Verwendung von HTML Access

VMware Horizon 4.1

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-002142-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Verwendung von HTML Access

Dieses Handbuch, *Verwendung von HTML Access*, bietet Informationen über die Installation und Verwendung der HTML Access-Funktion von VMware Horizon™ 7 zur Herstellung einer Verbindung mit virtuellen Desktops, ohne Software auf einem Clientsystem installieren zu müssen.

Die Informationen in diesem Dokument enthalten Systemanforderungen und Anleitungen zur Installation von HTML Access-Software auf einem View-Server und auf einer virtuellen Maschine des Remote-Desktops, damit Endbenutzer mit einem Webbrowser auf Remote-Desktops zugreifen können.

Wichtig Diese Informationen wurden für Administratoren verfasst, die bereits Erfahrung mit der Verwendung von View und VMware vSphere haben. Wenn Sie ein neuer Benutzer von View sind, müssen Sie möglicherweise gelegentlich die schrittweisen Anleitungen für grundlegende Verfahren in den Dokumenten *ViewInstallation von* und *ViewVerwaltung von* heranziehen.

1 Konfiguration und Installation

Bei der Einrichtung einer View-Bereitstellung für HTML Access müssen Sie HTML Access auf dem View-Verbindungsserver installieren, die erforderlichen Ports öffnen und die HTML Access-Komponente auf der virtuellen Maschine des Remote-Desktops installieren.

Benutzer können dann auf ihre Remote-Desktops zugreifen, indem sie einen unterstützten Browser öffnen und die URL für den View-Verbindungsserver eingeben.

Dieses Kapitel behandelt die folgenden Themen:

Systemanforderungen für HTML Access

Mit HTML Access wird für das Clientsystem keine weitere Software als ein unterstützter Browser benötigt. Die View-Bereitstellung muss bestimmte Software-Anforderungen erfüllen.

Hinweis Ab der Version 7.0 wird View Agent in Horizon Agent umbenannt.

Browser auf Clientsystemen

Browser	Version
Chrome	50, 51
Internet Explorer	11
Safari	8, 9
Safari auf mobilen Geräten	iOS 8, iOS 9

Browser	Version
Firefox	45, 46
Microsoft Edge	20, 25

Clientbetriebssysteme:

Betriebssystem	Version
Windows	7 SP1 (32- und 64-Bit-Version)
Windows	8.x (32- und 64-Bit-Version)
Windows	10 (32- und 64-Bit-Version)
Mac OS X	10.10.x (Yosemite)
Mac OS X	10.11 (El Capitan)
iOS	8
iOS	9
Chrome OS	28.x und höher

Remote-Desktops

HTML Access erfordert Horizon Agent 7.0 oder höher und unterstützt alle Desktop-Betriebssysteme, die Horizon 7.0 unterstützt. Weitere Informationen finden Sie unter „Unterstützte Betriebssysteme für View Agent“ in Version 7.0 der *View-Installation*.

Pool-Einstellungen

HTML Access erfordert die folgenden Pool-Einstellungen in View Administrator:

- Die Option **Maximale Auflösung eines Monitors** muss auf **1920x1200** oder höher festgelegt sein, damit der Remote-Desktop über mindestens 17,63 MB an Video-RAM verfügt.

  Wenn Sie beabsichtigen, 3D-Anwendungen zu verwenden, oder wenn die Endbenutzer mit einem Macbook mit Retina-Display oder einem Google Chromebook Pixel arbeiten, finden Sie weitere Informationen unter „Bildschirmauflösung“, auf Seite 37.

- Die Einstellung **HTML Access** muss aktiviert sein.

Konfigurationsanweisungen werden unter „Vorbereiten von Desktops, Pools und Farmen für HTML Access“, auf Seite 11 bereitgestellt.

View-Verbindungsserver

View-Verbindungsserver mit der Option HTML Access muss auf dem Server installiert sein.

Wenn Sie die HTML Access-Komponente installieren, wird die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** für die Windows-Firewall konfiguriert, damit eingehender Datenverkehr auf dem TCP-Port 8443 zugelassen wird.

Sicherheitsserver

View-Sicherheitsserver: Die auf dem Server zu installierende View-Sicherheitsserver-Software muss dieselbe Version wie die dort installierte View-Verbindungsserver-Software aufweisen.

Wenn Clientsysteme von außerhalb der firmeneigenen Firewall eine Verbindung herstellen, empfiehlt VMware die Verwendung eines Sicherheitsservers. Mit einem Sicherheitsserver erfordern die Clientsysteme keine VPN-Verbindung.

Hinweis Ein einzelner Sicherheitsserver kann bis zu 800 gleichzeitige Verbindungen mit Web Clients unterstützen.

Firewalls von Drittanbietern

Fügen Sie Regeln hinzu, um den folgenden Datenverkehr zuzulassen:

- Server (einschließlich Sicherheitsserver, View-Verbindungsserver-Instanzen und Replikatserver): eingehender Datenverkehr auf TCP-Port 8443.
- Virtuelle Maschinen des Remote-Desktops: eingehender Datenverkehr (von Servern) auf TCP-Port 22443.

Anzeigeprotokoll für View

VMware Blast

Wenn Sie einen Webbrowser für den Zugriff auf einen Remote-Desktop verwenden, wird anstelle von PCoIP oder Microsoft RDP das VMware Blast-Protokoll verwendet. VMware Blast basiert auf HTTPS (HTTP über SSL/TLS).

Vorbereiten von View-Verbindungsserver und Sicherheitsservern für HTML Access

Administratoren müssen spezifische Aufgaben ausführen, damit Endbenutzer über einen Webbrowser eine Verbindung mit Remote-Desktops herstellen können.

Bevor Endbenutzer eine Verbindung mit dem View-Verbindungsserver oder einem Sicherheitsserver herstellen und auf einen Remote-Desktop zugreifen können, müssen Sie den View-Verbindungsserver zusammen mit der HTML Access-Komponente sowie Sicherheitsserver installieren.

Im Folgenden finden Sie eine Checkliste mit Aufgaben, die vor der Verwendung von HTML Access auszuführen sind:

1 Installieren Sie View-Verbindungsserver zusammen mit der HTML Access-Option auf dem Server oder den Servern, der bzw. die eine replizierte View-Verbindungsservergruppe darstellen.

   Die HTML Access-Komponente ist im Installationsprogramm standardmäßig bereits ausgewählt. Anweisungen zur Installation finden Sie im Dokument *Installation von View*.

   Hinweis Um zu überprüfen, ob die HTML Access-Komponente installiert ist, können Sie im Windows-Betriebssystem das Applet zum Deinstallieren von Programmen öffnen und in der Liste nach „View HTML Access“ suchen.

2 Wenn Sie Sicherheitsserver verwenden, installieren Sie View-Sicherheitsserver.

   Anweisungen zur Installation finden Sie im Dokument *Installation von View*.

   Wichtig Die Version des View-Sicherheitsservers muss mit der Version des View-Verbindungsservers übereinstimmen.

3 Vergewissern Sie sich, dass jede View-Verbindungsserver-Instanz oder der Sicherheitsserver ein Sicherheitszertifikat besitzt, das der Client unter Verwendung des Hostnamens, den Sie im Browser eingeben, vollständig überprüfen kann.

   Weitere Informationen finden Sie im Dokument *Installation von View*.

4 Zum Verwenden der zweistufigen Authentifizierung, z. B. der RSA SecurID- oder RADIUS-Authentifizierung, muss diese Funktion auf dem View-Verbindungsserver aktiviert sein.

   Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Administration von View*

5 Wenn Sie eine Firewall eines Drittanbieters verwenden, konfigurieren Sie Regeln zum Zulassen von eingehendem Datenverkehr auf TCP-Port 8443 für alle Sicherheitsserver und View-Verbindungsserverhosts in einer replizierten Gruppe. Konfigurieren Sie außerdem eine Regel zum Zulassen von eingehendem Datenverkehr (von View-Servern) auf TCP-Port 22443 auf Remote-Desktops im Datencenter. Weitere Informationen finden Sie unter „Firewallregeln für HTML Access“, auf Seite 10.

Nach der Installation der Server werden Sie in View Administrator feststellen, dass die Einstellung **Blast Secure Gateway** für die betreffenden View-Verbindungsserver-Instanzen und Sicherheitsserver aktiviert ist. Darüber hinaus ist für die Einstellung **Externe Blast-URL** automatisch die Verwendung von Blast Secure Gateway auf den betreffenden View-Verbindungsserver-Instanzen und Sicherheitsservern konfiguriert. Standardmäßig enthält die URL den FQDN der externen URL für den sicheren Tunnel sowie die standardmäßige Portnummer, 8443. Die URL muss den FQDN und eine Portnummer enthalten, die ein Clientsystem zum Erreichen dieses View-Verbindungsserverhosts oder Sicherheitsserverhosts verwenden kann. Weitere Informationen finden Sie unter „Festlegen der externen URLs für eine View-Verbindungsserver-Instanz“ im Dokument *Installation von View*.

Hinweis Sie können HTML Access zusammen mit VMware Workspace Portal verwenden, damit Benutzer über einen HTML5-Browser eine Verbindung zu ihren Desktops herstellen können. Informationen zur Installation von Workspace Portal und der Konfiguration für die Verwendung mit dem View-Verbindungsserver finden Sie in der Workspace Portal-Dokumentation. Weitere Informationen zur Kopplung von View-Verbindungsserver mit einem SAML-Authentifizierungsserver finden Sie in der Dokumentation *Administration von View*.

Firewallregeln für HTML Access

Um Client-Webbrowsern zu ermöglichen, HTML Access zur Herstellung einer Verbindung zum Sicherheitsserver, zu View-Verbindungsserver-Instanzen und zu Remote-Desktops zu verwenden, müssen Ihre Firewalls eingehenden Datenverkehr auf bestimmten TCP-Ports erlauben.

HTML Access-Verbindungen müssen HTTPS verwenden. HTTP-Verbindungen sind nicht erlaubt.

Bei der Installation einer View-Verbindungsserver-Instanz oder eines Sicherheitsservers wird standardmäßig die Regel **VMware Horizon View-Verbindungsserver (Blast-In)** für die Windows-Firewall konfiguriert, damit eingehender Datenverkehr auf dem TCP-Port 8443 zugelassen wird.

Tabelle 1-1. Firewallregeln für HTML Access

Quelle	Standard-quell-Port	Protokoll	Ziel	Standardziel-Port	Hinweise
Client-Webbrowser	TCP beliebig	HTTPS	Sicherheitsserver oder View-Verbindungsserver-Instanz	TCP 443	Um die erste Verbindung zu View herzustellen, verbindet sich der Webbrowser auf einem Clientgerät an TCP-Port 443 mit einem Sicherheitsserver oder einer View-Verbindungsserver-Instanz.
Client-Webbrowser	TCP beliebig	HTTPS	Blast Secure Gateway	TCP 8443	Nachdem die erste Verbindung mit View hergestellt ist, stellt der Webbrowser auf einem Clientgerät an TCP-Port 8443 eine Verbindung mit dem Blast Secure Gateway her. Das Blast Secure Gateway muss auf einem Sicherheitsserver oder einer View-Verbindungsserver-Instanz aktiviert sein, damit diese zweite Verbindung erfolgen kann.

Tabelle 1-1. Firewallregeln für HTML Access (Fortsetzung)

Quelle	Standard-quell-Port	Protokoll	Ziel	Standardziel-Port	Hinweise
Blast Secure Gateway	TCP beliebig	HTTPS	HTML Access-Agent	TCP 22443	Ist das Blast Secure Gateway, nachdem der Benutzer einen Remote-Desktop ausgewählt hat, aktiviert, stellt das Blast Secure Gateway über den TCP-Port 22443 auf dem Desktop eine Verbindung zum HTML Access-Agent her. Diese Agent-Komponente ist Bestandteil der Installation von View Agent.
Client-Webbrowser	TCP beliebig	HTTPS	HTML Access-Agent	TCP 22443	Ist das Blast Secure Gateway, nachdem der Benutzer einen View-Desktop ausgewählt hat, nicht aktiviert, erstellt der Webbrowser auf einem Client-Gerät über den TCP-Port 22443 auf dem Desktop eine direkte Verbindung zum HTML Access-Agent. Diese Agent-Komponente ist Bestandteil der Installation von View Agent.

Vorbereiten von Desktops, Pools und Farmen für HTML Access

Bevor Endbenutzer auf einen Remote-Desktop oder eine Remoteanwendung zugreifen können, müssen Administratoren bestimmte Pool- und Farm-Einstellungen konfigurieren und View Agent auf den virtuellen Maschinen des Remote-Desktops sowie auf RDS-Hosts im Datencenter installieren.

Der HTML Access-Client ist eine gute Alternative, wenn die Horizon Client-Software nicht auf dem Clientsystem installiert ist.

Hinweis Die Horizon Client-Software bietet mehr Funktionen und eine höhere Leistung als der HTML Access-Client. Beispielsweise funktionieren beim HTML Access-Client einige Tastenkombinationen auf dem Remote-Desktop nicht, sie funktionieren allerdings bei Horizon Client.

Voraussetzungen

- Stellen Sie sicher, dass Ihre vSphere Infrastruktur- und View-Komponenten die Systemanforderungen für HTML Access erfüllen.

  Siehe „Systemanforderungen für HTML Access“, auf Seite 7.

- Vergewissern Sie sich, dass die HTML Access-Komponente zusammen mit dem View-Verbindungsserver auf dem Host bzw. den Hosts installiert ist, und dass die Windows-Firewall auf den View-Verbindungsserver-Instanzen und allen Sicherheitsservern eingehenden Datenverkehr auf TCP-Port 8443 zulassen.

  Siehe „Vorbereiten von View-Verbindungsserver und Sicherheitsservern für HTML Access“, auf Seite 9.

- Wenn Sie eine Firewall eines Drittanbieters verwenden, konfigurieren Sie eine Regel, mit der eingehender Datenverkehr von View Servern auf TCP-Port 22443 für die View-Desktops im Datencenter zugelassen wird.

- Stellen Sie sicher, dass die folgende Software in der angegebenen Reihenfolge auf der virtuellen Maschine installiert wurde, die Sie als Desktop-Quelle oder RDS-Host verwenden möchten: ein unterstütztes Betriebssystem und VMware Tools.

  Eine Liste der unterstützten Betriebssysteme finden Sie unter „Systemanforderungen für HTML Access“, auf Seite 7.

- Machen Sie sich mit den Verfahren für das Erstellen von Pools sowie Farmen und für das Zuweisen von Benutzerberechtigungen vertraut. Weitere Informationen finden Sie in den Themen zur Erstellung von Pools und Farmen im Dokument *Einrichten von Desktops und Anwendungen in View*.

- Um sicherzustellen, dass der Remote-Desktop oder die Remoteanwendung für Endbenutzer zugänglich ist, müssen Sie überprüfen, ob die Horizon Client-Software auf einem Clientsystem installiert wurde. Testen Sie die Verbindung, indem Sie die Horizon Client-Software verwenden, bevor Sie über einen Browser eine Verbindung herzustellen versuchen.

  Anweisungen zur Installation von Horizon Client finden Sie auf der Website für die Horizon Client-Dokumentation unter https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

- Stellen Sie sicher, dass Sie einen der unterstützten Browser für den Zugriff auf einen Remote-Desktop verwenden. Siehe „Systemanforderungen für HTML Access“, auf Seite 7.

Vorgehensweise

1. Für RDS-Desktops und -Anwendungen erstellen oder bearbeiten Sie die Farm mit View Administrator und aktivieren Sie die Option **HTML Access für Desktops und Anwendungen in dieser Farm zulassen** in den Farm-Einstellungen.
2. Bei Einzelsitzungs-Desktop-Pools erstellen oder bearbeiten Sie den Desktop-Pool mit View Administrator, damit dieser mit HTML Access verwendet werden kann.
   a. Aktivieren Sie **HTML Access** in den Desktop-Pool-Einstellungen.

      Die Einstellung **HTML Access** erscheint nicht im Assistenten „Desktop-Pool hinzufügen“ beim Erstellen von RDS-Desktop-Pools. Stattdessen aktivieren Sie die Option **HTML Access für Desktops und Anwendungen in dieser Farm zulassen** beim Erstellen oder Bearbeiten der Farm von RDS-Hosts.

   b. Stellen Sie sicher, dass in den Pool-Einstellungen die **Maximale Auflösung für alle Monitore** auf **1920x1200** oder höher festgelegt ist.
3. Nach der Erstellung, Neuzusammenstellung oder Aktualisierung der Pools für die Verwendung von View Agent mit der **HTML Access**-Option melden Sie sich mit Horizon Client bei einem Desktop oder einer Anwendung an.

   Mit diesem Schritt stellen Sie noch vor der Verwendung von HTML Access sicher, dass der Pool ordnungsgemäß arbeitet.
4. Öffnen Sie einen unterstützten Browser und geben Sie eine URL ein, die auf Ihre View-Verbindungsserver-Instanz zeigt.

   Beispiel:

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

   Stellen Sie sicher, dass Sie **`https`** in der URL verwenden.
5. Klicken Sie auf der angezeigten Webseite auf **VMware Horizon HTML Access** und melden Sie sich so wie bei der Horizon Client-Software an.
6. Klicken Sie auf der eingeblendeten Auswahlseite für Desktops und Anwendungen zur Herstellung der Verbindung auf ein Symbol.

Sie können jetzt über einen Webbrowser auf einen Remote-Desktop oder eine Remoteanwendung zugreifen, wenn Sie ein Clientgerät verwenden, für das die Horizon Client-Software nicht im Betriebssystem installiert ist oder installiert werden kann.

Weiter

Zur Erhöhung der Sicherheit oder für den Fall, dass Ihre Sicherheitsrichtlinien für den Blast-Agent auf dem Remote-Desktop die Verwendung eines SSL-Zertifikats einer Zertifizierungsstelle vorsehen, finden Sie weitere Informationen unter „Konfigurieren von HTML Access-Agents zur Verwendung von neuen SSL-Zertifikaten“, auf Seite 13.

Konfigurieren von HTML Access -Agents zur Verwendung von neuen SSL-Zertifikaten

Um Industrie- oder Sicherheitsvorschriften zu entsprechen, ersetzen Sie die Standard-SSL-Zertifikate, die vom HTML Access-Agent mit Zertifikaten erstellt wurden, die von einer Certificate Authority (CA) signiert wurden.

Wenn Sie den HTML Access-Agent auf View-Desktops installieren, erstellt der HTML Access-Agent-Dienst standardmäßig selbst signierte Zertifikate. Der Dienst liefert die Standardzertifikate an Browser, die HTML Access zur Herstellung einer Verbindung zu View verwenden.

Hinweis Im Gast-Betriebssystem auf der virtuellen Desktop-Maschine wird dieser Dienst VMware Blast-Dienst genannt.

Um die Standardzertifikate durch signierte Zertifikate zu ersetzen, die Sie von einer Zertifizierungsstelle erhalten haben, müssen Sie auf jedem View-Desktop ein Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers importieren. Außerdem müssen Sie auf jedem Desktop einen Registrierungswert festlegen, der es dem HTML Access-Agent ermöglicht, das neue Zertifikat zu verwenden.

Wenn Sie die standardmäßigen HTML Access-Agent-Zertifikate durch CA-signierte Zertifikate ersetzt haben, empfiehlt VMware, dass Sie ein eindeutiges Zertifikat auf jedem einzelnen Desktop konfigurieren. Konfigurieren Sie kein CA-Zertifikat auf einer übergeordneten virtuellen Maschine oder Vorlage, die Sie für das Erstellen eines Desktop-Pools verwenden. Dieser Ansatz würde zu Hunderten oder Tausenden Desktops mit identischen Zertifikaten führen.

Vorgehensweise

1 Hinzufügen des Zertifikat-Snap-In zur MMC auf einem View-Desktop auf Seite 14

Bevor Sie Zertifikate im lokalen Windows-Zertifikatspeicher des Computers hinzufügen können, müssen Sie das Zertifikats-Snap-In der Microsoft Management Console (MMC) auf den View-Desktops hinzufügen, auf denen der HTML Access-Agent installiert ist.

2 Importieren eines Zertifikats für den HTML Access Agent in den Windows-Zertifikatspeicher auf Seite 14

Um ein standardmäßiges HTML Access-Agent-Zertifikat durch ein CA-Zertifikat zu ersetzen, müssen Sie das CA-Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers importieren. Führen Sie diese Prozedur auf jedem Desktop durch, auf dem der HTML Access-Agent installiert ist.

3 Importieren von Stamm- und Zwischenzertifikaten für den HTML Access-Agent auf Seite 15

Wenn die Stamm- und Zwischenzertifikate in der Zertifikatskette nicht mit dem SSL-Zertifikat importiert werden, das Sie für den HTML Access-Agent importiert haben, müssen Sie diese Zertifikate in den lokalen Windows-Zertifikatsspeicher des Computers importieren.

4 Festlegen des Zertifikatfingerabdrucks in der Windows-Registrierung auf Seite 16

Um dem HTML Access-Agenten zu ermöglichen, ein durch eine Zertifizierungsstelle signiertes Zertifikat zu verwenden, das in den Windows-Zertifikatsspeicher importiert wurde, müssen Sie den Fingerabdruck des Zertifikats in einem Windows-Registrierungsschlüssel konfigurieren. Sie müssen diesen Schritt auf jedem Desktop vornehmen, auf dem Sie das Standardzertifikat durch ein durch eine Zertifizierungsstelle signiertes Zertifikat ersetzen.

Hinzufügen des Zertifikat-Snap-In zur MMC auf einem View-Desktop

Bevor Sie Zertifikate im lokalen Windows-Zertifikatspeicher des Computers hinzufügen können, müssen Sie das Zertifikats-Snap-In der Microsoft Management Console (MMC) auf den View-Desktops hinzufügen, auf denen der HTML Access-Agent installiert ist.

Voraussetzungen

Stellen Sie sicher, dass die MMC und das Zertifikats-Snap-In in dem Windows-Gast-Betriebssystem verfügbar sind, in dem der HTML Access-Agent installiert wurde.

Vorgehensweise

1 Klicken Sie auf dem View-Desktop auf **Start** und geben Sie **`mmc.exe`** ein.

2 Gehen Sie im Fenster MMC auf **Datei > Snap-In hinzufügen/entfernen**.

3 Wählen Sie im Fenster Snap-Ins hinzufügen oder entfernen **Zertifikate** aus und klicken Sie auf **Hinzufügen**.

4 Wählen Sie im Fenster Zertifikat-Snap-In **Computerkonto**, klicken Sie auf **Weiter**, wählen Sie **Lokaler Computer** und klicken Sie auf **Fertig stellen**.

5 Klicken Sie im Fenster Snap-In hinzufügen oder entfernen auf **OK**.

Weiter

Importieren Sie das SSL-Zertifikat in den Zertifikatsspeicher des lokalen Windows-Computers auf dem View Server-Host. Siehe „Importieren eines Zertifikats für den HTML Access Agent in den Windows-Zertifikatspeicher“, auf Seite 14.

Importieren eines Zertifikats für den HTML Access Agent in den Windows-Zertifikatspeicher

Um ein standardmäßiges HTML Access-Agent-Zertifikat durch ein CA-Zertifikat zu ersetzen, müssen Sie das CA-Zertifikat in den lokalen Windows-Zertifikatspeicher des Computers importieren. Führen Sie diese Prozedur auf jedem Desktop durch, auf dem der HTML Access-Agent installiert ist.

Voraussetzungen

- Stellen Sie sicher, dass der HTML Access-Agent auf dem View-Desktop installiert ist.
- Stellen Sie sicher, dass das CA-Zertifikat auf den Desktop kopiert wurde.
- Überprüfen Sie, ob das Zertifikat-Snap-In der MMC hinzugefügt wurde. Siehe „Hinzufügen des Zertifikat-Snap-In zur MMC auf einem View-Desktop“, auf Seite 14.

Vorgehensweise

1 Erweitern Sie im Fenster MMC auf dem View-Desktop den Knoten **Zertifikate (Lokaler Computer)** und wählen Sie den Ordner **Persönlich**.

2 Wechseln Sie im Bereich „Aktionen“ zu **Weitere Aktionen > Alle Aufgaben > Importieren**.

3 Klicken Sie im Zertifikatsimport-Assistenten auf **Weiter** und navigieren Sie zum Speicherort des Zertifikats.

4 Wählen Sie die Zertifikatsdatei und klicken Sie auf **Öffnen**.

Um den Typ Ihrer Zertifikatsdatei anzuzeigen, können Sie ihr Dateiformat im Dropdown-Menü **Dateiname** auswählen.

5 Geben Sie das Kennwort für den privaten Schlüssel in der Zertifikatsdatei ein.

6 Aktivieren Sie **Schlüssel als exportierbar markieren**.

7 Aktivieren Sie **Alle erweiterbaren Eigenschaften mit einbeziehen**.

8 Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Das neue Zertifikat wird im Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** angezeigt.

9 Überprüfen Sie, ob das neue Zertifikat einen privaten Schlüssel enthält.

a Doppelklicken Sie im Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** auf das neue Zertifikat.

b Überprüfen Sie, ob im Dialogfeld „Zertifikatinformationen“ auf der Registerkarte „Allgemein“ die folgende Aussage angezeigt wird: `Sie besitzen einen privaten Schlüssel für dieses Zertifikat`.

Weiter

Falls erforderlich, importieren Sie das Stammzertifikat und Zwischenzertifikate in den Windows-Zertifikatsspeicher. Siehe „Importieren von Stamm- und Zwischenzertifikaten für den HTML Access-Agent“, auf Seite 15.

Konfigurieren Sie die entsprechenden Registrierungsschlüssel mit dem Fingerabdruck des Zertifikats. Siehe „Festlegen des Zertifikatfingerabdrucks in der Windows-Registrierung“, auf Seite 16.

Importieren von Stamm- und Zwischenzertifikaten für den HTML Access -Agent

Wenn die Stamm- und Zwischenzertifikate in der Zertifikatskette nicht mit dem SSL-Zertifikat importiert werden, das Sie für den HTML Access-Agent importiert haben, müssen Sie diese Zertifikate in den lokalen Windows-Zertifikatsspeicher des Computers importieren.

Vorgehensweise

1 Auf der MMC-Konsole auf View-Desktop erweitern Sie den Knoten **Zertifikate (Lokaler Computer)** und gehen Sie zum Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.

- Wenn sich Ihr Stammzertifikat in diesem Ordner befindet und Ihre Zertifikatskette keine Zwischenzertifikate enthält, übergehen Sie diese Prozedur.
- Wenn Ihr Stammzertifikat sich nicht in diesem Ordner befindet, fahren Sie mit Schritt 2 fort.

2 Klicken Sie mit der rechten Maustaste auf den Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** und klicken Sie auf **Alle Aufgaben > Importieren**.

3 Klicken Sie im Zertifikatsimport-Assistenten auf **Weiter** und navigieren Sie zum Speicherort des Stamm-Zertifizierungsstellenzertifikats.

4 Wählen Sie die Datei mit dem Stamm-Zertifizierungsstellenzertifikat aus und klicken Sie auf **Öffnen**.

5 Klicken Sie auf **Weiter**, klicken Sie auf **Weiter** und klicken Sie auf **Fertigstellen**.

6 Wenn Ihr Serverzertifikat von einer Zwischenzertifizierungsstelle signiert wurde, importieren Sie alle Zwischenzertifikate in der Zertifikatskette in den Zertifikatspeicher des lokalen Windows-Computers.

a Navigieren Sie zum Ordner **Zertifikate (Lokaler Computer) > Zwischenzertifizierungsstellen > Zertifikate**.

b Wiederholen Sie die Schritte 3 bis 6 für jedes zu importierende Zwischenzertifikat.

Weiter

Konfigurieren Sie die entsprechenden Registrierungsschlüssel mit dem Fingerabdruck des Zertifikats. Siehe „Festlegen des Zertifikatfingerabdrucks in der Windows-Registrierung“, auf Seite 16.

Festlegen des Zertifikatfingerabdrucks in der Windows-Registrierung

Um dem HTML Access-Agenten zu ermöglichen, ein durch eine Zertifizierungsstelle signiertes Zertifikat zu verwenden, das in den Windows-Zertifikatsspeicher importiert wurde, müssen Sie den Fingerabdruck des Zertifikats in einem Windows-Registrierungsschlüssel konfigurieren. Sie müssen diesen Schritt auf jedem Desktop vornehmen, auf dem Sie das Standardzertifikat durch ein durch eine Zertifizierungsstelle signiertes Zertifikat ersetzen.

Voraussetzungen

Stellen Sie sicher, dass das durch die Zertifizierungsstelle signierte Zertifikat in den Windows-Zertifikatsspeicher importiert wurde. Siehe „Importieren eines Zertifikats für den HTML Access Agent in den Windows-Zertifikatspeicher“, auf Seite 14.

Vorgehensweise

1 Navigieren Sie im MMC-Fenster auf dem View-Desktop, auf dem der HTML Access-Agent installiert ist, zum Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate**.

2 Doppelklicken Sie auf das von Ihnen in den Windows-Zertifikatsspeicher importierte durch die Zertifizierungsstelle signierte Zertifikat.

3 Klicken Sie im Dialogfeld „Zertifikate“ auf die Registerkarte „Details“. Blättern Sie nach unten, und wählen Sie das Symbol **Fingerabdruck** aus.

4 Kopieren Sie den ausgewählten Fingerabdruck in eine Textdatei.

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

Hinweis Schließen Sie beim Kopieren des Fingerabdrucks das führende Leerzeichen nicht ein. Wenn Sie das führende Leerzeichen versehentlich zusammen mit dem Fingerabdruck in den Registrierungsschlüssel (in Schritt 7) einfügen, wird das Zertifikat möglicherweise nicht erfolgreich konfiguriert. Dieses Problem kann auftreten, auch wenn das führende Leerzeichen im Registrierungswert-Textfeld nicht angezeigt wird.

5 Starten Sie den Windows-Registrierungs-Editor auf dem Desktop, wo der HTML Access-Agent installiert ist.

6 Navigieren Sie zum Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config`.

7 Ändern Sie den Wert `SslHash`, und fügen Sie den Fingerabdruck des Zertifikats in das Textfeld ein.

8 Starten Sie Windows neu.

Wenn ein Benutzer über HTML Access eine Verbindung zu einem Desktop herstellt, stellt der HTML Access-Agent dem Browser des Benutzers das durch eine Zertifizierungsstelle signiertes Zertifikat aus.

Konfiguration der HTML Access-Agents zur Verwendung spezifischer Verschlüsselungsansammlungen

Sie können den HTML Access-Agent so konfigurieren, dass er anstelle der standardmäßigen Verschlüsselungen spezifische Verschlüsselungsansammlungen verwendet.

Der HTML Access-Agent erfordert standardmäßig eingehende SSL-Verbindungen, um Verschlüsselungen auf Basis bestimmter Verschlüsselungsverfahren, die umfassend gegen das Abhören und Fälschen von Netzwerken geschützt sind, verwenden zu können. Sie können eine alternative Liste mit Verschlüsselungsverfahren zur Verwendung durch den HTML Access-Agent konfigurieren. Der Satz mit akzeptablen Verschlüsselungsverfahren wird im OpenSSL-Format ausgedrückt, das unter https://www.openssl.org/docs/apps/ciphers.html beschrieben ist.

Vorgehensweise

1 Starten Sie den Windows-Registrierungs-Editor auf dem Desktop, wo der HTML Access-Agent installiert ist.

2 Navigieren Sie zum Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config`.

3 Fügen Sie einen neuen Zeichenfolgenwert (REG_SZ) hinzu, `SslCiphers`, und fügen Sie die Verschlüsselungsliste im OpenSSL-Format in das Textfeld ein.

4 Starten Sie den VMware Blast-Dienst neu, damit Ihre Änderungen wirksam werden.

   Im Windows-Gast-Betriebssystem wird der Dienst für den HTML Access-Agent VMware Blast genannt.

Um zur Nutzung der standardmäßigen Verschlüsselungsliste zurückzukehren, löschen Sie den `SslCiphers`-Wert und starten Sie den VMware Blast-Dienst neu. Löschen Sie nicht einfach den Datenteil des Werts, sonst behandelt der HTML Access-Agent alle Verschlüsselungsverfahren entsprechend der Formatdefinition für die OpenSSL-Verschlüsselungsliste als inakzeptabel.

Wenn der HTML Access-Agent startet, schreibt er die Verschlüsselungsdefinition in die Protokolldatei des VMware Blast-Dienstes. Sie können die aktuelle standardmäßige Verschlüsselungsliste ermitteln, indem Sie die Protokolle beim Start des VMware Blast-Dienstes prüfen, der keinen `SslCiphers`-Wert in der Windows-Registrierung konfiguriert hat.

Die standardmäßige Verschlüsselungsdefinition des HTML Access-Agent kann sich von einer Version zur anderen unterscheiden, um einen verbesserten Schutz zu bieten.

Konfigurieren von iOS zur Verwendung von durch Zertifizierungsstellen signierten Zertifikaten

Für die Verwendung von HTML Access auf iOS-Geräten müssen Sie SSL-Zertifikate installieren, die von einer Zertifizierungsstelle signiert wurden, anstelle von Standard-SSL-Zertifikaten, die durch den View-Verbindungsserver auf dem HTML Access Agent erstellt wurden.

Anweisungen dazu finden Sie unter „Konfigurieren von Horizon Client für iOS für vertrauenswürdige und Zwischenzertifikate“ im Dokument *View-Installation*.

Upgrade der HTML Access -Software

Für die meisten Versionen von HTML Access ist nur ein Upgrade der Verbindungsserver und von View Agent erforderlich.

Wenn Sie ein Upgrade für HTML Access durchführen, müssen Sie sicherstellen, dass die entsprechende Version des View-Verbindungsservers auf allen Instanzen einer replizierten Gruppe installiert ist.

Beim Aktualisieren des Verbindungsservers wird HTML Access automatisch installiert oder aktualisiert.

Hinweis Um zu überprüfen, ob die HTML Access-Komponente installiert ist, können Sie im Windows-Betriebssystem das Applet zum Deinstallieren von Programmen öffnen und in der Liste nach HTML Access suchen.

Deinstallieren von HTML Access vom View-Verbindungsserver

Sie können HTML Access mit der gleichen Methode entfernen, mit der Sie andere Windows-Software entfernen.

Vorgehensweise

1 Öffnen Sie auf den View-Verbindungsserverhosts, auf denen HTML Access installiert ist, in der Windows-Systemsteuerung das Applet zum Deinstallieren von Programmen.

2 Wählen Sie das Programm VMware Horizon 7 HTML Access aus, und klicken Sie auf **Deinstallieren**.

3 (Optional) Stellen Sie in der Windows-Firewall für diesen Host sicher, dass der TCP-Port 8443 keinen eingehenden Datenverkehr mehr erlaubt.

Weiter

Verhindern Sie eingehenden Datenverkehr an TCP-Port 8443 auf der Windows-Firewall aller gepaarten Sicherheitsserver. Auf Firewalls von Drittanbietern ändern Sie gegebenenfalls die Regeln, um eingehenden Datenverkehr an TCP-Port 8443 für alle gepaarten Sicherheitsserver und diesen View-Verbindungsserverhost zu verbieten.

Von VMware erfasste Daten

Wenn Ihr Unternehmen am Programm zur Verbesserung der Benutzerfreundlichkeit teilnimmt, erhebt VMware Daten aus bestimmten Client-Feldern. Felder mit vertraulichen Informationen werden anonymisiert.

VMware sammelt die Daten auf den Clients zur Priorisierung der Hardware- und Softwarekompatibilität. Wenn sich ein View-Administrator zur Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit entscheidet, sammelt VMware anonyme Daten über Ihre Bereitstellung, um die Reaktion von VMware auf die Kundenanforderungen verbessern zu können. Es werden jedoch keine Daten gesammelt, die Aufschluss über Ihr Unternehmen geben könnten. Die Client-Informationen werden erst an den View-Verbindungsserver und dann an VMware gesendet, zusammen mit den Daten der Server, Desktop-Pools und Remote-Desktops.

Zur Teilnahme am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit kann der Administrator, der die Installation des View-Verbindungsservers durchführt, bei der Ausführung des Installations-Assistenten für den View-Verbindungsserver diese Option „abonnieren“ oder nach der Installation eine entsprechende Option in View Administrator festlegen.

Tabelle 1-2. Für das Programm zur Verbesserung der Benutzerfreundlichkeit erfasste Clientdaten

Beschreibung	Feldname	Wird dieses Feld anonymisiert?	Beispielswert
Unternehmen, das die Anwendung hergestellt hat	`<client-vendor>`	Nein	VMware
Produktname	`<client-product>`	Nein	VMware Horizon View Access
Client-Produktversion	`<client-version>`	Nein	4.1.0-*build_number*

Tabelle 1-2. Für das Programm zur Verbesserung der Benutzerfreundlichkeit erfasste Clientdaten (Fortsetzung)

Beschreibung	Feldname	Wird dieses Feld anonymisiert?	Beispielswert
Client-Binärarchitektur	`<client_arch>`	Nein	Beispiele hierfür sind folgende Werte: ■ Browser ■ arm
Systemeigene Architektur des Browsers	`<browser_arch>`	Nein	Beispiele hierfür sind folgende Werte: ■ Win32 ■ Win64 ■ MacIntel ■ iPad
Zeichenfolge zum Browserbenutzer-Agent	`<browser_user_agent>`	Nein	Beispiele hierfür sind folgende Werte: ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 (KHTML, wie Gecko) ■ Chrome/3.0.1750 ■ Safari/703.00 ■ Edge/13.10586
Interne Versionszeichenfolge des Browsers	`<browser_version>`	Nein	Beispiele hierfür sind folgende Werte: ■ 7.0.3 (für Safari), ■ 44.0 (für Firefox) ■ 13.10586 (für Edge)
Core-Implementierung des Browsers	`<browser_core>`	Nein	Beispiele hierfür sind folgende Werte: ■ Chrome ■ Safari ■ Firefox ■ Internet Explorer ■ Edge
Angabe, ob der Browser auf einem Handheld-Gerät ausgeführt wird	`<browser_is_handheld>`	Nein	true

Konfigurieren von HTML Access für Endbenutzer 2

Sie können das Aussehen der Webseite ändern, die Endbenutzer bei Eingabe der URL für HTML Access sehen. Sie können außerdem Gruppenrichtlinien festlegen, mit denen Bildqualität, verwendete Ports und weitere Einstellungen gesteuert werden.

Dieses Kapitel behandelt die folgenden Themen:

Konfigurieren der VMware Horizon -Webportalseite für Endbenutzer

Sie können diese Webseite so konfigurieren, dass das Symbol zum Herunterladen von Horizon Client oder das Symbol für die Herstellung einer Verbindung mit einem Remote-Desktop über HTML Access angezeigt oder ausgeblendet wird. Sie können außerdem weitere Links auf dieser Seite konfigurieren.

Standardmäßig werden auf der Portalseite ein Symbol für den Download und die Installation des nativen Horizon Client sowie ein Symbol für die Verbindungsherstellung über HTML Access angezeigt. In einigen Fällen sollen die Links jedoch auf einen internen Webserver verweisen oder Sie möchten bestimmte Clientversionen auf Ihrem eigenen Server zur Verfügung stellen. Sie können die Seite neu konfigurieren, sodass sie auf eine andere URL verweist.

Sie können Links zu Installationsprogrammen für bestimmte Client-Betriebssysteme erstellen. Wenn Sie beispielsweise die Portalseite auf einem Mac OS X-System öffnen, wird der Link für das native Mac OS X-Installationsprogramm angezeigt. Für Windows-Clients können Sie separate Links für die 32-Bit- und 64-Bit-Installationsprogramme erstellen.

Wichtig Wenn Sie ein Upgrade von View-Verbindungsserver 5.x oder einer älteren Version durchgeführt haben, die HTML Access-Komponente bisher nicht installiert war und Sie die Portalseite zuvor so bearbeitet haben, dass sie auf Ihren eigenen Server zum Download von Horizon Client verweist, werden diese Anpassungen möglicherweise ausgeblendet, wenn Sie View-Verbindungsserver 6.0 oder höher installieren. Bei Horizon 6 oder höher wird die HTML Access-Komponente bei einem Upgrade von View-Verbindungsserver automatisch installiert.

Wenn Sie die HTML Access-Komponente bereits separat für View 5.x installiert hatten, werden alle Anpassungen, die Sie an der Webseite vorgenommen haben, beibehalten. Wenn Sie die HTML Access-Komponente nicht installiert hatten, werden Ihre Anpassungen ausgeblendet. Die Anpassungen für frühere Versionen befinden sich in der Datei `portal-links.properties`, die nicht mehr verwendet wird.

Vorgehensweise

1 Öffnen Sie auf dem View-Verbindungsserverhost die Datei `portal-links-html-access.properties` mit einem Texteditor.

Der Speicherort dieser Datei lautet *`CommonAppDataFolder`*`\VMware\VDM\portal\portal-links-html-access.properties`. Auf Windows Server 2008-Betriebssystemen entspricht das Verzeichnis *CommonAppDataFolder* dem Ordner `C:\ProgramData`. Zur Anzeige des Ordners `C:\ProgramData` in Windows Explorer müssen Sie im Dialogfeld mit den Ordneroptionen die Anzeige ausgeblendeter Ordner aktivieren.

Hinweis Die Anpassungen für View 5.x und frühere Versionen befanden sich in der Datei `portal-links.properties`, die sich im selben Verzeichnis *`CommonAppDataFolder`*`\VMware\VDM\portal\` befindet wie die Datei `portal-links-html-access.properties`.

2 Bearbeiten Sie die Konfigurationseigenschaften nach Bedarf.

Standardmäßig sind das Installationsprogramm-Symbol und das HTML Access-Symbol aktiviert und ein Link verweist auf die Client-Download-Seite auf der VMware-Website. Wenn Sie ein Symbol deaktivieren möchten, stellen Sie die Eigenschaft auf `false` ein. Dadurch wird das Symbol aus der Webseite entfernt.

Option	Eigenschafteneinstellung
HTML Access deaktivieren	`enable.webclient=false` Wenn für diese Option „false“ festgelegt ist, aber für die Option `enable.download` der Wert „true“ gesetzt ist, wird der Benutzer zu einer Webseite geleitet, von der das native Installationsprogramm für Horizon Client heruntergeladen werden kann. Wenn für beide Optionen der Wert „false“ festgelegt ist, wird dem Benutzer die folgende Nachricht angezeigt: „`Wenden Sie sich an Ihren lokalen Administrator, um Anweisungen zum Zugriff auf diesen Verbindungsserver zu erhalten.`“
Herunterladen von Horizon Client deaktivieren	`enable.download=false` Wenn für diese Option „false“ festgelegt ist, aber für die Option `enable.webclient` der Wert „true“ gesetzt ist, wird der Benutzer zur Anmeldeseite für HTML Access geleitet. Wenn für beide Optionen der Wert „false“ festgelegt ist, wird dem Benutzer die folgende Nachricht angezeigt: „`Wenden Sie sich an Ihren lokalen Administrator, um Anweisungen zum Zugriff auf diesen Verbindungsserver zu erhalten.`“
Ändern der URL für die Webseite zum Herunterladen von Horizon Client	`link.download=https://`*`url-of-web-server`* Verwenden Sie diese Eigenschaft, wenn Sie Ihre eigene Webseite erstellen möchten.

Option	Eigenschafteneinstellung

Create links for specific installers (Links für bestimmte Installationsprogramme erstellen)	Die folgenden Beispiele enthalten vollständige URLs; Sie können jedoch auch relative URLs verwenden, wenn Sie, wie im nächsten Schritt beschrieben, die Installationsdateien in dem Verzeichnis „`downloads`“ ablegen, das sich im Verzeichnis `C:\Programme\VMware\VMware View\Server\broker\webapps\` auf dem View-Verbindungsserver befindet.
	■ 32-Bit-Windows-Installationsprogramm:
	`link.win32=https://server/downloads/VMware-Horizon-Client.exe`
	■ 64-Bit-Windows-Installationsprogramm:
	`link.win64=https://server/downloads/VMware-Horizon-Client.exe`
	■ Linux-Installationsprogramm:
	`link.linux=https://server/downloads/VMware-Horizon-Client.tar.gz`
	■ Mac OS X-Installationsprogramm:
	`link.mac=https://server/downloads/VMware-Horizon-Client.dmg`
	■ iOS-Installationsprogramm:
	`link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS.zip`
	■ Android-Installationsprogramm:
	`link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS.apk`
	■ Installationsprogramm für ein unbekanntes Betriebssystem (z. B. können Sie diese Eigenschaft für das Installationsprogramm eines Chrome-Client verwenden):
	`link.unknown=https://server/downloads/VMware-Horizon-Client-AndroidOS-arm-ARC.apk`

Ändern der URL für den Hilfe-Link auf der Anmeldeseite	`link.help` Dieser Link verweist standardmäßig auf ein Hilfesystem, das auf der VMware-Website verwaltet wird. Der Hilfe-Link wird auf der Anmeldeseite unten angezeigt.

3 Damit Benutzer die Installationsprogramme von einem anderen Speicherort als der VMware-Website herunterladen, legen Sie die Installationsdateien auf dem HTTP-Server ab, auf dem sich auch die Installationsdateien befinden.

Dieser Speicherort muss mit den URLs übereinstimmen, die Sie in der Datei „`portal-links-html-access.properties`“ im vorherigen Schritt angegeben haben. Um die Dateien beispielsweise in einem Verzeichnis „`downloads`“ auf dem View-Verbindungsserver-Host zu speichern, verwenden Sie den folgenden Pfad:

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

Die Links zu den Installationsdateien können dann relative URLs mit dem Format `/downloads/`*`client-installationsdateiname`* verwenden.

4 Starten Sie den View Web-Komponentendienst neu.

Verwenden von URIs zur Konfiguration von HTML Access -Webclients

Mithilfe so genannter Uniform Resource Identifiers (URIs) können Sie eine Webseite oder E-Mail mit verschiedenen Verknüpfungen erstellen, auf die die Endbenutzer zum Start von HTML Access Web client, zur Verbindung mit dem View-Verbindungsserver oder zum Start eines bestimmten Desktops oder einer bestimmten Anwendung mit bestimmten Konfigurationsoptionen klicken.

Sie können die Verbindungsherstellung mit einem Remote-Desktop oder einer Anwendung durch Erstellen von Web- oder E-Mail-Verknüpfungen für die Endbenutzer deutlich vereinfachen. Diese Verknüpfungen werden durch die Generierung von URIs erstellt, die einige oder alle der folgenden Informationen bereitstellen, sodass die Endbenutzer diese nicht angeben müssen:

- Adresse des View-Verbindungsservers
- Portnummer für den View-Verbindungsserver
- Active Directory-Benutzername
- RADIUS- oder RSA SecurID-Benutzername, falls dieser nicht mit dem Active Directory-Benutzernamen identisch ist
- Domänenname
- Desktop- oder Anwendungsanzeigename
- Aktionen, darunter „Durchsuchen“, „Zurücksetzen“, „Abmelden“ und „Sitzung starten“

Syntax für die Erstellung von URIs für HTML Access

Die Syntax umfasst eine Pfadkomponente zur Angabe des Servers sowie optional eine Abfrage zur Angabe eines Benutzers, des Desktops oder der Anwendung sowie Aktionen oder Konfigurationsoptionen.

URI-Spezifikation

Verwenden Sie zum Generieren von URIs für den Start von HTML Access-Webclients die folgende Syntax:

`https://authority_part[/?query_part]`

authority-part Gibt die Serveradresse und optional eine nicht standardmäßige Portnummer an. Die Servernamen müssen der DNS-Syntax entsprechen.

Verwenden Sie zur Angabe einer Portnummer die folgende Syntax:

`server_address:port_number`

query-part Gibt die zu verwendenden Konfigurationsoptionen oder die durchzuführenden Aktionen an. Für die Abfragen muss die Groß- und Kleinschreibung nicht beachtet werden. Verwenden Sie für den Einsatz mehrerer Abfragen das kaufmännische Und-Zeichen (&) zwischen den Abfragen. Sollten die Abfragen miteinander in Konflikt stehen, wird die letzte Abfrage in der Liste verwendet. Verwenden Sie die folgende Syntax:

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

Beachten Sie beim Erstellen der Abfragekomponente (query-part) die folgenden Richtlinien:

- Wenn Sie nicht mindestens eine der unterstützten Abfragen verwenden, wird die standardmäßige VMware Horizon-Webportalseite angezeigt.

- Für die Abfragekomponente werden einige Sonderzeichen nicht unterstützt; es muss deshalb für diese das URL-Codierungsformat wie folgt angewendet werden: Für das Hashzeichen (#, Doppelkreuz) verwenden Sie **%23**, für das Prozentzeichen (%) **%25**, für das Kaufmännische Und (&) den Platzhalter **%26**, für das At-Zeichen (@) **%40** und für den Rückschrägstrich (\) verwenden Sie **%5C**.

  Weitere Informationen zur URL-Codierung finden Sie unter http://www.w3schools.com/tags/ref_urlencode.asp.

- Für die Abfragekomponente müssen Nicht-ASCII-Zeichen zunächst gemäß UTF-8 [STD63] codiert werden, anschließend muss für jedes Oktett der entsprechenden UTF-8-Sequenz eine Prozentcodierung durchgeführt werden, um diese als URI-Zeichen darzustellen.

  Informationen zur Codierung von ASCII-Zeichen finden Sie in der URL-Codierungsreferenz unter http://www.utf8-chartable.de/.

Unterstützte Abfragen

In diesem Abschnitt werden die Abfragen aufgeführt, die für den HTML Access Web client unterstützt werden. Wenn Sie URIs für mehrere Clienttypen generieren, so zum Beispiel für Desktop-Clients oder mobile Clients, finden Sie für jede Art von Clientsystem weitere Anweisungen im Handbuch *Verwendung von VMware Horizon Client*.

domainName	Der NETBIOS-Domänenname, der mit dem Benutzer verknüpft ist, der eine Verbindung zum Remote-Desktop oder zur Remoteanwendung herstellt. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.
userName	Der Active Directory-Benutzer, der eine Verbindung zum Remote-Desktop oder zur Remote-Anwendung herstellt
tokenUserName	Der RSA- oder RADIUS-Benutzername. Verwenden Sie diese Abfrage nur, wenn der RSA- oder RADIUS-Benutzername nicht mit dem Active Directory-Benutzernamen identisch ist. Wenn Sie diese Abfrage nicht angeben und die RSA- oder RADIUS-Authentifizierung erforderlich ist, wird der Windows-Benutzername verwendet.
desktopId	Der Anzeigename des Desktops. Dieser Name wurde in View Administrator beim Erstellen des Desktop-Pools angegeben. Weist der Anzeigename ein Leerzeichen auf, verwendet der Browser automatisch **%20** zur Darstellung des Leerzeichens.

applicationId

Der Anzeigename der Anwendung. Dieser Name wurde in View Administrator beim Erstellen des Anwendungspools angegeben. Weist der Anzeigename ein Leerzeichen auf, verwendet der Browser automatisch **`%20`** zur Darstellung des Leerzeichens.

action

Tabelle 2-1. Werte, die mit der Abfrage „action“ verwendet werden können

Wert	Beschreibung
`browse`	Zeigt eine Liste der verfügbaren, auf dem angegebenen Server gehosteten Desktops und Anwendungen an. Bei Verwendung dieser Aktion müssen Sie keinen Desktop bzw. keine Anwendung angeben.
`start-session`	Startet den angegebenen Desktop oder die angegebene Anwendung. Wenn keine „action“-Abfrage bereitgestellt wird und der Desktop- oder Anwendungsname angegeben wird, ist `start-session` die Standardaktion.
`reset`	Fährt den angegebenen Desktop herunter und startet ihn neu. Nicht gespeicherte Daten gehen verloren. Das Zurücksetzen eines Remote-Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen PC. Diese Aktion ist für eine Anwendung ungültig.
`logoff`	Meldet den Benutzer vom Gastbetriebssystem auf dem Remote-Desktop ab. Diese Aktion ist für eine Anwendung ungültig.

Beispiele für URIs

Sie können Hypertext-Links oder Schaltflächen mit einem URI erstellen und diese Links in E-Mails oder auf einer Webseite einbinden. Ihre Endbenutzer können dann auf diese Links klicken, um beispielsweise einen bestimmten Remote-Desktop oder eine bestimmte Remoteanwendung mit den von Ihnen angegebenen Startoptionen zu starten.

URI-Syntaxbeispiele

Nach jedem URI-Beispiel finden Sie eine Beschreibung, was der Endbenutzer nach Anklicken des URI-Links sieht. Beachten Sie, dass für Abfragen die Groß-/Kleinschreibung nicht beachtet werden muss. Sie können beispielsweise **`domainName`** oder **`domainname`** verwenden.

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

Der HTML Access Web Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Im Anmeldefeld wird das Textfeld **Benutzername** mit dem Namen **fred** und das Textfeld **Domäne** mit **finance** gefüllt. Der Benutzer muss das Kennwort eingeben.

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

Der HTML Access Web Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **Primary Desktop** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet.

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

Der HTML Access Web Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach der erfolgreichen Anmeldung wird der Editor gestartet.

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

Dieser URI hat die gleiche Wirkung wie im vorherigen Beispiel, außer dass er den nicht standardmäßigen Port 7555 für den View-Verbindungsserver verwendet. (Der standardmäßige Port lautet 443.) Da eine Desktop-ID bereitgestellt wird, wird der Desktop gestartet, obwohl die Aktion `start-session` nicht im URI enthalten ist.

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

Dieser URI gibt eine Anwendung und einen Desktop an. Wenn Sie eine Anwendung und einen Desktop angeben, wird nur der Desktop gestartet.

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

Der HTML Access Web Client wird gestartet und stellt eine Verbindung mit dem Server `view.mycompany.com` her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt der Client ein Dialogfeld an, in dem der Benutzer aufgefordert wird, das Zurücksetzen für „Primary Desktop“ zu bestätigen.

Hinweis Diese Aktion ist nur verfügbar, wenn der View-Administrator den Endbenutzern das Zurücksetzen ihrer Maschinen erlaubt hat.

Beispiel für HTML-Code

Sie können URIs verwenden, um Hypertext-Links und Schaltflächen zu erstellen, die in E-Mails oder auf Webseiten eingebunden werden können. Die folgenden Beispiele veranschaulichen, wie Sie den URI aus dem ersten Beispiel verwenden, um einen Hypertext-Link mit dem Text **Test Link** besagt und eine Schaltfläche mit dem Text **TestButton** zu codieren.

```
<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>
```

Gruppenrichtlinieneinstellungen für HTML Access

HTML Access verwendet das VMware Blast-Protokoll. Sie konfigurieren Gruppenrichtlinien für HTML Access, indem Sie Gruppenrichtlinien für das VMware Blast-Protokoll konfigurieren.

Weitere Informationen dazu finden Sie unter „Konfigurieren von Richtlinien für Desktop- und Anwendungspools“ und „VMware Blast-Richtlinieneinstellungen“ im Dokument *Einrichten von Desktop- und Anwendungspools für View*.

Verwenden eines Remote-Desktops oder einer Remoteanwendung

3

Der Client bietet eine Navigations-Sidebar mit Schaltflächen in einer Symbolleiste, mit denen Sie auf einfache Weise die Verbindung mit einem Remote-Desktop oder mit einer Remoteanwendung trennen können. Oder Sie senden das Pendant der Tastenkombination Strg+Alt+Entf durch Klicken auf eine Schaltfläche.

Dieses Kapitel behandelt die folgenden Themen:

Funktionsunterstützungs-Matrix

Wenn Sie über einen browserbasierten HTML Access-Client auf einen Remote-Desktop oder eine Remoteanwendung zugreifen, stehen einige Funktionen nicht zur Verfügung.

Funktionsunterstützung für Desktops virtueller Einzelbenutzer-Maschinen

Tabelle 3-1. Über HTML Access unterstützte Funktionen

Funktion	Windows 7-Desktop	Windows 8.x-Desktop	Windows 10-Desktop	Windows Server 2008 R2-Desktop	Windows Server 2012 R2-Desktop
RSA SecurID oder RADIUS	X	X	X	X	X
Einmaliges Anmelden	X	X	X	X	X

Tabelle 3-1. Über HTML Access unterstützte Funktionen (Fortsetzung)

Funktion	Windows 7-Desktop	Windows 8.x-Desktop	Windows 10-Desktop	Windows Server 2008 R2-Desktop	Windows Server 2012 R2-Desktop
RDP-Anzeigeprotokoll					
PCoIP-Anzeigeprotokoll					
VMware Blast-Anzeigeprotokoll	X	X	X	X	X
USB-Umleitung					
Echtzeit-Audio/Video (RTAV)	X	X	X	X	X
Wyse MMR					
Windows Media MMR					
Virtuelles Drucken					
Standortbasiertes Drucken	X	X	X	X	X
Smartcards					
Mehrere Monitore					

Weitere Erläuterungen für diese Funktionen und deren Einschränkungen finden Sie im Dokument *Planung der View-Architektur*.

Funktionsunterstützung für sitzungsbasierte Desktops und gehostete Anwendungen auf RDS-Hosts

RDS-Hosts sind Server-Computer, auf denen Windows-Remotedesktopdienste und View Agent installiert sind. Mehrere Benutzer können gleichzeitig über Desktop- und Anwendungssitzungen auf einem RDS-Host verfügen.

Die folgende Tabelle beschreibt, welche Funktionen auf einem RDS-Host verfügbar sind, wenn Sie HTML Access verwenden. Weitere Funktionen sind verfügbar, wenn Sie Horizon Client nativ installiert, wie Horizon Client für Windows verwenden.

Tabelle 3-2. Unterstützte Funktionen für HTML Access für RDS-Hosts mit installiertem View Agent 6.1.1 oder höher

Funktion	Windows Server 2008 R2 RDS Host auf einer physischen Maschine	Windows Server 2008 R2 RDS Host auf einer virtuellen Maschine	Windows Server 2012- oder Windows Server 2012 R2- RDS-Host auf einer physischen Maschine	Windows Server 2012- oder Windows Server 2012 R2-RDS-Host auf einer virtuellen Maschine
RSA SecurID oder RADIUS	X	X	X	X
Einmaliges Anmelden	X	X	X	X
VMware Blast-Anzeigeprotokoll	X	X	X	X
Virtuelles Drucken				
Standortbasiertes Drucken		X		X
Mehrere Monitore				

Hinweis Beim RDS-Host kann es sich um eine virtuelle Maschine oder physischen Computer handeln.

Informationen dazu, welche Versionen jedes Gastbetriebssystems oder welche Service Packs unterstützt werden, finden Sie unter „Unterstützte Betriebssysteme für Horizon Agent“ im Dokument *View-Installation*.

Internationalisierung

Die Benutzeroberfläche und die Dokumentation sind in den Sprachen Englisch, Japanisch, Französisch, Deutsch, vereinfachtes Chinesisch, traditionelles Chinesisch und Koreanisch verfügbar.

Weitere Informationen darüber, welche Sprachpakete Sie im Clientsystem, Browser und Remote-Desktop verwenden müssen, finden Sie unter „Internationale Tastaturen“, auf Seite 37.

Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung

Verwenden Sie Ihre Active Directory-Anmeldedaten zum Herstellen einer Verbindung mit den Remote-Desktops und -anwendungen, für deren Verwendung Sie autorisiert sind.

Voraussetzungen

- Besorgen Sie sich die zur Anmeldung benötigten Informationen, so etwa den Active Directory-Benutzernamen und das Active Directory-Kennwort, den RSA SecurID-Benutzernamen und -Passcode oder den RADIUS-Authentifizierungsbenutzernamen oder -Passcode.
- Besorgen Sie sich den NETBIOS-Domänennamen für die Anmeldung. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.

Vorgehensweise

1 Öffnen Sie einen Browser und geben Sie die URL für die View-Verbindungsserver-Instanz ein.

   Für die URL geben Sie **`https`** ein und den vollqualifizierten Domänennamen, z. B. `https://view.company.com`.

   Verbindungen zum View-Verbindungsserver verwenden immer SSL. Der Standardport für SSL-Verbindungen ist 443. Wenn der View-Verbindungsserver nicht zur Verwendung des Standardports konfiguriert ist, muss das in folgendem Beispiel gezeigte Format verwendet werden: **`view.company.com:1443`**.

   Das Webportal von VMware Horizon erscheint. Standardmäßig werden auf dieser Seite ein Symbol für den Download und für die Installation des nativen Horizon Client sowie ein Symbol für die Verbindungsherstellung über HTML Access angezeigt.

2 Klicken Sie auf das Symbol **VMware Horizon HTML Access**.

3 Wenn Sie im Anmeldedialogfeld zur Eingabe von RSA SecurID-Anmeldedaten oder RADIUS-Authentifizierungsinformationen aufgefordert werden, geben Sie den Benutzernamen und den Passcode ein und klicken Sie auf **Anmelden**.

   Der Passcode kann möglicherweise sowohl aus einer PIN als auch einer zum Token generierten Nummer bestehen.

4 Wenn Sie erneut aufgefordert werden, RSA SecurID-Anmeldedaten oder RADIUS-Authentifizierungs-Anmeldedaten einzugeben, geben Sie die nächste zum Token generierte Nummer ein.

   Geben Sie nicht Ihre PIN oder dieselbe, zuvor eingegebene generierte Nummer ein. Warten Sie, falls nötig, bis eine neue Nummer generiert wurde.

   Wenn dieser Schritt erforderlich ist, dann nur, wenn Sie den ersten Passcode falsch eingegeben haben oder wenn die Konfigurationseinstellungen im RSA-Server geändert werden.

5 Geben Sie im Anmeldedialogfenster Ihren Active Directory-Benutzernamen und Ihr Active Directory-Kennwort ein, wählen Sie einen Domänennamen aus und klicken Sie dann auf **Anmelden**.

6 (Optional) Bevor Sie das Element für den Zugriff auswählen, klicken Sie im Auswahlbildschirm für Desktops und Anwendungen zur Kennzeichnung eines Remote-Desktops oder einer Remoteanwendung als Favorit auf den grauen Stern im Symbol des Desktops oder der Anwendung.

   Das Sternsymbol erscheint dann nicht mehr grau, sondern gelb. Nach der nächsten Anmeldung klicken Sie, wenn Sie nur Favoriten darstellen möchten, dieses Sternsymbol oben rechts im Browserfenster an.

7 Klicken Sie auf das Symbol des Remote-Desktops oder der Remoteanwendung, auf den oder die Sie zugreifen möchten.

   Der Remote-Desktop oder die Remoteanwendung wird in Ihrem Browser angezeigt. Es ist auch eine Navigations-Sidebar verfügbar. Um die Sidebar einzublenden, klicken Sie auf die Registerkarte links im Browserfenster. Mit der Sidebar können Sie auf andere Remote-Desktops oder -anwendungen zugreifen, das Fenster „Einstellungen“ aufrufen, Text kopieren und einfügen und vieles mehr.

Weiter

Unmittelbar nach der Verbindungsherstellung mit einem Desktop oder einer Anwendung wird die Verbindung getrennt und eine Aufforderung angezeigt, auf einen Link zur Bestätigung des Sicherheitszertifikats zu klicken, wenn Sie dem Zertifikat vertrauen. Siehe „Einstufen eines selbstsignierten Zertifikats als vertrauenswürdig“, auf Seite 32.

Einstufen eines selbstsignierten Zertifikats als vertrauenswürdig

In einigen Fällen werden Sie bei der ersten Herstellung einer Verbindung mit einem Remote-Desktop oder mit einer Remoteanwendung vom Browser aufgefordert, ein selbstsigniertes Zertifikat, das von diesem Remotecomputer verwendet wird, zu akzeptieren. Bevor die Verbindung mit dem Remote-Desktop oder der Remoteanwendung hergestellt werden kann, müssen Sie dieses Zertifikat als vertrauenswürdig einstufen.

Die meisten Browser bieten die Möglichkeit, das selbstsignierte Zertifikat dauerhaft als vertrauenswürdig zu akzeptieren. Wenn Sie dieses Zertifikat nicht dauerhaft als vertrauenswürdig einstufen, müssen Sie das Zertifikat bei jedem Start Ihres Browsers neu überprüfen. Bei einem Safari-Browser muss das Sicherheitszertifikat dauerhaft als vertrauenswürdig akzeptiert werden, damit eine Verbindung hergestellt werden kann.

Vorgehensweise

1 Wenn in Ihrem Browser eine Warnmeldung zu einem nicht vertrauenswürdigen Zertifikat oder zum Status der Verbindung als nicht privat eingeblendet wird, müssen Sie das Zertifikat überprüfen, um sicherzustellen, dass es dem Zertifikat Ihres Unternehmens entspricht.

   Gegebenenfalls wenden Sie sich an Ihren View-Administrator, der Ihnen weiterhelfen kann. In einem Chrome-Browser gehen Sie beispielsweise wie nachfolgend dargestellt vor.

   a Klicken Sie auf das Schlosssymbol in der Adressleiste.

   b Klicken Sie auf den Link **Zertifikatsinformationen**.

   c Überprüfen Sie, ob das Zertifikat dem Zertifikat Ihres Unternehmens entspricht.

      Gegebenenfalls wenden Sie sich an Ihren View-Administrator, der Ihnen weiterhelfen kann.

2 Akzeptieren Sie das Sicherheitszertifikat.

Jeder Browser verfügt über eigene Meldungen und Eingabeaufforderungen für das Akzeptieren oder dauerhafte Einstufen eines Zertifikats als vertrauenswürdig In einem Chrome-Browser können Sie beispielsweise auf den Link **Erweitert** auf der Browserseite klicken und dann auf **Weiter zu *Servername* (unsicher)**.

In einem Safari-Browser gehen Sie für die permanente Einstufung eines Zertifikats als vertrauenswürdig vor, wie im Folgenden beschrieben.

a Klicken Sie auf die Schaltfläche **Zertifikat einblenden** im Dialogfeld „Zertifikat nicht vertrauenswürdig“.

b Aktivieren Sie das Kontrollkästchen **Immer vertrauen** und klicken Sie auf **Fortfahren**.

c Wenn Sie dazu aufgefordert werden, geben Sie Ihr Kennwort ein und klicken Sie auf **Einstellungen aktualisieren**.

Der Remote-Desktop bzw. die Remoteanwendung wird gestartet.

Tastenkombinationen

Unabhängig von der verwendeten Sprache können einige Tastenkombinationen nicht an einen Remote-Desktop oder an eine Remoteanwendung gesendet werden.

Webbrowser ermöglichen es, bestimmte Tasteneingaben und Tastenkombinationen sowohl an den Client als auch an das Zielsystem zu senden. Für andere Tasteneingaben und Tastenkombinationen wird die Eingabe nur lokal verarbeitet und nicht an das Zielsystem gesendet. Die Tastenkombinationen, die auf Ihrem System funktionieren, richten sich nach der Browsersoftware, dem Clientbetriebssystem und den Spracheinstellungen.

Hinweis Wenn Sie mit einem Mac arbeiten, können Sie die Befehlstaste ⌘ (command, cmd) der Windows-Strg-Taste zuordnen, wenn Sie Tastenkombinationen für das Auswählen, Kopieren und Einfügen von Text verwenden. Um diese Funktion zu aktivieren, klicken Sie auf die Schaltfläche **Einstellungenfenster öffnen** in der Symbolleiste der Sidebar und aktivieren **⌘-A, ⌘-C, ⌘-V und ⌘-X aktivieren**. (Diese Option erscheint im Fenster „Einstellungen“ nur bei Verwendung eines Mac.)

Die folgenden Tasteneingaben und Tastenkombinationen funktionieren häufig nicht bei Remote-Desktops:

- Strg+T
- Strg+W
- Strg+N
- Befehlstaste
- Alt+Enter
- Strg+Alt+*beliebige_Taste*

  Wichtig Für die Eingabe von Strg+Alt+Entf verwenden Sie die Schaltfläche **Strg+Alt+Entf senden** der Symbolleiste oben auf der Sidebar.

- Feststelltaste+*Zusatztaste* (z. B. Alt oder Umschalttaste)
- Funktionstasten, wenn Sie ein Chromebook verwenden
- Windows-Tastenkombinationen

Die folgenden Windows-Tastenkombinationen können in Remote-Desktops verwendet werden, wenn Sie die Windows-Taste (Win) für Desktops aktivieren. Um diese Taste zu aktivieren, klicken Sie auf die Schaltfläche **Einstellungenfenster öffnen** in der Symbolleiste der Sidebar und aktivieren **Windows-Tasten für Desktops aktivieren**.

Wichtig Nachdem Sie **Windows-Tasten für Desktops aktivieren** gedrückt haben, drücken Sie Strg+Win (auf Windows-Systemen), ctrl+⌘ (auf Macs) oder Strg+Suche (auf Chromebooks), um die Windows-Taste zu simulieren.

Diese Tastenkombinationen können nicht für von RDS-Hosts bereitgestellten Remoteanwendungen verwendet werden. Sie gelten wie angegeben für Windows Server 2008 R2- und Windows Server 2012 R2-Einzelbenutzer-Desktops sowie für von einem RDS-Host bereitgestellte sitzungsbasierte Desktops.

Einige Tastenkombinationen, die mit einem Windows 8.x- oder einem Windows Server 2012 R2-Betriebssystem verwendet werden können, funktionieren nicht in Remote-Desktops mit einem Windows 7-, Windows Server 2008 R2- oder Windows 10-Betriebssystem.

Tabelle 3-3. Windows-Tastenkombinationen für Windows 10-Remote-Desktops

Schlüssel	Aktion	Einschränkungen
Windows-Taste	Öffnet oder schließt „Start“.	
Win+A	Öffnet das Wartungscenter.	
Win+E	Öffnet den Datei-Explorer.	
Win+G	Öffnet die Spieleleiste, wenn ein Spiel geöffnet ist.	
Win+H	Öffnet den Charm „Teilen“	
Win+I	Öffnet den Charm „Einstellungen“	
Win+K	Öffnet die Aktion „Schnelle Verbindung“.	
Win+M	Minimiert alle Fenster.	
Win+R	Öffnet das Dialogfeld „Ausführen“.	
Win+S	Öffnet die Suche.	
Win+X	Öffnet das Menü **Quicklink**.	
Win+, (Komma)	Ermöglicht eine temporäre Vorschau am Desktop.	
Win+Pause	Stellt das Dialogfeld für die Systemeigenschaften dar.	Auf Chromebooks oder Macs ist keine Pause-Taste verfügbar.
Win+Umschalt+M	Stellt minimierte Fenster auf dem Desktop wieder her.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden.
Win+Alt+Num	Öffnet den Desktop und die Sprungliste für die an der Taskleiste an der durch die Ziffer angegebenen Position angeheftete App.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Enter	Öffnet die Sprachausgabe.	

Tabelle 3-4. Windows-Tastenkombinationen für Windows 8.x- und Windows Server 2012 R2-Remote-Desktops

Schlüssel	Aktion	Einschränkungen
Win+F1	Öffnet die Windows-Hilfe und den Windows-Support.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden.
Windows-Taste	Blendet den Startbildschirm ein oder aus.	
Win+B	Setzt den Fokus auf den Infobereich.	

Tabelle 3-4. Windows-Tastenkombinationen für Windows 8.x- und Windows Server 2012 R2-Remote-Desktops (Fortsetzung)

Schlüssel	Aktion	Einschränkungen
Win+C	Öffnet den Charms-Bereich	
Win+D	Blendet den Desktop ein oder aus.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden. Problemumgehung: Drücken Sie ⌘-D auf Macs.
Win+E	Öffnet den Datei-Explorer.	
Win+H	Öffnet den Charm „Teilen“	
Win+I	Öffnet den Charm „Einstellungen“	
Win+K	Öffnet den Charm „Geräte“	
Win+M	Minimiert alle Fenster.	
Win+Q	Öffnet den Charm „Suche“ für eine allgemeine Suche oder für eine Suche in der geöffneten App, wenn diese eine App-Suche unterstützt.	
Win+R	Öffnet das Dialogfeld „Ausführen“.	
Win+S	Öffnet den Charm „Suche“ für eine Suche in Windows oder im Internet.	
Win+X	Öffnet das Menü **Quicklink**.	
Win+Z	Zeigt die in der App verfügbaren Befehle an.	
Win+, (Komma)	Zeigt vorübergehend den Desktop an, solange Sie diese Tasten drücken.	**Hinweis** Diese Tastenkombination kann nicht für Windows 2012 R2-Betriebssysteme verwendet werden.
Win+Pause	Stellt das Dialogfeld für die Systemeigenschaften dar.	Auf Chromebooks oder Macs ist keine Pause-Taste verfügbar.
Win+Umschalt+M	Stellt minimierte Fenster auf dem Desktop wieder her.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden. Problemumgehung: Drücken Sie ⌘-D auf Macs.
Win+Alt+Num	Öffnet den Desktop und die Sprungliste für die an der Taskleiste an der durch die Ziffer angegebenen Position angeheftete App.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach oben	Maximiert das Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach unten	Entfernt die aktuelle App vom Bildschirm oder minimiert das Desktop-Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach links	Maximiert das App- oder Desktop-Fenster zur linken Seite des Bildschirms.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach rechts	Maximiert das App- oder Desktop-Fenster zur rechten Seite des Bildschirms.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pos1	Minimiert alle Fenster bis auf das aktive Desktop-Fenster (durch nochmaliges Drücken werden alle Fenster wiederhergestellt).	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden.

Tabelle 3-4. Windows-Tastenkombinationen für Windows 8.x- und Windows Server 2012 R2-Remote-Desktops (Fortsetzung)

Schlüssel	Aktion	Einschränkungen
Win+Umschalt +Pfeil nach oben	Zieht das Desktop-Fenster nach oben und unten auf.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Umschalt +Pfeil nach unten	Stellt das Desktop-Fenster vertikal unter Beibehaltung der Breite wieder her, nachdem es mit der Tastenkombination „Win+Umschalt+Pfeil nach oben“ aufgezogen wurde, oder minimiert das aktive Desktop-Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Enter	Öffnet die Sprachausgabe.	

Tabelle 3-5. Windows-Tastenkombinationen für Windows 7- und Windows Server 2008 R2-Remote-Desktops

Schlüssel	Aktion	Einschränkungen
Windows-Taste	Öffnet oder schließt das Startmenü.	
Win+Pause	Stellt das Dialogfeld für die Systemeigenschaften dar.	Auf Chromebooks oder Macs ist keine Pause-Taste verfügbar.
Win+D	Blendet den Desktop ein oder aus.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden. Problemumgehung: Drücken Sie ⌘-D auf Macs.
Win+M	Minimiert alle Fenster.	
Win+E	Öffnet den Computerordner.	
Win+R	Öffnet das Dialogfeld „Ausführen“.	
Win+Pfeil nach oben	Maximiert das Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach unten	Minimiert das Fenster.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach links	Maximiert das App- oder Desktop-Fenster zur linken Seite des Bildschirms.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pfeil nach rechts	Maximiert das App- oder Desktop-Fenster zur rechten Seite des Bildschirms.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+Pos1	Minimiert alle Fenster bis auf das aktive Desktop-Fenster.	Diese Tastenkombination kann nicht in Safari-Browsern verwendet werden.
Win+Umschalt +Pfeil nach oben	Zieht das Desktop-Fenster nach oben und unten auf.	Diese Tastenkombination kann nicht in Chromebook verwendet werden.
Win+G	Wechselt der Reihe nach zu den ausgeführten Desktop-Minianwendungen.	
Win+U	Öffnet das „Center für erleichterte Bedienung“.	

Internationale Tastaturen

Wenn Sie nicht englische Tastaturen und Ländereinstellungen verwenden, müssen Sie bestimmte Einstellungen für das Clientsystem, den Browser und den Remote-Desktop festlegen. Einige Sprachen erfordern die Verwendung eines IME (Eingabemethoden-Editor) auf dem Remote-Desktop.

Wenn die richtigen lokalen Einstellungen und Eingabemethoden installiert sind, können Sie für folgende Sprachen Zeichen eingeben: Englisch, Japanisch, Französisch, Deutsch, Chinesisch (Vereinfacht), Chinesisch (Traditionell) und Koreanisch.

Tabelle 3-6. Erforderliche Einstellungen für die Eingabesprache

Sprache	Eingabesprache auf dem lokalen Clientsystem	IME auf dem lokalen Clientsystem erforderlich?	Browser und Eingabesprache auf dem Remote-Desktop	Ist IME auf dem Remote-Desktop erforderlich?
Englisch	Englisch	Nein	Englisch	Nein
Französisch	Französisch	Nein	Französisch	Nein
Deutsch	Deutsch	Nein	Deutsch	Nein
Chinesisch (Vereinfacht)	Chinesisch (Vereinfacht)	Englischer Eingabemodus	Chinesisch (Vereinfacht)	Ja
Chinesisch (Traditionell)	Chinesisch (Traditionell)	Englischer Eingabemodus	Chinesisch (Traditionell)	Ja
Japanisch	Japanisch	Englischer Eingabemodus	Japanisch	Ja
Koreanisch	Koreanisch	Englischer Eingabemodus	Koreanisch	Ja

Bildschirmauflösung

Wenn ein Remote-Desktop mithilfe von View Administrator mit ausreichend Video-RAM (VRAM) konfiguriert wurde, ist der Webclient in der Lage, die Größe eines Remote-Desktops an die Größe des Browserfensters anzupassen. Standardmäßig sind 36 MB an Video-RAM konfiguriert, d. h. der verfügbare Arbeitsspeicher liegt deutlich über der Mindestanforderung von 16 MB, wenn Sie keine 3D-Anwendungen verwenden.

Wenn Sie einen Browser oder ein Chrome-Gerät mit einer hohen Pixeldichte-Auflösung verwenden, z. B. ein Macbook mit Retina-Display oder ein Google Chromebook Pixel, können Sie den Remote-Desktop oder die Remoteanwendung auf diese Auflösung festlegen. Aktivieren Sie die Option **Modus mit hoher Auflösung** im Fenster „Einstellungen“, das auf der Sidebar verfügbar ist. (Diese Option erscheint im Fenster „Einstellungen“ nur bei einer Anzeige mit hoher Auflösung.)

Um die 3D-Renderfunktion zu verwenden, müssen Sie ausreichend VRAM für jeden Remote-Desktop zuteilen.

- Die softwarebeschleunigte Grafikfunktion, die ab vSphere 5.0 zur Verfügung steht, ermöglicht es Ihnen, 3D-Anwendungen wie Windows Aero-Themen oder Google Earth zu verwenden. Für diese Funktion sind zwischen 64 MB und 128 MB VRAM erforderlich.
- Die hardwarebeschleunigte Grafikfunktion (vSGA), die mit vSphere 5.1 oder höher verfügbar ist, ermöglicht die Verwendung von 3D-Anwendungen für Entwurf, Modellierung und Multimedia. Für diese Funktion sind zwischen 64 MB und 512 MB VRAM erforderlich. Der Standardwert ist 96 MB.

- Die dedizierte vDGA-Funktion (Virtual Dedicated Graphics Acceleration, virtuelle hardwarebeschleunigte Grafikfunktion), die ab vSphere 5.5 oder höher verfügbar ist, weist eine einzige physische GPU (Graphical Processing Unit, Grafikverarbeitungseinheit) auf einem ESXi-Host einer einzelnen virtuellen Maschine zu. Verwenden Sie diese Funktion, wenn Sie hochwertige, hardwarebeschleunigte Workstation-Grafiken benötigen. Für diese Funktion sind zwischen 64 MB und 512 MB VRAM erforderlich. Der Standardwert ist 96 MB.

Wenn das 3D-Rendern aktiviert ist, beträgt die Höchstzahl der Monitore 1 und die maximale Auflösung beträgt 3840 x 2160.

In gleicher Weise müssen Sie, wenn Sie einen Browser oder ein Gerät mit einer hohen Pixeldichte-Auflösung verwenden, z. B. ein Macbook mit Retina-Display oder ein Google Chromebook Pixel, jedem Remote-Desktop ausreichend VRAM zuteilen.

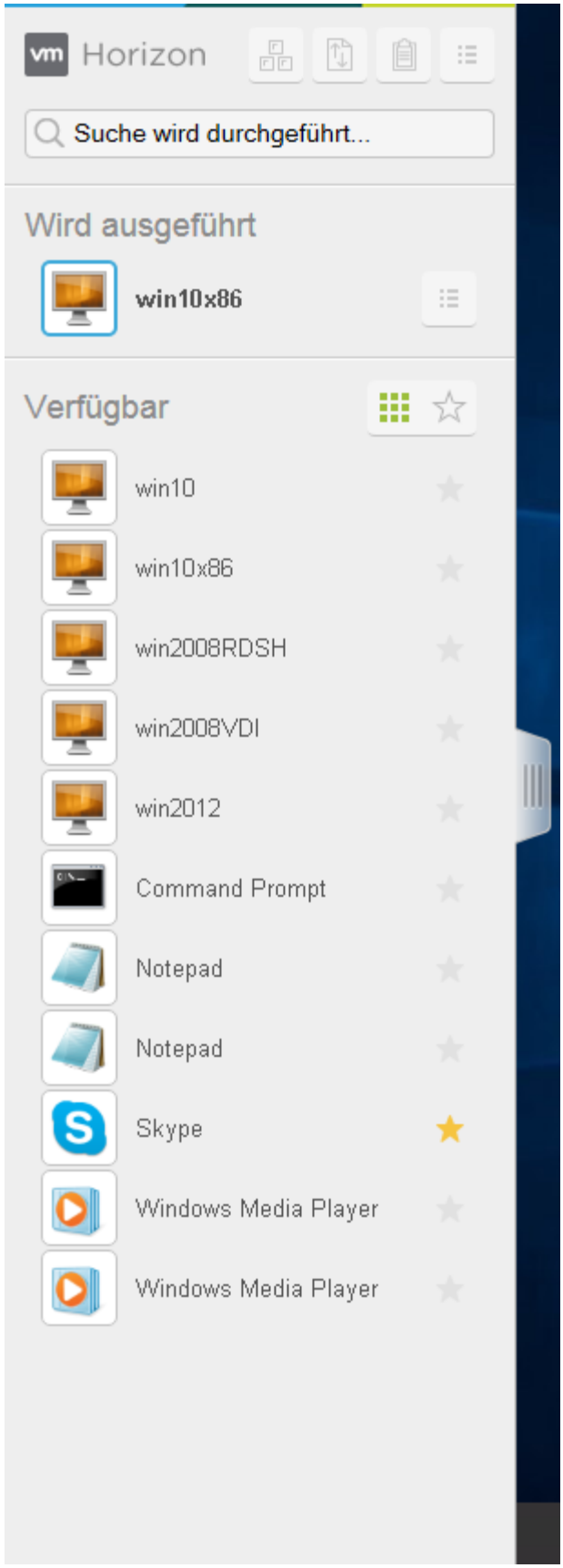
Wichtig Die Schätzung der für das VMware Blast-Anzeigeprotokoll benötigten Menge an VRAM ähnelt der Schätzung des benötigten VRAM für das PCoIP-Anzeigeprotokoll. Richtlinien finden Sie im Abschnitt „Festlegen der Arbeitsspeichergröße für bestimmte Monitorkonfigurationen bei der Verwendung von PCoIP“ im Kapitel „Einschätzen der Arbeitsspeicheranforderungen für virtuelle Desktops“ des Dokuments *Planung der View-Architektur*.

Verwenden der Randleiste

Nachdem Sie eine Verbindung zu einem Remote-Desktop oder zu einer Remoteanwendung hergestellt haben, können Sie mit der Sidebar andere Anwendungen und Desktops starten, zwischen ausgeführten Desktops bzw. Anwendungen wechseln und weitere Aktionen durchführen.

Wenn Sie auf eine Remoteanwendung oder einen Remote-Desktop zugreifen, wird die Sidebar auf der linken Seite des Bildschirms angezeigt. Das Anklicken der Sidebar-Registerkarte blendet die Sidebar ein und aus. Sie können die Registerkarte auch nach oben oder unten verschieben.

Abbildung 3-1. Angezeigte Sidebar beim Starten eines Remote-Desktops oder einer Remoteanwendung



Klicken Sie auf den Erweiterungspfeil neben einer ausgeführten Anwendung und es erscheint die Liste der von dieser Anwendung geöffneten Dokumente. Beachten Sie, dass bei zwei mit eigenständigen Excel-Programmen auf zwei verschiedenen Servern geöffneten Excel-Dokumenten die Excel-Anwendung zweimal in der Liste **Wird ausgeführt** der Sidebar erscheint.

Sie können von der Sidebar aus verschiedene Aktionen ausführen.

Tabelle 3-7. Sidebar-Aktionen

Aktion	Prozedur
Anzeigen the Sidebar	Wenn eine Remoteanwendung oder ein Remote-Desktop geöffnet ist, klicken Sie auf die Registerkarte der Sidebar. Bei geöffneter Sidebar können Sie im Anwendungs- oder Desktop-Fenster weiterhin Aktionen ausführen.
Ausblenden der Sidebar	Klicken Sie auf die Registerkarte der Sidebar.
Starten einer Remoteanwendung oder eines Remote-Desktops	Klicken Sie auf den Namen der Anwendung oder des Desktops unter **Verfügbar** auf der Sidebar. Die Desktops werden zuerst aufgeführt.
Suchen nach einer Remoteanwendung oder einem Remote-Desktop	■ Klicken Sie auf das Feld **Suche** und beginnen Sie mit der Eingabe des Namens der Anwendung oder des Desktops. ■ Um eine Anwendung oder einen Desktop zu starten, klicken Sie auf den Namen der Anwendung bzw. des Desktops in den Suchergebnissen. ■ Um zur Startansicht der Sidebar zurückzukehren, tippen Sie im Suchfeld auf **X**.
Erstellen einer Liste der beliebtesten Anwendungen und Desktops	Klicken Sie auf den grauen Stern neben dem Namen des Desktops oder der Anwendung in der Liste **Verfügbar** der Sidebar. Sie können dann mit der Schaltfläche **Favoriten anzeigen** in der Symbolleiste (Sternsymbol) neben **Verfügbar** eine Liste mit den festgelegten Favoriten aufrufen.
Wechseln zwischen Anwendungen und Desktops	Klicken Sie auf den Namen der Anwendung oder des Desktops in der Liste **Wird ausgeführt** der Sidebar.
Öffnen des Fensters zum Kopieren und Einfügen	Klicken Sie auf die Schaltfläche **Kopieren und Einfügen** oben auf der Sidebar. Mit dieser Schaltfläche können Sie Text in Ihre Anwendungen aus Ihrem lokalen Clientsystem und aus Ihren Anwendungen auf Ihr lokales Clientsystem kopieren. Weitere Informationen finden Sie unter „Kopieren und Einfügen von Text“, auf Seite 42. In iOS Safari ist diese Schaltfläche nicht verfügbar, da die Funktion zum Kopieren und Einfügen nicht unterstützt wird.
Öffnen des Fensters „Dateiübertragung“	Klicken Sie oben auf der Seitenleiste auf die Schaltfläche **Dateiübertragung**, um Dateien vom Remote-Desktop herunterzuladen oder zu diesem hochzuladen. Weitere Informationen dazu finden Sie unter „Herunterladen von Dateien von einem Desktop auf den Client“, auf Seite 44 und „Hochladen von Dateien vom Client zu einem Desktop“, auf Seite 44.
Aktivieren von ⌘-A, ⌘-C, ⌘-V und ⌘-X	Die Option „⌘-A, ⌘-C, ⌘-V und ⌘-X aktivieren“ erscheint im Fenster „Einstellungen“ nur bei Verwendung eines Mac. Klicken Sie auf die Schaltfläche **Menü öffnen** in der Symbolleiste oben auf der Sidebar und klicken Sie dann auf **Einstellungen**. Nach Aktivierung dieser Funktion wird die ⌘-Taste auf dem Mac der Strg-Taste auf dem Windows-Remote-Desktop bzw. in der Windows-Remoteanwendung zugeordnet. Beispielsweise entspricht dann das Drücken der Tastenkombination ⌘-A auf dem Mac dem Drücken von Strg-A auf dem Windows-Remote-Desktop bzw. in der Remoteanwendung.
Schließen eines ausgeführten Desktops	Klicken Sie auf die Schaltfläche **Menü öffnen** neben dem Namen des Desktops in der Liste **Wird ausgeführt** und wählen Sie die gewünschte Aktion aus: ■ Wählen Sie **Schließen** aus, um die Verbindung zum Desktop ohne Abmeldung von dessen Betriebssystem zu trennen. Beachten Sie, dass Ihr View-Administrator Ihren Desktop so konfigurieren kann, dass Sie beim Trennen der Verbindung automatisch abgemeldet werden. In diesem Fall gehen die nicht gespeicherten Änderungen in den geöffneten Anwendungen verloren. ■ Wählen Sie **Abmelden** aus, um sich vom Betriebssystem abzumelden und die Verbindung zum Desktop zu trennen. Alle nicht gespeicherten Änderungen in den geöffneten Anwendungen gehen dabei verloren.

Tabelle 3-7. Sidebar-Aktionen (Fortsetzung)

Aktion	Prozedur
Schließen einer laufenden Anwendung	Klicken Sie auf das **X** neben dem Dateinamen unter dem Namen der Anwendung in der Liste **Wird ausgeführt** der Sidebar. Klicken Sie auf das **X** neben dem Namen der Anwendung, um die Anwendung zu verlassen und alle geöffneten Dateien dieser Anwendung zu schließen. Sie werden gegebenenfalls dazu aufgefordert, die durchgeführten Änderungen in den Dateien zu speichern.
Zurücksetzen eines Desktops	Klicken Sie auf die Schaltfläche **Menü öffnen** neben dem Namen des Desktops in der Liste **Wird ausgeführt** der Sidebar und wählen Sie **Zurücksetzen** aus. Alle Dateien, die auf dem Remote-Desktop geöffnet sind, werden ohne vorheriges Speichern geschlossen. Sie können einen Desktop nur zurücksetzen, wenn Ihr Administrator diese Funktion aktiviert hat.
Zurücksetzen aller ausgeführten Anwendungen	Klicken Sie auf die Schaltfläche **Menü öffnen** in der Symbolleiste oben auf der Sidebar, klicken Sie dann auf **Einstellungen** und schließlich auf **Zurücksetzen**. Alle nicht gespeicherten Änderungen gehen dann verloren.
Verwenden von Tastenkombinationen mit der Windows-Taste	Klicken Sie auf die Schaltfläche **Menü öffnen** in der Symbolleiste oben auf der Sidebar, klicken Sie dann auf **Einstellungen** und aktivieren Sie **Windows-Tasten für Desktops aktivieren**. Weitere Informationen finden Sie unter „Tastenkombinationen“, auf Seite 33.
Senden von Strg+Alt+Entf zum aktuellen Arbeitsbereich	Klicken Sie auf die Schaltfläche **Strg+Alt+Entf senden** in der Symbolleiste oben auf der Sidebar.
Trennen der Verbindung mit dem Server	Klicken Sie auf die Schaltfläche **Menü öffnen** in der Symbolleiste oben auf der Sidebar oder klicken Sie auf das Horizon-Logo oben auf der Sidebar und dann auf **Abmelden**.
Verwenden des Modus mit hoher Auflösung auf Computern mit einer hochauflösenden Anzeige (wie Retina Macbook Pro)	Klicken Sie auf die Schaltfläche **Menü öffnen** in der Symbolleiste oben auf der Sidebar, klicken Sie dann auf **Einstellungen** und aktivieren Sie **Modus mit hoher Auflösung**. (Diese Option erscheint im Fenster „Einstellungen“ nur bei einer Anzeige mit hoher Auflösung.)
Aktivieren und Deaktivieren der Bildschirmtastatur	(Nur für iOS Safari) Klicken Sie auf das Tastatursymbol oben auf der Sidebar. Sie können die Bildschirmtastatur auch durch Tippen auf den Bildschirm mit drei Fingern aktivieren bzw. deaktivieren.
Anzeigen der Hilfethemen	Klicken Sie auf die Schaltfläche **Menü öffnen** in der Symbolleiste oben auf der Sidebar oder klicken Sie auf das Horizon-Logo oben auf der Sidebar und dann auf **Hilfe**.
Anzeige des Feldes „Info zu VMware Horizon“	Klicken Sie auf die Schaltfläche **Menü öffnen** in der Symbolleiste oben auf der Sidebar oder klicken Sie auf das Horizon-Logo oben auf der Sidebar und dann auf **Info**.

Sound

Sie können in Ihren Remote-Desktops und -anwendungen Sound abspielen, wobei einige Einschränkungen zu beachten sind.

Standardmäßig ist die Audiowiedergabe für Remote-Desktops und -anwendungen aktiviert, allerdings kann Ihr View-Administrator eine Richtlinie festlegen, um die Audiowiedergabe zu deaktivieren.

Berücksichtigen Sie die folgenden Richtlinien:

- Verwenden Sie zum Erhöhen der Lautstärke die Sound-Steuerung auf Ihrem Clientsystem und nicht die des Remote-Desktops oder der Remoteanwendung.
- Gelegentlich kann es zu einer fehlerhaften Synchronisierung zwischen Audio und Video kommen.
- Bei starkem Netzwerkverkehr oder beim Durchführen vieler Aufgaben (I/O) des Browsers, kann es zu einer eingeschränkten Audioqualität kommen. Einige Browser eignen sich in dieser Hinsicht besser als andere.

Kopieren und Einfügen von Text

Sie haben die Möglichkeit, Text in und aus Remote-Desktops und -anwendungen zu kopieren. Ihr View-Administrator kann diese Funktion so einstellen, dass Kopier- und Einfügevorgänge nur von Ihrem Clientsystem zu einem Remote-Desktop bzw. einer Anwendung oder nur von einem Remote-Desktop bzw. einer Anwendung zu Ihrem Clientsystem zugelassen werden oder beide bzw. keiner der beiden Vorgänge möglich sind.

Die Administratoren konfigurieren die Möglichkeit zum Kopieren/Einfügen durch die Verwendung von Gruppenrichtlinienobjekten (GPOs), die View Agent oder Horizon Agent auf den Remote-Desktops zugeordnet sind. Weitere Informationen finden Sie unter „Gruppenrichtlinieneinstellungen für HTML Access“, auf Seite 27.

Sie haben die Möglichkeit, bis zu 1 MB Text zu kopieren, inklusive aller Unicode-Nicht-ASCII-Zeichen. Sie können Text aus Ihrem Clientsystem auf einen Remote-Desktop bzw. in eine Remoteanwendung kopieren und umgekehrt. Beim eingefügten Text handelt es sich aber immer um einfachen Text.

Sie können keine Grafiken kopieren und einfügen. Sie können außerdem keine Dateien zwischen einem Remote-Desktop und dem Dateisystem auf Ihrem Clientcomputer kopieren und einfügen.

Hinweis Die Funktion zum Kopieren und Einfügen wird für iOS Safari nicht unterstützt.

Verwenden der Kopier- und Einfügen-Funktion

Für das Kopieren und Einfügen von Text verwenden Sie die Schaltfläche **Kopieren und Einfügen** oben auf der Sidebar.

Diese Prozedur beschreibt die Verwendung des Fensters „Kopieren und Einfügen“ für das Kopieren von Text von Ihrem lokalen Clientsystem in eine Remoteanwendung bzw. umgekehrt von Text von einer Remoteanwendung in Ihr lokales Clientsystem. Wenn Sie nur Text zwischen Remoteanwendungen und Remote-Desktops kopieren und einfügen, können Sie wie gewohnt vorgehen und benötigen dafür nicht das Fenster „Kopieren und Einfügen“.

Das Fenster „Kopieren und Einfügen“, das mit einer Schaltfläche oben in der HTML Access-Sidebar geöffnet werden kann, wird nur für die Synchronisierung der Zwischenablage auf Ihrem lokalen System mit der Zwischenablage des Remotecomputers benötigt.

Der Text im Fenster „Kopieren und Einfügen“ zeigt eine der folgenden Meldungen an, um anzugeben, in welcher Richtung der Benutzer Inhalt kopieren und einfügen kann.

- `Verwenden Sie dieses Fenster zum Kopieren und Einfügen von Inhalt zwischen Ihrem lokalen Client und dem Remote-Desktop bzw. der -Anwendung.`
- `Verwenden Sie das Fenster zum Kopieren und Einfügen von Inhalt von Ihrem lokalen Client zum Remote-Desktop bzw. zur -Anwendung.`
- `Verwenden Sie das Fenster zum Kopieren und Einfügen von Inhalt von Ihrem Remote-Desktop bzw. Ihrer Remote-Anwendung zum lokalen Client.`

Voraussetzungen

Wenn Sie mit einem Mac arbeiten, stellen Sie sicher, dass die Zuordnung der Befehlstaste ⌘ (command, cmd) zur Windows-Strg-Taste aktiviert wurde, wenn Sie Tastenkombinationen für das Auswählen, Kopieren und Einfügen von Text verwenden. Klicken Sie auf die Schaltfläche **Einstellungenfenster öffnen** in der Symbolleiste der Sidebar und aktivieren Sie **⌘-A, ⌘-C, ⌘-V und ⌘-X aktivieren**. (Diese Option erscheint im Fenster „Einstellungen“ nur bei Verwendung eines Mac.)

Der View-Administrator muss entweder die Standardrichtlinie beibehalten, die es Benutzern ermöglicht, Text aus ihren Clientsystemen zu kopieren und in ihren Remote-Desktops und -anwendungen einzufügen, oder eine andere Richtlinie konfigurieren, die das Kopieren und Einfügen zulässt. Weitere Informationen finden Sie unter „Gruppenrichtlinieneinstellungen für HTML Access“, auf Seite 27.

Vorgehensweise

- So kopieren Sie Text von Ihrem Clientsystem auf den Remote-Desktop oder in die Remoteanwendung:
  a. Kopieren Sie den Text in die lokale Clientanwendung.
  b. In Ihrem Browser klicken Sie auf die Registerkarte der HTML Access-Sidebar, um die Sidebar zu öffnen, und dann auf **Kopieren und Einfügen** oben auf der Sidebar.

     Das Fenster „Kopieren und Einfügen“ wird eingeblendet. Sollte in diesem Fenster noch Text von einem früheren Kopiervorgang enthalten sein, wird dieser durch das Einfügen des neu kopierten Textes überschrieben.
  c. Drücken Sie Strg+V (oder ⌘-V auf Macs), um den Text in das Fenster einzufügen.

     Es wird kurz die folgende Meldung angezeigt: „`Die Remote-Zwischenablage wurde synchronisiert.`“
  d. Klicken Sie in der Remoteanwendung an die Stelle, an der Sie den Text einfügen möchten, und drücken Sie die Tastenkombination Strg-V.

     Der Text wird in die Remoteanwendung einfügt.
- So kopieren Sie Text aus Ihrem Remote-Desktop oder Ihrer Remoteanwendung in Ihr Clientsystem:
  a. Kopieren Sie den Text in Ihrer Remoteanwendung.
  b. In Ihrem Browser klicken Sie auf die Registerkarte der HTML Access-Sidebar, um die Sidebar zu öffnen, und dann auf **Kopieren und Einfügen** oben auf der Sidebar.

     Das Fenster „Kopieren und Einfügen“ wird mit dem zuvor eingefügten Text dargestellt. Es wird kurz die folgende Meldung angezeigt: „`Die Remote-Zwischenablage wurde synchronisiert.`“
  c. Klicken Sie in das Fenster „Kopieren und Einfügen“ und drücken Sie Strg+C (oder ⌘-C auf Macs), um erneut zu kopieren.

     Der Text wird dabei nicht ausgewählt und kann auch von Ihnen nicht ausgewählt werden. Es wird kurz die folgende Meldung angezeigt: „`Aus der Zwischenablage kopiert.`“
  d. Klicken Sie auf Ihrem Clientsystem an die Stelle, an der Sie den Text einfügen möchten, und drücken Sie die Tastenkombination Strg-V.

     Der Text wird in die Anwendung auf Ihrem Clientsystem einfügt.

Übertragen von Dateien zwischen dem Client und einem Remote-Desktop

Mithilfe der Funktion zum Übertragen von Dateien können Sie Dateien zwischen dem Client und einem Remote-Desktop übertragen (hochladen und herunterladen). Die Dateiübertragung zu oder aus Anwendungen wird nicht unterstützt.

Der Horizon-Administrator kann die Fähigkeit zum Erlauben, Verweigern oder unidirektionalen Erlauben der Übertragung von Dateien konfigurieren, indem er die GPO-Einstellungen (Gruppenrichtlinienobjekt) für das VMware Blast-Protokoll ändert. Weitere Informationen finden Sie unter „Gruppenrichtlinieneinstellungen für HTML Access“, auf Seite 27. Der Standard lautet nur hochladen.

Sie können eine Datei mit einer maximalen Dateigröße von 500 MB herunterladen und eine maximal 2 GB große Datei hochladen. Das Herunterladen einer Datei, die größer als 300 MB ist, ist für die 32-Bit-Version von Internet Explorer 11 nicht möglich. Führen Sie zum Beheben des Problems Internet Explorer 11 im 64-Bit-Modus aus.

Sie können Ordner mit einer Größe von 0 weder herunter- noch hochladen.

Safari für iOS und Safari 8 unterstützen weder Up- noch Downloads. Von Safari 9 werden Downloads nicht unterstützt.

Wenn die Dateiübertragung in einer Desktop-Sitzung im Gange ist und ein Benutzer eine Verbindung zu einem zweiten Desktop öffnet und wenn eine Sicherheitswarnung angezeigt wird (beispielsweise wenn kein gültiges Zertifikat installiert wurde), führt das Ignorieren der Warnung und das Fortsetzen der Verbindung zum zweiten Desktop dazu, dass die Dateiübertragung in der ersten Desktop-Sitzung abgebrochen wird. Dies ist das erwartete Verhalten.

Hinweis Die Fähigkeit zum Herunterladen wird durch die Gruppenrichtlinieneinstellung für die Zwischenablageumleitung beeinflusst. Wenn die Zwischenablageumleitung vom Server zum Client deaktiviert ist, ist der Dateidownload ebenfalls deaktiviert.

Herunterladen von Dateien von einem Desktop auf den Client

Mit Horizon Client können Sie Dateien von einem Remote-Desktop auf einen Clientcomputer herunterladen.

Vorgehensweise

1 Klicken Sie oben auf der Seitenleiste auf das Symbol für die Dateiübertragung.

Das Fenster Dateien übertragen wird geöffnet.

2 Klicken Sie auf **Herunterladen**.

3 Wählen Sie mindestens eine Datei auf dem Remote-Desktop aus.

4 Drücken Sie Strg+C zum Starten des Downloads.

5 Klicken Sie nach Abschluss des Downloads auf das Downloadsymbol, um die Dateien auf dem Clientcomputer zu speichern.

Hochladen von Dateien vom Client zu einem Desktop

Mit Horizon Client können Sie Dateien von der Clientmaschine zu einem Remote-Desktop hochladen.

Vorgehensweise

1 Klicken Sie oben auf der Seitenleiste auf das Symbol für die Dateiübertragung.

Das Fenster Dateien übertragen wird geöffnet.

2 Klicken Sie auf **Hochladen**.

3 Ziehen Sie Dateien und legen Sie sie im Fenster Dateien übertragen ab, oder klicken Sie auf **Dateien auswählen**, um Dateien auszuwählen.

Die ausgewählten Dateien werden in den Ordner `Eigene Dokumente` hochgeladen.

Wenn Sie bei Internet Explorer 11 und Chrome auf ChromeBook Ordner, Dateien, die eine Größe von 0 KB oder mehr als 2 GB aufweisen, ziehen und ablegen, wird erwartungsgemäß eine Fehlermeldung angezeigt. Nach dem Verwerfen der Fehlermeldung können übertragbare Dateien nicht weiter gezogen und abgelegt werden.

Verwenden der Echtzeit-Audio/Video-Funktion für Webcams und Mikrofone

Mit der Echtzeit-Audio/Video-Funktion (RTAV) können Sie die Webcam oder das Mikrofon Ihrer lokalen Maschine auf Ihrem Remote-Desktop verwenden. Echtzeit-Audio/Video ist mit Standard-Konferenzanwendungen und browserbasierten Videoanwendungen kompatibel und unterstützt standardmäßige Webcams, USB-Audiogeräte und analoge Audioeingänge.

RTAV wird nur auf Chrome, Microsoft Edge und Firefox unterstützt. Die Standardvideoauflösung lautet 320 x 240. Die standardmäßigen RTAV-Einstellungen funktionieren problemlos mit den meisten Webcam- und Audioanwendungen. Information über das Ändern der RTAV-Einstellungen finden Sie unter „Konfigurieren von Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video“ im Dokument *Einrichten von Desktop- und Anwendungspools für View*.

Wenn der Remote-Desktop mit der Webcam oder dem Mikrofon der Clientmaschine verbunden ist, wird oben auf der Seitenleiste ein Symbol für jedes dieser Geräte angezeigt. Bevor der Desktop eine Verbindung zur Webcam oder dem Mikrofon herstellen kann, fragt der Browser möglicherweise nach der entsprechenden Berechtigung. Unterschiedliche Browser verhalten sich unterschiedlich.

- Microsoft Edge fragt jedes Mal nach der entsprechenden Berechtigung und dieses Verhalten kann nicht geändert werden. Weitere Informationen finden Sie unter https://blogs.windows.com/msedge-dev/2015/05/13/announcing-media-capture-functionality-in-microsoft-edge.
- Firefox fragt jedes Mal nach der entsprechenden Berechtigung. Dieses Verhalten kann jedoch geändert werden. Weitere Informationen finden Sie unter 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.
- Chrome fragt beim ersten Mal nach der entsprechenden Berechtigung. Wenn Sie die Verwendung des Geräts ermöglichen, werden Sie nicht erneut gefragt.

Wenn RTAV in einer Desktop-Sitzung verwendet wird und ein Benutzer eine Verbindung zu einem zweiten Desktop öffnet und wenn eine Sicherheitswarnung angezeigt wird (beispielsweise wenn kein gültiges Zertifikat installiert wurde), führt das Ignorieren der Warnung und das Fortsetzen der Verbindung zum zweiten Desktop dazu, dass RTAV die Arbeit in der ersten Desktop-Sitzung einstellt. Dies ist das erwartete Verhalten.

Abmelden oder trennen

Wenn Sie die Verbindung mit einem Remote-Desktop trennen, ohne sich abzumelden, bleiben bei einigen Konfigurationen die Anwendungen im Desktop geöffnet. Sie können auch die Verbindung mit einem Server trennen und Remoteanwendungen geöffnet lassen.

Vorgehensweise

- Melden Sie sich vom View-Server ab und trennen Sie die Verbindung mit dem Desktop (ohne sich abzumelden) oder verlassen Sie die gehostete Anwendung.

Option	Aktion
Im Auswahlbildschirm für Desktops und Anwendungen vor der Herstellung einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung	Klicken Sie in der rechten oberen Ecke des Bildschirms auf die Schaltfläche **Abmelden** der Symbolleiste.
In der Sidebar nach hergestellter Verbindung mit einem Remote-Desktop oder einer Remoteanwendung	Klicken Sie oben auf der Seitenleiste auf die Symbolleistenschaltfläche **Abmelden**.

- Schließen Sie eine Remoteanwendung.

Option	Aktion
In der Anwendung	Beenden Sie die Anwendung auf die übliche Weise. Klicken Sie beispielsweise in der Ecke des Anwendungsfensters auf die Schaltfläche **X** (Schließen).
In der Sidebar	Klicken Sie auf das **X** neben dem Dateinamen der Anwendung in der Liste **Wird ausgeführt** der Sidebar.

- Melden Sie sich ab oder trennen Sie die Verbindung mit einem Remote-Desktop.

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Melden Sie sich über das Windows-**Start**-Menü ab.
In der Sidebar	Um sich abzumelden und die Verbindung zu trennen, klicken Sie auf die Schaltfläche **Menü öffnen** neben dem Namen des Desktops in der Liste **Wird ausgeführt** der Sidebar und wählen Sie **Abmelden**. Dateien, die auf dem Remote-Desktop geöffnet sind, werden ohne vorheriges Speichern geschlossen. Um die Verbindung zu trennen, ohne sich abzumelden, klicken Sie auf die Schaltfläche **Menü öffnen** neben dem Namen des Desktops in der Liste **Wird ausgeführt** und wählen Sie **Schließen**. **Hinweis** Der View Administrator kann Ihren Desktop so konfigurieren, dass Sie beim Trennen der Verbindung automatisch abgemeldet werden. In diesem Fall werden alle geöffneten Anwendungen auf Ihrem Desktop geschlossen.
Verwendung eines URI	Verwenden Sie zum Abmelden den URI `https://`*`ConnectionServerFQDN`*`?desktopId=`*`desktop_name`*`&action=logoff`.

Zurücksetzen eines Remote-Desktops oder einer Remoteanwendung

Eventuell muss der Desktop oder die Anwendung zurückgesetzt werden, wenn die Anwendung oder das Desktop-Betriebssystem nicht mehr reagiert. Beim Zurücksetzen eines Remote-Desktops wird dieser heruntergefahren und neu gestartet. Beim Zurücksetzen von Remoteanwendungen werden diese beendet. Nicht gespeicherte Daten gehen verloren.

Das Zurücksetzen eines Remote-Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen Computer, mit der der Neustart des Computers erzwungen wird. Alle Dateien, die auf dem Remote-Desktop geöffnet sind, werden ohne vorheriges Speichern geschlossen.

Das Zurücksetzen von Anwendungen entspricht dem Beenden aller Remoteanwendungen, ohne nicht gespeicherte Daten zu speichern. Alle offenen Anwendungen werden geschlossen, auch wenn die Anwendungen zu verschiedenen RDS-Server-Farmen gehören.

Sie können einen Remote-Desktop nur zurücksetzen, wenn Ihr Administrator diese Funktion aktiviert hat.

Vorgehensweise

- Verwenden Sie den **Zurücksetzen**-Befehl.

Option	Aktion
Zurücksetzen von Anwendungen im Bildschirm zur Auswahl von Anwendungen	Im Bildschirm zur Auswahl von Desktops und Anwendungen klicken Sie zum Zurücksetzen aller ausgeführten Anwendungen vor der Herstellung einer Verbindung mit einem Remote-Desktop oder mit einer Remoteanwendung auf die Schaltfläche **Einstellungen** in der Symbolleiste rechts oben im Bildschirm und dann auf **Zurücksetzen**.
Zurücksetzen eines Remote-Desktops auf der Sidebar	Besteht eine Verbindung mit einem Remote-Desktop, klicken Sie auf die Schaltfläche **Menü öffnen** in der Symbolleiste neben dem Namen des Desktops in der Liste **Wird ausgeführt** der Sidebar und wählen Sie **Zurücksetzen**.
Zurücksetzen einer Remoteanwendung auf der Sidebar	Um alle ausgeführten Anwendungen zurückzusetzen, klicken Sie auf die Schaltfläche **Einstellungenfenster öffnen** in der Symbolleiste oben auf der Sidebar und klicken Sie dann auf **Zurücksetzen**.
Zurücksetzen eines Desktops mithilfe eines URI	Verwenden Sie zum Zurücksetzen eines Desktops den URI `https://`*`ConnectionServerFQDN`*`?desktopId=`*`desktop_name`*`&action=reset`.

Zum Zurücksetzen eines Remote-Desktops wird das Betriebssystem im Remote-Desktop neu gestartet. Der Client wird vom Desktop getrennt. Zum Zurücksetzen von Remoteanwendungen werden diese beendet.

Weiter

Warten Sie eine Weile, bis das System gestartet wurde, und versuchen Sie anschließend, eine Verbindung zum Remote-Desktop herzustellen.

Index

U

V

W

Z