VMware Horizon HTML Access のインストールとセットアップ ガイド

2019 年 12 月
VMware Horizon HTML Access 5.3
VMware Horizon 7 7.10

vmware®

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

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

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

目次

VMware Horizon HTML Access のインストールとセットアップ ガイド

この『VMware Horizon HTML Access のインストールとセットアップ ガイド』では、VMware Horizon® HTML Access™ ソフトウェアを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。クライアント システムにソフトウェアをインストールせずに仮想デスクトップに接続する方法についても説明します。

このドキュメントでは、エンド ユーザーが Web ブラウザを使用してリモート デスクトップにアクセスできるように、VMware Horizon 7 Server およびリモート デスクトップ仮想マシンに HTML Access ソフトウェアをインストールするためのシステム要件および手順について説明しています。

重要： この情報は、Horizon 7 および VMware vSphere を使用した経験がある管理者を対象としています。Horizon 7 に慣れていないユーザーである場合、『Horizon 7 インストール ガイド』および VMware Horizon Console の管理で具体的な手順の確認が必要になる場合があります。

セットアップとインストール

1

HTML Access 用の Horizon 7 環境のセットアップでは、Horizon Connection Server に HTML Access をインストールして必要なポートを開き、リモート デスクトップ仮想マシンで HTML Access コンポーネントをインストールする作業が含まれます。

エンド ユーザーは、サポートされるブラウザを開いて、Horizon Connection Server の URL を入力してリモート デスクトップにアクセスできます。

この章には、次のトピックが含まれています。

HTML Access のシステム要件

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。Horizon 7 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

ブラウザ	バージョン
Chrome	75、76
Internet Explorer	11
Safari	12
Firefox	67、68
Microsoft Edge	42、44
VMware Workspace ONE Web	Apple App Store（iOS デバイス）または Google Play Store（Android デバイス）にある最新バージョン。

注：

- Android デバイスの Chrome は、Windows キー、マルチモニター、システムへのコピーと貼り付け、ファイル転送、印刷、H.264 デコード、認証情報のクリーンアップ、外部マウスをサポートしていません。ソフトウェア キーボードで次のキーとキーの組み合わせは機能しません。Del、Ctrl+A、Ctrl+C、Ctrl+V、Ctrl+X、Ctrl+Y、Ctrl+Z。
- モバイル デバイスの Safari は、Windows キー、マルチモニター、システムへのコピーと貼り付け、ファイル転送、印刷、H.264 デコード、認証情報のクリーンアップをサポートしていません。

クライアント オペレーティング システム

オペレーティング システム	バージョン
Windows	7 SP1（32 ビットおよび 64 ビット） 8.x（32 ビットおよび 64 ビット） 10（32 ビットおよび 64 ビット）
macOS	10.14.x (Mojave) 10.13.x (High Sierra)
iOS	10 以降
Chrome OS	28.x 以降
Android	7 以降

リモート デスクトップ

HTML Access では Horizon Agent 7.0 以降が必要となり、Horizon Agent 7.0 がサポートするすべてのデスクトップ オペレーティング システムがサポートされます。詳細については、バージョン 7.0 以降の『Horizon 7 のインストール』の「Horizon Agent でサポートされるオペレーティング システム」を参照してください。

プールの設定	HTML Access では、次のプール設定が必要です。 ■ [1 台のモニターの最大解像度] 設定は [1920x1200] 以上にする必要があるため、リモート デスクトップは少なくとも 17.63 MB のビデオ RAM が必要です。 3D アプリケーションを使用する場合や、エンド ユーザーが MacBook を Retina Display や Google Chromebook Pixel と併用する場合には、リモート デスクトップと公開アプリケーションの画面解像度の設定 を参照してください。 ■ [HTML Access] 設定は有効にする必要があります。 構成手順は、デスクトップ、プール、ファームの準備を参照してください。
Connection Server	Connection Server と HTML Access オプションをサーバにインストールする必要があります。 HTML Access コンポーネントをインストールするときに、ファイアウォールが TCP ポート 8443 へのインバウンド トラフィックを許可するように自動的に構成するため、Windows ファイアウォールで [VMware Horizon View Connection Server (Blast-In)] ルールが有効になります。
セキュリティ サーバ	Connection Server と同じバージョンをセキュリティ サーバにインストール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 接続は不要です。 **注：** 1 つセキュリティ サーバは、最大で 800 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： ■ サーバ（セキュリティ サーバ、Connection Server インスタンス、およびレプリカ 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。 ■ リモート デスクトップ仮想マシン：TCP ポート 22443 へのインバウンド トラフィック（サーバから）。
Horizon の表示プロトコル	VMware Blast Web ブラウザを使用してリモート デスクトップにアクセスするときは、PCoIP または Microsoft RDP ではなく VMware Blast プロトコルが使用されます。VMware Blast は HTTPS (HTTP over SSL/TLS) を使用します。

Connection Server とセキュリティ サーバの準備

エンドユーザーがサーバに接続し、リモート デスクトップや公開アプリケーションにアクセスできるようにするには、Horizon 管理者が Connection Server をインストールする必要があります。セキュリティ サーバを使用する場合は、このサーバもインストールする必要があります。

外部アクセスを安全に行うために、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することもできます。詳細については、Unified Access Gateway の導入および設定を参照してください。

以下のチェック リストに、HTML Access を使用するために必要な Horizon 管理者のタスクを示します。

1 Connection Server の複製グループを含む 1 つ以上のサーバで、[HTML Access のインストール] の設定を使用して Connection Server をインストールします。この設定は、HTML Access コンポーネントをインストールします。インストーラで、この設定はデフォルトで選択されます。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。

   HTML Access コンポーネントがインストールされていることを確認するには、Windows の [プログラムのアンインストール] アプレットを開き、リストで [VMware Horizon 7 HTML Access] を検索します。

2 セキュリティ サーバを使用する場合は、セキュリティ サーバをインストールします。セキュリティ サーバのバージョンは、Connection Server のバージョンと一致している必要があります。インストール方法については、Horizon 7 のインストールを参照してください。

3 それぞれの Connection Server インスタンスまたはセキュリティ サーバが、ユーザーが Web ブラウザで入力するホスト名を使用して完全に検証できる TLS 証明書を持つことを確認します。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。

4 RSA SecurID または RADIUS 認証などの 2 要素認証を使用するには、Connection Server でこの機能が有効であることを確認してください。Horizon 7 バージョン 7.11 から、RADIUS 認証のログイン ページでラベルのカスタマイズが可能になりました。詳細については、VMware Horizon Console 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。

5 Horizon Client で [ドメイン] ドロップダウン メニューを非表示にするには、[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] グローバル設定を有効にします。この設定は、Horizon 7 バージョン 7.1 以降で利用できます。Horizon 7 バージョン 7.8 以降では、この設定がデフォルトで有効になっています。詳細については、VMware Horizon Console の管理を参照してください。

6 Horizon Client にドメイン リストを送信するには、[ドメイン リストを送信] グローバル設定を有効にします。この設定は、Horizon 7 バージョン 7.8 以降で利用できますが、デフォルトでは無効になっています。Horizon 7 の以前のバージョンでは、ドメイン リストが送信されます。詳細については、Horizon 7 バージョン 7.8 以降の VMware Horizon Console の管理ドキュメントを参照してください。

7 サードパーティのファイアウォールを使用する場合は、複製されたグループのすべてのセキュリティ サーバおよび Connection Server のホストで TCP ポート 8443 へのインバウンド トラフィックを許可するようにルールを構成し、データセンターのリモート デスクトップの仮想マシンと RDS ホストの TCP ポート 22443 に（サーバからの）インバウンド トラフィックを許可するためのルールを構成します。詳細については、クライアント Web ブラウザ アクセスのファイアウォール ルールを参照してください。

8 認証しなくても公開アプリケーションにアクセスできるようにするには、Connection Server でこの機能を有効にします。詳細については、VMware Horizon Console の管理を参照してください。

次の表に、[ドメイン リストを送信] と [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] グローバル設定によって、Horizon Client からサーバへのログイン方法がどのように決まるかを示します。

「ドメイン リストを送信」の設定	「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」の設定	ユーザーのログイン方法
無効（デフォルト）	有効	[ドメイン] ドロップダウン メニューは表示されません。ユーザーは、[ユーザー名] テキスト ボックスに次のいずれかの値を入力する必要があります。 ■ ユーザー名（複数のドメインの場合は使用できません） ■ *domain\username* ■ *username@domain.com*
無効（デフォルト）	無効	クライアントでデフォルトのドメインが設定されている場合、デフォルトのドメインが [ドメイン] ドロップダウン メニューに表示されます。クライアントがデフォルトのドメインを認識していない場合は、[ドメイン] ドロップダウン メニューに *DefaultDomain* が表示されます。ユーザーは、[ユーザー名] テキスト ボックスに次のいずれかの値を入力する必要があります。 ■ ユーザー名（複数のドメインの場合は使用できません） ■ *domain\username* ■ *username@domain.com*
有効	有効	[ドメイン] ドロップダウン メニューは表示されません。ユーザーは、[ユーザー名] テキスト ボックスに次のいずれかの値を入力する必要があります。 ■ ユーザー名（複数のドメインの場合は使用できません） ■ *domain\username* ■ *username@domain.com*
有効	無効	ユーザーは、[ユーザー名] テキスト ボックスにユーザー名を入力して、[ドメイン] ドロップダウン メニューからドメインを選択できます。あるいは、[ユーザー名] テキスト ボックスに次のいずれかの値を入力できます。 ■ *domain\username* ■ *username@domain.com*

サーバがインストールされると、Horizon Console で該当する Connection Server インスタンスとセキュリティ サーバの [Blast Secure Gateway] 設定が有効になります。また、該当する Connection Server インスタンスとセキュリティ サーバの Blast Secure Gateway で使用するように、[Blast 外部 URL] 設定を構成します。デフォルトでは、URL には安全なトンネル外部 URL の FQDN およびデフォルトのポート番号 8443 が含まれます。URL には、クライアント システムが Connection Server のホストまたはセキュリティ サーバのホストに到達できる FQDN およびポート番号を含める必要があります。詳細については、Horizon 7 のインストールドキュメントの「Connection Server インスタンスの外部 URL を設定する」を参照してください。

注： HTML Access を VMware Workspace ONE 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。Workspace ONE のインストールおよび Connection Server で使用するための構成についての詳細は、Workspace ONE のマニュアルを参照してください。Connection Server を SAML 認証サーバとペアにする詳細については、VMware Horizon Console の管理を参照してください。

クライアント Web ブラウザ アクセスのファイアウォール ルール

セキュリティ サーバ、接続サーバ インスタンス、リモート デスクトップ、公開アプリケーションに接続することをクライアント Web ブラウザに許可するには、ファイアウォールで特定の 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。

デフォルトでは、接続サーバ インスタンスまたはセキュリティ サーバをインストールする場合、ファイアウォールが TCP ポート 8443 へのインバウンド トラフィックを許可するように構成するため、Windows ファイアウォールで [VMware Horizon View 接続サーバ (Blast-In)] ルールが有効になります。

表 1-1. クライアント ブラウザ アクセスのファイアウォール ルール

Source	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	注
クライアント Web ブラウザ	すべての TCP	HTTPS	セキュリティ サーバまたは接続サーバ インスタンス	TCP 443	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	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。この第 2 の接続を許可するためには、Blast Secure Gateway をセキュリティ サーバまたは接続サーバ インスタンスで有効にする必要があります。
Blast Secure Gateway	すべての TCP	HTTPS	HTML Access Agent	TCP 22443	Blast Secure Gateway が有効になっている場合、ユーザーがリモート デスクトップまたは公開アプリケーションを選択すると、Blast Secure Gateway はリモート デスクトップ仮想マシンまたは RDS ホストの TCP ポート 22443 で HTML Access Agent に接続します。このエージェント コンポーネントは、Horizon Agent のインストールに含まれています。
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 が有効になっていない場合、ユーザーがリモート デスクトップまたは公開アプリケーションを選択すると、クライアント デバイスの Web ブラウザはデスクトップ仮想マシンまたは RDS ホストの TCP ポート 22443 で HTML Access Agent に直接接続します。このエージェント コンポーネントは、Horizon Agent のインストールに含まれています。

キャッシュから認証情報を削除するための Horizon 7 の構成

ユーザーがリモート デスクトップまたはアプリケーションに接続しているタブを閉じるか、また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接続しているタブを閉じた際に、ユーザーの認証情報をキャッシュから削除するように Horizon 7 を設定できます。

この機能が無効になっている場合（デフォルト設定）、認証情報はキャッシュに残ります。

注： この機能を有効にすると、ユーザーがデスクトップやアプリケーションの選択ページやリモート セッション ページを更新するとき、またはリモート セッションが含まれるタブで URI コマンドを実行するときに、認証情報はキャッシュからも削除されます。サーバで自己署名証明書を提示する場合、ユーザーがリモート デスクトップや公開アプリケーションを起動し、セキュリティの警告が表示されるときに証明書を受け入れた後に、認証情報はキャッシュから削除されます。

前提条件

この機能には、Horizon 7 バージョン 7.0.2 以降が必要です。

手順

1 Horizon Console で、[設定] - [グローバル設定] の順に選択し、[全般設定] タブをクリックして [編集] をクリックします。

2 [HTML Access のタブを閉じるときに認証情報をクリーンアップする] チェック ボックスをオンにします。

3 変更内容を保存するには、[OK] をクリックします。

変更は直ちに有効になります。Connection Server の再起動は不要です。

デスクトップ、プール、ファームの準備

エンド ユーザーがリモート デスクトップや公開アプリケーションにアクセスできるようにするには、まず Horizon 管理者が特定のプールおよびファームの設定を構成し、データセンターのデスクトップ仮想マシンと RDS ホストに Horizon Agent をインストールする必要があります。

Horizon Client ソフトウェアがクライアント システムにインストールされていない場合は、HTML Access クライアントが代わりになります。

注： Horizon Client ソフトウェアは、HTML Access クライアントより多くの機能と優れたパフォーマンスを提供します。たとえば、HTML Access クライアントではリモート デスクトップで一部のキーの組み合わせが機能しませんが、Horizon Client ではこれらのキーの組み合わせが機能します。

前提条件

- Horizon コンポーネントが HTML Access のシステム要件を満たしていることを確認します。HTML Access のシステム要件を参照してください。
- HTML Access コンポーネントがホストの Connection Server にインストールされていること、および Connection Server インスタンスと任意のセキュリティ サーバの Windows ファイアウォールによって、TCP ポート 8443 でインバウンド トラフィックが許可されることを確認してください。Connection Server とセキュリティ サーバの準備を参照してください。
- サードパーティのファイアウォールを使用する場合、Horizon サーバからデータセンターのデスクトップ仮想マシンと RDS ホストの TCP ポート 22443 にインバウンド トラフィックを許可するルールを設定します。クライアント Web ブラウザ アクセスのファイアウォール ルールを参照してください。

- デスクトップ ソースとして使用する仮想マシンまたは公開デスクトップとアプリケーションをホストする RDS ホストに、サポート対象のオペレーティング システムと VMware Tools がインストールされていることを確認します。HTML Access のシステム要件を参照してください。
- プールおよびファームを作成し、ユーザーに資格を付与する手順について理解しておきます。Horizon 7 での仮想デスクトップのセットアップと Horizon 7 での公開されたデスクトップとアプリケーションのセットアップを参照してください。
- エンドユーザーがリモート デスクトップまたは公開アプリケーションにアクセス可能であることを確認するには、クライアント システムに Horizon Client for Windows をインストールします。Web ブラウザから接続を試みる前に、Horizon Client for Windows を使用して接続をテストできます。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。
- 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ためにサポートされているブラウザのいずれかがあることを確認します。HTML Access のシステム要件を参照してください。

手順

1 公開デスクトップとアプリケーションについては、Horizon Console を使用してファームを作成または編集し、[このファームのデスクトップおよびアプリケーションへの HTML Access を許可] オプションをファームの設定で有効にします。

2 仮想デスクトップ プールについては、プールを HTML Access で使用できるように Horizon Console を使用してデスクトップ プールを作成または編集します。

   a [デスクトップ プール] 設定で、[HTML Access] を有効にします。

   b このプール設定では、[1 台のモニターの最大解像度] 設定が [1920x1200] 以上であることを確認します。

3 Horizon Agent を使用するように、[このファームのデスクトップおよびアプリケーションへの HTML Access を許可] オプションまたは [HTML Access] オプションを使用してプールの作成、再構成、またはアップグレードを行った後に、Horizon Client for Windows 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接続します。

   このステップでは、HTML Access の使用を試みる前に、プールが正常に動作することを確認してください。

4 サポートされるブラウザを開き、Connection Server インスタンスを指定する URL を入力します。

   例：

   ```
   https://horizon.mycompany.com
   ```

   URL には **https** を含める必要があります。

5 表示される Web ページで、Horizon Client for Windows の場合と同じように、[VMware Horizon HTML Access] をクリックしてログインします。

6 表示されるデスクトップおよびアプリケーション選択のページで、アイコンをクリックして接続します。

これで、Web ブラウザからリモート デスクトップや公開アプリケーションにアクセスできるようになりました。

次のステップ

セキュリティの強化のため、リモートデスクトップで HTML Access Agent による認証局からの TLS 証明書を使用することがセキュリティ ポリシーで必須とされている場合は 新しい TLS 証明書を使用するように HTML Access Agent を構成するを参照してください。

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。
Connection Server	セッション共同作業機能を利用するには、Connection Server 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。

新しい TLS 証明書を使用するように HTML Access Agent を構成する

業界の規制やセキュリティ規制を遵守するため、証明書認証局 (CA) が署名した証明書と HTML Access Agent が生成するデフォルトの TLS 証明書を置き換えることができます。

リモート 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、HTML Access を使用するブラウザにデフォルトの証明書を提示します。

注： 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、証明書を各リモート 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。また、HTML Access Agent が新しい証明書を使用できるように、レジストリ値を設定する必要があります。

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、各リモート デスクトップで一意の証明書を構成します。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。この方法では、数百または数千台のリモート デスクトップが同じ証明書を持つことになります。

手順

1 リモート デスクトップの MMC への証明書スナップインの追加

Windows ローカル コンピュータ証明書ストアに証明書を追加する前に、HTML Access Agent がインストールされるリモート 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 証明書の Windows 証明書ストアへのインポート

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リモート 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

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 レジストリへの証明書のサムプリントを設定する

HTML Access Agent が、Windows 証明書ストアへインポートされた CA 署名の証明書を使用できるように、Windows レジストリ キーの証明書サムプリントを構成する必要があります。デフォルト証明書を CA 署名の証明書に交換する各リモート デスクトップでこの手順を実行する必要があります。

リモート デスクトップの MMC への証明書スナップインの追加

Windows ローカル コンピュータ証明書ストアに証明書を追加する前に、HTML Access Agent がインストールされるリモート 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。

前提条件

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 リモート デスクトップで、[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、[ファイル] - [スナップインの追加と削除] に移動します。

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

4 [証明書スナップイン] ウィンドウで、[コンピュータ アカウント] を選択し、[次へ] をクリックし、[ローカル コンピュータ] を選択し、[終了] 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。

次のステップ

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 証明書の Windows 証明書ストアへのインポートを参照してください。

HTML Access Agent 証明書の Windows 証明書ストアへのインポート

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リモート デスクトップでこの手順を実行します。

前提条件

- リモート 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リモート 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。リモート デスクトップの MMC への証明書スナップインの追加を参照してください。

手順

1 リモート デスクトップの MMC ウィンドウで、[証明書 (ローカル コンピュータ)] ノードを拡張して [個人] フォルダを選択します。

2 [操作] ペインで、[追加の操作] - [すべてのタスク] - [インポート] の順に移動します。

3 [Certificate Import（証明書のインポート)] ウィザードで、[次へ] をクリックして証明書が格納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て [開く] をクリックします。

証明書ファイルのタイプを表示するには、[ファイル名] ドロップダウン メニューからそのファイル形式を選択できます。

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 [この鍵をエクスポート可能にマークする] を選択します。

7 [すべての拡張可能なプロパティを含む] を選択します。

8 [次へ] をクリックして [終了] をクリックします。

新しい証明書が [証明書（ローカル コンピュータ)] - [個人] - [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 キーが含まれていることを確認します。

a [証明書（ローカル コンピュータ)] - [個人] - [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 [証明書情報] ダイアログ ボックスの [全般] タブで、「この証明書に対応するプライベート キーがあります。」というメッセージが表示されることを確認します。

次のステップ

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を参照してください。

適切なレジストリ キーを証明書のサムプリントで構成します。Windows レジストリへの証明書のサムプリントを設定する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 リモート デスクトップの MMC コンソールで、[証明書（ローカル コンピュータ）] ノードを拡張して [信頼されたルート証明機関] - [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、証明書チェーン内に中間証明書がない場合は、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 [信頼されたルート証明機関] - [証明書] フォルダを右クリックし、[すべてのタスク] - [インポート] をクリックします。

3 [証明書のインポート] ウィザードで、[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、[開く] をクリックします。

5 [次へ] をクリックし、[次へ] をクリックし、そして [終了] をクリックします。

6 サーバ証明書に中間 CA が署名している場合は、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 [証明書（ローカル コンピュータ）] - [中間証明機関] - [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。

次のステップ

適切なレジストリ キーを証明書のサムプリントで構成します。Windows レジストリへの証明書のサムプリントを設定するを参照してください。

Windows レジストリへの証明書のサムプリントを設定する

HTML Access Agent が、Windows 証明書ストアへインポートされた CA 署名の証明書を使用できるように、Windows レジストリ キーの証明書サムプリントを構成する必要があります。デフォルト証明書を CA 署名の証明書に交換する各リモート デスクトップでこの手順を実行する必要があります。

前提条件

CA 署名の証明書が、Windows 証明書ストアへインポートされていることを確認します。 HTML Access Agent 証明書の Windows 証明書ストアへのインポートを参照してください。

手順

1 HTML Access Agent がインストールされているリモート デスクトップの MMC ウィンドウで、[証明書（ローカル コンピュータ)] - [個人] - [証明書] フォルダの順に移動します。

2 Windows 証明書ストアへインポートした CA 署名の証明書をダブルクリックします。

3 [証明書] ダイアログ ボックスで、[詳細] タブをクリックし、スクロール ダウンして、[サムプリント]アイコンを選択します。

4 選択したサムプリントをテキスト 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：** サムプリントをコピーする場合は、先頭にあるスペースを含めないでください。サムプリントとともに先頭にあるスペースをレジストリ キー（手順 7 ）に誤って貼り付けると、証明書は正常に構成されない場合があります。先頭にあるスペースがレジストリの値テキスト ボックスに表示されなくても、この問題が発生する場合があります。

5 HTML Access Agent がインストールされたデスクトップで Windows レジストリ エディタを起動します。

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` 値を修正して、テキスト ボックスへ証明書サムプリントを貼り付けます。

8 Windows を再起動します。

ユーザーが HTML Access を介してリモート デスクトップへ接続する場合、HTML Access Agent はユーザーのブラウザに CA 署名の証明書を提供します。

特定の暗号化スイートを使用するために HTML Access Agent を構成する

HTML Access Agent を構成して、デフォルトの暗号化セットではなく特定の暗号化スイートを使用できます。

デフォルトでは、HTML Access Agent は、ネットワークからのデータの盗み出しや偽装に対して、強力な保護を提供する特定の暗号化に基づいた暗号をを使用するために、SSL 接続の受信を必要とします。HTML Access Agent が使用する暗号化の代替リストを構成できます。 許可される暗号化のセットは、OpenSSL 形式で表記されます。表記については、https://www.openssl.org/docs/manmaster/man1/ciphers.html に記載されています。

手順

1 HTML Access Agent がインストールされたデスクトップで Windows レジストリ エディタを起動します。

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

3 新しい文字列 (REG_SZ) の値 **SslCiphers** を追加して、OpenSSL 形式で暗号化リストをテキスト ボックスに貼り付けます。

4 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。

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** 値を削除して、VMware Blast サービスを再起動します。 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、VMware Blast サービスのログ ファイルに暗号化の定義を書き込みます。**SslCiphers** 値が Windows レジストリで構成されていない状態で VMware Blast サービスが起動するときに、ログを調査して現在のデフォルトの暗号化リストを把握できます。

HTML Access Agent のデフォルトの暗号化定義は、セキュリティを向上するためにリリースごとに変更される場合があります。

iOS で CA 署名証明書の使用を構成

iOS デバイスで HTML Access を使用するには、Horizon Connection Server サーバまたは HTML Access Agent により生成されたデフォルトの SSL 証明書ではなく、認証局 (CA) によって署名された SSL 証明書をインストールする必要があります。

手順については、『Horizon 7 のインストール』ドキュメントの「ルート証明書と中間証明書を信頼するように Horizon Client for iOS を構成する」を参照してください。

Unified Access Gateway での CA 署名付き証明書の使用

接続サーバまたはセキュリティ サーバではなく Unified Access Gateway アプライアンスを使用する場合は、Subject Alternative Names (SAN) が設定された CA 署名付き証明書をインストールする必要があります。

SAN が設定されていない CA 署名付き証明書または自己署名証明書を使用すると、接続がプライベートではないエラーが発生し、HTML Access で接続できません。

注： 接続サーバ インスタンスまたはセキュリティ サーバを使用する場合は、「*ip-address* にアクセスする (安全ではありません)」リンクをクリックして接続できます。

Horizon 7 の証明書のインストールと設定の詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。TLS 証明書を使用するように HTML Access エージェントを構成する方法については、新しい TLS 証明書を使用するように HTML Access Agent を構成するを参照してください。

Chrome と Safari での自動再生の設定

Chrome 71 以降または Safari 12 で HTML Access を使用し、リモート デスクトップまたは公開アプリケーションを初めて起動した場合や、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中にブラウザを更新した場合に、「クリックして、オーディオを有効にします」というダイアログ ボックスが表示されることがあります。このダイアログ ボックスで [OK] をクリックすると、オーディオが通常どおり再生されます。

このダイアログ ボックスが表示されないように、ブラウザで自動再生ポリシーを設定できます。

- Chrome のナビゲーション バーで、**chrome://flags/#autoplay-policy** と入力し、[自動再生ポリシー] までスクロールして、ドロップダウン メニューから [No user gesture required] を選択します。
- Mac の Safari で、[Safari] - [この Web サイトでの設定を表示] の順に選択し、[自動再生] の右側にポインタを置き、ドロップダウン メニューをクリックして [すべてのメディアを自動再生] を選択します。

HTML Access ソフトウェアのアップグレード

HTML Access のほとんどのバージョンでは、Horizon Connection Server と Horizon Agent をアップグレードするだけです。

HTML Access をアップグレードするときは、対応する Horizon Connection Server のバージョンが、複製されたグループのすべてのインスタンスにインストールされていることを確認します。

接続サーバをアップグレードすると、HTML Access が自動的にインストールされたり、アップグレードされます。

注： HTML Access コンポーネントがインストールされているかどうかを確認するには、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] アプレットを開き、リストで HTML Access を探してください。

接続サーバからの HTML Access コンポーネント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 HTML Access コンポーネントを削除できます。

手順

1 HTML Access がインストールされている接続サーバ インスタンスで、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 7 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。

次のステップ

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 サーバとこの接続サーバ インスタンスで 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。

Horizon Client データ共有の設定

Horizon 管理者が VMware カスタマー エクスペリエンス向上プログラム (CEIP) への参加を選択している場合、VMware は Connection Server 経由でクライアント システムから匿名データを収集して受信します。このクライアント データを Connection Server と共有するかどうかを設定できます。

CEIP に参加するように Horizon を設定する方法については、VMware Horizon Console の管理を参照してください。

デフォルトでは、HTML Access でデータ共有は有効に設定されています。サーバに接続した後は、データ共有の設定を変更できません。

Horizon 管理者は、すべてのユーザーに対して HTML Access でのデータ共有を無効にして、ユーザーが HTML Access でデータ共有設定を変更できないようにすることができます。詳細については、すべての HTML Access ユーザーのデータ共有の無効化を参照してください。

手順

1 Horizon Client を開始します。

2 VMware Horizon ログイン ページで、[設定]（歯車のアイコン）をクリックします。

3 [データの共有を許可する] オプションをオンまたはオフにします。

すべての HTML Access ユーザーのデータ共有の無効化

Horizon 管理者は、ユーザーが [データの共有を許可する] オプションを変更できないように、すべての HTML Access ユーザーのデータ共有を無効にすることができます。この設定を行うには、Connection Server インスタンスの `C:\Program Files\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\classes\portal-version.properties` ファイルに次の設定を追加します。

```
CEIP.disabled=true
```

この設定を `true` に設定すると、HTML Access の VMware Horizon ログイン ページに [設定]（歯車アイコン）が表示されません。

注： この設定を変更しても、Horizon Client を使用して Connection Server インスタンスに接続するユーザーに影響はありません。Horizon Client でデータ共有を無効にする方法については、該当する Horizon Client プラットフォームの『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。

VMware によって収集されるデータ

VMware カスタマー エクスペリエンス向上プログラム (CEIP) に参加し、クライアント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、クライアント上で情報を収集し、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 CEIP への参加を決めた場合、VMware はお客様のご要望への対応を強化する目的で、現在ご使用の環境に関する匿名データを収集します。企業が特定できるような情報は収集されません。クライアントの情報はまず Connection Server に送信され、次いで、サーバ、デスクトップ プール、およびリモート デスクトップの情報とともに VMware に送信されます。

CEIP に参加するには、Connection Server をインストールする管理者が Connection Server インストール ウィザードを実行しているときに選択するか、インストール後に Horizon Console でオプションを設定します。

表 1-2. CEIP で収集されるクライアント データ

説明	フィールド名	このフィールドは匿名になりますか？	値の例
アプリケーションを開発する企業	<client_vendor>	いいえ	VMware
製品名	<client_product>	いいえ	VMware Horizon HTML Access
クライアント製品のバージョン	<client_version>	いいえ	5.3.0-*build_number*
クライアントのバイナリ アーキテクチャ	<client_arch>	いいえ	以下のような値があります。 ■ ブラウザ ■ arm
ブラウザのネイティブ アーキテクチャ	<browser_arch>	いいえ	以下のような値があります。 ■ Win32 ■ Win64 ■ MacIntel ■ iPad ■ Linux armv81（Android Chrome サポート）
ブラウザ ユーザー エージェント文字列	<browser_user_agent>	いいえ	以下のような値があります。 ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 (KHTML、Gecko など) ■ Chrome/3.0.1750 ■ Safari/703.00 ■ Edge/13.10586
ブラウザの内部バージョン文字列	<browser_version>	いいえ	以下のような値があります。 ■ 7.0.3 （Safari 用） ■ 44.0 (Firefox 用) ■ 13.10586（Edge 用）
ブラウザのコア実装	<browser_core>	いいえ	以下のような値があります。 ■ Chrome ■ Safari ■ Firefox ■ Internet Explorer ■ Edge
ブラウザがハンドヘルド デバイスで実行しているかどうか	<browser_is_handheld>	いいえ	true

エンド ユーザー用に HTML Access を構成 2

HTML Access の URL を入力する時にエンド ユーザーに表示される Web ページの外観を変更できます。イメージ品質を制御するグループ ポリシ、使用されるポート、および他の項目も設定することができます。

この章には、次のトピックが含まれています。

エンド ユーザー用の VMware Horizon Web ポータル ページの構成

この Web ページを構成して、Horizon Client ダウンロード用のアイコン、または HTML Access 経由でリモート デスクトップに接続するアイコンの表示と非表示を切り替えることができます。このページの他のリンクも構成できます。

デフォルトでは、Web ポータル ページに、ネイティブ Horizon Client のダウンロードおよびインストールのアイコンと、HTML Access 経由で接続するためのアイコンの両方が表示されます。使用されるダウンロード リンクは、`portal-links-html-access.properties` ファイルで定義されているデフォルト値で決定されます。

ただし、社内の Web サーバへのリンクを表示したり、特定のクライアント バージョンをサーバで使用できるようにした方がよい場合もあります。`portal-links-html-access.properties` ファイルの内容を変更して、別のダウンロード URL を示すようにポータル ページを再構成できます。このファイルが使用できない、または空白であり、`oslinks.properties` ファイルが存在する場合は、`oslinks.properties` ファイルを使用して、インストーラ ファイルのリンクの値が決定されます。

`oslinks.properties` ファイルは、*`installation-directory`*`\VMware\VMware View\Server\broker\webapps\portal\WEB-INF` フォルダにインストールされます。HTML Access セッションでこのファイルが見つからない場合、このダウンロード リンクによって、ユーザーはデフォルトで `https://www.vmware.com/go/viewclients` にアクセスします。このファイルには、次のデフォルト値が含まれます。

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
```

```
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaipljfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

特定のクライアント オペレーティング システム用のインストーラ リンクは、portal-links-html-access.properties または oslinks.properties ファイルのいずれかで作成できます。たとえば、Mac OS X システムからポータル ページを参照すると、ネイティブ Mac OS X インストーラのリンクが表示されます。Windows や Linux クライアントの場合、32 ビット版インストーラのリンクと 64 ビット版インストーラのリンクを個別に作成できます。

手順

1 Connection Server ホストで、テキスト エディタを使用して `portal-links-html-access.properties` ファイルを開きます。

このファイルの場所は *`CommonAppDataFolder`*`\VMware\VDM\portal\portal-links-html-access.properties` です。Windows Server 2008 オペレーティング システムでは、*CommonAppDataFolder* ディレクトリは `C:\ProgramData` です。Windows Explorer で `C:\ProgramData` フォルダを表示するには、[フォルダ オプション] ダイアログ ボックスを使用して非表示のフォルダを表示する必要があります。

`portal-links-html-access.properties` ファイルが存在せず、`oslinks.properties` ファイルが存在する場合は、*<installation-directory>*`\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties` ファイルを開いて、特定のインストーラ ファイルをダウンロードするために使用する URL を変更します。

注： `portal-links.properties` ファイル（`portal-links-html-access.properties` ファイルと同じ *`CommonAppDataFolder`*`\VMware\VDM\portal\` ディレクトリにある）に入っている Horizon 7 5.x 以前用のカスタマイズです。

2 構成プロパティを編集し、適切に設定します。

デフォルトでは、インストーラ アイコンと HTML Access アイコンの両方が有効で、リンクは VMware Web サイトのクライアント ダウンロード ページを参照します。アイコンを無効にする (Web ページからアイコンを削除する) には、プロパティを `false` に設定します。

注： `oslinks.properties` ファイルは、特定のインストーラ ファイルへのリンクの構成にのみ使用できます。下記に表示される他のオプションはサポートされません。

オプション	プロパティ設定
HTML Access を無効にする	`enable.webclient=false` このオプションが false に設定されているにもかかわらず `enable.download` オプションが true に設定されていると、ユーザーは Web ページでネイティブの Horizon Client インストーラのダウンロードを求められます。両オプションが false に設定されていると、次のメッセージが表示されます。「この Connection Server へのアクセスについての説明は、ローカルの管理者にお問い合わせください。」
Horizon Client のダウンロードを無効にする	`enable.download=false` このオプションが false に設定されているにもかかわらず `enable.webclient` オプションが true に設定されていると、ユーザーに HTML Access のログイン Web ページが表示されます。両オプションが false に設定されていると、次のメッセージが表示されます。「この Connection Server へのアクセスについての説明は、ローカルの管理者にお問い合わせください。」
Horizon 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	`link.download=https://`*url-of-web-server* 独自の Web ページを作成する予定がある場合は、このプロパティを使用します。

オプション	プロパティ設定

特定のインストーラ用のリンクを作成する	以下に示すのは完全 URL の例ですが、インストーラ ファイルが次の手順の説明のように Connection Server の `C:\Program Files\VMware\VMware View\Server\broker\webapps\` ディレクトリの `downloads` ディレクトリにある場合は、相対 URL を使用できます。
	■ インストーラをダウンロードするための一般的なリンク：
	`link.download=https://server/downloads`
	■ 32 ビット Windows インストーラ：
	`link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe`
	■ 64 ビット Windows インストーラ：
	`link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe`
	■ Windows Phone インストーラ：
	`link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx`
	■ 32 ビット Linux インストーラ：
	`link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle`
	■ 64 ビット Linux インストーラ：
	`link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle`
	■ Mac OS X インストーラ：
	`link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg`
	■ iOS インストーラ:
	`link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa`
	■ Android インストーラ：
	`link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk`
	■ Chrome OS インストーラ：
	`link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-build#.apk`

ログイン ページの [ヘルプ] リンクの URL を変更します。	`link.help` デフォルトでは、このリンクは VMware の Web サイトにホストされているヘルプ システムを参照します。[ヘルプ] リンクが、ログイン ページの下部に表示されます。

3 ユーザーに VMware Web サイト以外の場所からインストーラをダウンロードさせるには、インストーラ ファイルを置くことになる HTTP サーバにインストーラ ファイルを配置します。

この場所は、前の手順の `portal-links-html-access.properties` ファイルまたは `oslinks.properties` ファイルで指定した URL に対応している必要があります。たとえば、Connection Server ホストの `downloads` ディレクトリにファイルを配置するには、以下のパスを使用します。

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

これで、インストーラ ファイルに対するリンクで `/downloads/`*`client-installer-file-name`* というフォーマットの相対 URL を使用できます。

4 Horizon Web コンポーネント サービスを再起動します。

URI を使用した HTML Access Web Client の構成

Uniform Resource Identifier (URI) を使用して作成できるリンク付きの Web ページや E メールでは、エンド ユーザーがクリックすると HTML Access Web client が起動したり、Horizon Connection Server に接続したり、特定の構成オプションを持つ特定のデスクトップまたはアプリケーションを起動したりできます。

エンド ユーザー用の Web または電子メールのリンクを作成することで、リモート デスクトップまたはアプリケーションへの接続プロセスを簡素化できます。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。

- Horizon Connection Server のアドレス
- Horizon Connection Server 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
- デスクトップまたはアプリケーション表示名
- セッションの参照、リセット、ログオフ、開始を含むアクション

HTML Access の URI を作成するための構文

この構文には、サーバを指定するパス部分だけでなく、必要に応じて、ユーザー、リモート デスクトップまたは公開アプリケーション、アクションまたは設定オプションを指定するクエリが含まれます。

URI 仕様

以下の構文を使用して HTML Access を起動する URI を作成します。

```
https://authority-part[/?query-part]
```

authority-part サーバ アドレス、および必要に応じて非デフォルト ポート番号を指定します。サーバ名は、DNS 構文に一致する必要があります。

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
```

query-part

使用するための構成オプション、または実行するアクションを指定します。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。クエリが違いに競合する場合、リストの最後のクエリが使用されます。次の構文を使用します:

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

query-part を作成するときは、以下のガイドラインに注意してください。

- サポートされているクエリを 1 つも使用しない場合は、デフォルトの VMware Horizon Web ポータル ページが表示されます。
- クエリ部分では、一部の特殊文字がサポートされていません。それらの文字には URL エンコーディング形式を使用する必要があります。番号記号 (#) には **%23**、パーセント記号 (%) には **%25**、アンパサンド (&) には **%26**、アット マーク (@) には **%40**、バックスラッシュ (\) には **%5C** を使用します。

  URL エンコーディングの詳細については、http://www.w3schools.com/tags/ref_urlencode.asp を参照してください。
- クエリ部分で、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。

サポートされるクエリ

このトピックでは、HTML Access でサポートされるクエリを示します。デスクトップ クライアントやモバイル クライアントなどの複数のクライアント タイプ用に URI を作成する場合は、クライアント システムの各タイプのインストールとセットアップのドキュメントを参照してください。

操作

表 2-1. 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起動します。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。

表 2-1. アクション クエリで使用できる値 （続き）

値	説明
`reset`	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。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 ボタンを押すことに相当します。このアクションは、公開アプリケーションに実行できません。
`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。このアクションは、公開アプリケーションに実行できません。
`restart`	再起動操作の要求をユーザーが確認したら、プライマリ 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。このアクションは、公開アプリケーションに実行できません。

applicationId

公開アプリケーションの表示名。この表示名は、アプリケーション プールの作成時に Horizon Console 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、ブラウザは **`%20`** でスペースを表します。

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。

desktopId

リモート デスクトップの表示名。この表示名は、デスクトップ プールの作成時に Horizon Console 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、ブラウザは **`%20`** でスペースを表します。

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。たとえば、`mycompany.com` ではなく `mycompany` を使用してください。

tokenUserName

RSA または RADIUS ユーザー名。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、Windows ユーザー名が使用されます。

userName

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いる Active Directory ユーザー。ユーザー名は、次のいずれかの形式で指定できます。

- *userName*

- *domainName%5CuserName*
- *userName@domainName* 形式のユーザー プリンシパル名 (UPN)

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。HTML Access が起動し、匿名ユーザー アカウントが表示されます。構文の例は、**unauthenticatedAccessEnabled=true** です。
unauthenticatedAccessAccount	非認証アクセス機能が有効な場合、このアカウントを使用するように設定します。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。

URI の例

URI でハイパーテキスト 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 ページに含めることができます。エンド ユーザーはこれらのリンクをクリックして、たとえば、指定した起動オプションで特定のリモート デスクトップやアプリケーションを開くことができます。

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。クエリは大文字と小文字の区別がありません。たとえば、**domainName** または **domainname** を使用できます。

1 `https://horizon.mycompany.com/?domainName=finance&userName=fred`

HTML Access Web client が起動し、horizon.mycompany.com サーバに接続します。ログイン ボックスで、[ユーザー名] テキスト ボックスに [fred] という名前が入力され、[ドメイン] テキスト ボックスに [finance] が入力されます。ユーザーはパスワードを入力する必要があるだけです。

2 `https://horizon.mycompany.com/?userName=finance%5Cfred`

HTML Access Web client が起動し、horizon.mycompany.com サーバに接続します。ログイン ボックスで、[ユーザー名] テキスト ボックスに [finance\fred] という名前が入力されます。ユーザーはパスワードを入力する必要があるだけです。

3 `https://horizon.mycompany.com/?userName=fred@finance`

HTML Access Web client が起動し、horizon.mycompany.com サーバに接続します。ログイン ボックスで、[ユーザー名] テキスト ボックスに [fred@finance] という名前が入力されます。ユーザーはパスワードを入力する必要があるだけです。

4 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=start-session`

HTML Access Web client が起動し、horizon.mycompany.com サーバに接続します。ログイン ボックスが表示され、ユーザー名、ドメイン名、およびパスワードが求められます。ログインに成功すると、クライアントはディスプレイ名が [Primary Desktop（プライマリ デスクトップ）] として表示されるデスクトップに接続し、ユーザーはゲスト OS にログインされます。

5 `https://horizon.mycompany.com/?applicationId=Notepad&action=start-session`

HTML Access Web client が起動し、`horizon.mycompany.com` サーバに接続します。ログイン ボックスが表示され、ユーザー名、ドメイン名、およびパスワードが求められます。ログインが成功すると、ノートパッド アプリケーションが起動されます。

6 `https://horizon.mycompany.com:7555/?desktopId=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）。デスクトップ ID が提供されるので、デスクトップは `start-session` アクションが URI に含まれていない場合であっても起動されます。

7 `https://horizon.mycompany.com/?applicationId=Primary%20Application&desktopId=Primary%20Desktop`

この URI は、アプリケーションとデスクトップの両方を指定します。アプリケーションとデスクトップの両方を指定すると、デスクトップだけが起動されます。

8 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=reset`

HTML Access Web Client が起動され、`horizon.mycompany.com` サーバに接続します。ログイン ボックスが表示され、ユーザー名、ドメイン名、およびパスワードが求められます。ログインに成功すると、クライアントによって、プライマリ デスクトップのリセット操作の確認を求めるダイアログ ボックスが表示されます。

注： このアクションは、Horizon 管理者がエンド ユーザーにマシンのリセットを許可している場合にのみ使用できます。

9 `https://horizon.mycompany.com/?My%20Notepad++?args=%22My%20new%20file.txt%22`

Notepad++ をサーバ `horizon.mycompany.com` で開いて、引数 `My new file.txt` をアプリケーションの起動コマンドに渡します。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。

10 `https://horizon.mycompany.com/?Notepad++%2012?args=a.txt%20b.txt`

Notepad++ 12 をサーバ `horizon.mycompany.com` で開いて、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。引数は二重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： 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。

11 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=restart`

HTML Access Web client が起動し、**horizon.mycompany.com** サーバに接続します。ログイン ボックスが表示され、ユーザー名、ドメイン名、およびパスワードが求められます。ログインに成功すると、クライアントによって、プライマリ デスクトップの再起動操作の確認を求めるダイアログ ボックスが表示されます。

注： このアクションは、Horizon 管理者がエンド ユーザーにマシンの再起動を許可している場合にのみ使用できます。

12
```
https://horizon.mycompany.com/?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_user1
```

HTML Access Web client が起動し、**anonymous_user1** アカウントを使用して、**horizon.mycompany.com** サーバに接続します。

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。以下の例は、[Test Link（テスト リンク）] と言うハイパー リンクおよび [TestButton] と言うボタンのコードを記述するために最初の URI の例から URI を使用する方法を示します。

```
<html>
<body>

<a href="https://horizon.mycompany.com/?domainName=finance&userName=fred">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'https://horizon.mycompany.com/?domainName=finance&userName=fred'"></form> <br>

</body>
</html>
```

HTML Access グループ ポリシー設定

HTML Access は、VMware Blast プロトコルを使用します。VMware Blast プロトコルのグループ ポリシーの構成により、HTML Access のグループ ポリシーを構成します。

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』ドキュメントの「デスクトップ プールとアプリケーション プールのポリシーの設定」と「「VMware Blast ポリシー設定」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

3

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こともできます。

この章には、次のトピックが含まれています。

リモート デスクトップまたは公開アプリケーションへの接続

使用を許可されているリモート 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、Active Directory の認証情報を使用します。

前提条件

- Active Directory 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 認証情報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。

手順

1 ブラウザを開き、接続サーバ インスタンスの URL を入力します。

URL では **`https`** を使用し、`https://horizon.company.com` のように完全修飾ドメイン名を使用します。

接続サーバとの接続には常に SSL を使用します。SSL 接続のデフォルト ポートは 443 です。接続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、次の例の形式を使用します。**`horizon.company.com:1443`**。

VMware Horizon Web ポータルが表示されます。デフォルトでは、このページに、ネイティブ Horizon Client のダウンロードおよびインストールのアイコンと、HTML Access 経由で接続するためのアイコンの両方が表示されます。

2 （オプション）[この画面をスキップして HTML Access を常に使用するには、これを選択してください。] チェック ボックスを選択します。

選択内容は、現在使用しているブラウザのローカル ストレージに格納されます。次回、同じブラウザ タイプと同じクライアント マシンを使用して接続サーバ インスタンスの URL を入力すると、すぐにログイン画面が表示されます。同じクライアント マシンで別のブラウザ タイプを使用する場合、または別のクライアント マシンで同じタイプのブラウザを使用すると、VMware Horizon Web ポータルが表示されます。VMware Horizon Web ポータルを表示するには、ブラウザのキャッシュをクリアします。

3 [VMware Horizon HTML Access] アイコンをクリックします。

4 [ログイン] ダイアログ ボックスで 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 [ログイン] をクリックします。

パスコードには、PIN とトークンで生成された番号が含まれる場合があります。

5 再度、RSA SecurID 認証情報または RADIUS 認証情報を入力するダイアログが表示されたら、トークンで次に生成された番号を入力します。

PIN および、過去に生成され、入力したものと同じ番号は入力しないでください。必要に応じて、新しい番号が生成されるのを待ちます。

この手順は、最初のパスコードの入力をミスした、または RSA サーバの設定が変更された時にのみ、必要になります。

6 [ログイン] ダイアログ ボックスで、ログイン認証情報を入力します。

a [ユーザー名] テキスト ボックスに、*username*、*domain**username*、または *username@domain* のいずれかの形式で有効な Active Directory ユーザー名を入力します。

[ドメイン] テキストボックスが無効になっている場合、*domain**username* または *username@domain* のいずれかの形式を使用する必要があります。

b パスワードを入力してください。

c （オプション）[ドメイン] フィールドが有効で、ドメイン名が正しく入力されていない場合には、このフィールドから選択します。

注： ログイン プロセスを中断するには、ログイン プロセスが完了する前に [キャンセル] をクリックします。

7 （オプション） 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タイムゾーンを手動で設定する必要がある場合は、デスクトップおよびアプリケーション選択画面の右上隅にある [設定] ツールバー ボタンをクリックします。[タイム ゾーンを自動的に設定する] オプションをオフにして、ドロップダウン メニューからタイム ゾーンを 1 つ選択します。タイム ゾーンの設定を参照してください。

8 （オプション） デスクトップおよびアプリケーションの選択画面で、アクセスする項目を選択する前に、お気に入りとしてリモート デスクトップや公開アプリケーションをマークするには、デスクトップや公開アプリケーションのアイコンの中にある灰色の星をクリックします。

星のアイコンが灰色から黄色に変わります。次回ログインするときに、ブラウザ ウィンドウの右上部分にある星のアイコンをクリックして、お気に入りのみを表示できます。

9 アクセスするリモート デスクトップまたは公開アプリケーションのアイコンをクリックします。

ブラウザにリモート デスクトップまたは公開アプリケーションが表示されます。ナビゲーション サイドバーも利用できます。ブラウザ ウィンドウの左側にあるタブをクリックして、サイドバーを表示できます。サイドバーを使用して、他のリモート デスクトップや公開アプリケーションにアクセスしたり、[設定] ウィンドウを表示したり、テキストをコピーおよび貼り付けたり、その他の操作を実行したりできます。

次のステップ

デスクトップや公開アプリケーションに接続した後にすぐ切断され、リンクをクリックしてセキュリティ証明書を受け入れるよう求めるプロンプトが表示さる場合、ユーザーはその証明書を信頼するかどうかを選択できます。自己署名付ルート証明書の信頼を参照してください。

自己署名付ルート証明書の信頼

リモート デスクトップまたは公開アプリケーションに初めて接続したときに、リモート マシンで使用する自己署名証明書を受け入れるように指示するプロンプトが表示される場合があります。リモート デスクトップまたは公開アプリケーションに接続する前に、証明書を信頼する必要があります。

ほとんどのブラウザでは、自己署名証明書を永続的に信頼するオプションを利用できます。証明書を永続的に信頼する場合は、ブラウザを再起動するときに毎回証明書を確認する必要があります。Safari ブラウザを使用している場合、接続を確立するにはセキュリティ証明書を永続的に信頼する必要があります。

手順

1 信頼されていない証明書の警告や、接続がプライベートではないという警告がブラウザに表示される場合、証明書を調べて、ユーザーの企業によって使用されている証明書と一致しているか確認します。

システム管理者への連絡が必要になる場合があります。たとえば、Chrome では、次の手順を使用します。

a アドレス バーのロック アイコンをクリックします。

b [証明書情報] リンクをクリックします。

c 証明書がユーザーの企業で使用されている証明書と一致しているか確認します。

システム管理者への連絡が必要になる場合があります。

2 セキュリティ証明書を受け入れます。

証明書を受け入れるあるいは常に信頼するためのプロンプトは各ブラウザで異なります。たとえば、Chrome ブラウザでブラウザ ページの [詳細] リンクをクリックして、[*server-name* にアクセスする（安全ではありません）] をクリックすることができます。

Safari ブラウザでは、次の手順で証明書を永続的に信頼します。

a 信頼されない証明書のダイアログ ボックスが表示されたら、[証明書の表示] ボタンをクリックします。

b [常に信頼] チェック ボックスを選択し、[続ける] をクリックします。

c 入力を求められたらパスワードを入力し、[設定の更新] 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が起動します。

Workspace ONE モードでのサーバへの接続

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。

Workspace ONE モードが有効な場合、Workspace ONE Web ポータルを介してサーバに接続できます。HTML Access 経由でサーバに接続しようとすると、Workspace ONE Web ポータルにリダイレクトされます。Workspace ONE Web ポータル経由でサーバに接続すると、Workspace ONE Web ポータル経由でのみリモート デスクトップと公開アプリケーションを開始できます。

Workspace ONE モードが有効になっている場合、サイドバーに一部の資格が表示されません。現在実行中のデスクトップや公開アプリケーションのみが表示されます。

Workspace ONE モードを有効にすると、次の問題が発生することがあります。

- HTML Access を介してサーバに接続できません。サーバに接続できないか、サーバが別のアプリケーションまたはサーバのログイン認証情報を想定していることを示すメッセージが表示される場合があります。
- Workspace ONE Web ポータル経由でリモート デスクトップまたは公開アプリケーションを開始すると、HTML Access でリモート デスクトップと公開アプリケーションを表示または開始できません。

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

非認証アクセス ユーザーのアカウントを使用すると、サーバに匿名でログインし、公開アプリケーションに接続できます。

前提条件

- 管理タスクの実行については、Connection Server とセキュリティ サーバの準備で説明しています。
- Connection Server 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、『VMware Horizon Console 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。

手順

1 非認証アクセスを許可しているサーバに接続するには、ブラウザを開き、URI (Uniform Resource Identifier) を入力します。

次のいずれかの URI 構文を使用します。

- https://*authority-part*?unauthenticatedAccessEnabled=true
- https://*authority-part*?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=*anonymous_account*

authority-part はサーバ アドレスです。必要に応じて、デフォルト以外のポート番号も指定できます。ポート番号を指定する必要がある場合は、*server-address:port-number* を入力します。

anonymous_account は、非認証アクセス ユーザー アカウントです。

接続は常に TLS を使用します。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、次の形式を使用します。**horizon.company.com:1443**。

2 （オプション） 非認証アクセス ユーザー アカウントを URI に指定していない場合、必要であれば、[ユーザー アカウント] ドロップダウン メニューから非認証アクセス ユーザー アカウントを選択して、[送信] をクリックします。

使用可能な非認証アクセス ユーザー アカウントが 1 つしかない場合、このユーザー アカウントがデフォルトで選択されます。

アプリケーション選択ウィンドウが表示されます。

3 アクセスする公開アプリケーションのアイコンをクリックします。

公開アプリケーションがブラウザに表示されます。ナビゲーション サイドバーも利用できます。ブラウザの左側にあるタブをクリックして、サイドバーを表示できます。サイドバーを使用すると、他の公開アプリケーションへのアクセス、[設定] ウィンドウの表示、テキストのコピー アンド ペーストなどの操作の実行が可能になります。

注： 非認証のアプリケーション セッションに再接続することはできません。クライアントから切断されると、ローカルのユーザー セッションから自動的にログオフします。

タイム ゾーンの設定

リモート デスクトップまたは公開アプリケーションのタイムゾーンには、ローカル システムのタイムゾーンが自動的に設定されます。

ただし、HTML Access クライアントで、特定の夏時間ポリシーのためタイムゾーンを正しく特定できない場合は、タイムゾーンを手動で設定する必要があります。

リモート デスクトップまたは公開アプリケーションに手動で接続する前に、適切なタイムゾーン情報を設定するには、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右上隅にある [設定] ツールバー ボタンをクリックします。[設定] ウィンドウで [タイムゾーンを自動的に設定する] オプションをオフにして、ドロップダウン メニューからタイムゾーンを 1 つ選択します。

選択した値は、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ときに優先的に使用されるタイムゾーンとして保存されます。

リモート デスクトップまたは公開アプリケーションにすでに接続している場合は、デスクトップおよびアプリケーション選択ウィンドウに戻り、現在のタイムゾーン設定を変更します。

サイドバーからアクセスできる [設定] ウィンドウでは、[タイムゾーンを自動的に設定する] オプションは使用できません。

注： [タイムゾーンを自動的に設定する] オプションが **true** に設定されている場合、Android デバイスで Chrome ブラウザを使用するときに Android のシステムのタイムゾーンを変更しても、新しいタイムゾーンはリモート デスクトップに自動的に同期されません。この問題は、Android システムの Chrome の制約で発生します。選択したタイムゾーンに同期するには、Android デバイスと Chrome ブラウザを再起動する必要があります。

H.264 デコードの許可

Chrome ブラウザを使用している場合、リモート デスクトップや公開アプリケーション セッションにクライアントで H.264 デコードを許可できます。

H.264 はビデオ圧縮規格で、デジタル ビデオの保存または転送時にビデオを容量の少ない形式に変換します。

H.264 デコードを許可すると、エージェントが H.264 エンコードをサポートする場合に、HTML Access クライアントは H.264 デコードを使用します。エージェントが H.264 エンコードをサポートしない場合、HTML Access クライアントは JPEG/PNG デコードを使用します。

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場合、サイドバーから利用できる [設定] ウィンドウの [H.264 デコードを許可する] オプションをオンにして H.264 デコードを許可できます。新しい設定を有効にするには、リモート デスクトップや公開アプリケーションを切断してから再接続する必要があります。

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ない場合、デスクトップとアプリケーションの選択ウィンドウの右上隅にある [設定] ツールバー ボタンをクリックして、[設定] ウィンドウで [H.264 デコードを許可する] オプションをオンにできます。設定を変更した後に接続したセッションで、新しい設定が有効になります。

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。

手順

- サーバからログアウトして、リモート デスクトップから切断（ただしログアウトはしません）するか、公開アプリケーションを終了します。

オプション	アクション
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、デスクトップとアプリケーションの選択ウィンドウから	ウィンドウの右上隅にある [ログアウト] ツールバー ボタンをクリックします。
リモート デスクトップや公開アプリケーションに接続したときにサイドバーから	サイドバーの上部にある [ログアウト] ボタンをクリックします。

- 公開アプリケーションを閉じます。

オプション	アクション
公開アプリケーションから	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、公開アプリケーション ウィンドウの隅の [X]（閉じる）ボタンをクリックします。
サイドバーから	サイドバーの [実行中] リストにある公開アプリケーション名の横にある [X] をクリックします。

- リモート デスクトップからログオフまたは切断します。

オプション	アクション
リモート デスクトップから	ログオフするには、Windows の [スタート] メニューを使用してログオフします。
サイドバーから	ログオフおよび切断するには、サイドバーの [実行中] リストにあるリモート デスクトップ名の横の [メニューを開く] ツールバー ボタンをクリックして、[ログオフ] を選択します。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。 ログオフせずに切断するには、[実行中] リストにあるリモート デスクトップ名の横の [メニューを開く] ツールバー ボタンをクリックして、[閉じる] を選択します。 **注：** Horizon 管理者は、切断時に自動的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 デスクトップまたは公開アプリケーションの使用

4

クライアントには、ナビゲーション サイドバーとツールバーが用意されているので、リモート デスクトップや公開アプリケーションから簡単に切断したり、ボタンをクリックして Ctrl + Alt + Delete キーの組み合わせと同じコマンドを送信したりすることができます。

この章には、次のトピックが含まれています。

機能サポート一覧

ブラウザベースの HTML Access クライアントからリモート デスクトップやアプリケーションにアクセスする場合、一部の機能は使用できません。

シングルユーザーの仮想マシン デスクトップの機能サポート

表 4-1. HTML Access を通してサポートされる機能

機能	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 R2 デスクトップ	Windows Server 2012 R2 デスクトップ	Windows Server 2016 または Windows Server 2019 デスクトップ
RSA SecurID または RADIUS	X	X	X	X	X	X
シングル サインオン	X	X	X	X	X	X
RDP 表示プロトコル						
PCoIP 表示プロトコル						
VMware Blast 表示プロトコル	X	X	X	X	X	X
USB リダイレクト						
リアルタイム オーディオビデオ (RTAV)	X	X	X	X	X	X
Windows Media MMR						
仮想印刷						
ロケーション ベースの印刷	X	X	X	X	X	X
スマート カード						
複数のモニター	X	X	X	X	X	X

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。

RDS ホストでのセッションベースのデスクトップおよびホスト型アプリケーションの機能サポート

RDS ホストは、Windows リモート デスクトップ サービスと Horizon Agent がインストールされたサーバ コンピュータです。RDS ホスト上のデスクトップおよびアプリケーション 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、HTML Access を使用する場合に RDS ホストから利用可能な機能の行だけが含まれます。Horizon Client for Windows など、ネイティブでインストールされた Horizon Client を使用している場合は、追加の機能が使用できます。

表 4-2. HTML Access から RDS ホストへの接続でサポートされる機能

機能	Windows Server 2008 R2 RDS ホスト	Windows Server 2012 または 2012 R2 RDS ホスト	Windows Server 2016	Windows Server 2019
RSA SecurID または RADIUS	X	X	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

表 4-2. HTML Access から RDS ホストへの接続でサポートされる機能 （続き）

機能	Windows Server 2008 R2 RDS ホスト	Windows Server 2012 または 2012 R2 RDS ホスト	Windows Server 2016	Windows Server 2019
VMware Blast 表示プロトコル	X	X	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	X（仮想マシン専用）	X（仮想マシン専用）	Horizon Agent 7.0.2 以降（仮想マシン専用）	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
複数のモニター（セッション ベースのデスクトップのみ）	X	X	X	X

各ゲスト OS でサポートされるエディションとサービス パックの詳細については、『Horizon 7 のインストール』の「Horizon Agent でサポートされているオペレーティング システム」を参照してください。

サイドバーの使用

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ら、サイドバーを使用して、他のリモート デスクトップや公開アプリケーションを起動したり、実行中のリモート デスクトップと公開アプリケーションを切り替えたり、その他の操作を実行したりできます。

サイドバーは、リモート デスクトップや公開アプリケーションのウィンドウの左側に表示されます。サイドバーを表示または非表示にするには、サイドバーのタブをクリックします。このタブは上下にスライドできます。

実行中の公開アプリケーションで開いているドキュメントのリストを表示するには、[実行中] リストで公開アプリケーションの横にある拡張矢印をクリックします。

注： 2 つの異なるサーバにホストされている同じ公開アプリケーションから 2 つのドキュメントを開いている場合、サイドバーの [実行中] リストに同じ公開アプリケーションが 2 回表示されます。

サイドバーで多くのアクションを実行できます。

表 4-3. サイドバーの操作

アクション	手順
サイドバーを表示	公開アプリケーションまたはリモート デスクトップが開いている場合は、サイドバーのタブをクリックします。このサイドバーが開いているときでも、公開アプリケーションまたはリモート デスクトップのウィンドウで操作を実行できます。
サイドバーを非表示にする	サイドバー タブをクリックします。
公開アプリケーションまたはリモート デスクトップを起動する	サイドバーの [使用可能] リストにある公開アプリケーションまたはリモート デスクトップの名前をクリックします。リモート デスクトップが最初に表示されます。
公開アプリケーションまたはリモート デスクトップを検索する	■ [検索] ボックスをクリックし、公開アプリケーションまたはリモート デスクトップの名前を入力します。 ■ 公開アプリケーションまたはリモート デスクトップを起動するには、検索結果に表示された名前をクリックします。 ■ サイドバーのホーム表示に戻るには、検索ボックスの [X] をタップします。

表 4-3. サイドバーの操作 （続き）

アクション	手順
お気に入りの公開アプリケーションまたはリモート デスクトップの一覧を作成する	サイドバーの [使用可能] リストにあるリモート デスクトップや公開アプリケーションの名前の横にある灰色の星をクリックします。次に、[使用可能] の横にある [お気に入りを表示] ツールバー ボタン（星のアイコン）をクリックして、お気に入りだけのリストを表示できます。
公開アプリケーションまたはリモート デスクトップを切り替える	サイドバーの [実行中] リストにある公開アプリケーションまたはリモート デスクトップの名前をクリックします。
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	サイドバーにある [メニューを開く] ボタンをクリックして、[設定] をクリックし、[マルチ起動] 設定までスクロールします。詳細については、異なるクライアント デバイスでの公開アプリケーションの複数のセッションの使用を参照してください。
[コピーおよび貼り付け] パネルを開く	サイドバーの上部にある [コピーおよび貼り付け] ボタンをクリックします。このボタンを使用して、ローカル クライアント システムにあるアプリケーションにテキストをコピーしたり、このアプリケーションからテキストをコピーしたりします。詳細については、テキストのコピーおよび貼り付けを参照してください。iOS Safari では、コピーおよび貼り付けの機能がサポートされていないため、このボタンを使用できません。
[転送ファイル] ウィンドウを開く	リモート デスクトップからファイルをダウンロードしたり、リモート デスクトップにファイルをアップロードするには、サイドバーの上部にある [ファイル転送] ボタンをクリックします。詳細は、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 システムへのファイルのダウンロードおよびクライアント 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ファイルのアップロードを参照してください。
Command + A、Command + C、Command + V、および Command + X を有効にする	このオプションは、Mac を使用している場合にのみ [設定] ウィンドウに表示されます。サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[設定] をクリックします。この機能が有効になっていると、Mac の Command キーがリモートの Windows デスクトップやアプリケーションの Ctrl キーにマッピングされます。たとえば、Mac キーボードの Command + A キーは、リモートの Windows デスクトップやアプリケーションで Ctrl + A キーを押したときと同じ効果になります。
実行中のリモート デスクトップを閉じる	サイドバーの [実行中] リストにあるリモート デスクトップ名の横の [メニューを開く] ボタンをクリックして、アクション選択します。 ■ [閉じる] を選択すると、オペレーティング システムからログアウトせずに、リモート デスクトップから切断します。Horizon 管理者は、切断時に自動的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。この場合、開いているアプリケーションで保存されていない変更は失われます。 ■ [ログオフ] を選択すると、オペレーティング システムからログアウトして、リモート デスクトップから切断します。開いているアプリケーションで保存されていない変更は失われます。
動作中の公開アプリケーションを閉じる	サイドバーの [実行中] リストにある公開アプリケーション名のファイル名の横にある [X] をクリックします。公開アプリケーション名の横にある [X] をクリックして、公開アプリケーションを終了して、その公開アプリケーションの開いているすべてのファイルを閉じます。 これらのファイルへの変更を保存するように求められます。
リモート デスクトップのリセット	サイドバーの [実行中] リストにあるリモート デスクトップ名の横の [メニューを開く] ボタンをクリックして、[リセット] を選択します。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。リモート デスクトップをリセットできるのは、Horizon 管理者がこの機能を有効にしている場合のみです。
リモート デスクトップの再起動	サイドバーの [実行中] リストにあるリモート デスクトップ名の横の [メニューを開く] ボタンをクリックして、[再起動] を選択します。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。リモート デスクトップを再起動できるのは、Horizon 管理者がこの機能を有効にしている場合のみです。

表 4-3. サイドバーの操作 （続き）

アクション	手順
実行中のすべての公開アプリケーションのリセット	サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[設定] をクリックし、[実行中のすべてのアプリケーションをリセットします] をクリックします。保存されていないすべての変更は失われます。
Windows キーを含むキーの組み合わせを使用する	サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[設定] をクリックし、[デスクトップで Windows キーを有効にします] をオンにします。詳細については、ショートカット キーの組み合わせを参照してください。
現在の作業領域に Ctrl+Alt+Del を送信する	サイドバーの上部にある [Ctrl+Alt+Delete を送信] ツールバー ボタンをクリックします。
サーバからの切断	サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[ログアウト] をクリックします。
高解像度ディスプレイ マシンでの高解像度モードの使用 (Retina 搭載の Macbook Pro など)	サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[設定] をクリックし、[高解像度モード] をオンにします。
H.264 デコードを許可する	サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[設定] をクリックし、[H.264 デコードを許可する] をオンにします。詳細については、H.264 デコードの許可を参照してください。
複数のモニターの使用	(Chrome バージョン 55 以降のみ) サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[表示設定] を選択します。詳細については、複数のモニターの使用を参照してください。
ソフト キーボードの表示と消去	(iOS Safari のみ) サイドバーの上部にあるキーボード アイコンをクリックします。また、3 本の指で画面をタップして、ソフト キーボードを表示または消去することも可能です。
ヘルプ トピックを表示する	サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[設定] をクリックし、[ヘルプ] をクリックします。サイドバーの上部にある Horizon のロゴをクリックして、[ヘルプ] をクリックします。
[VMware Horizon Client のバージョン情報] ダイアログ ボックスを表示する	サイドバーの上部にある [メニューを開く] ツールバー ボタンまたは Horizon のロゴをクリックして、[バージョン情報] をクリックします。サイドバーの上部にある Horizon ロゴをクリックします。
リモート デスクトップや公開アプリケーションを全画面表示モードで表示する	サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[全画面表示] をクリックします。
全画面表示モードを終了する	サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[全画面表示モードを終了] をクリックします。
全画面表示モードでリモート デスクトップまたは公開アプリケーションに Esc を送信する	サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[ESC の送信] をクリックします。

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。

複数のモニターの使用

Chrome ブラウザ（バージョン 55 以降）を使用すると、HTML Access でマルチモニタを使用してリモート デスクトップ ウィンドウを表示できます。

プライマリ モニターに最大で 1 台のモニターを追加して、接続している現在のリモート デスクトップ ウィンドウを表示できます。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。マルチモニタのセットアップでは、隣接するモニターを選択する必要があります。モニターは横または縦に並べて配置できます。

手順

1 HTML Access 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、アクセスするリモート デスクトップのアイコンをクリックします。

3 サイドバーを表示するには、サイドバーのタブをクリックします。

4 サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックして、[マルチ モニター] を選択します。

5 [マルチ モニター] ウィンドウで、[ディスプレイの追加] をクリックします。

注： [ディスプレイ セレクタ] ブラウザ ウィンドウが表示されない場合は、ブラウザの [コンテンツの設定] ウィンドウの [ポップアップの例外] セクションにサーバの FQDN アドレスを追加します。

6 [ディスプレイ セレクタ] ブラウザ ウィンドウをドラッグして、使用する別のモニターのディスプレイに表示させます。

[ディスプレイ セレクタ] ブラウザ ウィンドウのメッセージが変わり、グレーの長方形のアイコンが追加されます。

7 [ディスプレイ セレクタ] ブラウザ ウィンドウで、[+] モニター アイコンをクリックして、現在のモニター ディスプレイを使用することを確認します。

他のディスプレイを待機しています というメッセージが、現在のモニター ディスプレイに表示され、プライマリ ディスプレイの [マルチ モニター] ウィンドウにあるグレーのモニター アイコンが緑色に変わります。

8 セッションに使用するモニター ディスプレイを追加したら、[マルチ モニター] ウィンドウで [OK] をクリックします。

[マルチ モニター] ウィンドウが閉じて、プライマリではないモニターのディスプレイで **他のディスプレイを待機しています** というメッセージがクリアされ、リモート デスクトップ ウィンドウが表示されます。

9 マルチ ディスプレイ モードを終了するには、Esc キーを押して、[マルチ ディスプレイ モードの終了] ダイアログ ボックスで [はい] をクリックして、終了することを確認します。

注： リモート デスクトップで Esc キーを使用する必要がある場合は、毎回、サイドバー タブを開き、サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックし、[ESC の送信] を選択します。

リモート デスクトップと公開アプリケーションの画面解像度の設定

Horizon Administrator が適切な容量のビデオ RAM で構成されていると、HTML Access でリモート デスクトップのサイズをブラウザ ウィンドウのサイズに合わせて変更できます。ビデオ RAM (VRAM) のデフォルト設定は 36 MB で、3D アプリケーションを使用しなければ、最小要件の 16 MB を超える環境となります。

Retina ディスプレイの MacBook や Google Chromebook Pixel など、ピクセル密度解像度が高いブラウザや Chrome デバイスを使用している場合は、その解像度を使用するようにリモート デスクトップや公開アプリケーションを設定できます。[設定] ウィンドウで [高解像度モード] オプションをオンにします。このウィンドウには、サイドバーからアクセスできます。このオプションが [設定] ウィンドウに表示されるのは、高解像度ディスプレイを使用しているか、通常の画面を 100% を超えるスケールで使用している場合だけです。

高解像度モード機能では、アクティブなリモート セッションの解像度を変更できません。機能を有効にするには、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。

3D レンダリング機能を使用するには、それぞれのリモート デスクトップに十分な VRAM を割り当てる必要があります。

- vSphere 5.0 以降では、ソフトウェア アクセラレータによるグラフィック機能が利用できます。この機能により、Windows Aero テーマや Google Earth などの 3D アプリケーションを使用できます。この機能には、64MB ～ 128MB の VRAM が必要です。
- vSphere 5.1 以降で利用できる、ハードウェア アクセラレータによるグラフィック機能 (vSGA) によって、デザイン、モデリング、およびマルチメディア用の 3D アプリケーションを使用できます。この機能には、64MB ～ 512MB の VRAM が必要です。デフォルトは 96MB です。
- vSphere 5.5 以降で使用できる専用のハードウェア高速グラフィックス機能 (vDGA) は、ESXi ホスト上の単一の物理的な GPU（グラフィック処理ユニット）を単一の仮想マシン専用にするための機能です。この機能は、ハイエンドのハードウェア高速ワークステーション グラフィックスが必要な場合に使用します。この機能には、64MB ～ 512MB の VRAM が必要です。デフォルトは 96MB です。

3D レンダリングが有効である場合、モニターの最大数は 1 で、最大解像度は 3840 x 2160 です。

同様に、Retina ディスプレイの MacBook や Google Chromebook Pixel など、ピクセル密度解像度が高いブラウザやデバイスを使用している場合は、各リモート デスクトップに十分な VRAM を割り当てる必要があります。

重要： VMware Blast 表示プロトコルに必要な VRAM 容量の計算は、PCoIP 表示プロトコルに必要な VRAM の計算に類似しています。ガイドラインについては、『Horizon 7 アーキテクチャの計画』の「仮想デスクトップのメモリ要件の計算」を参照してください。

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。

DPI 同期を無効にすると、ディスプレイ スケーリングが使用されます。ディスプレイ スケーリング機能は、リモート デスクトップまたは公開アプリケーションを適切にスケーリングします。

解像度を手動で設定するときに、[高解像度モード] 設定を有効にできる場合があります。詳細については、リモート デスクトップと公開アプリケーションの画面解像度の設定を参照してください。

DPI 同期機能は、[DPI 同期] エージェント グループ ポリシー設定で有効または無効にします。この機能は、デフォルトで有効になっています。DPI 同期を使用すると、リモート デスクトップまたは公開アプリケーションに接続したときに、クライアント コンピュータの DPI 値に合わせてリモート セッションの DPI 値が変更されます。DPI 同期機能には、Horizon Agent 7.0.2 以降が必要です。

[DPI 同期] グループ ポリシー設定だけでなく、[接続ごとの DPI の同期] エージェント グループ ポリシー設定も有効にした場合、リモート デスクトップに再接続したときに DPI 同期がサポートされます。デフォルトでは、この機能は無効になっています。接続ごとの DPI の同期機能には、Horizon Agent 7.8 以降が必要です。

[DPI 同期] と [接続ごとの DPI の同期] 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 を参照してください。

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公開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

仮想デスクトップの場合、接続ごとの DPI の同期機能は次のゲスト OS に対応します。

- Windows 10 バージョン 1607 以降
- デスクトップとして構成されている Windows Server 2016 以降

接続ごとの DPI の同期機能は、公開デスクトップまたは公開アプリケーションでサポートされていません。

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 設定を変更しても、リモート デスクトップの DPI 設定が変わらない場合は、ログアウトしてから再度ログインして、クライアント システムの新しい DPI 設定を Horizon Client に認識させます。
- 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リモート セッションに再度ログインします。
- Windows 10 および Windows 8.x システムは異なるモニターで異なる DPI 設定をサポートしますが、HTML Access クライアント セッションの起動に使用された Web ブラウザがあるクライアント システムのモニターで設定された DPI 値が、DPI 同期機能で使用されます。HTML Access は、異なるモニターで異なる DPI 設定をサポートしません。

- 別の DPI 設定を使用して別のモニターと同期するには、リモート デスクトップまたは公開アプリケーションからログアウトし、HTML Access クライアント セッションの起動に使用された Web ブラウザを他のモニターにドラッグしてから、リモート デスクトップまたは公開アプリケーションに再ログインして、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の DPI 設定を一致させます。

全画面表示モードの使用

リモート デスクトップや公開アプリケーションを全画面表示モードで表示できます。

以下の状況では、全画面表示モードを使用できません。

- 複数のモニターを使用している。
- ブラウザが全画面表示モードで実行されているか、マウスのドラッグで最大化されている。
- Safari を使用している。

前提条件

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。

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全画面表示モードで表示するに、サイドバーの上部にある [メニューを開く] ボタンをクリックし、[全画面表示] をクリックします。
- 全画面表示モードを終了するに、サイドバーの上部にある [メニューを開く] ボタンをクリックし、[全画面表示モードを終了] をクリックします。

  または、クライアント システムのキーボードで Esc キーを押します。

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

リアルタイム オーディオビデオは、Chrome、Microsoft Edge、および Firefox でのみサポートされます。デフォルトのビデオ解像度は 320 x 240 ピクセルです。リアルタイム オーディオビデオのデフォルト設定は、ほとんどの Web カメラおよびオーディオ アプリケーションで適切に機能します。

リアルタイム オーディオビデオの設定変更の詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』の「リアルタイム オーディオ ビデオ グループ ポリシー設定の構成」を参照してください。

リモート デスクトップや公開アプリケーションがクライアント マシンの Web カメラやマイクに接続している場合、Web カメラやマイクがリモート デスクトップや公開アプリケーションで使用できるようになる前に、ブラウザから許可を求められる場合があります。この動作はブラウザによって異なります。

- Microsoft Edge は毎回許可を要求します。この動作は変更できません。詳細については、https://blogs.windows.com/msedgedev/2015/05/13/announcing-media-capture-functionality-in-microsoft-edge を参照してください。

- Firefox は毎回許可を要求してきます。この動作は変更できます。詳細については、https://support.mozilla.org/en-US/kb/permissions-manager-give-ability-store-passwords-set-cookies-more?redirectlocale=en-US&redirectslug=how-do-i-manage-website-permissions を参照してください。
- Chrome は、初回に許可を要求します。デバイスの使用を許可すると、Chrome は再度許可を要求しなくなります。

リモート デスクトップがクライアント マシンの Web カメラまたはマイクロフォンに接続されると、各デバイスのアイコンがサイド バーの上部に表示されます。サイドバーのデバイス アイコンの上に赤色のクエスチョン マークが表示され、許可が要求されていることが示されます。デバイスの使用を許可すると、赤色のクエスチョン マークは非表示になります。許可の要求を拒否すると、デバイスのアイコンが非表示になります。

リモート デスクトップや公開アプリケーションのセッションでリアルタイム オーディオビデオを使用しており、セカンド デスクトップや公開アプリケーションへの接続するときに、セキュリティの警告が表示される場合（たとえば、有効な証明書がインストールされていないなど）、この警告を無視して 2 番目のリモート デスクトップや公開アプリケーションへの接続を続行すると、最初のセッションでリアルタイム オーディオビデオの動作が停止します。

リモート デスクトップ セッションの共有

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。この方法で共有されているリモート デスクトップ セッションは、共同作業セッションといいます。別のユーザーとセッションを共有するユーザーは、セッション所有者といいます。共有セッションに参加するユーザーはセッション共同作業者といいます。

Horizon 管理者は、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。

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

セッション共同作業機能を使用する場合、E メールまたはインスタント メッセージ（Windows リモート デスクトップのみ）を送信するか、クリップボードにリンクをコピーしてユーザーに転送することで、ユーザーをリモート デスクトップ セッションに招待できます。

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。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。

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。
- 共有するリモート 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

- セッション共同作業機能を有効にして設定する必要があります。
- 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。

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。Windows リモート デスクトップの場合、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。

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、セッション共同作業のユーザー 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。セッション共同作業者が招待を受け入れ、Linux リモート デスクトップのセッションに参加すると、プライマリ セッション デスクトップに通知が表示されます。

次のステップ

[VMware Horizon Collaboration] ダイアログ ボックスで、リモート デスクトップ セッションを管理します。共有リモート デスクトップ セッションの管理を参照してください。

共有リモート デスクトップ 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、共有リモート デスクトップ セッション (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。

Horizon 管理者は、別のセッション共同作業者へのコントロールの移動を防ぐことができます。Windows リモート デスクトップの場合は、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 [共同作業者へのコントロールの移動を許可する] グループ ポリシー設定を参照してください。Linux リモート デスクトップの場合、Horizon 7 for Linux デスクトップのセットアップ ドキュメントの `collaboration.enableControlPassing` パラメータを参照してください。

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。

リモート デスクトップ セッションへの参加

セッション共同作業機能を使用すると、共同作業の招待状のリンクをクリックして、リモート デスクトップ セッションに参加することができます。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リモート デスクトップ 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。

セッション共同作業機能を使用してリモート デスクトップ セッションに参加する場合、リモート デスクトップ セッションで次の機能を使用することはできません。

- リアルタイム オーディオビデオ (RTAV)
- ロケーション ベースの印刷
- クリップボード リダイレクト

また、リモート デスクトップ セッションでリモート デスクトップの解像度を変更することはできません。

前提条件

セッション共同作業を使用してリモート デスクトップ 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、サイドバーの [閉じる] をクリックします。

テキストのコピーおよび貼り付け

クライアント デバイスのプレーン テキストと HTML 形式のリッチ テキストをコピーして、リモート デスクトップまたは公開アプリケーションに貼り付けることができます。Horizon 管理者は、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コピー アンド ペースト操作のみを許可する、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 システムへのコピー アンド ペースト操作のみを許可する、その両方を許可する、またはどちらも許可しないように、この機能を設定できます。

Horizon 管理者は、View Agent または Horizon Agent をリモート デスクトップに関連付けるグループ ポリシー設定を使用して、コピー アンド ペースト機能を設定できます。詳細については、HTML Access グループ ポリシー設定を参照してください。

リッチ テキストをコピーして貼り付ける場合、次の制限があります。

- イメージのコピー アンド ペーストはサポートされません。
- クライアント デバイスから WordPad アプリケーションにリッチ テキストをコピーすると、プレーン テキストのみがコピーされ、貼り付けられます。
- Internet Explorer (IE)、Microsoft Edge または Safari ブラウザで HTML Access を使用する場合、リッチ テキストのコピー アンド ペーストはサポートされません。[コピーおよび貼り付け] ウィンドウを使用する必要があります。コピー アンド ペースト ウィンドウの使用を参照してください。
- Horizon 管理者は、コピー アンド ペースト操作で、グループ ポリシー設定を使用してクリップボードの形式を制限できます。HTML Access では、クリップボード内のテキストの転送のみをサポートするため、HTML Access ではテキスト フィルタだけが動作します。クリップボードの形式フィルタ ポリシー設定については、『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。

Chrome または Firefox ブラウザで HTML Access を使用し、クリップボード機能を使用する場合は、次のヒントを参考にしてください。

- リモート デスクトップまたは公開アプリケーションに初めて接続した場合、[クリップボード ユーザー ガイド] ダイアログ ボックスが表示されます。ダイアログ ボックスを消去し、再び表示されないようにするには、[OK] をクリックします。

- デフォルトでは、サイドバーでクリップボードのアイコン が選択され、グレー表示されます。
  - クリップボードのアイコンが選択された状態で、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テキストをコピーすると、ローカル クライアント システムのクリップボードにテキストをコピーすることを確認するダイアログ ボックスが表示されます。[OK] をクリックします。
  - クリップボードのアイコ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からローカル クライアント システムのクリップボードにテキストをコピーするときに、確認のダイアログ ボックスは表示されません。
- サイドバーにあるクリップボードのアイコンの上にカーソルを置くと、クリップボード機能を説明するヒントが表示されます。

どのタイプのコピー アンド ペーストの操作でも、クリップボードは最大で 1 MB のデータを処理できます。プレーン テキストとリッチ テキスト 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。リッチ テキスト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、リッチ テキストが破棄されてプレーン テキストが貼り付けられます。1 回の操作では選択したフォーマット テキストすべてを貼り付けできない場合は、1 回の操作でコピー アンド ペーストを行うサイズを小さくする必要があります。

画像をコピーおよび貼り付けできません。リモート デスクトップとクライアント コンピュータのファイル システム間では、ファイルもコピー アンド ペーストできません。

注： iOS Safari と Android デバイスでは、コピー アンド ペースト機能がサポートされていません。

コピー アンド ペースト ウィンドウの使用

Internet Explorer (IE)、Microsoft Edge または Safari ブラウザでテキストをコピーして貼り付けるには、サイドバーの上部にある [コピーおよび貼り付け] ボタンを使用して [コピーおよび貼り付け] ウィンドウを表示します。

この手順では、[コピーおよび貼り付け] ウィンドウを使用して、クライアント システムの IE、Edge または Safari ブラウザからリモート デスクトップまたは公開アプリケーションにテキストをコピーしたり、リモート デスクトップのアプリケーションまたは公開アプリケーションからローカル クライアント システムにテキストをコピーする方法について説明します。

公開アプリケーション間またはリモート デスクトップ間でテキストのコピー アンド ペーストを行う場合は、通常と同じ操作でコピー アンド ペーストを実行できます。[コピーおよび貼り付け] ウィンドウを使用する必要はありません。

IE、Edge または Safari ブラウザを使用し、ローカル システムのクリップボードとリモート マシンのクリップボードを同期している場合にのみ、[コピーおよび貼り付け] ウィンドウが必要になります。

[コピーおよび貼り付け] ウィンドウには、コンテンツのコピー アンド ペーストが可能な方向を示す次のいずれかのメッセージが表示されます。

- このパネルを使用して、ローカルのクライアントとリモートデスクトップ/アプリケーション間にコピーおよび貼り付けします。
- このパネルを使用して、ローカルのクライアントからリモートデスクトップ/アプリケーションにコピーおよび貼り付けします。

- このパネルを使用して、リモートデスクトップ/アプリケーションからローカルのクライアントにコピーおよび貼り付けします。

注： デフォルトのクリップボード リダイレクト グループ ポリシー設定を使用すると、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貼り付けのみが許可されます。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 システムへのコピーを許可するには、両方向でグループ ポリシー設定を有効にする必要があります。

前提条件

Mac を使用している場合、キーの組み合わせを使用して、テキストを選択、コピー、および貼り付ける際に、Command キーを Windows の Ctrl キーにマッピングする設定を有効にしていることを確認します。サイドバーにある [[設定] ウィンドウを開く] ツールバー ボタンをクリックして、[Command + A、Command + C、Command + V、および Command + X を有効にする] をオンにします Mac の場合、このオプションは [設定] ウィンドウでのみ表示されます。

Horizon 管理者は、クライアント システムからリモート デスクトップと公開アプリケーションへのコピー アンド ペーストをユーザーに許可するデフォルトのポリシーをそのまま使用するか、コピー アンド ペーストを許可する別のポリシーを設定する必要があります。詳細については、HTML Access グループ ポリシー設定を参照してください。

手順

- 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、またはクライアント システムから公開アプリケーションにテキストをコピーするには、次の手順を実行します。
  a. ローカル クライアント アプリケーションでテキストをコピーします。
  b. HTML Access でサイドバーを開き、サイドバーの上部にある [コピーおよび貼り付け] をクリックします。

     [コピーおよび貼り付け] ウィンドウが表示されます。以前にコピーしたテキストがすでにウィンドウに表示されている場合、新しくコピーされたテキストを貼り付けると、そのテキストは置換されます。
  c. [コピーおよび貼り付け] ウィンドウにテキストを貼り付けるには、Ctrl+V キー（Windows の場合）または Command-V キー（Mac の場合）を押します。

     「リモート クリップボードが同期されました」というメッセージが一時的に表示されます。
  d. テキストを貼り付けるアプリケーション内の場所をクリックして、Ctrl + V キーを押します。

     テキストがアプリケーションに貼り付けされます。
- リモート デスクトップのアプリケーションからクライアント システム、または公開アプリケーションからクライアント システムにテキストをコピーするには、次の手順を実行します。
  a. アプリケーションでテキストをコピーします。
  b. HTML Access でサイドバーを開き、サイドバーの上部にある [コピーおよび貼り付け] をクリックします。

     [コピーおよび貼り付け] ウィンドウが開き、貼り付けたテキストが表示されます。「リモート クリップボードが同期されました」というメッセージが一時的に表示されます。

c テキストをもう一度コピーするには、[コピーおよび貼り付け] ウィンドウをクリックし、Ctrl+C キー（Windows の場合）または Command-C キー（Mac の場合）を押します。

このアクションを実行するとテキストは選択されず、テキストを選択することはできません。「クリップボード パネルからコピーされました」というメッセージが一時的に表示されます。

d クライアント システムで、テキストを貼り付ける場所をクリックして、Ctrl + V キーを押します。

テキストは、クライアント システムのアプリケーションに貼り付けられます。

リモート デスクトップまたは公開アプリケーションとクライアントの間でのファイルの転送

ファイル転送機能を使用すると、リモート デスクトップまたは公開アプリケーションとクライアント システムの間でファイルを転送できます。

Horizon 管理者は、VMware Blast の [ファイル転送を設定] グループ ポリシー設定を変更することにより、ファイルの転送を許可、禁止、または一方向のみ許可するように設定できます。このグループ ポリシー設定の値は次のとおりです。

- [アップロードとダウンロードの両方を無効にする] が選択されていると、[ファイルの転送] ボタンが無効になります。
- [ファイルのアップロードのみを有効にする] が選択されていると（デフォルトの設定）、[ファイルの転送] ウィンドウに [アップロード] タブのみが表示されます。
- [ファイルのダウンロードのみを有効にする] が選択されている場合、[ファイルの転送] ウィンドウに [ダウンロード] タブのみが表示されます。

サーバからクライアントの方向で [クリップボード リダイレクトの設定] グループ ポリシー設定が無効になっている場合、ファイルのダウンロードも無効になります。

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』を参照してください。

この機能には次の制限があります。

- ダウンロードできるファイルは最大で 500 MB までです。アップロードできるファイルは最大で 2 GB までです。
- 32 ビット Internet Explorer 11 の場合、300 MB より大きなファイルのダウンロードは機能しない場合があります。この問題を解決するには、Internet Explorer 11 を 64 ビット モードで 実行します。
- フォルダまたはサイズがゼロのファイルのダウンロードまたはアップロードはできません。
- iOS の Safari と Safari 8 では、アップロードもダウンロードもサポートしていません。Safari 9 以降では、ダウンロードをサポートしていません。
- リモート セッションでファイルを転送中に、別のリモート セッションとの接続を試みてセキュリティ警告が表示されたときに、この警告を無視してリモート セッションとの接続を続行すると、最初のセッションで実行中のファイル転送が中止されます。

- Internet Explorer 11 または Chromebook の Chrome でファイルをアップロードするときに、フォルダ、サイズがゼロのファイル、または 2 GB より大きいファイルのドラッグ アンド ドロップを行うと、予期したとおりエラー メッセージが表示されます。エラー メッセージを閉じた後は、転送可能なファイルのドラッグ アンド ドロップはできません。
- Linux リモート デスクトップまたは Android デバイスでは、この機能を使用できません。

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 システムへのファイルのダウンロード

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 システムにファイルをダウンロードできます。

Horizon 管理者は、この機能を無効にできます。詳細については、リモート デスクトップまたは公開アプリケーションとクライアントの間でのファイルの転送を参照してください。

手順

1 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。

2 サイドバーを表示するには、サイドバーのタブをクリックします。

3 サイドバーの上部にあるファイル転送アイコン をクリックします。

[ファイルの転送] ウィンドウが開きます。

4 [ファイルの転送] ウィンドウで [ダウンロード] をクリックします。

5 ダウンロードするファイルを 1 つ以上選択します。

6 ファイルの転送を開始するには、Ctrl+c キーを押します。

[ファイルの転送] ウィンドウの [ダウンロード] タブにファイルが表示されます。

7 ダウンロード アイコン（下矢印）をクリックして、クライアント システムにファイルをダウンロードします。

クライアント システムの Downloads フォルダにファイルが表示されます。

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ファイルのアップロード

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ファイルをアップロードできます。

Horizon 管理者は、この機能を無効にできます。詳細については、リモート デスクトップまたは公開アプリケーションとクライアントの間でのファイルの転送を参照してください。

手順

1 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。

2 サイドバーを表示するには、サイドバーのタブをクリックします。

3 サイドバーの上部にあるファイル転送アイコン をクリックします。

[ファイルの転送] ウィンドウが開きます。

4 ファイルをアップロードするには、ファイルをドラッグして [ファイルの転送] ウィンドウの [アップロード] タブにドロップします。あるいは、[アップロード] タブの [ファイルの選択] をクリックして、アップロードするファイルを選択します。

アップロードされたファイルが `Documents` フォルダに表示されます。

異なるクライアント デバイスでの公開アプリケーションの複数のセッションの使用

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 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にある [設定] ツールバー ボタンをクリックします。[マルチ起動] 設定までスクロールし、[設定] 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以前に開始した場合は、サイドバーにある [メニューを開く] ボタンをクリックし、[設定] をクリックして [マルチ起動] 設定までスクロールします。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] 設定はグレーアウトされます。

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。

音声

リモート デスクトップおよび公開アプリケーションで音声を再生できますが、いくつか制限があります。

デフォルトでは、リモート デスクトップおよびアプリケーションでの音声の再生が有効になっていますが、Horizon 管理者がポリシーを設定することで、音声の再生を無効にできます。

リモート デスクトップや公開アプリケーションで音声を再生するときに、次の制限が適用されます。

- 音量を上げるには、リモート デスクトップのサウンド コントロールではなく、クライアント システムのサウンド コントロールを使用します。
- 時々、音声がビデオと同期しなくなることがあります。
- ネットワーク トラフィックが集中していたり、ブラウザが大量のタスクを実行していると、音質が低下することがあります。使用するブラウザを変えると改善されることがあります。

ショートカット キーの組み合わせ

使用する言語に関係なく、一部のキーの組み合わせはリモート デスクトップまたは公開アプリケーションに送信できません。

Web ブラウザによって、一部のキーおよびキーの組み合わせをクライアント システムおよび送付先システムの両方に送信することができます。他のキーおよびキーの組み合わせについては、ローカルでの入力だけが処理され、送付先システムには送信されません。システムで動作するキーの組み合わせは、ブラウザ ソフトウェア、クライアント オペレーティング システム、および言語設定によって異なります。

注： Mac を使用している場合、キーの組み合わせを使用して、テキストを選択、コピー、および貼り付ける場合に、Command キーを Windows の Ctrl キーにマッピングできます。この機能を有効にするには、サイドバーにある [[設定] ウィンドウを開く] ツールバー ボタンをクリックして、[コマンド A、コマンド C、コマンド V、およびコマンド X を有効にする] をオンにします。このオプションは、Mac クライアント システムを使用している場合にのみ [設定] ウィンドウに表示されます。

以下のキーおよびキーの組み合わせは、リモート デスクトップで動作しない場合があります。

- Ctrl + T
- Ctrl + W
- Ctrl + N
- コマンド キー
- Alt + Enter
- Ctrl + Alt + *任意のキー*

  重要： Ctrl + Alt + Del キーを入力するには、サイドバーの先頭にある [Ctrl+Alt+Delete を送信] ツールバー ボタンを使用します。

- Caps Lock + *modifier_key* (Alt または Shift など)
- Chromebook のファンクション キー

- Windows キーの組み合わせ

リモート デスクトップで Windows キーを有効にした場合、リモート デスクトップで次の Windows キーの組み合わせが動作します。この機能を有効にするには、サイドバーにある [[設定] ウィンドウを開く] ツールバー ボタンをクリックして、[デスクトップで Windows キーを有効にします] をオンにします。

重要： [デスクトップで Windows キーを有効にします] をオンにした後は、Ctrl + Win キー（Windows システム）、Ctrl + Command キー (Mac)、または Ctrl + Search キー (Chromebook) を押して Windows キーの押下をシミュレーションします。

これらのキーの組み合わせは、公開アプリケーションで動作しません。これらのキーの組み合わせは、Windows Server 2008 R2、Windows Server 2012 R2、Windows Server 2016 のリモート デスクトップと公開デスクトップで動作します。

Windows 8.x や Windows Server 2012 R2 オペレーティング システムのリモート デスクトップで動作するいくつかのキーの組み合わせは、Windows 7、Windows Server 2008 R2、または Windows 10 オペレーティング システムのリモート デスクトップでは動作しません。

表 4-4. Windows 10 リモート デスクトップと Windows Server 2016 リモート デスクトップの Windows キー ショートカット

キー	アクション	制限
Win	スタートを開くまたは閉じます。	
Win + A	アクション センターを開きます。	
Win + E	ファイル エクスプローラーを開きます。	
Win + G	ゲームが開いているときに、ゲーム バーを開きます。	
Win + H	[共有] チャームを開きます。	
Win + I	[設定] チャームを開きます。	
Win + K	[接続] クイック アクションを開きます。	
Win + M	すべてのウィンドウを最小化します。	
Win + R	[ファイル名を指定して実行] ダイアログ ボックスを開きます。	
Win + S	[検索] を開きます。	
Win + X	[クイック リンク] メニューを開きます。	
Win + ,（カンマ）	リモート デスクトップを一時的に表示します。	
Win + Pause	[システム プロパティ] ダイアログ ボックスを表示します。	Chromebooks や Mac には Pause キーはありません。
Win + Shift + M	リモート デスクトップで最小化されたウィンドウを元に戻します。	Safari では動作しません。
Win + Alt + 数字キー	リモート デスクトップを開いて、数字で示す位置にタスクバーでピン留めされているアプリケーションのジャンプ リストを開きます。	Chromebook では動作しません。
Win + Enter	ナレーターを開きます。	

表 4-5. Windows 8.x および Windows Server 2012 R2 リモート デスクトップの Windows キー ショートカット

キー	アクション	制限
Win + F1	Windows ヘルプとサポートを開きます。	Safari では動作しません。
Win	[スタート] ウィンドウを表示または非表示にします。	
Win + B	通知領域にフォーカスを設定します。	
Win + C	チャーム パネルを開きます。	
Win + D	リモート デスクトップを表示または非表示にします。	Safari では動作しません。Mac で Command-D キーを押します。
Win + E	ファイル エクスプローラーを開きます。	
Win + H	[共有] チャームを開きます。	
Win + I	[設定] チャームを開きます。	
Win + K	[デバイス] チャームを開きます。	
Win + M	すべてのウィンドウを最小化します。	
Win + Q	アプリケーションの検索がサポートされている場合、開いているアプリ内または任意の場所を検索するため、[検索] チャームを開きます。	
Win + R	[ファイル名を指定して実行] ダイアログ ボックスを開きます。	
Win + S	Windows と Web を検索するため、[検索] チャームを開きます。	
Win + X	[クイック リンク] メニューを開きます。	
Win + Z	アプリケーションで利用可能なコマンドを表示します。	
Win + ,（カンマ）	このキーの組み合わせを押し続けている限り、リモート デスクトップを一時的に表示します。	Windows 2012 R2 オペレーティング システムでは動作しません。
Win + Pause	[システム プロパティ] ダイアログ ボックスを表示します。	Chromebook と Mac には Pause キーがありません。
Win + Shift + M	リモート デスクトップで最小化されたウィンドウを元に戻します。	Safari では動作しません。Mac で Command-D キーを押します。
Win + Alt + 数字キー	リモート デスクトップを開いて、数字で示す位置にタスクバーでピン留めされているアプリケーションのジャンプ リストを開きます。	Chromebook では動作しません。
Win + 上向き矢印	ウィンドウを最大化します。	Chromebook では動作しません。
Win + 下向き矢印	画面から現在のアプリケーションを削除するか、リモート デスクトップのウィンドウを最小化します。	Chromebook では動作しません。
Win + 左向き矢印	アプリケーションまたはリモート デスクトップのウィンドウを画面の左側で最大化します。	Chromebook では動作しません。
Win + 右向き矢印	アプリケーションまたはリモート デスクトップのウィンドウを画面の右側で最大化します。	Chromebook では動作しません。
Win + Home	アクティブなリモート デスクトップのウィンドウ以外のすべてのウィンドウを最小化します（Win + Home キーをもう一度押すとすべてのウィンドウが元に戻ります）。	Safari ブラウザでは動作しません。
Win + Shift + 上向き矢印	リモート デスクトップのウィンドウを画面の上下にまで拡大します。	Chromebook では動作しません。

表 4-5. Windows 8.x および Windows Server 2012 R2 リモート デスクトップの Windows キー ショートカット（続き）

キー	アクション	制限
Win + Shift + 下向き矢印	Win + Shift + 上向き矢印キーを押した後に、幅を維持しながらリモート デスクトップのウィンドウの縦幅を元に戻します。または、アクティブなデスクトップ ウィンドウを最小化します。	Chromebook では動作しません。
Win + Enter	ナレーターを開きます。	

表 4-6. Windows 7 および Windows Server 2008 R2 リモート デスクトップの Windows キー ショートカット

キー	アクション	制限
Win	[スタート] メニューを開くまたは閉じます。	
Win + Pause	[システム プロパティ] ダイアログ ボックスを表示します。	Chromebook と Mac には Pause キーがありません。
Win + D	リモート デスクトップを表示または非表示にします。	Safari では動作しません。Mac で Command-D キーを押します。
Win + M	すべてのウィンドウを最小化します。	
Win + E	`Computer` フォルダを開きます。	
Win + R	[ファイル名を指定して実行] ダイアログ ボックスを開きます。	
Win + 上向き矢印	ウィンドウを最大化します。	Chromebook では動作しません。
Win + 下向き矢印	ウィンドウを最小化します。	Chromebook では動作しません。
Win + 左向き矢印	アプリケーションまたはリモート デスクトップのウィンドウを左側で最大化します。	Chromebook では動作しません。
Win + 右向き矢印	アプリケーションまたはリモート デスクトップのウィンドウを右側で最大化します。	Chromebook では動作しません。
Win + Home	アクティブなリモート デスクトップのウィンドウを除くすべてのウィンドウを最小化します。	Safari では動作しません。
Win + Shift + 上向き矢印	リモート デスクトップのウィンドウを画面の上下にまで拡大します。	Chromebook では動作しません。
Win + G	実行中のリモート デストップ ガジェットを順に切り換えます。	
Win + U	[コンピューターの簡単操作センター] を開きます。	

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。

クライアント システム、ブラウザ、およびリモート デスクトップで使用する必要がある言語パックについての詳細は、国際キーボードを参照してください。

国際キーボード

英語以外のキーボードとロケールを使用している場合、クライアント システム、ブラウザおよびリモート デスクトップで特定の設定を使用する必要があります。一部の言語では、リモート デスクトップで IME (Input Method Editor) を使用する必要があります。

ローカル設定とインプット メソッドを正しくインストールすれば、以下の言語で文字を入力できます：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。

表 4-7. 必要な入力言語設定

言語	ローカル クライアント システムの入力言語	ローカル クライアント システムで IME が必要かどうか	リモート デスクトップのブラウザと入力言語	リモート デスクトップで IME は必要か
英語	英語	いいえ	英語	いいえ
フランス語	フランス語	いいえ	フランス語	いいえ
ドイツ語	ドイツ語	いいえ	ドイツ語	いいえ
簡体中国語	簡体中国語	英語入力モード	簡体中国語	はい
繁体中国語	繁体中国語	英語入力モード	繁体中国語	はい
日本語	日本語	英語入力モード	日本語	はい
韓国語	韓国語	英語入力モード	韓国語	はい
スペイン語	スペイン語	いいえ	スペイン語	いいえ

Horizon Client のトラブルシューティング

5

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。

手順

- [再起動] コマンドを使用します。

オプション	アクション
サイドバーから	リモート デスクトップに接続しているときに、サイドバーの [実行中] リストにあるリモート デスクトップ名の横の [メニューを開く] ツールバー ボタンをクリックして、[再起動] を選択します。
URI の使用	デスクトップを再起動するには、URI `https://ConnectionServerFQDN?desktopId=desktop_name&action=restart` を使用します。

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。

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、開いているすべてのアプリケーションが終了します。

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

- [リセット] コマンドを使用します。

オプション	アクション
アプリケーションの選択ウィンドウから公開アプリケーションをリセットする	リモート デスクトップや公開アプリケーションに接続する前に、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、実行中のすべての公開アプリケーションをリセットするには、画面の右上にある [設定] ツールバー ボタンをクリックして、[リセット] をクリックします。
サイドバーからリモート デスクトップをリセットする	リモート デスクトップに接続しているときに、サイドバーの [実行中] リストにあるデスクトップ名の横の [メニューを開く] ツールバー ボタンをクリックして、[リセット] を選択します。
サイドバーから公開アプリケーションをリセットする	実行中のすべてのアプリケーションをリセットするには、サイドバーの上部にある [[設定] ウィンドウを開く] ツールバー ボタンをクリックして、[リセット] をクリックします。
URI を使用したリモート デスクトップのリセット	リモート デスクトップをリセットするには、URI `https://`*`ConnectionServerFQDN`*`?desktopId=`*`desktop_name`*`&action=reset` を使用します。

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。