HTML Access の使用

2015 年 9 月

VMware Horizon

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

JA-001802-01

vmware®

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

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

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

目次

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™ 6 の HTML Access 機能をインストールして使用する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 インストール ガイド』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。

1 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。

この章では次のトピックについて説明します。

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。View の導入では、特定のソフトウェア要件を満たす必要があります。

クライアント システムのブラウザ

- HTML Access 3.5 では、次のブラウザがサポートされます。

ブラウザ	バージョン
Chrome	43、44
Internet Explorer	10、11
Safari	7、8（Mobile Safari はサポートされません。）
Firefox	38、39
Microsoft Edge	20

- HTML Access 3.4 では、次のブラウザがサポートされます。

ブラウザ	バージョン
Chrome	41、42、43
Internet Explorer	10、11

ブラウザ	バージョン
Safari	7、8（Mobile Safari はサポートされません。）
Firefox	36、37、38

クライアント オペレーティング システム

- HTML Access 3.5 は次のオペレーティング システムをサポートします。

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	10.9.x (Mavericks)
Mac OS X	10.10.x (Yosemite)
Chrome OS	28.x 以降

- HTML Access 3.4 は次のオペレーティング システムをサポートします。

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（32 ビットおよび 64 ビット）
Mac OS X	10.9.x (Mavericks)
Mac OS X	10.10.x (Yosemite)
Chrome OS	28.x 以降

注意　スマートフォンおよびタブレットなどの iOS デバイスは、サポートされません。代わりに iOS 版の Horizon Client を使用することを推奨します。これらのデバイスで HTML Access をサポートする必要がある場合には、HTML Access 3.x はインストールしないでください。代わりに、View 接続サーバ 6.1.1 でインストールされるデフォルト バージョンである HTML Access 2.6 を使用します。

リモート デスクトップ

- HTML Access 3.5 では View Agent 6.1 以降が必要となり、View 6.2 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 6.2 の『View インストール ガイド』のトピック「View 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。
- HTML Access 3.4 では View Agent 6.1.1 以降が必要となり、View 6.1 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 6.1 の『View インストール ガイド』のトピック「View 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。

重要　リモート デスクトップは仮想マシンである必要があります。View Agent を物理マシンにインストールすることもできますが、Blast プロトコルを HTML Access と共に使用する場合は、物理マシンにアクセスできません。View Agent は仮想マシンにインストールする必要があります。

プールの設定

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

- [1 台のモニタの最大解像度] 設定は [1920x1200] 以上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、「スクリーン解像度 (P. 36)」 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 (P. 12)」を参照してください。

View 接続サーバ

View 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 3.5 では、View 接続サーバ 6.2 が必要です。View 接続サーバ 6.2 をインストールする場合、[HTML Access のインストール] オプションを選択する必要があります。

HTML Access 3.4 では、View 接続サーバ 6.1.1 が必要です。View 接続サーバ 6.1.1 をインストールしたり、View 接続サーバ 6.1.1 にアップグレードしたりした後に、リモート デスクトップおよび RDS ホストが View Agent 6.1.1 を実行していることを確認したら、View 接続サーバ インスタンスで別の HTML Access インストーラを実行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

View セキュリティ サーバ： View 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。

注意　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、View 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）。

View 用の表示プロトコル

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 Blast プロトコルが使用されます。Blast は HTTPS (HTTP over SSL/TLS) を使用します。

HTML Access のための View 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 View 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なるには、HTML Access コンポーネントとともに View 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。

重要　一部のバージョンの HTML Access では、誤って HTML Access オプションなしで View 接続サーバをインストールし、後で HTML Access コンポーネントが必要になった場合には、View 接続サーバをアンインストールし、HTML Access オプションを選択してインストーラを再実行する必要があります。View 接続サーバをアンインストールするときには、AD LDS Instance VMwareVDMDS インスタンスと呼ばれる View LDAP 構成をアンインストールしないでください。

その他のバージョンの HTML Access の場合は、HTML Access のために別のインストーラを使用します。このため、View 接続サーバを再インストールする必要はありません。

表 1-1. HTML Access の各バージョンのインストーラ要件

HTML Access のバージョン	View 接続サーバのバージョン	インストール要件
3.5	6.2	個別の HTML Access インストーラなし
3.4	6.1.1	個別のインストーラ
2.6	6.1、6.1.1	個別の HTML Access インストーラなし

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 View 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 View 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 インストール ガイド』を参照してください。

注意　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 HTML Access 3.4 および新規インストールの場合は、HTML Access Web ポータル インストーラを View 接続サーバ インスタンスにダウンロードし実行します。HTML Access 3.5 では、HTML Access は手順 1 で自動的にインストールされるため、この手順は不要です。

HTML Access 3.4 のインストーラは、Horizon 6 バージョン 6.1.1 のダウンロード ページ (http://www.vmware.com/go/downloadview) から入手できます。インストーラの名前は、**VMware-Horizon-View-HTML-Access_X64-3.4.0-<xxxxxx>.exe** です（<xxxxxx> はビルド番号）。

注意　新規インストールではなく、アップグレードを実行している場合、この手順を実行する前に View Agent をアップグレードする必要があります。「HTML Access ソフトウェアのアップグレード (P. 17)」 の手順に従います。

3 セキュリティ サーバを使用する場合は、View 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 インストール ガイド』を参照してください。

重要　View セキュリティ サーバのバージョンは、View 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。

4 それぞれの View 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 インストール ガイド』を参照してください。

5 RSA SecurID または RADIUS 認証などの 2 要素認証を使用するには、View 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。

6 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 View 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 (P. 11)」を参照してください。

サーバのインストール後に View Administrator を確認すると、該当する View 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 View 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、安全なトンネルの外部 URL の FQDN とデフォルト ポート番号 8443 が含まれています。URL に、この View 接続サーバ ホストまたはセキュリティ サーバ ホストに到達するためにクライアント システムが使用できる FQDN とポート番号が含まれている必要があります。詳細については、『View インストール ガイド』の「View 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。

注意 HTML Access を VMware Workspace Portal 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 Portal のインストールおよび View 接続サーバで使用するための構成についての詳細は、Workspace Portal のマニュアルを参照してください。View 接続サーバを SAML 認証サーバとペアにする詳細については、『View 管理ガイド』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 1-2. HTML Access のファイアウォール ルール

送信元	デフォルトの送信元ポート	プロトコル	送信先	デフォルトの送信先ポート	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 インスタンス	TCP 443	View に最初に接続するために、クライアント デバイスの Web ブラウザは、TCP ポート 443 でセキュリティ サーバまたは View 接続サーバ インスタンスに接続します。
クライアント Web ブラウザ	すべての TCP	HTTPS	Blast Secure Gateway	TCP 8443	View への最初の接続後に、クライアント デバイスの Web ブラウザは TCP ポート 8443 上の Blast Secure Gateway に接続します。2 番目の接続を実行できるようにするために、セキュリティ サーバまたは View 接続サーバ インスタンスで Blast Secure Gateway を有効にする必要があります。

表 1-2. HTML Access のファイアウォール ルール (続き)

送信元	デフォルトの送信元ポート	プロトコル	送信先	デフォルトの送信先ポート	注
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、View 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、View Agent のインストールに含まれています。

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 View 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。

注意　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。

開始する前に

- vSphere インフラストラクチャと View 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 (P. 7)」を参照してください。

- HTML Access コンポーネントがホストの View 接続サーバにインストールされていること、および View 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 View 接続サーバおよびセキュリティ サーバの準備 (P. 10)」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、View サーバからデータ センターの View 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 (P. 7)」 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 (P. 7)」を参照してください。

手順

1. リンク クローン プールのすべての親仮想マシン、フル クローン プールの仮想マシン テンプレート、手動プールの仮想マシン、およびデスクトップとホスト型アプリケーション プールの RDS ホストに、[HTML Access] オプションを関連付けて View Agent をインストールします。
2. RDS デスクトップとアプリケーションについては、View 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。
3. 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 View 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 台のモニタの最大解像度] 設定が [1920x1200] 以上であることを確認します。
4. View 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。
5. サポートされるブラウザを開き、View 接続サーバ 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。
6. 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。
7. 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。

次に進む前に

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 (P. 13)」 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。

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

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

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

手順

1 Horizon View デスクトップで証明書のスナップインを MMC に追加する (P. 14)

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

2 HTML Access Agent の証明書を Windows 証明書ストアにインポート (P. 15)

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

3 HTML Access Agent のルート証明書と中間証明書のインポート (P. 16)

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

4 Windows レジストリで証明書の拇印を設定 (P. 16)

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

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

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

開始する前に

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

手順

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

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

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

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

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

次に進む前に

SSL 証明書を Windows ローカル コンピュータ証明書ストアにインポートします。「HTML Access Agent の証明書を Windows 証明書ストアにインポート (P. 15)」を参照してください。

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

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

開始する前に

- View デスクトップで HTML Access Agent がインストールされていることを確認します。
- CA によって署名された証明書がデスクトップにコピーされたことを確認します。
- 証明書のスナップインが MMC に追加されたことを確認します。「Horizon View デスクトップで証明書のスナップインを MMC に追加する (P. 14)」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。**

次に進む前に

必要に応じて、ルート証明書と中間証明書を Windows 証明書ストアにインポートします。「HTML Access Agent のルート証明書と中間証明書のインポート (P. 16)」を参照してください。

適切なレジストリ キーを証明書の拇印で構成します。「Windows レジストリで証明書の拇印を設定 (P. 16)」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ければ、手順 2 に進みます。

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

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

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

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

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

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

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

次に進む前に

適切なレジストリ キーを証明書の拇印で構成します。「Windows レジストリで証明書の拇印を設定 (P. 16)」を参照してください。

Windows レジストリで証明書の拇印を設定

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

開始する前に

CA によって署名された証明書が Windows 証明書ストアにインポートされることを確認します。「HTML Access Agent の証明書を Windows 証明書ストアにインポート (P. 15)」を参照してください。

手順

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

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

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

4 選択した拇印をテキスト ファイルにコピーします。

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

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

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

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

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

8 VMware Blast サービスを再起動して変更を有効にします。

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

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

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/apps/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。

HTML Access ソフトウェアのアップグレード

最新バージョンの HTML Access をインストールして、最新の更新および機能向上を入手します。

最新バージョンの HTML Access にアップグレードするには、複製されたグループのすべてのインスタンスに最新バージョンの View 接続サーバがインストールされていることを確認する必要があります。

HTML Access のいくつかのリリースでは、個別の HTML Access インストーラが必要となります。次の表に、個別のインストーラが必要な HTML Access のバージョンを示します。

表 1-3. HTML Access の各バージョンのインストーラ要件

HTML Access のバージョン	View 接続サーバのバージョン	インストール要件
3.5	6.2	個別の HTML Access インストーラなし
3.4	6.1.1	個別のインストーラ
2.6	6.1、6.1.1	個別の HTML Access インストーラなし

重要　個別の HTML Access インストーラについては、View 接続サーバをアップグレードするときには常に、View 接続サーバをアップグレードした後に、HTML Access のインストーラも実行する必要があります。たとえば、新しいパッチやメンテナンス リリースに View 接続サーバをアップグレードした後に、HTML Access Web ポータル ページに HTML Access アイコンが表示されない場合があります。利用できる HTML Access の新しいバージョンがない場合、Windows の [プログラムのアンインストール] 機能を使用して、HTML Access をアンインストールしてから、同じバージョンを再インストールします。

HTML Access 3.5 では、View 接続サーバ 6.2 にアップグレードするときに、自動的に HTML Access がインストールされるか、3.5 にアップグレードされます。別のインストーラは必要ありません。

以下は、HTML Access 3.4 にアップグレードするために実行する必要がある作業のチェックリストです。

1 View 接続サーバの複製されたグループを構成するサーバで、HTML Access オプションを使用して View 接続サーバ 6.1.1 にアップグレードします。

  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。

  View 接続サーバ 6.1.1 を対話形式でインストールする場合、インストールされる HTML Access のバージョンは HTML Access 2.6 になります。この段階では、HTML Access でリモート（ホスト型）アプリケーションは使用できません。 View Agent 6.1 を実行しているデスクトップに接続するには、HTML Access 2.6 を引き続き使用できます。

2 セキュリティ サーバを使用する場合は、View セキュリティ サーバ 6.1.1 にアップグレードします。

  View セキュリティ サーバのバージョンは、View 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 親マシンやテンプレート仮想マシンおよびデスクトップ プールにある仮想マシンを含むすべての RDS ホストおよび VDI マシンで View Agent 6.1.1 にアップグレードします。

  この手順で、View 接続サーバ インスタンスで HTML Access をアップグレードする前に、View Agent をアップグレードします。サーバで最初に HTML Access をアップグレードした場合、エンド ユーザーは、Web クライアントから古い View Agent（バージョン 6.1 以前）に接続できなくなります。

  注意　現在、View Agent インストーラには、Horizon 6.0 (with View) より前のリリースの Remote Experience Agent に付属していた HTML Access エージェント コンポーネントが含まれています。Remote Experience Agent は、Horizon View Feature Pack の一部でした。Remote Experience Agent でインストールされた機能をアップグレードするには、View Agent インストーラを実行してください。このインストーラを実行すると、Remote Experience Agent が削除され、次にアップグレードが行われます。何らかの理由で Remote Experience Agent を手動で削除する場合は、新バージョンの View Agent のインストーラを実行する前に削除してください。

4 Horizon 6 バージョン 6.1.1 のダウンロード ページ (http://www.vmware.com/go/downloadview) から、HTML Access Web ポータル インストーラを View 接続サーバ インスタンスにダウンロードして実行します。

  インストーラの名前は、`VMware-Horizon-View-HTML-Access_X64-3.4.0-<xxxxxx>.exe` です（<xxxxxx> はビルド番号）。

注意　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。

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 HTML Access プログラムを選択し、[アンインストール] をクリックします。

HTML Access のバージョン	HTML Access のプログラム名
3.5	VMware Horizon 6 HTML Access
3.4	VMware Horizon View HTML Access

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

次に進む前に

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

VMware によって収集されるデータ

所属する企業がカスタマー エクスペリエンス向上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。View 管理者がカスタマー エクスペリエンス向上プログラムへの参加を決めた場合、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、現在ご使用の配置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 View 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 カスタマー エクスペリエンス向上プログラムに参加するには、View 接続サーバ をインストールする管理者が View 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 View Administrator でオプションを設定します。

表 1-4. カスタマー エクスペリエンス向上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	3.5.0-<build_number>
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

表 1-4. カスタマー エクスペリエンス向上プログラムのために収集されたクライアント データ (続き)

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
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/12.10240
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） ■ 29.0 (Firefox 用) ■ 12.10240（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 ■ MSIE (Internet Explorer 用) ■ 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。

この章では次のトピックについて説明します。

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、View Portal 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。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りしたい場合もあるでしょう。異なる URL をポイントするためにページを再構成できます。

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 リンクを作成できます。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 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。

注意 `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。

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	`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	`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 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。
	■ 32 ビット Windows インストーラ:
	`link.win32=https://<server>/downloads/VMware-Horizon-Client.exe`
	■ 64 ビット Windows インストーラ：
	`link.win64=https://<server>/downloads/VMware-Horizon-Client.exe`
	■ Linux インストーラ:
	`link.linux=https://<server>/downloads/VMware-Horizon-Client.tar.gz`
	■ Mac OS X インストーラ:
	`link.mac=https://<server>/downloads/VMware-Horizon-Client.dmg`
	■ iOS インストーラ:
	`link.ios=https://<server>/downloads/VMware-Horizon-Client-iPhoneOS.zip`
	■ Android インストーラ:
	`link.android=https://<server>/downloads/VMware-Horizon-Client-AndroidOS.apk`
	■ 不明な OS 向けのインストーラ（たとえば、このプロパティを Chrome クライアント インストーラに使用できます）：
	`link.unknown=https://<server>/downloads/VMware-Horizon-Client-AndroidOS-arm-ARC.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 ユーザーがリンクをクリックして HTML Access Web client を起動したり、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、および必要に応じてユーザー、デスクトップ、デスクトップのアクションまたは構成オプションを指定するためのクエリが含まれます。

URI 仕様

以下の構文を使用して 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>

使用するための設定オプション、または 実行するデスクトップ 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 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。

domainName
リモート デスクトップに接続しているユーザーに関連付けられている NETBIOS ドメイン名。例として、`mycompany.com` ではなく `mycompany` を使用してください。

userName
リモート デスクトップに接続している Active Directory ユーザー。

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。

desktopId
デスクトップ表示名。この名前は、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** を自動的に使用してスペースを表します。

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 デスクトップのリストを表示します。このアクションを使用している場合、 デスクトップ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、デスクトップ名 が提供される場合、`start-session` がデフォルト アクションとなります。
`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。
`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。

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、これらのリンクを電子メールまたは 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起動できます。

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。クエリでは、大文字と小文字が区別されません。たとえば、**domainName** または **domainname** を使用できます。

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

HTML Access Web Client が起動され、`view.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://view.mycompany.com/?desktopId=Primary%20Desktop&action=start-session`

HTML Access Web Client が起動され、`view.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。

3 `https://view.mycompany.com:7555/?desktopId=Primary%20Desktop`

この URI は前の例と同じ効果がありますが、View 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。

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

HTML Access Web Client が起動され、`view.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。

注意　このアクションは、View 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。

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、電子メールまたは 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://view.mycompany.com/?domainName=finance&userName=fred">Test
Link</a><br>

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

</body>
</html>
```

HTML Access グループ ポリシー設定を構成する

リモート デスクトップでの HTML Access の動作を制御するグループ ポリシー設定を構成できます。これらの設定を適用するには、HTML Access ADM テンプレート ファイルを Active Directory のグループ ポリシー オブジェクト (GPO) に追加します。

開始する前に

- HTML Access グループ ポリシー設定用に Active Directory GPO が作成されていることを確認します。GPO は、リモート デスクトップを含む OU にリンクする必要があります。Active Directory で View グループ ポリシー設定を行う一般情報については、『View でのデスクトップとアプリケーションの設定』の「ポリシーの構成」を参照してください。
- Active Directory サーバで、Microsoft MMC およびグループ ポリシー オブジェクト エディタ スナップインが使用できることを確認します。
- HTML Access グループ ポリシー設定について理解しておきます。「HTML Access グループ ポリシ設定 (P. 27)」を参照してください。

手順

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

デスクトップおよびエンドユーザーのコンピュータで VMware Horizon 6 のダウンロードを選択します。これには GPO Bundle が含まれます。

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

2 ファイルを Active Directory サーバにコピーして解凍します。

HTML Access GPO は、`vdm-blast.adm` ADM テンプレート ファイルに含まれています。

3 Active Directory サーバで GPO を編集します。

a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。

b ドメインを展開し、グループ ポリシー設定を作成した GPO を右クリックして、[編集] を選択します。

[グループ ポリシー オブジェクト エディタ] ウィンドウが表示されます。

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

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

6 [閉じる]をクリックして、ADM テンプレート ファイルのポリシー設定を GPO に適用します。

[VMware Blast] フォルダは、左側のペインの [管理用テンプレート] - [従来の管理用テンプレート] の下に表示されます。

7 HTML Access グループ ポリシー設定を構成します。

8 ポリシー設定がリモート デスクトップに適用されていることを確認します。

a デスクトップで `gpupdate.exe` コマンドを実行します。

b デスクトップを再起動します。

HTML Access グループ ポリシ設定

HTML Access ADM テンプレート ファイル `vdm-blast.adm` には、リモート デスクトップに適用できるグループ ポリシー設定が含まれます。テンプレート ファイルが Active Directory にインポートされると、HTML Access グループ ポリシー設定がグループ ポリシー エディタの `VMware Blast` フォルダに格納されます。

表 2-2. HTML Access グループ ポリシ設定

設定	説明
空の画面	リモート仮想マシンが、HTML Access セッション中に View の外から見ることができるかどうかを制御します。たとえば、管理者は vSphere Web クライアントを使用して、ユーザーが HTML Access を介してデスクトップに接続されている間に仮想マシンでコンソールを開く場合があります。 この設定が有効にされるか構成されない場合で、HTML Access セッションがアクティブである間に誰かが View の外からリモート仮想マシンにアクセスを試みる場合、リモート仮想マシンは空の画面を表示します。 この設定を無効にすると、先行条件下ではリモート仮想マシンは、アクティブ View デスクトップ セッションを第 2 のリモート アクセサに表示します。
セッションのガーベッジ コレクション	破棄されたリモート セッションのガーベッジ コレクションを制御します。この設定を有効にすると、ガーベッジ コレクションの間隔としきい値を構成できます。 間隔はガーベッジ コレクタが実行される頻度を制御します。ミリ秒単位で間隔を設定します。 しきい値は、セッションが破棄された後でそれが削除候補となる前までに必要となる経過時間を決定します。秒単位でしきい値を設定します。

表 2-2. HTML Access グループ ポリシ設定 (続き)

設定	説明
オーディオ再生	リモート デスクトップでオーディオ再生を許可するかどうかを制御します。デフォルトでは、この設定は有効です。
イメージ品質	リモート ディスプレイのイメージ品質を制御します。低画質、中画質、および高画質の 3 種類のイメージ品質プロファイルがあります。利用可能な帯域幅、最近使用したフレームレート、現在のフレームで最近変更された部分のサイズの制限の範囲で、エンコーダは可能な限り最高品質レベルを使用しようとします。エンコーダは、クライアント画面のどの部分が低画質または中画質であるのかを追跡し、それらの領域を画像を少しずつ上げて高画質に近づけます。 この設定を有効にすると、低品質、中画質、および高品質の JPEG 設定を異なる値に個別に変更できます。実際の低画質、中画質、および高画質の設定で使用される JPEG 画質レベルは、0 ～ 100 の範囲の数値として個々に構成できます。 彩度のサブサンプリングは、選択された JPEG 品質レベルに対応して有効になります。JPEG 品質が 80 以上に設定されると、彩度のサンプリングがオフになり、比率は使用可能な最高値 YUV-4:4:4 に設定されます。JPEG 品質が 79 以下に設定されると、比率は YUV-4:2:0 に設定されます。 ■ [低品質 JPEG]。デフォルトでは、この値は 25 です。低い JPEG 彩度のサブサンプリングを様々な比率に設定することもできます。デフォルトでは、低い比率は使用可能な最低値 4:1:0 に設定されています。 ■ [中品質 JPEG]。デフォルトの場合、この値は 35 です。低い JPEG 彩度のサブサンプリングを様々な比率に設定することもできます。デフォルトの場合、低い比率は使用可能な最低値 4:2:0 に設定されています。 ■ [高品質 JPEG]。デフォルトでは、この値は 90 です。高い JPEG 彩度のサブサンプリングを様々な比率に設定することもできます。デフォルトでは、高い比率は使用可能な最高値 4:4:4 に設定されています。
クリップボード リダイレクトの構成	クリップボード リダイレクトを許可する方向を決定します。テキストのみをコピーおよび貼り付けできます。次のいずれかの値を選択できます。 ■ [クライアントからサーバの方向のみ有効] （すなわち、クライアント システムからリモート デスクトップにのみ、コピーおよび貼り付けを許可します。） ■ [どちらの方向も無効] ■ [どちらの方向も有効] ■ [サーバからクライアントの方向のみ有効] （すなわち、リモート デスクトップからクライアント システムにのみ、コピーおよび貼り付けを許可します。） この設定は View Agent にのみ適用されます。 この設定が無効または構成されていない場合、デフォルト値は [クライアントからサーバの方向のみ有効] です。
HTTP サービス	Blast Agent サービス用のセキュアな (HTTPS) TCP ポートに変更可能です。デフォルトのポートは 22443 です。 この設定を有効にしてポート番号を変更します。この設定を変更する場合は、影響を受けるリモート デスクトップ（View Agent のインストール先）のファイアウォールの設定も更新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の使用 3

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。

この章では次のトピックについて説明します。

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 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
RSA SecurID または RADIUS	X	X	X	X	X
シングル サインオン	X	X	X	X	X
RDP 表示プロトコル					
PCoIP 表示プロトコル					
Blast プロトコル	X	X	X	X	X

表 3-1. HTML Access を通してサポートされる機能 (続き)

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
USB リダイレクト					
リアルタイム オーディオ ビデオ (RTAV)					
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
スマート カード					
複数のモニタ					

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。

次の表は、HTML Access を使用した場合に RDS ホストから使用可能な機能を示しています。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 または 6.2 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	物理マシン上の Windows Server 2008 R2 RDS ホスト	仮想マシン上の Windows Server 2008 R2 RDS ホスト	物理マシン上の Windows Server 2012 または 2012 R2 RDS ホスト	仮想マシン上の Windows Server 2012 または 2012 R2 RDS ホスト
RSA SecurID または RADIUS		X		X
シングル サインオン		X		X
Blast プロトコル		X		X
仮想プリンタ				
ロケーション ベースの印刷		X		X
複数のモニタ				

重要　RDS ホストは仮想マシンにインストールする必要があります。View Agent を物理マシンにインストールすることもできますが、Blast プロトコルを HTML Access と共に使用する場合は、物理マシンにアクセスできません。View Agent は仮想マシンにインストールする必要があります。

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 6.x インストール ガイド』の「View Agent でサポートされているオペレーティング システム」のトピック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、および韓国語で利用可能です。

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 (P. 36)」を参照してください。

リモート デスクトップまたはアプリケーションに接続する

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。

開始する前に

- 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に必要な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、View 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://view.company.com` のように完全修飾ドメイン名を使用します。

View 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。 View 接続サーバはデフォルト ポートを使用するように構成されていない場合、以下の例にあるフォーマットを使用します。**`view.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 [VMware Horizon HTML Access] アイコンをクリックします。

3 [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。

4 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 サーバの構成設定が変更された時にのみ、必要になります。

5 [ログイン] ダイアログ ボックスで Active Directory のユーザー名とパスワードを入力し、ドメインを選択し、[ログイン] をクリックします。

6 (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。

7 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。

次に進む前に

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 (P. 32)」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。

View 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。

View 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。

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。

注意　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、[デスクトップ用 Windows キーの有効化] をオンにします。

重要　[デスクトップ用 Windows キーの有効化] 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。	

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 (続き)

キー	アクション	制限
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。
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。対応策：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。	注意　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。対応策：Mac では Command + D キーを押します。

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 (続き)

キー	アクション	制限
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。
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。対応策：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。

ローカル設定および入力方法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、および韓国語。

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

スクリーン解像度

View Administrator が適切な容量のビデオ RAM で構成されていると、クライアントでリモート 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 [高解像度モードに切り替え] 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（このオプションは、高解像度ディスプレイ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）。

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。

Horizon Client 3.4 では 3D レンダリングが有効である場合、モニタの最大数は 1 で最大解像度は 1920 x 1200 です。

Horizon Client 3.5 では 3D レンダリングが有効である場合、モニタの最大数は 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　Blast 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構成の RAM サイジング」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 度表示されます。

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。

表 3-7. サイドバーの操作 (続き)

アクション	手順
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	■ [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] ウィンドウを表示する	サイドバーの下部にある [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 (P. 39)」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 [[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、この機能をオンにします。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	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。 ■ [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。
動作中の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。 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。
デスクトップをリセットする	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。
実行中のすべてのアプリケーションをリセットする	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。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 [[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、[デスクトップ用 Windows キーの有効化] 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 (P. 33)」を参照してください。
Ctrl + Alt + Del キーの組み合わせをリモート デスクトップまたはアプリケーションに送信する	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。
サーバから切断する	サイドバーの上部にある [VMware Horizon からログオフ] ツールバー ボタンをクリックします。
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	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、[高解像度モードに切り替え] をオンにします（このオプションは、高解像度ディスプレイ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）。
ヘルプ トピックを表示する	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。
[VMware Horizon について] ボックスを表示します。	サイドバーの下部にある Horizon ロゴをクリックします。

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 (I/O) を実行中であったりすると、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 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 オブジェクト（GPO）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 ポリシ設定 (P. 27)」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、ファイルもココピーおよび貼り付けできません。

コピーおよび貼り付け機能の使用

テキストをコピーおよび貼り付けるには、サイドバーの下部にある [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 のサイドバーの下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。

開始する前に

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 ポリシ設定 (P. 27)」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、サイドバーを開いて、サイドバーの下部にある [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。

  注意　コピーが無効になっていると、[コピーおよび貼り付け] ウィンドウの下部にメッセージが表示されます。

  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、サイドバーを開いて、サイドバーの下部にある [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。

  注意　コピーが無効になっていると、[コピーおよび貼り付け] ウィンドウの下部にメッセージが表示されます。

  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。

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

- View server 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 [VMware Horizon からログオフ] ツールバー 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	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。 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。 注意　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。
URI の使用	ログオフするには、URI `https://<Connection_Server_name_or_IP_address>?desktopId=<desktop_name>&action=logoff` を使用します。

リモート デスクトップまたはアプリケーションのリセット

アプリケーションまたはデスクトップ オペレーティング システムが応答しなくなった場合、デスクトップまたはアプリケーションのリセットが必要な場合があります。リモート デスクトップをリセットすると、デスクトップがシャットダウンおよび再起動されます。リモート アプリケーションをリセットすると、アプリケーションが終了します。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、保存されずに閉じられることになります。

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リモート アプリケーションを終了するのと同じことです。アプリケーションが複数の RDS サーバ ファームのアプリケーションであっても、開いているアプリケーションはすべて閉じます。

リモート 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。

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 を使用したデスクトップのリセット	デスクトップをリセットするには、URI `https://<Connection_Server_name_or_IP_address>?desktopId=<desktop_name>&action=reset` を使用します。

リモート デスクトップの場合、リモート デスクトップのオペレーティング システムが再起動されます。クライアントがデスクトップから切断されます。リモート アプリケーションの場合、アプリケーションが終了します。

次に進む前に

リモート デスクトップに接続する前に、システムが完全に起動するまで待機します。

インデックス