

HTML Access の使用

VMware Horizon HTML Access 4.5
VMware Horizon 7 7.2



vmware®

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>) でご確認ください。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

ヴァ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

Copyright © 2013 年～ 2017 年 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

HTML Access の使用 5

1 セットアップとインストール 6

- HTML Access のシステム要件 6
- HTML Access のための接続サーバおよびセキュリティ サーバの準備 8
 - HTML Access のファイアウォール ルール 9
- キャッシュから認証情報を削除するための View の構成 10
- HTML Access のためのデスクトップ、プール、およびファームを準備する 11
- HTML Access Agent を構成して新しい SSL 証明書を使用 12
 - View デスクトップの MMC に証明書スナップインを追加する 13
 - HTML Access Agent の証明書を Windows 証明書ストアにインポート 14
 - HTML Access Agent のルート証明書と中間証明書のインポート 15
 - Windows レジストリへの証明書のサムプリントを設定する 16
- 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 16
- iOS で CA 署名証明書の使用を構成 17
- HTML Access ソフトウェアのアップグレード 17
- View 接続サーバからの HTML Access のアンインストール 18
- VMware によって収集されるデータ 18

2 エンド ユーザー用に HTML Access を構成 20

- エンド ユーザー用の VMware Horizon Web ポータル ページの構成 20
- URI を使用した HTML Access Web Client の構成 24
 - HTML Access の URI を作成するための構文 24
 - URI の例 27
- HTML Access グループ ポリシー設定 29

3 リモート デスクトップまたはアプリケーションの使用 30

- 機能サポート一覧 31
- 国際化 32
- 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 32
 - 自己署名付ルート証明書の信頼 34
- Workspace ONE モードでのサーバへの接続 35
- リモート アプリケーションへの接続での非認証アクセスの使用 35
- ショートカット キーの組み合わせ 36
- 国際キーボード 40
- スクリーン解像度 40
- H.264 デコード 41
- タイム ゾーンの設定 41

サイドバーの使用	42
複数のモニターの使用	45
DPI 同期の使用	46
音声	47
テキストのコピーおよび貼り付け	48
コピーおよび貼り付け機能の使用	48
クライアントとリモート デスクトップ間でのファイルの転送	50
デスクトップからクライアントにファイルをダウンロード	50
クライアントからデスクトップへファイルのアップロード	51
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	51
ログオフまたは切断	52
リモート デスクトップまたはリモート アプリケーションのリセット	53
リモート デスクトップの再起動	54

HTML Access の使用

本『HTML Access の使用』ガイドでは、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ために VMware Horizon™ 7 の HTML Access 機能をインストールして使用方法について説明します。

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、View 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、View 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。View に慣れていないユーザーである場合、『View のインストール』および『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。

セットアップとインストール

HTML Access 用の View 環境のセットアップでは、View 接続サーバでの HTML Access をインストールし、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、View 接続サーバの 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 のための接続サーバおよびセキュリティ サーバの準備](#)
- [キャッシュから認証情報を削除するための View の構成](#)
- [HTML Access のためのデスクトップ、プール、およびファームを準備する](#)
- [HTML Access Agent を構成して新しい SSL 証明書を使用](#)
- [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](#)
- [iOS で CA 署名証明書の使用を構成](#)
- [HTML Access ソフトウェアのアップグレード](#)
- [View 接続サーバからの HTML Access のアンインストール](#)
- [VMware によって収集されるデータ](#)

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。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。

注: バージョン 7.0 から、View Agent が Horizon Agent という名前に変更されました。

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	57、58
Internet Explorer	11
Safari	9、10
モバイル デバイスの Safari	iOS 9、iOS 10

ブラウザ	バージョン
Firefox	52、53
Microsoft Edge	38、40

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)
Windows	8.x (32 ビットおよび 64 ビット)
Windows	10 (32 ビットおよび 64 ビット)
Mac OS X	10.11 (El Capitan)
macOS	10.12.x (Sierra)
iOS	9
iOS	10
Chrome OS	28.x 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 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『View 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」トピックを参照してください。

プールの設定

HTML Access では、Horizon Administrator で以下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] 以上にすることが必要のため、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、[スクリーン解像度](#) 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、[HTML Access のためのデスクトップ、プール、およびファームを準備する](#)を参照してください。

接続サーバ

接続サーバと 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 接続サーバ (Blast-In)] ルールが有効になります。

セキュリティ サーバ

接続サーバ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: 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、接続サーバ 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。

HTML Access のための接続サーバおよびセキュリティ サーバの準備

エンド ユーザーが Web ブラウザを使用してリモート デスクトップに接続できるようにするには、管理者が特定のタスクを実行する必要があります。

エンド ユーザーが接続サーバまたはセキュリティ サーバに接続してリモート デスクトップにアクセスできるようにするためには、HTML Access コンポーネントとともに接続サーバをインストールし、セキュリティ サーバをインストールする必要があります。

以下は、HTML Access を使用するために管理者が実行する必要がある作業のチェックリストです。

- 1 接続サーバの複製されたグループを構成するサーバに、HTML Access オプションを使用して接続サーバをインストールします。

デフォルトでは、インストーラで HTML Access コンポーネントがすでに選択されています。インストールの説明については、『View のインストール』を参照してください。

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 View HTML Access を探してください。

- 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。

インストールの説明については、『View のインストール』を参照してください。

重要: セキュリティ サーバのバージョンは、接続サーバのバージョンと一致している必要があります。

- 3 それぞれの接続サーバ インスタンスまたはセキュリティ サーバが、ユーザーが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セキュリティ 証明書を持つことを確認します。

詳細については、『View 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、接続サーバでこの機能が有効であることを確認してください。

詳細については、『View 管理ガイド』の 2 要素認証についてのトピックを参照してください。

重要: [クライアントのユーザー インターフェイスでドメイン リストを非表示] 設定を有効にしており、接続サーバインスタンスで 2 要素認証 (RSA SecureID または RADIUS) を選択している場合、Windows ユーザー名の一致を強制しないでください。Windows ユーザー名の一致を強制すると、ユーザーはユーザー名のテキストボックスにドメイン情報を入力できなくなり、ログインが常に失敗するようになります。詳細については、『VMware View 管理者ガイド』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 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 サーバおよび接続サーバのホストで 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 TCP ポート 22443 に (View 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、[HTML Access のファイアウォール ルール](#)を参照してください。
- 6 ユーザーが認証しなくても Horizon Client で公開されたアプリケーションにアクセスできるようにするには、接続サーバでこの機能を有効にする必要があります。詳細については、『View 管理』の非認証アクセスについてのトピックを参照してください。

サーバのインストール後に Horizon Administrator を確認すると、該当する接続サーバ インスタンスおよびセキュリティ サーバで [Blast Secure Gateway] 設定が有効になっていることがわかります。また、該当する接続サーバ インスタンスおよびセキュリティ サーバで Blast Secure Gateway 用に使用するように [Blast 外部 URL] 設定が自動的に構成されています。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 システムがこの接続サーバ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、『View のインストール』の「接続サーバ 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接続サーバ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。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、『View 管理』を参照してください。

HTML Access のファイアウォール ルール

クライアント Web ブラウザが HTML Access を使用してセキュリティ サーバ、View 接続サーバ インスタンス、およびリモート デスクトップに接続できるようにするには、ファイアウォールが特定の TCP ポートのインバウンド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、View 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自動的に構成するため、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. HTML Access 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 View 接続サーバーインスタンス	TCP 443	Horizon 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 Horizon 接続サーバー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 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。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 Horizon 接続サーバー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 が有効にされ、ユーザーがリモート 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。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 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。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 View の構成

View を構成して、リモート デスクトップやアプリケーションに接続するタブや、HTML Access クライアントのデスクトップとアプリケーションの選択ページに接続するタブをユーザーが閉じるときに、キャッシュからユーザーの認証情報を削除できます。

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

この機能を使用するには、Horizon 7 バージョン 7.0.2 以降が必要となります。

手順

- 1 Horizon Administrator で、[View 構成] - [グローバル設定] を選択し、[全般] ペインで [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 [OK] をクリックして変更を保存します。

変更は直ちに有効になります。接続サーバの再起動は不要です。

HTML Access のためのデスクトップ、プール、およびファームを準備する

エンド ユーザーがリモート デスクトップや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、データセンターのリモート デスクトップ仮想マシンおよび 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

- vSphere インフラストラクチャと Horizon コンポーネントが HTML Access のシステム要件を満たすことを確認してください。

[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接続サーバにインストールされていること、および接続サーバ 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。

[HTML Access のための接続サーバおよびセキュリティ 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 Horizon デスクトップの TCP ポート 22443 にインバウンドトラフィックを許可するためのルールを設定します。
- デスクトップ ソースまたは RDS ホストとして使用する予定の仮想マシンにサポートされている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。

サポートされているオペレーティングシステムの一覧については、[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。『View でのデスクトップとアプリケーションの設定』のプールおよびファームの作成についてのトピックを参照してください。
- エンド ユーザーがリモート デスクトップや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 ソフトウェアがインストールされていることを確認します。ブラウザから接続を試みる前に Horizon Client ソフトウェアを使用して接続試験を行います。

Horizon Client のインストール手順については、https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html の Horizon Client のマニュアル サイトを参照してください。

- リモート デスクトップ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 RDS デスクトップとアプリケーションについては、Horizon Administrator 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 シングルセッションのデスクトップ プールについては、プールを HTML Access で使用できるように Horizon Administrator 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。

RDS デスクトップ プールを作成するときには、[HTML Access] 設定は [デスクトップ プールの追加] ウィザードに表示されません。代わりに、RDS ホストのファームを作成または編集するときに、[このファームのデスクトップへの HTML Access を許可] オプションを有効にします。

- 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 で [HTML Access] オプションを使用するようにプールが作成、再構成、またはアップグレードされたら、Horizon Client を使用して、デスクトップまたはアプリケーションにログインします。

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、接続サービインスタンスを指定する URL を入力します。

例：

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

URL では必ず **https** を使用してください。

- 5 表示される Web ページで、Horizon Client ソフトウェア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、オペレーティング システムに Horizon Client ソフトウェアがインストールされていないとき、またはインストールできないクライアント デバイスを使用しているときに、Web ブラウザからリモート 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 Blast エージェントによる証明機関からの SSL 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 [HTML Access Agent を構成して新しい SSL 証明書を使用](#) を参照してください。

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。

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 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: 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 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的な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 View デスクトップの MMC に証明書スナップインを追加する

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

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

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デスクトップでこの手順を実行する必要があります。

View デスクトップの MMC に証明書スナップインを追加する

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

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 View 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 の証明書を Windows 証明書ストアにインポート](#) 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。

前提条件

- 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。 [View デスクトップの MMC に証明書スナップインを追加する](#) を参照してください。

手順

- 1 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 キーを証明書の拇印で構成します。 [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 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。

次のステップ

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 の証明書を Windows 証明書ストアにインポート](#)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 View デスクトップの MMC ウィンドウでは、[証明書 (ローカル コンピュータ)] - [個人] - [証明書] フォルダに移動します。
- 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、View 接続サーバまたは 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、証明機関 (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、『View 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 iOS 版 Horizon Client を構成する」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

HTML Access のほとんどのバージョンのアップグレードでは、接続サーバと View Agent のアップグレードだけが行われます。

HTML Access をアップグレードするときは、View 接続サーバの対応するバージョンが、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。

View 接続サーバからの HTML Access 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 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 プログラム 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

ベアのセキュリティ 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、すべてのベアのセキュリティ 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。

VMware によって収集されるデータ

所属する企業がカスタマ エクスペリエンス改善プログラムに参加している場合、VMware はクライアントの特定フィールドのデータを収集します。機密情報が含まれるフィールドは、匿名扱いとなります。

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 管理者がカスタマ エクスペリエンス改善プログラムへの参加を決めた場合、VMware はお客様のご要望に対する VMware の対応を改善する目的で、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接続サーバに送信され、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。

VMware カスタマ エクスペリエンス改善プログラムに参加するには、接続サーバ をインストールする管理者が接続サーバインストール 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 Administrator でオプションを設定します。

表 1-2. カスタマ エクスペリエンス改善プログラムのために収集されたクライアント 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	<クライアント-ベンダー>	いいえ	VMware
製品名	<クライアント-製品>	いいえ	VMware Horizon HTML Access
クライアント製品のバージョン	<クライアント-バージョン>	いいえ	4.5.0-build_number

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
クライアントのバイナリ アーキテクチャ	<クライアント-アーキテクチャ>	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	<ブラウザ-アーキテクチャ>	いいえ	以下のような値があります。 ■ Win32 ■ Win64 ■ MacIntel ■ iPad
ブラウザ ユーザー エージェント文字列	<ブラウザ-ユーザー-エージェント>	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	<ブラウザ-バージョン>	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	<ブラウザ-コア>	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	<ブラウザ-は-ハンドヘルド>	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
- URI を使用した HTML Access Web Client の構成
- HTML Access グループ ポリシー設定

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/
pckbpdplfajmgaip1jfamclkinbjdnma
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。

重要: View 接続サーバ 5.x 以前のリリースからのアップグレードで HTML Access コンポーネントをインストールしておらず、Horizon Client ダウンロード用の社内サーバを指定するポータル ページを編集してある場合、これらのカスタマイズは View 接続サーバ 6.0 以降をインストールすると非表示になることがあります。Horizon 6 以降では、HTML Access コンポーネントが View 接続サーバのアップグレード時に自動的にインストールされます。

View 5.x 用に別途 HTML Access コンポーネントをインストールした場合は、Web ページに行ったカスタマイズはすべて保持されています。HTML Access コンポーネントをインストールしなかった場合、カスタマイズはすべて非表示になります。以前のリリース用のカスタマイズは、使用されなくなった portal-links.properties ファイルに入っています。

手順

- 1 View 接続サーバ 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 View 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	<code>enable.webclient=false</code> このオプションが <code>false</code> に設定されているにもかかわらず <code>enable.download</code> オプションが <code>true</code> 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 <code>false</code> に設定されていると、次のメッセージが表示されます。「この接続サーバ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	<code>enable.download=false</code> このオプションが <code>false</code> に設定されているにもかかわらず <code>enable.webclient</code> オプションが <code>true</code> 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 <code>false</code> に設定されていると、次のメッセージが表示されます。「この接続サーバ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	<code>link.download=https:// url-of-web-server</code> 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	<p>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 View 接続サーバの 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。</p> <ul style="list-style-type: none"> ■ 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 : <pre>link.download=https://server/downloads</pre> ■ 32 ビット Windows インストーラ : <pre>link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe</pre> ■ 64 ビット Windows インストーラ : <pre>link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe</pre> ■ Windows Phone インストーラ : <pre>link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx</pre> ■ 32 ビット Linux インストーラ : <pre>link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle</pre> ■ 64 ビット Linux インストーラ : <pre>link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle</pre> ■ Mac OS X インストーラ : <pre>link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg</pre> ■ iOS インストーラ: <pre>link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa</pre> ■ Android インストーラ : <pre>link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk</pre> ■ Chrome OS インストーラ : <pre>link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-build#.apk</pre>
ログイン ページの [ヘルプ] リンクの URL を変更します。	<pre>link.help</pre> <p>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。</p>

- 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、View 接続サーバホストの `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 View 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 ページや電子メールでは、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、View 接続サーバに接続したり、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。

- View 接続サーバのアドレス
- View 接続サーバのポート番号
- Active Directory ユーザー名
- Active Directory ユーザー名と異なる場合、RADIUS または RSA SecurID ユーザー名
- ドメイン名
- 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

構文には、サーバを指定するためのパス部分、また必要に応じて、ユーザー、デスクトップまたはアプリケーション、およびアクションまたは構成オプションを指定するためのクエリが含まれます。

URI 仕様

以下の構文を使用して HTML Access Web Client を起動するための 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ます。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 Web client 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『VMware Horizon Client の使用』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デスクトップおよび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、デスクトップまたはアプリケーションを指定する必要はありません。
start-session	指定したデスクトップまたは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、デスクトップまたは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。

値	説明
reset	指定した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、アプリケーションに有効ではありません。
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、アプリケーションに有効ではありません。
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 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、アプリケーションに有効ではありません。

applicationId アプリケーション表示名。この表示名は、アプリケーション プールの作成時に Horizon Administrator で指定した名前です。表示名にスペースが含まれている場合、ブラウザは **%20** を使用してスペースを表します。

args リモート アプリケーションの起動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 デスクトップ表示名。この表示名は、デスクトップ プールの作成時に View Administrator で指定した名前です。表示名にスペースが含まれている場合、ブラウザは **%20** を使用してスペースを表します。

domainName リモート デスクトップや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 Web client 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.txt 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)] というハイパー リンクおよび [TestButton] とい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 デスクトップまたはアプリケーションの使用

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](#)
- [国際化](#)
- [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](#)
- [Workspace ONE モードでのサーバへの接続](#)
- [リモート アプリケーションへの接続での非認証アクセスの使用](#)
- [ショートカット キーの組み合わせ](#)
- [国際キーボード](#)
- [スクリーン解像度](#)
- [H.264 デコード](#)
- [タイム ゾーンの設定](#)
- [サイドバーの使用](#)
- [複数のモニターの使用](#)
- [DPI 同期の使用](#)
- [音声](#)
- [テキストのコピーおよび貼り付け](#)
- [クライアントとリモート デスクトップ間でのファイルの転送](#)
- [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](#)
- [ログオフまたは切断](#)
- [リモート デスクトップまたはリモート アプリケーションのリセット](#)
- [リモート デスクトップの再起動](#)

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 3-1. 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 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
Wyse MMR						
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、『View 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 View 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 3-2. View Agent 6.1.1 以降、または Horizon Agent 7.0 以降がインストールされた RDS ホストに対して HTML Access でサポートされている機能

機能	Windows Server 2008 R2 RDS ホスト	Windows Server 2012 または 2012 R2 RDS ホスト	Windows Server 2016
RSA SecurID または RADIUS	X	X	Horizon Agent 7.0.2 以降
シングル サインオン	X	X	Horizon Agent 7.0.2 以降
VMware Blast 表示プロトコル	X	X	Horizon Agent 7.0.2 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)
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
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

各ゲスト OS のどのエディションがサポートされるか、またはどのサービス パックがサポートされるかについての詳細は、『View のインストール』ドキュメントの「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。

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。

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

使用を許可されているリモート デスクトップおよび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 認証ユーザー名とパスコード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 の認証証明書を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、入力したものと同一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アプリケーションで使用す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 デスクトップやアプリケーションをマークするには、デスクトップやアプリケーション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アプリケーションのアイコンをクリックします。

リモート デスクトップまたは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 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れる場合、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 デスクトップやアプリケーションに初めて接続するときに、リモート マシンによって使用される自己署名証明書を受け入れるかどうかを確認するプロンプトがブラウザで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アプリケーションに接続するには、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ことを選択しない場合には、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。

Horizon 管理者に問い合わせる必要がある場合があります。たとえば、Chrome ブラウザでは、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 お使いの証明書が、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ことを確認します。

Horizon 管理者に問い合わせる必要がある場合があります。

- 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、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、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 デスクトップとアプリケーションを開始できます。

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ます。
- Workspace ONE Web ポータル経由でデスクトップまたはアプリケーションを開始すると、HTML Access でリモート デスクトップとアプリケーションを表示または開始できません。

リモート アプリケーションへの接続での非認証アクセスの使用

Horizon 管理者は、非認証アクセス機能を使用して、非認証アクセス ユーザーを作成し、これらのユーザーに接続サーバ インスタンスにあるリモート アプリケーションに対する資格を付与できます。非認証アクセス ユーザーは、サーバに匿名でログインして、これらのリモート 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、[HTML Access のための接続サーバおよびセキュリティ サーバの準備](#)で説明しています。
- 接続サーバ インスタンスで非認証アクセス ユーザーを設定します。詳細については、『View 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 ブラウザを開きます。リモート アプリケーションへの非認証アクセスが許可された接続サーバ インスタンスに接続するには、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`

上の URI 構文の *authority-part* にはサーバのアドレスを指定します。オプションで、デフォルト以外のポート番号を指定できます。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、*server-address:port-number* を使用します。*anonymous_account* は、匿名ログイン用に作成される非認証アクセスユーザー アカウントです。

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。

- 2 (オプション) `unauthenticatedAccessAccount` クエリを指定していない場合には、必要に応じて [ユーザー アカウント] ドロップダウン メニューから非認証アクセス ユーザー アカウントを選択し、[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 アクセスするリモート アプリケーションのアイコンをクリックします。

リモート 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、他のリモート 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、RDS ホストは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。

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 デスクトップや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 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、[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)
- ファンクション キー (Chromebook を使用する場合)
- Windows キーの組み合わせ

次の Windows キーの組み合わせは、デスクトップで Windows キーを有効にしている場合、リモート デスクトップでは動作しません。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、RDS ホストで提供されるリモート アプリケーションでは動作しません。RDS ホストで提供される Windows Server 2008 R2 および Windows Server 2012 R2 シングルユーザー デスクトップおよびセッションベース デスクトップでは表示されているように動作します。

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 3-3. Windows 10 リモート デスクトップの Windows キーのショートカット

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)	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。

キー	アクション	制限
Win + Shift + M	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 ブラウザでは動作しません。
Win + Alt + 数字キー	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 3-4. 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 ブラウザでは動作しません。
Win	[スタート] 画面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	デスクトップを表示および非表示にします。	Safari ブラウザでは動作しません。回避策 : Mac では 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	[検索] チャームを開き、アプリケーションがアプリケーション検索をサポートしている場合、すべての場所または開いているアプリケーション内を検索します。	
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] チャームを開いて、Windows と Web を検索します。	
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、デスクトップを一時的に表示します。	注: 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。	Chromebooks や Mac には Pause キーはありません。
Win + Shift + M	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 ブラウザでは動作しません。回避策 : Mac では Command + D キーを押します。
Win + Alt + 数字キー	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、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。

キー	アクション	制限
Win + 左向き矢印	アプリケーションまたはデスクトップ 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デスクトップ 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	アクティブなデスクトップ 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	デスクトップ 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 + Shift + 下向き矢印	Win + Shift + 上向き矢印キーを押した後に、幅を維持しながらデスクトップ 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 3-5. 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。	Chromebooks や Mac には Pause キーはありません。
Win + D	デスクトップを表示および非表示にします。	Safari ブラウザでは動作しません。回避策 : Mac では 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	コンピューター 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デスクトップ 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デスクトップ 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	アクティブなデスクトップ 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 ブラウザでは動作しません。
Win + Shift + 上向き矢印	デスクトップ 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	実行中のデスクトップ 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 3-6. 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

スクリーン解像度

Horizon Administrator が適切な容量のビデオ RAM で構成されていると、Web Client 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 のデフォルト設定は 36MB で、3D アプリケーションを使用しなければ、最小要件の 16MB よりも快適な環境となります。

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。

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 以降で利用できる、ソフトウェア アクセラレータによるグラフィック機能によって、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 以降で利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、『View アーキテクチャ プランニング』のトピック「仮想デスクトップのメモリ要件の計算」の「PCoIP を使用する場合の特定のモニター構成の RAM サイジング」を参照してください。

H.264 デコード

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

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 デスクトップやアプリケーションに接続していない場合、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。

タイム ゾーンの設定

リモート デスクトップまたはアプリケーションで使用されるタイム ゾーンは、ローカル マシンのタイム ゾーンに自動的に設定されます。ただし、HTML Access クライアントを使用している場合に、いくつかの夏時間ポリシーによってタイム ゾーンを正しく決定できない場合は、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アプリケーションに接続する前に、適切なタイム ゾーン情報を手動で設定するには、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。[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。

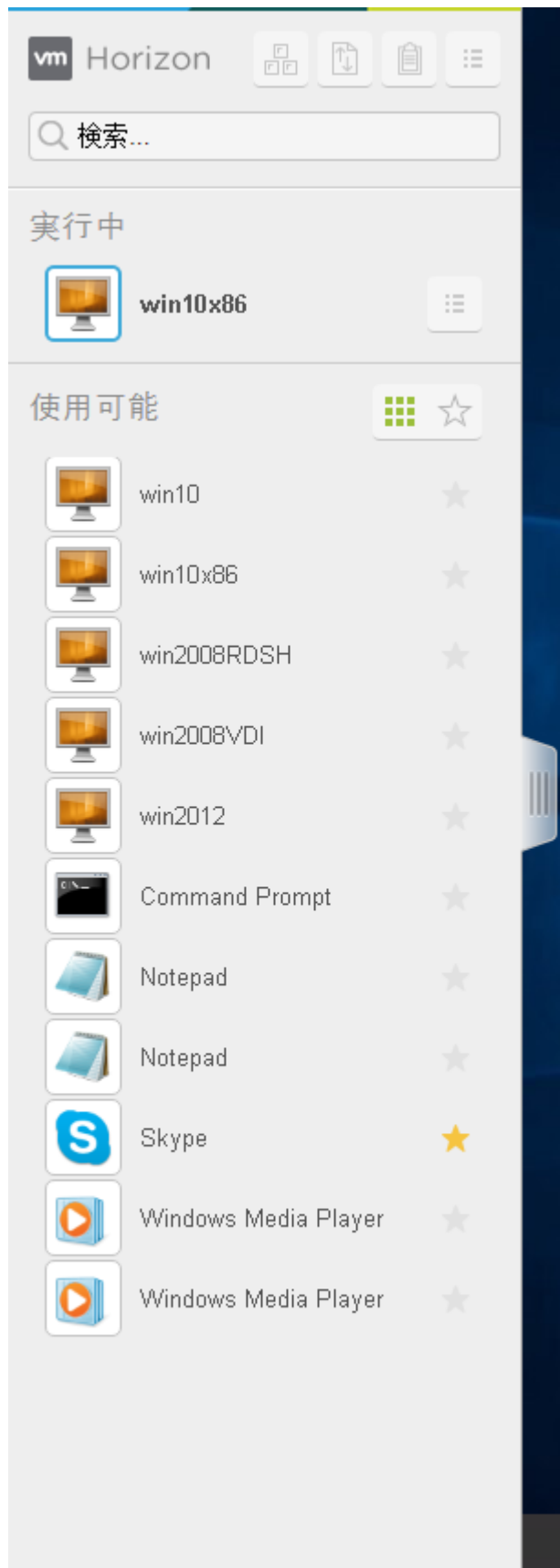
リモート デスクトップまたはアプリケーションにすでに接続している場合は、デスクトップおよびアプリケーション選択画面に戻り、現在のタイム ゾーン設定を変更します。サイドバーからアクセスできる [設定] ウィンドウでは、[タイム ゾーンを自動的に設定する] オプションは使用できません。

サイドバーの使用

リモート デスクトップまたはホスト型アプリケーションに接続したら、サイドバーを使用して、他のアプリケーションおよびデスクトップを起動したり、実行中のデスクトップと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。

リモート アプリケーションまたはデスクトップにアクセスすると、サイドバーが画面左側に表示されます。サイドバー タブをクリックして、サイドバーを表示または非表示にします。このタブは上下にスライドできます。

図 3-1. リモート デスクトップまたはアプリケーションを起動したときに表示されるサイドバー



実行中のアプリケーションの横にある展開矢印をクリックして、その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します。しかし、たとえば 2 台の異なるサーバにホストされている別々の Excel プログラムで開いている 2 つの Excel ドキュメントがある場合、Excel アプリケーションはサイドバーの [実行中] リストに 2 度表示されません。

サイドバーからいくつかの操作を実行できます。

表 3-7. サイドバーの操作

アクション	手順
サイドバーを表示	リモート アプリケーションまたはデスクトップが開いている場合、サイドバー 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、アプリケーションまたはデスクトップ 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。
リモート アプリケーションまたはデスクトップを起動する	サイドバーの [使用可能] でアプリケーションまたはデスクトップの名前をクリックします。デスクトップが最初に表示されます。
リモート アプリケーションまたはデスクトップを検索する	<ul style="list-style-type: none"> ■ [検索] ボックスをクリックし、アプリケーションまたはデスクトップの名前を入力します。 ■ アプリケーションまたはデスクトップを起動するには、検索結果でアプリケーションまたはデスクトップの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。
お気に入りのアプリケーションまたはデスクトップの一覧を作成する	サイドバーの [使用可能] リストにあるデスクトップや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。
アプリケーションまたはデスクトップを切り替える	サイドバーの [実行中] リストにあるアプリケーション ファイル名またはデスクトップ名をクリックします。
[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	サイドバーの上部の、[ファイル転送] ボタンをクリックして、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 デスクトップへファイルをアップロードします。詳細は、 デスクトップからクライアントにファイルをダウンロードおよびクライアントからデスクトップへ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。
動作中のデスクトップを閉じる	<p>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] ボタンをクリックして、実行する操作を選択します。</p> <ul style="list-style-type: none"> ■ [閉じる] を選択すると、オペレーティング システムからログオフせずに、デスクトップから切断します。しかし、View 管理者は、切断された時点で自動的にログオフするように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 システムからログオフして、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。

アクション	手順
動作中のアプリケーションを閉じる	<p>サイドバーの [実行中] リストにある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。アプリケーション名の横にある [X] をクリックして、アプリケーションを修了して、その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。</p> <p>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。</p>
デスクトップをリセットする	<p>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] 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すべてのファイルが、保存されずに閉じられることになります。デスクトップをリセットできるのは、管理者がこの機能を有効にしている場合のみです。</p>
デスクトップの再起動	<p>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] ボタンをクリックして、[再起動] を選択します。デスクトップ オペレーティング システムでは、通常、再起動する前に未保存データを保存するように求められます。デスクトップを再起動できるのは、管理者がこの機能を有効にしている場合のみです。</p>
実行中のすべてのアプリケーションをリセットする	<p>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。</p>
Windows キーを含むキーの組み合わせを使用する	<p>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。</p>
現在の作業領域に Ctrl+Alt+Del を送信する	<p>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。</p>
サーバから切断する	<p>サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックするか、サイドバーの上部にある Horizon ロゴをクリックして、[ログオフ] をクリックします。</p>
高解像度ディスプレイ（Retina Macbook Pro など）があるマシンで高解像度モードを使用する	<p>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。</p>
H.264 デコードを許可する	<p>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 デコードを参照してください。</p>
複数のモニターの使用	<p>(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。</p>
ソフト キーボードを表示または消去する	<p>(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。</p>
ヘルプ トピックを表示する	<p>サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックするか、サイドバーの上部にある Horizon ロゴをクリックして、[ヘルプ] をクリックします。</p>
[VMware Horizon について] ボックスを表示します。	<p>サイドバーの上部にある [メニューを開く] ツールバー ボタンをクリックするか、サイドバーの上部にある Horizon ロゴをクリックして、[バージョン情報] をクリックします。</p>

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 Web client 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。

HTML Access Web client 4.5 以降では、マルチモニタ機能を有効にすると、デバイスごとに DPI 同期が適用されます。DPI の設定が異なる 2 台のモニターを使用している場合、HTML Access Agent の DPI は、HTML Access Web client セッションを使用したクライアント マシンのモニターの DPI と同じ値に設定されます。

手順

- 1 Horizon Client を起動し、サーバにログインします。
- 2 デスクトップとアプリケーションの選択ウィンドウで、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、[表示設定] をクリックします。
- 5 [表示設定] ダイアログ ボックスで、[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、Horizon サーバの FQDN アドレスをブラウザの [コンテンツの設定] ウィンドウの [ポップアップの例外] セクションに追加します。

- 6 [ディスプレイ セレクタ] 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 [表示設定] 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、[表示設定] ウィンドウで [OK] をクリックします。
[表示設定] ウィンドウが閉じられ、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には、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。

DPI 同期の使用

DPI 同期機能によって、新しいリモート セッションでリモート デスクトップの DPI 設定がクライアント マシンの DPI 設定と必ず一致するようになります。新しいセッションを開始するときに、Horizon Agent によって、クライアント マシンの DPI 値と一致するようにリモート デスクトップの DPI 値が設定されます。

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

[設定] ウィンドウで [高解像度モード] が無効な場合に、DPI 同期機能は有効になります。HTML Access バージョン 4.5 以降では、管理者が Horizon Agent[DPI 同期] グループ ポリシー設定を無効にすると、DPI 同期機能を無効にできますが、ディスプレイのスケーリング機能は無効にできません。設定の変更を有効にするには、ログアウトしてからもう一度ログインする必要があります。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。

DPI 同期機能を使用する場合、シングルセッションのデスクトップでは Windows 7 以降、RDS ホストの公開デスクトップやアプリケーションでは Windows Server 2008 R2 以降、Horizon Agent 7.0.2 以降、および HTML Access バージョン 4.4 以降が必要となります。

DPI 同期機能を使用するときのヒントを、次に説明します。

- クライアント マシンで DPI 設定を変更する場合、Horizon Client にクライアント マシンの新しい DPI 設定を認識させるため、ログアウトしてからもう一度ログインする必要があります。クライアント マシンで Windows 10 が実行されている場合でも、この要件は適用されます。
- DPI 設定が 100 パーセント以上になっているクライアント マシンでリモート 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 マシン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 マシンで DPI を同期するには、2 番目のクライアント マシンでログアウトしてから再度ログインしてセッションに戻る必要があります。
- Windows 10 および Windows 8.x マシン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 マシン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。
- 管理者が、Horizon Agent の [DPI Synchronization] グループ ポリシー設定の値を変更する場合、新しい設定を有効にするためにログアウトしてからもう一度ログインする必要があります。
- 別の DPI 設定を使用して別のモニターと同期する場合は、リモート デスクトップまたは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 デスクトップやアプリケーションの DPI 設定を一致させます。

音声

リモート デスクトップおよび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、View 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。

以下のガイドラインを考慮してください。

- 音量を上げるには、リモート デスクトップやアプリケーションのサウンド 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、音声ビデオと同期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 (I/O) を実行中であつたりすると、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。

テキストのコピーおよび貼り付け

リモート デスクトップおよびアプリケーションにテキストをコピーしたり、リモート デスクトップおよびアプリケーションからテキストをコピーしたりできます。View 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アプリケーションへのコピーおよび貼り付け操作のみを許可する、リモート デスクトップまたはアプリケーションからクライアント システムへのコピーおよび貼り付け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。

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 ポリシーを使用して、コピーおよび貼り付けの機能を構成できます。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。管理者は、コピーおよび貼り付け操作の時に、グループ ポリシー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 クライアントではテキスト フィルタだけが動作します。グループ ポリシーを使用してクリップボードの形式をフィルタする詳細については、『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。

任意の Unicode の非 ASCII 文字を含め、最大で 1MB のテキストをコピーできます。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アプリケーション、あるいはその逆にテキストをコピーできますが、貼り付けたテキストはプレーン テキストになります。

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、ファイルもコピーおよび貼り付けできません。

注: コピーおよび貼り付けの機能は、iOS Safari ではサポートされていません。

コピーおよび貼り付け機能の使用

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] ボタンを使用する必要があります。

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ローカル クライアント システムからリモート アプリケーションにテキストをコピーする方法や、リモート 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を説明します。しかし、リモート アプリケーションとデスクトップ間でテキストをコピーしている場合には、通常と同じ操作でコピーおよび貼り付けすることができ、[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。

HTML Access のサイドバーの上部にあるボタンから開くことができる [コピーおよび貼り付け] ウィンドウは、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する場合にのみ必要となります。

[コピーおよび貼り付け] ウィンドウのテキストは、ユーザーがコンテンツをコピーおよび貼り付けできる方向を示す次のメッセージのいずれかを表示します。

- 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。

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（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）。

View 管理者は、ユーザーにクライアント システムからリモート デスクトップおよびアプリケーションへのコピーおよび貼り付けを許可するというデフォルトのポリシーを有効なままにするか、コピーおよび貼り付けを許可するそれ以外のポリシーを構成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 デスクトップやアプリケーションにテキストをコピーするには、以下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 ブラウザで、HTML Access サイドバー タブをクリックしてサイドバーを開き、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 Ctrl + V キー（Mac では Command + V キー）を押して、[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リモート 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。

テキストがリモート アプリケーションに貼り付けられます。
- ◆ リモート デスクトップや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、以下の手順を実行します。
 - a リモート アプリケーションでテキストをコピーします。
 - b ブラウザで、HTML Access サイドバー タブをクリックしてサイドバーを開き、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。

すでにテキストが貼り付けられた状態で [コピーおよび貼り付け] ウィンドウが表示されます。「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 [コピーおよび貼り付け] ウィンドウの中をクリックして、Ctrl + C キー（Mac では Command + C）を押して再度コピーします。

この操作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。

クライアントとリモート デスクトップ間でのファイルの転送

ファイル転送機能を使用して、クライアントとリモート デスクトップ間でファイルを転送（アップロードとダウンロード）できます。アプリケーションへの（または、アプリケーションからの）ファイル転送はサポートされません。

Horizon 管理者は、VMware Blast プロトコルに対する [Configure file transfer] 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構成できます。デフォルトはアップロードのみです。VMware Blast プロトコルに [設定されたファイル転送] グループのポリシー設定で、[アップロードとダウンロードの両方が無効] になっている場合、[ファイル転送] ボタンは無効になります。[ファイルのアップロードのみが有効] になっている場合、[アップロード] タブのみが [ファイル転送] ダイアログ ウィンドウに表示されます。[ファイルのダウンロードのみを有効にする] の値が選択されている場合、[ダウンロード] タブのみが [ファイル転送] ダイアログ ウィンドウに表示されます。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。

ダウンロードの場合の最大ファイル サイズは 500 MB、アップロードの場合の最大ファイル サイズは 2 GB 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 および Safari 8 はアップロードもダウンロードもサポートしません。Safari 9 以降では、ダウンロードをサポートしていません。

ファイル転送がデスクトップ セッションで進行中の状態で、ユーザーが 2 つ目のデスクトップに対する接続を開き、かつセキュリティ警告が表示された場合（たとえば、有効な証明書がインストールされなかった場合に警告が表示される）、この警告を無視して 2 つ目のデスクトップとの接続を継続した場合、最初のデスクトップ セッションでのファイル転送は中断することになります。これは、想定どおりの動作です。

注: ダウンロード機能は、クリップボード リダイレクトに対するグループ ポリシー設定の影響を受けます。サーバからクライアントへのクリップボード リダイレクト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。

デスクトップからクライアントにファイルをダウンロード

Horizon Client で、リモート デスクトップからクライアント マシンにファイルをダウンロードできます。

手順

- 1 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。
[[転送ファイル]] ウィンドウが開きます。
- 2 [ダウンロード] をクリックします。
- 3 リモート デスクトップの 1 つ以上のファイルを選択します。
- 4 Ctrl + C キーを押して、ダウンロードを開始します。
- 5 ダウンロードの完了後、ダウンロード アイコンをクリックしてクライアント マシンにファイルを保存します。

クライアントからデスクトップへファイルのアップロード

Horizon Client で、クライアント マシンからリモート デスクトップへファイルをアップロードできます。

手順

- 1 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。
[転送ファイル] ウィンドウが開きます。
- 2 [アップロード] をクリックします。
- 3 [転送ファイル] ウィンドウへ ファイルをドラッグアンドドロップするか、[ファイルの選択] をクリックしてファイルを選択します。

選択されたファイルは、My Documents フォルダへアップロードされます。

Internet Explorer 11 および ChromeBook の Chrome では、フォルダ、ゼロサイズのファイル、あるいは 2 GB を超えるファイルをドラッグアンドドロップすると、予測通りエラー 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。

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 デスクトップや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روفोन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 ビデオ解像度は 320 x 240 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 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روفोनに接続している場合、Web カメラやマイクروفोनがリモート デスクトップや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セカンド デスクトップや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。

ログオフまたは切断

いくつかの構成では、ログオフせずにリモート デスクトップから切断すると、デスクトップ内のアプリケーションは開いたままになる場合があります。サーバから切断し、リモート 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、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、ホスト型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画面から	画面の右上隅にある [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。

- ◆ リモート アプリケーションを閉じます。

オプション	アクション
アプリケーション内から	通常の方法でアプリケーションを終了します。たとえば、アプリケーション ウィンドウの隅の [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] リストにあるアプリケーションのファイル名の横にある [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
デスクトップのオペレーティング システムで	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	<p>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、保存されずに閉じられることになります。</p> <p>ログオフせずに切断するには、[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、[閉じる] を選択します。</p> <p>注: View 管理者は、切断された時点で自動的にログオフするようにデスクトップを設定できます。その場合、デスクトップで開いているアプリケーションは閉じられます。</p>
URI の使用	ログオフするには、URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=logoff</code> を使用します。

リモート デスクトップまたはリモート 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 アプリケーションをリセットすると、開いているすべてのアプリケーションが終了します。

リモート デスクトップをリセットする操作は、物理的な PC を強制的に再起動するためにその PC のリセット ボタンを押す操作に相当します。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。

リモート アプリケーションをリセットすることは、未保存データを保存せずにすべてのアプリケーションを終了することと同じことです。複数の RDS サーバ ファームから提供されているアプリケーションであっても、開いているリモート アプリケーションはすべて閉じます。

Horizon 管理者が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画面からリモート アプリケーションをリセットする	リモート デスクトップやリモート アプリケーションに接続する前に、デスクトップおよびアプリケーション選択画面から実行中のすべてのリモート アプリケーションをリセットするには、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。

オプション	アクション
サイドバーからリモート 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 <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=reset</code> 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 がデスクトップから切断され、ログオフされます。リモート 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

システムが完全に起動するまで待機してから、リモート デスクトップやアプリケーションに再接続します。

リモート デスクトップの再起動

デスクトップ オペレーティング システムが応答しなくなった場合、リモート デスクトップの再起動が必要な場合があります。リモート デスクトップの再起動は、Windows オペレーティング システムを再起動することと同じです。デスクトップ オペレーティング システムでは、通常、再起動する前に未保存データを保存するよう求められます。

Horizon 管理者が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 <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=restart</code> 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[リモート アプリケーションのリセット](#)を参照してください。