Verwendung von HTML Access

März 2015

VMware Horizon 6

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-001116-06

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™ mit View™ 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 *Installation von View* und *Verwaltung von View* 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.

Browser auf Clientsystem

Die folgenden Webbrowser werden unterstützt:

	Chrome	Internet Explorer	Safari	Mobile Safari	Firefox
HTML Access 2.6	38 und 39	10 und 11	6.2, 7 und 8	iOS 7 oder höher	33
HTML Access 2.5	35, 36 und 37	9 (eingeschränkte Unterstützung), 10 und 11	6.1.3 und 7	iOS 7 oder höher	30 und 31
HTML Access 2.4	33 und 34	9 (eingeschränkte Unterstützung), 10 und 11	6.1.3 und 7	iOS 7 oder höher	28 und 29

Clientbetriebssysteme:

- Windows XP SP3 (32 Bit)
- Windows 7 SP1 oder kein SP (32 Bit oder 64 Bit)

- Windows 8.x-Desktop (32 oder 64 Bit)
- Windows Vista SP1 oder SP2 (32 Bit)
- Mac OS X Snow Leopard (10.6.8)
- Mac OS X Lion (10.7)
- Mac OS X Mountain Lion (10.8)
- Mac OS X Mavericks (10.9)
- Mac OS X Yosemite (10.10)
- iPad mit iOS 7.0 oder später (d. h. iPad 1 wird nicht unterstützt)
- Chrome OS 28.*x* oder höher

Remote-Desktop

In der virtuellen Maschine, auf die der Endbenutzer zugreift, muss die folgende Software installiert sein:

- Betriebssysteme für View-Einzelbenutzer-Desktops: Bei Verwendung von View Agent 6.0.x werden Windows XP SP3 (32-Bit) und Windows Vista (32-Bit) unterstützt. Wenn Sie über View Agent 6.0.x oder höher verfügen, werden außerdem Windows 7 (32- oder 64-Bit) und Windows Server 2008 R2 unterstützt. Wenn Sie über View Agent 6.0.1 oder höher verfügen, werden zusätzlich auch Remote-Desktops mit Windows 8 (32 oder 64 Bit) und Windows 8.1 (32 oder 64 Bit) unterstützt. Wenn Sie über View Agent 6.1 oder höher verfügen, wird außerdem Windows Server 2012 R2 unterstützt.
- Betriebssysteme für sitzungsbasierte View-Desktops auf RDS-Hosts: Wenn Sie über View Agent 6.0.2 oder höher verfügen, werden Windows Server 2008 R2, Windows Server 2012 und Windows Server 2012 R2 unterstützt.
- View Agent: HTML Access 2.6 erfordert View Agent 6.1 oder View Agent 6.0.2. HTML Access 2.5 erfordert View Agent 6.0.1. HTML Access 2.4 erfordert View Agent 6.0.

  Installationsanweisungen finden Sie im Dokument *Einrichten von Desktops und Anwendungen in View*.

WICHTIG Der Remote-Desktop muss eine virtuelle Maschine sein. Obwohl Sie View Agent auf einer physischen Maschine installieren können, kann das Blast-Protokoll, das mit HTML Access verwendet wird, nicht auf eine physische Maschine zugreifen. View Agent muss auf einer virtuellen Maschine installiert sein.

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 38.
- Die Einstellung **HTML Access** muss aktiviert sein.

Konfigurationsanweisungen werden unter „Vorbereiten von Remote-Desktops und Pools“, auf Seite 12 bereitgestellt.

View-Verbindungsserver

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

- HTML Access 2.6 erfordert View-Verbindungsserver 6.1 oder View-Verbindungsserver 6.0.x. Wenn Sie über View-Verbindungsserver 6.0.x verfügen, muss außerdem das separate HTML Access-Installationsprogramm auf dem Server ausgeführt werden.
- HTML Access 2.5 erfordert View-Verbindungsserver 6.0.1. Bei dieser Version von View-Verbindungsserver ist HTML Access 2.5 integriert.
- HTML Access 2.4 erfordert View-Verbindungsserver 6.0. Bei dieser Version von View-Verbindungsserver ist HTML Access 2.4 integriert.

Die HTML Access-Komponente ist im Installationsprogramm für View-Verbindungsserver standardmäßig bereits ausgewählt. Installationsanleitungen finden Sie im Dokument *Installation von View*.

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

Blast

Wenn Sie einen Webbrowser für den Zugriff auf einen Remote-Desktop verwenden, wird anstelle von PCoIP oder Microsoft RDP das Blast-Protokoll verwendet. 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.

WICHTIG Für einige Versionen von HTML Access gilt: Wenn Sie den View-Verbindungsserver versehentlich ohne die Option HTML Access installieren und später zu dem Entschluss kommen, dass Sie die HTML Access-Komponente doch verwenden möchten, müssen Sie den View-Verbindungsserver deinstallieren und dann das Installationsprogramm mit ausgewählter Option HTML Access erneut ausführen. Deinstallieren Sie bei der Deinstallation des View-Verbindungsservers nicht die View LDAP-Konfiguration mit der Bezeichnung AD LDS-Instanz VMwareVDMDS.

Bei Verwendung von anderen Versionen von HTML Access installieren Sie HTML Access mit einem separaten Installationsprogramm und müssen den View-Verbindungsserver nicht neu installieren.

Tabelle 1-1. Installationsvoraussetzungen für HTML Access -Versionen

HTML Access-Version	View-Verbindungsserver-Version	Installationsvoraussetzungen
2.6	6.1	Kein separates Installationsprogramm
2.6	6.0.x	Separates HTML Access-Installationsprogramm
2.5	6.0.x	Kein separates Installationsprogramm
2.4	6.0	Kein separates Installationsprogramm

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 ein separates HTML Access-Installationsprogramm erforderlich ist, laden Sie auf einem oder mehreren View-Verbindungsserver-Hosts in einer replizierten Gruppe das HTML Access-Installationsprogramm von der Downloads-Seite für View herunter und führen Sie das Installationsprogramm aus.

   Der Dateiname des Installationsprogramms lautet `VMware-Horizon-View-HTML-Access_X64-y.y.y-xxxxxx.exe`, wobei *y.y.y* die Versionsnummer und *xxxxxx* die Buildnummer ist.

3 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.

4 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*.

5 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*

6 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 11.

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 1-2. 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.
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 Remote-Desktops und Pools

Bevor Endbenutzer auf einen Remote-Desktop zugreifen können, müssen Administratoren bestimmte Pool-Einstellungen konfigurieren und View Agent auf den virtuellen Maschinen des Remote-Desktops 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 10.

- 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 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 zum Erstellen von Desktop-Pools und dem Zuweisen von Benutzerberechtigungen für Desktops vertraut. Weitere Informationen finden Sie in den Themen zur Erstellung von Desktop-Pools im Dokument *Einrichten von Desktops und Anwendungen in View*.

- Um sicherzustellen, dass der Remote-Desktop 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. Installieren Sie View Agent auf der übergeordneten virtuellen Maschine, die Sie als Quelle für einen Linked-Clone-Pool verwenden möchten, oder auf der VM-Vorlage, die Sie für einen Full-Clone-Pool verwenden möchten.

   Die View Agent-Software enthält eine HTML Access-Komponente.

2. Wenn Sie einen Linked-Clone-Pool erstellen, verwenden Sie vSphere Client, um einen Snapshot der übergeordneten virtuellen Maschine zu erstellen.

3. Verwenden Sie View Administrator, um einen Pool aus dieser virtuellen Maschine zu erstellen, und aktivieren Sie die Einstellung **HTML Access**, wenn Sie den Assistenten zum Hinzufügen von Desktop-Pools abschließen.

   HTML Access wird für VM-Desktop-Pools und, sofern Sie über HTML Access 2.6 verfügen, auch für sitzungsbasierte Desktop-Pools auf RDS-Hosts unterstützt. Remote-Anwendungen (gehostete Anwendungen) auf RDS-Hosts werden nicht unterstützt.

4. Stellen Sie sicher, dass in den Pool-Einstellungen die **Maximale Auflösung für alle Monitore** auf **1920x1200** oder höher festgelegt ist.

5. Weisen Sie Benutzern Berechtigungen für diesen Pool zu.

6. Verwenden Sie Horizon Client, um sich an einem Desktop aus diesem Pool anzumelden.

   Mit diesem Schritt stellen Sie noch vor der Verwendung von HTML Access sicher, dass der Pool ordnungsgemäß arbeitet.

7. 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.

8. Klicken Sie auf der angezeigten Webseite auf **VMware Horizon HTML Access** und melden Sie sich so wie bei der Horizon Client-Software an.

9. Klicken Sie auf der angezeigten Seite für die Desktop-Auswahl auf ein Desktop-Symbol.

Sie können jetzt über einen Webbrowser auf einen Remote-Desktop 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 14.

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 eines Zertifikats-Snap-In zu MMC auf einem Horizon View-Desktop auf Seite 15

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 15

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 16

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 Einrichten des Zertifikatsfingerabdrucks in der Windows-Registrierung auf Seite 17

Damit der HTML Access-Agent ein CA-Zertifikat benutzen kann, das in den Windows-Zertifikatspeicher importiert wurde, müssen Sie den Fingerabdruck des Zertifikats in einem Windows-Registrierungsschlüssel konfigurieren. Sie müssen diesen Schritt auf jedem einzelnen Desktop ausführen, auf dem Sie das Standardzertifikat durch ein CA-signiertes Zertifikat ersetzen.

Hinzufügen eines Zertifikats-Snap-In zu MMC auf einem Horizon 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 ist, in dem der HTML Access-Agent installiert wurde.

Vorgehensweise

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

2 Im Fenster MMC gehen Sie zu **Datei > Snap-In hinzufügen/entfernen**.

3 Im Fenster Snap-In hinzufügen oder entfernen wählen Sie **Zertifikate** und klicken auf **Hinzufügen**.

4 Im Fenster Zertifikate-Snap-In wählen Sie **Computer-Konto** aus. Klicken Sie auf **Weiter**, wählen Sie **Lokaler Computer** und klicken Sie auf **Beenden**.

5 Im Fenster Snap-In hinzufügen oder entfernen klicken Sie 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 15.

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 eines Zertifikats-Snap-In zu MMC auf einem Horizon View-Desktop“, auf Seite 15.

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 16.

Konfigurieren Sie die entsprechenden Registrierungsschlüssel mit dem Fingerabdruck des Zertifikats. Siehe „Einrichten des Zertifikatsfingerabdrucks in der Windows-Registrierung“, auf Seite 17.

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 „Einrichten des Zertifikatsfingerabdrucks in der Windows-Registrierung“, auf Seite 17.

Einrichten des Zertifikatsfingerabdrucks in der Windows-Registrierung

Damit der HTML Access-Agent ein CA-Zertifikat benutzen kann, das in den Windows-Zertifikatspeicher importiert wurde, müssen Sie den Fingerabdruck des Zertifikats in einem Windows-Registrierungsschlüssel konfigurieren. Sie müssen diesen Schritt auf jedem einzelnen Desktop ausführen, auf dem Sie das Standardzertifikat durch ein CA-signiertes Zertifikat ersetzen.

Voraussetzungen

Stellen Sie sicher, dass das CA-signierte Zertifikat in den Windows-Zertifikatspeicher importiert wurde. Siehe „Importieren eines Zertifikats für den HTML Access Agent in den Windows-Zertifikatspeicher“, auf Seite 15.

Vorgehensweise

1 Im MMC-Fenster auf dem View-Desktop, wo der HTML Access-Agent installiert ist, navigieren Sie zum Ordner **Zertifikate (Lokaler Computer) > Persönliche > Zertifikate**.

2 Doppelklicken Sie auf das CA-Zertifikat, das Sie in den Windows-Zertifikatsspeicher importiert haben.

3 Im Dialogfeld Zertifikate klicken Sie auf die Registerkarte Details. Blättern Sie nach unten und wählen Sie das Symbol **Fingerabdruck**.

4 Kopieren Sie den ausgewählten Fingerabdruck in eine Textdatei.

   Beispiel: `31 2a 32 50 1A 0B 34 b1 65 46 13 a8 0A 5E f7 43 6E a9 2C 3E`

   Hinweis Wenn Sie den Fingerabdruck kopieren, dürfen Sie das führende Leerzeichen nicht mitkopieren. Wenn Sie versehentlich das führende Leerzeichen mit dem Fingerabdruck zusammen in den Registrierungsschlüssel (in Schritt 7) einfügen, kann es sein, dass das Zertifikat nicht erfolgreich konfiguriert werden kann. Dieses Problem kann auftreten, obwohl das führende Leerzeichen nicht im Textfeld Registrierungswert 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 `SslHash`-Wert und fügen Sie den Fingerabdruck des Zertifikats in das Textfeld ein.

8 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.

Wenn sich ein Benutzer über HTML Access mit einem Desktop verbindet, präsentiert der HTML Access-Agent dem Browser des Benutzers das CA-Zertifikat.

Upgrade der HTML Access -Software

Installieren Sie die neueste HTML Access-Version, um von den neuesten Updates und Verbesserungen zu profitieren.

Um ein Upgrade auf die neueste Version von HTML Access durchzuführen, müssen Sie sicherstellen, dass die neueste Version des View-Verbindungsservers auf allen Instanzen in einer replizierten Gruppe installiert ist.

Für einige Versionen von HTML Access ist ein separates HTML Access-Installationsprogramm erforderlich, da keine entsprechende Wartungsversion des View-Verbindungsservers freigegeben ist. Die folgende Tabelle gibt Aufschluss über die Versionen von HTML Access, für die ein separates Installationsprogramm erforderlich ist.

Tabelle 1-3. Installationsvoraussetzungen für HTML Access -Versionen

HTML Access-Version	View-Verbindungsserver-Version	Installationsvoraussetzungen
2.6	6.1	Kein separates Installationsprogramm
2.6	6.0.x	Separates HTML Access-Installationsprogramm
2.5	6.0.x	Kein separates Installationsprogramm
2.4	6.0	Kein separates Installationsprogramm

Zum Abschließen des Upgrades von HTML Access müssen Sie außerdem das Installationsprogramm für View Agent auf den entsprechenden übergeordneten virtuellen Maschinen oder VM-Vorlagen für Ihre Desktop-Pools ausführen. Die Version von View Agent sollte mit der Version des View-Verbindungsservers übereinstimmen.

Wichtig Zum View Agent-Installationsprogramm gehört die HTML Access-Agentenkomponente, die im Remote Experience Agent für Versionen vor Horizon 6.0 (mit View) enthalten war. Der Remote Experience Agent war Bestandteil des Horizon View Feature Pack. Zum Upgrade von Funktionen, die mit dem Remote Experience Agent installiert wurden, können Sie einfach das View Agent-Installationsprogramm ausführen. Dieses Installationsprogramm entfernt den Remote Experience Agent, bevor das Upgrade ausgeführt wird. Wenn Sie den Remote Experience Agent manuell entfernen möchten, müssen Sie dies tun, bevor Sie das Installationsprogramm für die neue View Agent-Version ausführen.

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 **VMware Horizon View 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 gesammelte Daten

Wenn Ihr Unternehmen am Programm zur Verbesserung der Benutzerfreundlichkeit teilnimmt, erhebt VMware Daten aus bestimmten Clientfeldern. 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 Clientinformationen 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 Installationsassistenten für den View-Verbindungsserver diese Option „abonnieren“ oder nach der Installation eine entsprechende Option in View Administrator festlegen.

Tabelle 1-4. Für das Programm zur Verbesserung der Benutzerfreundlichkeit erfasste Client-Daten

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	2.6.0-*build_number*
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
Interne Versionszeichenfolge des Browsers	`<browser_version>`	Nein	Beispiele hierfür sind folgende Werte: ■ 7.0.3 (für Safari), ■ 29.0 (für Firefox)

Tabelle 1-4. Für das Programm zur Verbesserung der Benutzerfreundlichkeit erfasste Client-Daten (Fortsetzung)

Beschreibung	Feldname	Wird dieses Feld anonymisiert?	Beispielswert
Core-Implementierung des Browsers	`<browser_core>`	Nein	Beispiele hierfür sind folgende Werte: ■ Chrome ■ Safari ■ Firefox ■ MSIE (für Internet Explorer)
Angabe, ob der Browser auf einem Handheld-Gerät ausgeführt wird	`<browser_is_hand_held>`	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 Clientbetriebssysteme 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-Verbindungsserver-Host 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

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`

Ändern Sie die URL für den Hilfe-Link auf der Anmeldeseite und dem Bildschirm zur Desktop-Auswahl.	`link.help` Dieser Link verweist standardmäßig auf ein Hilfesystem, das auf der VMware-Website verwaltet wird. Der Link zur Hilfe wird in der rechten oberen Ecke des Bildschirms angezeigt. Auf dem Anmeldebildschirm für HTML Access und auf dem Bildschirm zur Desktop-Auswahl erscheint der Hilfe-Link als Fragezeichen-Symbol.

3 (Optional) Ändern Sie die URL für den Hilfe-Link in der Horizon Client-Symbolleiste.

Mit der Anmeldung an einem Desktop wird der Hilfe-Link zu einem **Hilfe**-Befehl im Dropdown-Menü am rechten Ende des Clients. Um die URL für diesen Link zu ändern, bearbeiten Sie die `HELP_URL_VIEW`-Eigenschaft in der entsprechenden Datei im jeweiligen Ordner.

Option	Beschreibung
Für HTML Access 2.6	Auf dem View-Verbindungsserver-Host befindet sich die Datei in: *`ViewConnectionServer_InstallDir`*`\webapps\portal\desktop\locale\`
Für HTML Access 2.4 und 2.5	Im Remote-Desktop-Betriebssystem (in dem View Agent installiert ist) befindet sich die Datei in: `C:\Program Files\VMware\VMware Blast\web\locale\`

Wenn Sie beispielsweise Englisch verwenden, bearbeiten Sie die `HELP_URL_VIEW`-Eigenschaft in der Datei `en.json`.

4 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 Ordner „`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`.

5 Starten Sie den View Web-Komponentendienst neu.

Aktivieren von Desktops von RDS-Hosts

Mit HTML Access 2.6 können Administratoren View-Verbindungsserver konfigurieren, damit ein Microsoft RDS-Host sitzungsbasierte Desktops zur Verfügung stellen kann.

Voraussetzungen

Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogramms ADSI-Editor mit Ihrer Windows-Betriebssystemversion. Bei der Verwendung eines Windows Server 2012 RDS-Hosts müssen Sie möglicherweise die AD DS & LDS Tools aus den Remote Server Administration Tools (RSAT) in **Rollen & Funktionen hinzufügen** installieren.

Vorgehensweise

1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem View-Verbindungsserver-Host.

2 Wählen Sie im Dialogfeld „Verbindungseinstellungen“ **DC=vdi,DC=vmware,DC=int** aus oder verbinden Sie sich damit.

3 In the Computer pane, select or type **`localhost:389`** or the fully qualified domain name (FQDN) of the View-Verbindungsserver host followed by port 389.

   Zum Beispiel: **`localhost:389`** oder **`meincomputer.meinedomäne.com:389`**

4 Sofern der Pool bereits erstellt wurde, suchen Sie dessen Namen unter dem Objekt **OU=Applications** und fügen Sie **BLAST** zum Attribut **pae-ServerProtocolLevel** hinzu.

5 Suchen Sie den Namen der Farm unter dem Objekt **OU=Server Groups** und fügen Sie **BLAST** im Attribut **pae-ServerProtocolLevel** hinzu.

Die Farm-Elemente erscheinen nun im Web-Client von HTML Access.

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 mit bestimmten Konfigurationsoptionen klicken.

Sie können die Verbindungsherstellung mit einem Remote-Desktop 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
- Desktopanzeigename
- 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 des Benutzers, des Desktops und der Desktop-Aktionen oder Konfigurationsoptionen.

URI-Spezifikation

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

```
https://[<varname id="VARNAME_E0F8F9951BC4471D9871655A18782C9E">authority-part</varname>][?<var-
name id="VARNAME_217F9AF17A3745369FD8E2154505D735">query-part</varname>]
```

Wichtig Beim Codieren der HTML-Hyperlinks oder Schaltflächen, die den URI enthalten, dürfen Sie nicht `target='_Blank'` für den Link verwenden. Dieser Code wird zum Öffnen eines neuen Browserfensters verwendet, verursacht aber Probleme in Internet Explorer 9, 10 und 11. Wenn Sie diesen Code in einer `href`-Anweisung verwenden und der Benutzer dann den Menübefehl **Verbindung trennen** auswählt, versucht der Client nach dem Trennen des Desktops sofort eine erneute Verbindung herzustellen. Der Benutzername und der Domänenname sind außerdem nicht festgelegt.

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:

```
<varname id="VARNAME_1BAB6153D2834B1490509093A1961D1F">server-add-
ress</varname>:<varname id="VARNA-
ME_2296A4E54893485C852FFE94067114D7">port-number</varname>
```

query-part

Gibt die zu verwendenden Konfigurationsoptionen oder die durchzuführenden Desktopaktionen 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:

```
<varname id="VARNAME_48A6B3A0E1184943BC1206017B78B9D5">query1</varna-
me>=<varname id="VARNAME_9B9916FF3D3540D4AA5622F9C828F072">va-
lue1</varname>[&<varname id="VARNA-
ME_6BCA2912EC454A5683D586754BF89DCE">query2</varname>=<varname
id="VARNAME_F698C39E83D34D639C943ACDF828BAFE">value2</varname>...]
```

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, und Sie müssen dafür wie folgt das URL-Codierungsformat verwenden: Für das Pfundsymbol (#) verwenden Sie **%23**, für das Prozentzeichen (%) verwenden Sie **%25**, für das kaufmännische Und-Zeichen (&) verwenden Sie **%26**, für das @-Zeichen verwenden Sie **%40** und für den umgekehrten Schrägstrich (\) 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

Die Domäne, die mit dem Benutzer verknüpft ist, der eine Verbindung zum Remote-Desktop herstellt.

userName

Der Active Directory-Benutzer, der eine Verbindung zum Remote-Desktop 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.

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 an. Bei Verwendung dieser Aktion müssen Sie keinen Desktop angeben.
`start-session`	Startet den angegebenen Desktop. Wenn keine „action“-Abfrage bereitgestellt wird und der Desktopname angegeben wird, ist `start-session` die Standardaktion.
`zurücksetzen`	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.
`logoff`	Meldet den Benutzer vom Gastbetriebssystem auf dem Remote-Desktop ab.

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 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: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.

4 `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>
```

HINWEIS Verwenden Sie nicht `target='_Blank'` für den Link, wie beispielsweise im folgenden Code:

```
<a href="https://view.mycompany.com?desktopId=Primary%20Desktop&action=start-session"
target="_Blank">Test Link</a>
```

`target='_Blank'` wird zum Öffnen eines neuen Browserfensters verwendet, verursacht aber Probleme in Internet Explorer 9, 10 und 11. Wenn Sie diesen Code in einer `href`-Anweisung verwenden und der Benutzer dann den Menübefehl **Verbindung trennen** auswählt, versucht der Client nach dem Trennen des Desktops sofort eine erneute Verbindung herzustellen. Der Benutzername und der Domänenname sind außerdem nicht festgelegt.

Konfigurieren von Gruppenrichtlinieneinstellungen für HTML Access

Sie können Gruppenrichtlinieneinstellungen konfigurieren, die das Verhalten von HTML Access auf Ihren Remote-Desktops steuern. Um diese Einstellungen anzuwenden, fügen Sie die ADM-Vorlagendatei von HTML Access zu Gruppenrichtlinienobjekten (GPOs) in Active Directory hinzu.

Voraussetzungen

- Stellen Sie sicher, dass View Agent 6.0 oder höher auf Ihren Remote-Desktops installiert ist. View Agent 6.0 oder höher enthält eine HTML Access-Komponente. Für vorherige Versionen mussten Sie den Remote Experience Agent installieren, um die HTML Access-Komponente zu erhalten.
- Stellen Sie sicher, dass Active Directory-GPOs für die HTML Access-Gruppenrichtlinieneinstellungen erstellt wurden. Die GPOs müssen mit der Organisationseinheit (Organizational Unit, OU) verknüpft werden, die Ihre Remote-Desktops enthält. Allgemeine Informationen zum Einrichten von View-Gruppenrichtlinieneinstellungen in Active Directory finden Sie unter „Konfigurieren von Richtlinien“ im Dokument *Einrichten von Desktops und Anwendungen in View*.
- Vergewissern Sie sich, dass Microsoft Management Console (MMC) und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Machen Sie sich mit den HTML Access-Gruppenrichtlinieneinstellungen vertraut. Siehe „Gruppenrichtlinieneinstellungen für HTML Access“, auf Seite 30.

Vorgehensweise

1 Laden Sie die View-GPO-Bundle-`ZIP`-Datei von der VMware Horizon 6-Download-Site unter http://www.vmware.com/go/downloadview herunter.

   Der Dateiname ist `VMware-Horizon-View-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` (*x.x.x* ist die Version, *yyyyyyy* die Build-Nummer). Alle ADM- und ADMX-Dateien, die Gruppenrichtlinieneinstellungen für View bereitstellen, sind in dieser Datei verfügbar.

2 Kopieren Sie die Datei auf Ihren Active Directory-Server und extrahieren Sie die Datei.

   Die HTML Access-GPOs sind in der ADM-Vorlagendatei `Blast-enUS.adm` enthalten.

3 Bearbeiten Sie das GPO auf dem Active Directory-Server.

Option	Beschreibung
Windows 2008 oder 2012	a Wählen Sie **Start > Verwaltung > Gruppenrichtlinienverwaltung**. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **Bearbeiten** aus.
Windows 2003	a Wählen Sie **Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer**. b Klicken Sie mit der rechten Maustaste auf die OU, die Ihre Remote-Desktops enthält, und wählen Sie **Eigenschaften** aus. c Klicken Sie auf der Registerkarte **Group Policy (Gruppenrichtlinie)** auf **Open (Öffnen)**, um das Plug-In **Group Policy Management (Gruppenrichtlinienverwaltung)** zu öffnen. d Klicken Sie im rechten Fensterbereich auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **Edit (Bearbeiten)**.

Das Fenster Group Policy Object Editor (Gruppenrichtlinienobjekt-Editor) wird angezeigt.

4 Klicken Sie im Gruppenrichtlinienobjekt-Editor mit der rechten Maustaste unter **Computerkonfiguration** auf **Administrative Vorlagen** und wählen Sie **Vorlagen hinzufügen/entfernen**.

5 Klicken Sie auf **Hinzufügen**, suchen Sie nach der Datei `Blast-enUS.adm` und klicken Sie auf **Öffnen**.

6 Klicken Sie auf **Close (Schließen)**, um die Richtlinieneinstellungen in der ADM-Vorlagendatei auf das GPO anzuwenden.

Der VMware Blast-Ordner wird im linken Fensterbereich unter **Administrative Vorlagen > Klassische administrative Vorlagen** angezeigt.

7 Konfigurieren Sie die Gruppenrichtlinieneinstellungen für HTML Access.

8 Stellen Sie sicher, dass Ihre Richtlinieneinstellungen auf die Remote-Desktops angewendet werden.

a Führen Sie den Befehl `gpupdate.exe` auf den Desktops aus.

b Starten Sie die Desktops neu.

Gruppenrichtlinieneinstellungen für HTML Access

Die HTML Access ADM-Vorlagendatei `Blast-enUS.adm` enthält Gruppenrichtlinieneinstellungen, die Sie auf Ihre Remote-Desktops anwenden können. Nachdem die Vorlagendatei in Active Directory importiert wurde, sind die Gruppenrichtlinieneinstellungen für HTML Access im `VMware Blast`-Ordner im Gruppenrichtlinien-Editor enthalten.

Tabelle 2-2. Gruppenrichtlinieneinstellungen für HTML Access

Einstellung	Beschreibung
Löschen des Bildschirms	Steuert, ob die virtuelle Remote-Maschine während einer HTML Access-Sitzung außerhalb von View gesteuert werden kann. Beispielsweise kann ein Administrator vSphere Web Client verwenden, um auf der virtuellen Maschine eine Konsole zu öffnen, während ein Benutzer über HTML Access mit dem Desktop verbunden ist. Wenn diese Einstellung aktiviert oder nicht konfiguriert ist und ein Benutzer versucht, während einer HTML Access-Sitzung außerhalb von View auf die virtuelle Remote-Maschine zuzugreifen, zeigt die virtuelle Remote-Maschine einen leeren Bildschirm an. Wenn diese Einstellung deaktiviert ist, zeigt die virtuelle Remote-Maschine unter den zuvor genannten Bedingungen dem zweiten Remote-Benutzer die aktive View-Desktop-Sitzung an.
Sitzungsspeicherbereinigung	Steuert die Speicherbereinigung für abgebrochene Remote-Sitzungen. Wenn diese Einstellung aktiviert ist, können Sie Intervall und Schwellenwert für die Speicherbereinigung konfigurieren. Das Intervall steuert, wie häufig die Speicherbereinigung durchgeführt wird. Sie legen das Intervall in Millisekunden fest. Der Schwellenwert gibt an, wie viel Zeit nach dem Abbruch einer Sitzung verstreichen muss, damit diese zum Löschen markiert wird. Sie legen den Schwellenwert in Sekunden fest.
Tonwiedergabe	Steuert, ob die Tonwiedergabe auf dem Remote-Desktop zulässig ist. Standardmäßig ist diese Einstellung aktiviert.
Bildqualität	Steuert die Bildqualität für das Remote-Display. Es gibt drei Profile für die Bildqualität, niedrig, mittel und hoch. Der Encoder versucht, die bestmögliche Qualitätsstufe einzustellen, unter Berücksichtigung der Einschränkungen, wie verfügbare Bandbreite, aktuelle Frame-Rate und Größe der Region, die vor Kurzem im aktuellen Frame geändert wurde. Der Encoder verfolgt, welche Regionen des Clientbildschirms derzeit eine niedrige oder mittlere Qualität aufweisen und erhöht schrittweise diese Bereiche auf eine hohe Qualität. Wenn diese Einstellung aktiviert ist, können Sie die JPEG-Einstellungen für niedrige, mittlere und hohe Qualität auf unterschiedliche Werte festlegen. Die tatsächlichen JPEG-Qualitätsstufen für die Einstellungen „niedrig“, „mittel“ und „hoch“ sind einzeln konfigurierbar durch die Eingabe von Zahlen zwischen 0 und 100. Die Farbunterabtastung wird gemäß der gewählten JPEG-Qualitätsstufe aktiviert. Wenn die JPEG-Qualität auf 80 oder höher gesetzt ist, wird die Farbunterabtastung deaktiviert und das Verhältnis wird auf den höchsten verfügbaren Wert gesetzt, nämlich YUV-4:4:4. Wenn die JPEG-Qualität auf 79 oder einen kleineren Wert gesetzt wird, wird das Verhältnis auf YUV-4:2:0 festgelegt. ■ **Niedrige JPEG-Qualität**. Standardmäßig ist dieser Wert auf 25 festgelegt. Sie können außerdem die niedrige JPEG-Farbuntertastung auf verschiedene Verhältniswerte festlegen. Standardmäßig ist das Verhältnis auf den kleinsten verfügbaren Wert festgelegt: 4:1:0. ■ **Mittlere JPEG-Qualität**. Standardmäßig ist dieser Wert auf 35 festgelegt. Sie können außerdem die niedrige JPEG-Farbuntertastung auf verschiedene Verhältniswerte festlegen. Standardmäßig ist das Verhältnis auf den kleinsten verfügbaren Wert festgelegt: 4:2:0. ■ **Hohe JPEG-Qualität**. Standardmäßig ist dieser Wert auf 90 festgelegt. Sie können außerdem die hohe JPEG-Farbuntertastung auf verschiedene Verhältniswerte festlegen. Standardmäßig ist das Verhältnis auf den höchsten verfügbaren Wert festgelegt: 4:4:4.

Tabelle 2-2. Gruppenrichtlinieneinstellungen für HTML Access (Fortsetzung)

Einstellung	Beschreibung
Zwischenablagenumleitung konfigurieren	Bestimmt die Richtung, in der die Zwischenablagenumleitung zulässig ist. Es kann nur Text kopiert und eingefügt werden. Sie können einen der folgenden Werte wählen: ■ **Nur Client zu Server aktiviert** (Dadurch ist der Kopier- und Einfügevorgang nur vom Clientsystem zum Remote-Desktop zulässig.) ■ **In beide Richtungen deaktiviert** ■ **In beide Richtungen aktiviert** ■ **Nur Server zu Client aktiviert** (Dadurch ist der Kopier- und Einfügevorgang nur vom Remote-Desktop zum Clientsystem zulässig.) Diese Einstellung gilt nur für View Agent. Für Einzelbenutzer-Remote-Desktops lautet der Standardwert **Nur Client zu Server aktiviert**, wenn diese Einstellung deaktiviert oder nicht konfiguriert ist. Für sitzungsbasierte Remote-Desktops auf RDS-Hosts (die mit HTML Access 2.6 verfügbar sind), lautet der Standardwert **In beide Richtungen deaktiviert**, wenn diese Einstellung deaktiviert oder nicht konfiguriert ist.
HTTP-Dienst	Ermöglicht es Ihnen, den sicheren TCP-Port (HTTPS) für den Blast Agent-Dienst zu ändern. Der Standardport ist 22443. Aktivieren Sie diese Einstellung, um die Portnummer zu ändern. Wenn Sie diese Einstellung ändern, müssen Sie auch Einstellungen für die Firewall auf den betroffenen Remote-Desktops (auf denen View Agent installiert ist) aktualisieren.

Verwendung eines Remote-Desktops 3

Der Client weist eine Dropdown-Symbolleiste und ein Dropdown-Menü auf, damit Sie die Verbindung zu einem Remote-Desktop problemlos trennen können. Sie können hierfür aber auch die Tastenkombination Strg+Alt+Entf verwenden.

Dieses Kapitel behandelt die folgenden Themen:

Funktionsunterstützungs-Matrix

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

Tabelle 3-1. Über HTML Access unterstützte Funktionen

Funktion	Windows 8.x Remote-Desktop	Windows 7-Remote-Desktop	Windows XP-Remote-Desktop	Windows Vista-Remote-Desktop	Windows Server 2008 R2-Desktop
RSA SecurID oder RADIUS	X	X	X	X	X
Einmaliges Anmelden	X	X	X	X	X
RDP-Anzeigeprotokoll					
PCoIP-Anzeigeprotokoll					
Blast-Protokoll	X	X	X	X	X
USB-Zugriff					

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

Funktion	Windows 8.x Remote-Desktop	Windows 7-Remote-Desktop	Windows XP-Remote-Desktop	Windows Vista-Remote-Desktop	Windows Server 2008 R2-Desktop
Echtzeit-Audio/Video (RTAV)					
Wyse MMR					
Windows 7 MMR					
Virtuelles Drucken					
Standortbasiertes Drucken					
Smartcards					
Mehrere Monitore					

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

Funktionsunterstützung für sitzungsbasierte Desktops auf RDS-Hosts

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

Wenn Sie über HTML Access 2.6 oder höher verfügen, können Sie auch auf einem Microsoft RDS-Host auf sitzungsbasierte Remote-Desktops zugreifen. 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 RDS-Hosts mit installiertem View Agent 6.0.2

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

Informationen dazu, welche Versionen jedes Gastbetriebssystems oder welche Service Packs unterstützt werden, finden Sie unter „Unterstützte Betriebssysteme für View Agent“ in der Installationsdokumentation für View 6.x.

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

Verwenden Sie Ihre Active Directory-Anmeldedaten zum Herstellen einer Verbindung mit den Remote-Desktops, 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 Domänennamen für die Anmeldung.

Vorgehensweise

1. Wenn Sie zur Eingabe von RSA SecurID- oder RADIUS-Authentifizierungsdaten 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.

2. 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.

3. Geben Sie im Anmeldedialogfeld Ihren Active Directory-Benutzernamen, Ihr Kennwort und den Domänennamen ein und klicken Sie auf **Anmelden**.

4. Wenn Sie zur Verwendung mehrerer Remote-Desktops berechtigt sind, klicken Sie auf das Symbol für den Remote-Desktop, auf den Sie zugreifen möchten.

   Der Remote-Desktop wird in Ihrem Browser angezeigt.

Weiter

Wenn Sie Safari verwenden und bald nach der Verbindungsherstellung mit dem Desktop die Verbindung getrennt und eine Aufforderung angezeigt wird, auf einen Link zur Bestätigung eines Sicherheitszertifikats zu klicken, können Sie wählen, ob Sie dem Zertifikat vertrauen. Siehe „Einstufen eines selbstsignierten Zertifikats als vertrauenswürdig“, auf Seite 35.

Einstufen eines selbstsignierten Zertifikats als vertrauenswürdig

Bei Verwendung eines Safari-Browsers ist in einigen Fällen zu beobachten, dass recht schnell nach dem Herstellen einer Verbindung zu einem Remote-Desktop die Verbindung getrennt und ein Dialogfeld „Desktop-Verbindung getrennt“ angezeigt wird Sie können den Browser dazu verwenden, das selbstsignierte Sicherheitszertifikat zu akzeptieren und erneut eine Verbindung zum Remote-Desktop herzustellen.

Dieses Problem kann auftreten, wenn das Blast Secure Gateway nicht verwendet wird.

Vorgehensweise

1. Klicken Sie im Dialogfeld „Desktop-Verbindung getrennt“ auf den Link **Klicken Sie hier, um das Sicherheitszertifikat zu akzeptieren**.
2. Klicken Sie in der nächsten angezeigten Eingabeaufforderung auf die Schaltfläche **Zertifikat anzeigen**.
3. Klicken Sie im anschließend angezeigten Bereich „Blast“ auf die Dropdown-Liste **Vertrauen**, um sie zu erweitern.

4 Wählen Sie in der Dropdown-Liste **Bei Verwendung dieses Zertifikats** die Option **Immer vertrauen** aus und klicken Sie auf **Weiter**.

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

6 Klicken Sie im Desktop-Auswahlfenster auf den Remote-Desktop.

Sie werden anschließend erneut mit dem Remote-Desktop verbunden und angemeldet.

Produkteinschränkungen

Das von Web client zur Verfügung gestellte Programm HTML Access weist Produkteinschränkungen in Bezug auf die Tonwiedergabe und Tastaturen auf.

- Die Tonwiedergabe wird für Remote-Desktops unter Windows XP und Windows Vista nicht unterstützt.
- Internet Explorer 9 wird von HTML Access 2.6 nicht unterstützt. Die Versionen HTML Access 2.4 und 2.5 unterstützen zwar Internet Explorer 9, doch diese Version des Browsers unterstützt ihrerseits zahlreiche HTML5-Funktionen nicht, die von HTML Access bereitgestellt werden. Zu den Funktionen, die von Internet Explorer 9 (selbst in Kombination mit HTML Access 2.4 oder 2.5) nicht unterstützt werden, gehören u. a. die Tonwiedergabe, die Zwischenablagenumleitung, Mauszeiger-Änderungen und der Vollbildmodus.
- Wenn Sie einen Internet Explorer-Browser oder einen Browser auf Handheld-Geräten wie iPads und Android-Tablets verwenden, ändern sich die Mauszeiger-Typen nicht dynamisch anhand der Position des Zeigers.

  Momentan stehen diese Typen nicht zur Verfügung: Aktivitäts-Cursor, Ziehen-Cursor und Cursor für Größenänderung. Wenn Sie im Internet Explorer oder in Browsern von mobilen Endgeräten den Mauszeiger beispielsweise in einem Remote-Desktop über einem Link auf einer Webseite positionieren, ändert sich der Mauszeiger nicht in ein Handsymbol. Wenn Sie den Mauszeiger an den Rand eines Fensters bewegen, ändert sich der Zeiger nicht in einen Pfeil zur Größenänderung. Wenn Sie Text bearbeiten, ändert sich der Mauszeiger nicht in einen Cursor. Sie können diese Aktionen ausführen, der Mauszeiger wird jedoch weiter als Zeiger angezeigt.
- Einige Änderungstasten, Sondertasten und Tastenkombinationen funktionieren mit einem Remote-Desktop nicht. Weitere Informationen, darunter Informationen zur Verwendung internationaler Tastaturen finden Sie unter „Tastatureinschränkungen“, auf Seite 36 und „Internationale Tastaturen“, auf Seite 37.

Tastatureinschränkungen

Unabhängig von der verwendeten Sprache können einige Tastenkombinationen nicht an einen Remote-Desktop 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.

Die folgenden Tasteneingaben und Tastenkombinationen funktionieren häufig nicht:

- Strg+T
- Strg+W
- Strg+N
- Windows-Taste

- Befehlstaste
- Alt+Enter
- Strg+Alt+*beliebige_Taste*
- Feststelltaste+*Zusatztaste* (z. B. Alt oder Umschalttaste)
- Funktionstasten, wenn Sie ein Chromebook verwenden

WICHTIG Zur Eingabe der Tastenkombination Strg+Alt+Del verwenden Sie die Option **Strg+Alt+Delete senden** im Dropdown-Menü, das sich am rechten Ende der Client-Menüleiste befindet.

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 3-3. 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 der Remote-Desktop mit der richtigen Video-RAM-Größe konfiguriert wurde, kann der Client die Größe des Remote-Desktops an die Größe des Clientfensters anpassen. 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.

Wichtig Um die 3D-Renderfunktion zu verwenden, müssen Sie ausreichend VRAM für jeden Remote-Desktop mit Windows 7 oder höher zuweisen.

- 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.

Wenn das 3D-Rendern aktiviert ist, beträgt die Höchstzahl der Monitore 1 und die maximale Auflösung beträgt 1920 x 1200. Die Schätzung der für das Blast-Protokoll 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*.

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 auf diese Auflösung festlegen. Wählen Sie aus dem Dropdown-Menü rechts in der Client-Menüleiste den Befehl **Hochauflösungsmodus umschalten** aus. Klicken Sie zum Aufrufen dieser Menüleiste auf den Abwärtspfeil auf der Registerkarte oben in der Mitte des Fensters.

HTML Access stellt auch den Befehl **Umschalten auf Vollbild** zur Verfügung, der im Dropdown-Menü ausgewählt werden kann.

Wichtig Um den Hochauflösungsmodus im Vollbildmodus zu verwenden, müssen Sie ausreichend VRAM für jeden Remote-Desktop mit Windows 7 oder höher zuweisen. Die Schätzung der für das Blast-Protokoll 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*.

Ton

Wenn Sie ein Chrome-Gerät oder einen Browser mit WebSockets-Unterstützung verwenden, ist auf Ihrem Remote-Desktop die Tonwiedergabe möglich. Es gelten jedoch einige Einschränkungen.

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

Berücksichtigen Sie die folgenden Richtlinien:

- Die Tonwiedergabe wird für Remote-Desktops unter Windows XP und Windows Vista nicht unterstützt.
- Verwenden Sie zum Erhöhen der Lautstärke die Tonsteuerung auf Ihrem Clientsystem und nicht die des Remote-Desktops.
- 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 Tonqualität kommen. Einige Browser eignen sich in dieser Hinsicht besser als andere.

Kopieren und Einfügen von Text

Ihr View-Administrator kann diese Funktion so einstellen, dass Kopier- und Einfügevorgänge nur von Ihrem Clientsystem zu einem Remote-Desktop oder nur von einem Remote-Desktop zu Ihrem Clientsystem zugelassen werden oder beide bzw. keiner der beiden Vorgänge möglich sind. Hierfür gelten allerdings einige Einschränkungen.

Diese Funktion ist mit einem Chrome-Gerät oder einem Browser, der WebSockets unterstützt, verfügbar.

Die Administratoren konfigurieren die Möglichkeit zum Kopieren/Einfügen durch die Verwendung von Gruppenrichtlinienobjekten (GPOs), die View Agent auf den Remote-Desktops zugeordnet sind. Weitere Informationen finden Sie unter „Gruppenrichtlinieneinstellungen für HTML Access“, auf Seite 30.

Sie können einfachen oder formatierten Text, einschließlich aller Nicht-ASCII-Zeichen, aus Horizon Client zu einem Remote-Desktop kopieren oder umgekehrt, aber der eingefügte Text ist einfacher Text. Sie können bis zu 5000 Zeichen kopieren und einfügen.

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.

Verwenden der Kopier- und Einfügen-Funktion

Zum Kopieren und Einfügen von Text müssen Sie die Befehle **Text einfügen** und **Kopierten Text übernehmen** aus dem Dropdown-Menü am rechten Ende der Client-Menüleiste verwenden.

Voraussetzungen

- Der View-Administrator muss entweder die Standardrichtlinie beibehalten, die es Benutzern ermöglicht, Text aus ihren Clientsystemen zu kopieren und in ihren virtuellen Remote-Desktop einzufügen, oder eine andere Richtlinie konfigurieren, die das Kopieren und Einfügen zulässt. Weitere Informationen finden Sie unter „Gruppenrichtlinieneinstellungen für HTML Access“, auf Seite 30.
- Sie müssen ein Chrome-Gerät oder einen Browser verwenden, das bzw. der WebSockets unterstützt. Browser, die diese Technologie nicht unterstützen, zeigen die Menübefehle **Text einfügen** und **Kopierten Text übernehmen** nicht an.

Vorgehensweise

- So kopieren Sie Text von Ihrem Clientsystem auf den Remote-Desktop:

  a Kopieren Sie den Text auf Ihrem Clientsystem.

  b Klicken Sie im Remote-Desktop zum Aufrufen der Menüleiste auf den Abwärtspfeil auf der Registerkarte oben in der Mitte des Fensters.

  c Wählen Sie aus dem Dropdown-Menü rechts in der Client-Menüleiste den Befehl **Text einfügen** aus.

  d Fügen Sie den Text in das daraufhin angezeigte Dialogfeld ein.

  e Setzen Sie Ihren Mauszeiger in der Anwendung an die Stelle, an der Sie den Text einfügen möchten.

  f Klicken Sie im Dialogfeld „Einfügen“ auf **Einfügen** und schließen Sie dann das Dialogfeld.

  Der Text wird in die Anwendung einfügt.

- So kopieren Sie Text aus Ihrem Remote-Desktop in Ihr Clientsystem:
  a Kopieren Sie den Text in Ihrem Remote-Desktop.
  b Klicken Sie im Remote-Desktop zum Aufrufen der Menüleiste auf den Abwärtspfeil auf der Registerkarte oben in der Mitte des Fensters.
  c Wählen Sie aus dem Dropdown-Menü rechts in der Client-Menüleiste den Befehl **Kopierten Text übernehmen** aus.

    Wenn der Befehl **Kopierten Text übernehmen** nicht im Dropdown-Menü angezeigt wird, kann es sein, dass Sie einen Browser verwenden, der WebSockets nicht unterstützt oder dass der View-Administrator Ihr Setup nicht derart konfiguriert hat, dass das Kopieren von Text aus dem Remote-Desktop in Ihr Clientsystem zulässig ist, wie in den Voraussetzungen für dieses Verfahren beschrieben wurde.
  d Wählen Sie im Dialogfeld Kopierten Text übernehmen den Text erneut aus und kopieren Sie ihn.

    Der Text wurde jetzt in die Zwischenablage kopiert.
  e Fügen Sie den Text auf Ihrem Clientsystem wie gewohnt ein.

Abmelden oder trennen

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

Selbst wenn Sie keinen Remote-Desktop geöffnet haben, können Sie sich vom Remote-Desktop-Betriebssystem abmelden. Die Verwendung dieser Option hat dieselbe Funktion, wie wenn Sie die Tastenkombination Strg+Alt+Entf drücken und anschließend auf **Abmelden** klicken.

Hinweis Die Eingabe der Windows-Tastenkombination Strg+Alt+Entf wird für Remote-Desktops nicht unterstützt. Wenn Sie die Entsprechung der Tastenkombination Strg+Alt+Entf verwenden möchten, wählen Sie **Strg+Alt+Entf senden** im Dropdown-Menü, das sich am rechten Ende der Client-Menüleiste befindet. Klicken Sie zum Aufrufen der Menüleiste auf den Abwärtspfeil auf der Registerkarte oben in der Mitte des Fensters.

Vorgehensweise

- Melden Sie sich vom View Server ab und trennen Sie ihn (ohne sich abzumelden) vom Desktop.

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Wählen Sie **Trennen** im Dropdown-Menü am rechten Ende der Client-Menüleiste und klicken Sie anschließend auf die Schaltfläche **Abmelden** oben rechts auf dem Bildschirm.
Auf dem Bildschirm zur Desktop-Auswahl	Klicken Sie in der rechten oberen Ecke des Bildschirms auf **Abmelden**.

- Melden Sie sich ab und trennen Sie die Verbindung zum Desktop, indem Sie **Abmelden** im Menü **Start** im Desktop-Betriebssystem auswählen.

- Trennen Sie die Verbindung, ohne sich abzumelden.

Option	Aktion
Den Client ebenfalls beenden	Schließen Sie die Browser-Registerkarte.
Einen anderen Remote-Desktop auf demselben Server auswählen	Wählen Sie im Dropdown-Menü am rechten Ende der Menüleiste **Verbindung trennen** und anschließend einen anderen Remote-Desktop aus.
Einen Remote-Desktop auf einem anderen Server auswählen	Wählen Sie **Verbindung trennen** im Dropdown-Menü und geben Sie anschließend die URL des anderen Servers in Ihrem Browser ein.

Hinweis Der View-Administrator kann Ihren Desktop so konfigurieren, dass beim Trennen der Verbindung die Abmeldung automatisch erfolgt. In diesem Fall werden alle geöffneten Programme auf Ihrem Desktop angehalten.

- Melden Sie sich vom Desktop-Betriebssystem ab, wenn kein Remote-Desktop geöffnet ist.

  Bei Verwendung dieser Option werden alle Dateien, die auf dem Remote-Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

  a Öffnen Sie den Bildschirm zur Desktop-Auswahl und klicken Sie auf dem Desktop-Symbol auf die Schaltfläche **Abmelden**.

  b Geben Sie bei Aufforderung die Anmeldeinformationen für den Zugriff auf den Remote-Desktop an.

Zurücksetzen eines Desktops

Eventuell muss der Desktop zurückgesetzt werden, wenn das Desktop-Betriebssystem nicht mehr reagiert. Beim Zurücksetzen wird der Desktop heruntergefahren und neu gestartet. 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.

Sie können den Desktop nur zurücksetzen, wenn Ihr View-Administrator diese Funktion aktiviert hat.

Vorgehensweise

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

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Auswählen **Verbindung trennen** im Dropdown-Menü am rechten Ende der Client-Menüleiste und klicken Sie anschließend auf **Zurücksetzen** unter dem Desktop-Symbol.
Im Bildschirm zur Desktop-Auswahl	Klicken Sie auf die Schaltfläche **Zurücksetzen** unter dem Desktop-Symbol.

Das Betriebssystem im Remote-Desktop wird neu gestartet. Der Client wird vom Desktop getrennt.

Weiter

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

Index

W

Z