Windows レジストリ キーを構成することで、検証のハンドシェイクが完了するまでの許容時間を長くできます。

Windows レジストリ キーは、ハンドシェイクの Time To Live (TTL) 値を制御し、ミリ秒単位で設定されます。このキーは REG_DWORD (hex) フォーマットで、デフォルト値は 5000 ミリ秒 (5 秒) です。

Windows 7 MMR を Horizon View ユーザーに展開する前に、少数のクライアント システムをテストして、お使いの環境でハンドシェイクが完了するまでのデフォルト許容時間が適切であるかどうかを確認します。ネットワークの状態によって 5 秒を超えるハンドシェイクが必要な場合は、TTL 値を大きくします。

手順

1 仮想デスクトップで Windows Registry Editor を起動します。

2 MMR 検証のハンドシェイクを制御する Windows レジストリ キーに移動します。

オプション	説明
Windows 7 64 ビット	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware VDPService\handshakeTTL`
Windows 7 32 ビット	`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware VDPService\handshakeTTL`

3 `handshakeTTL` 値を 5000 より大きい数にします。

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

インデックス