Verwenden von VMware Horizon Client für Mac

VMware Horizon Client for Mac 4.5

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-002508-00

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

Verwenden von VMware Horizon Client für Mac

Verwenden von VMware Horizon Client für Mac bietet Informationen zur Installation und Verwendung der VMware Horizon® Client™-Software auf einem Mac, um eine Verbindung zu einem Remote-Desktop oder einer Remoteanwendung im Datencenter herzustellen.

Diese Informationen sind für Administratoren vorgesehen, die Horizon mit Mac-Clientgeräten bereitstellen müssen. Die Informationen wurden für erfahrene Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Datencenter-Vorgängen vertraut sind.

Konfiguration und Installation 1

Zur Einrichtung einer Horizon-Bereitstellung für Mac-Clients gehört die Festlegung bestimmter, speziell auf die Anforderungen des Client- und Serversystems abgestimmter Konfigurationseinstellungen für den Verbindungsserver sowie das Herunterladen und Installieren von Horizon Client für Mac von der VMware-Website.

Hinweis In Horizon 7 und höher wurde der View Administrator in Horizon Administrator umbenannt. Wenn in diesem Dokument von Horizon Administrator die Rede ist, dann bezieht sich dies immer sowohl auf View Administrator als auch auf Horizon Administrator.

Dieses Kapitel behandelt die folgenden Themen:

Systemanforderungen für Mac-Clients

Sowohl der Mac, auf dem Sie Horizon Client installieren, als auch die Peripheriegeräte müssen bestimmte Systemanforderungen erfüllen.

Mac-Modelle	Jeder 64-Bit-Mac, Intel-basiert
Arbeitsspeicher	Mindestens 2GB Arbeitsspeicher (RAM)
Betriebssysteme	■ Mac OS X Yosemite (10.10.x) ■ Mac OS X El Capitan (10.11) ■ Mac OS Sierra (10.12)
Smartcard-Authentifizierung	Siehe „Anforderungen für die Smartcard-Authentifizierung“, auf Seite 9.
Authentifizierung über Touch ID	Siehe „Anforderungen für Authentifizierung über Touch ID“, auf Seite 10.
Verbindungsserver, Sicherheitsserver und View Agent oder Horizon Agent	Aktuelle Wartungsversion von View 6.x und neuere Versionen. Wenn Clientsysteme von außerhalb der firmeneigenen Firewall eine Verbindung herstellen, empfiehlt VMware die Verwendung eines Sicherheitsservers oder der Unified Access Gateway-Appliance, damit Clientsysteme keine VPN-Verbindung benötigen.
Anzeigeprotokolle	■ PCoIP ■ RDP- ■ VMware Blast (erfordert Horizon Agent 7.0 oder höher)
Softwareanforderungen für RDP	Microsoft Remotedesktopverbindungs-Client für Mac, Version 2.0 bis 2.1.1. Dieser Client steht auf der Microsoft-Website zum Download zur Verfügung. **Hinweis** Horizon Client für Mac ist nicht mit Microsoft Remotedesktop 8.0 und höheren Versionen kompatibel.

Systemanforderungen für Echtzeit-Audio/Video

Echtzeit-Audio/Video arbeitet mit Standardwebcams, USB-Audio- und analogen Audiogeräten und kann mit standardmäßigen Konferenzanwendungen wie z. B. Skype, WebEx und Google Hangouts verwendet werden. Zur Unterstützung von Echtzeit-Audio/Video muss Ihre Horizon-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

Remote-Desktops	Auf den Desktops muss View Agent 5.2 oder höher oder Horizon Agent 7.0 oder höher installiert sein. Für View Agent 5.2-Desktops muss auf den Desktops auch der entsprechende Remote Experience Agent installiert sein. Wenn beispielsweise View Agent 5.2 installiert ist, müssen Sie auch den Remote Experience Agent aus dem View 5.2 Feature Pack 2 installieren. Informationen dazu finden Sie im Dokument *Installation und Administration von*

	View Feature Pack. Wenn Sie über View Agent 6.0 oder höher oder über Horizon Agent 7.0 oder höher verfügen, ist kein Feature Pack erforderlich. Um die Echtzeit-Audio-Video-Funktion mit veröffentlichten Desktops und Anwendungen zu verwenden, benötigen Sie Horizon Agent 7.0.2 oder höher.
Horizon Client-Computer oder Clientzugriffsgerät	■ Auf dem Clientcomputer müssen Treiber für Webcam und Audiogeräte installiert sein, und die Webcam oder das Audiogerät muss betriebsbereit sein. Zur Unterstützung von Echtzeit-Audio/Video ist es nicht erforderlich, die Gerätetreiber auf dem Desktop-Betriebssystem zu installieren, auf dem der Agent installiert ist.
Anzeigeprotokolle	■ PCoIP ■ VMware Blast (erfordert Horizon Agent 7.0 oder höher)

Anforderungen für die Smartcard-Authentifizierung

Clientsysteme, die eine Smartcard für die Benutzerauthentifizierung verwenden, müssen bestimmte Anforderungen erfüllen.

VMware hat außerdem die folgenden Smartcards getestet:

- U.S. Department of Defense Common Access Card (CAC)
- U.S. Federal Government Personal Identity Verification (PIV), auch als FIPS-201 bezeichnet

Für jedes Clientsystem, das zur Benutzerauthentifizierung eine Smartcard verwendet, gelten die folgenden Software- und Hardwareanforderungen:

- Horizon Client
- Ein kompatibler Smartcard-Leser
- Produktspezifische Anwendungstreiber

Sie müssen auf den Remote-Desktops oder dem Microsoft RDS-Host zusätzlich produktspezifische Anwendungstreiber installieren. Für Remote-Desktops unter Windows 7 installiert das Betriebssystem den entsprechenden Treiber, wenn Sie einen Smartcard-Leser anschließen und eine PIV-Karte einführen. Für Remote-Desktops unter Windows XP und Windows Vista können Sie den entsprechenden Treiber mithilfe von ActivIdentify ActivClient installieren.

Benutzer, die sich mithilfe von Smartcards authentifizieren, müssen über eine Smartcard verfügen, und jede Smartcard muss ein Benutzerzertifikat enthalten. Wenn Sie ein Zertifikat für eine leere PIV-Karte generieren, geben Sie im PIV Data Generator-Tool auf der Registerkarte **Crypto Provider** (Kryptografieanbieter) den Pfad zur Serververtrauensspeicher-Datei auf dem Verbindungsserver oder Sicherheitsserverhost ein. Informationen zum Erstellen einer Serververtrauensspeicher-Datei finden Sie im Dokument *Administration von View*.

Neben der Einhaltung dieser Anforderungen für Horizon Client-Systeme müssen andere Horizon-Komponenten zur Unterstützung von Smartcards bestimmte Anforderungen an die Konfiguration erfüllen:

- Informationen zur Konfiguration des Verbindungsservers für die Unterstützung von Smartcards finden Sie im Dokument *Administration von View*.

  Hinweis Smartcards werden nur von Servern und Desktops mit View 5.3.2 und höher unterstützt.

  Sie müssen alle gültigen Zertifizierungsstellenzertifikate für alle vertrauenswürdigen Benutzerzertifikate einer Serververtrauensspeicher-Datei auf dem Verbindungsserver- oder Sicherheitsserver-Host hinzufügen. Diese Zertifikate beinhalten Stammzertifikate und müssen auch Zwischenzertifikate enthalten, wenn das Smartcard-Zertifikat des Benutzers von einer Zwischenzertifizierungsstelle herausgegeben wurde.

- Informationen zu den Aufgaben, die Sie eventuell in Active Directory zur Implementierung der Smartcard-Authentifizierung durchführen müssen, finden Sie im Dokument *Administration von View*.

Aktivieren des Feldes „Benutzernamenhinweis“ in Horizon Client

In einigen Umgebungen können Smartcard-Benutzer ein einziges Smartcard-Zertifikat zur Authentifizierung bei mehreren Benutzerkonten verwenden. Benutzer geben bei der Smartcard-Anmeldung ihren Benutzernamen in das Feld **Benutzernamenhinweis** ein.

Damit das Feld **Benutzernamenhinweis** im Anmeldungsdialogfeld von Horizon Client angezeigt wird, müssen Sie die Funktion für Smartcard-Benutzernamenhinweise für die Verbindungsserver-Instanz in Horizon Administrator aktivieren. Die Funktion für Smartcard-Benutzernamenhinweise wird nur mit Servern und Agenten von Horizon 7 Version 7.0.2 und höher unterstützt. Informationen zur Aktivierung von Smartcard-Benutzernamenhinweisen erhalten Sie im Dokument *Administration von View*.

Wenn Ihre Umgebung für den sicheren externen Zugriff statt eines Sicherheitsservers eine Unified Access Gateway-Appliance verwendet, müssen Sie die Unified Access Gateway-Appliance zur Unterstützung von Smartcard-Benutzernamenhinweisen konfigurieren. Die Funktion für Smartcard-Benutzernamenhinweise wird nur mit Unified Access Gateway 2.7.2 und höher unterstützt. Informationen zur Aktivierung von Smartcard-Benutzernamenhinweisen in Unified Access Gateway erhalten Sie im Dokument *Bereitstellen und Konfigurieren von Unified Access Gateway*.

Hinweis Horizon Client unterstützt weiterhin Smartcard-Zertifikate für Einzelkonten, wenn die Funktion für Smartcard-Benutzernamenhinweise aktiviert ist.

Anforderungen für Authentifizierung über Touch ID

Um Touch ID für die Benutzerauthentifizierung in Horizon Client zu verwenden, müssen Sie bestimmte Anforderungen erfüllen.

Mac-Modelle	Jedes Mac-Modell, das Touch ID unterstützt, z. B. MacBook Pro.
Betriebssystemanforderungen	Fügen Sie der Touch ID- Einstellung mindestens einen Fingerabdruck hinzu.
Verbindungsserveranforderungen	■ Horizon 6 Version 6.2 oder eine höhere Version. ■ Aktivieren Sie die biometrische Authentifizierung im Verbindungsserver. Informationen hierzu finden Sie im *Administration von View*-Dokument. ■ Die Verbindungsserver-Instanz muss Horizon Client ein gültiges stammsigniertes Zertifikat vorweisen.
Horizon Client-Anforderungen	■ Aktivieren Sie für den Zertifikatsprüfungsmodus **Nie mit nicht vertrauenswürdigen Servern verbinden** oder **Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben**. Informationen zum Einstellen des Zertifikatsprüfungsmodus finden Sie unter „Festlegen des Zertifikatsprüfungsmodus für Horizon Client“, auf Seite 26. ■ Aktivieren Sie Touch ID, wenn Sie eine Verbindung zum Server herstellen. Nach der erfolgreichen Anmeldung werden Ihre Active Directory-Anmeldedaten sicher auf dem Mac-Clientsystem gespeichert. Die Touch ID-Option wird nur bei der ersten Anmeldung und dann nicht mehr angezeigt, wenn Touch ID aktiviert ist.

Sie können Touch ID mit der Smartcard-Authentifizierung und als Bestandteil der Zwei-Faktor-Authentifizierung mit der RSA SecurID- und RADIUS-Authentifizierung verwenden. Wenn Sie Touch ID mit der Smartcard-Authentifizierung verwenden, stellt Horizon Client eine Verbindung zum Server her, nachdem Sie Ihre PIN eingegeben haben. Der Touch ID-Anmeldebildschirm wird dann nicht angezeigt.

Anforderungen für die Verwendung der URL-Inhaltsumleitung

Mit der Funktion der URL-Inhaltsumleitung können URL-Inhalte vom Clientcomputer zu einem Remote-Desktop oder zu einer Remoteanwendung (Client-zu-Agent-Umleitung) oder von einem Remote-Desktop bzw. von einer Remoteanwendung zum Clientcomputer (Agent-zu-Client-Umleitung) umgeleitet werden.

So kann beispielsweise nach dem Klicken auf einen Link in der nativen Anwendung „Microsoft Word“ auf dem Client dieser Link in der Remoteanwendung „Internet Explorer“ geöffnet werden. Umgekehrt lässt sich nach dem Klicken auf einen Link in der Remoteanwendung „Internet Explorer“ der Link in einem nativen Browser auf dem Clientcomputer öffnen. Es kann eine beliebige Anzahl von Protokollen für die Umleitung konfiguriert werden, u. a. HTTP, Mailto und Callto.

Die Umleitung einer URL ist für Internet Explorer 9, 10 und 11 verfügbar.

Hinweis Die Funktion steht nicht für Links zur Verfügung, die in universellen Windows 10-Apps inklusive Microsoft Edge Browser angeklickt werden.

Für die Anwendung der Agent-zu-Client-Umleitung muss ein Horizon-Administrator die URL-Inhaltsumleitung bei der Installation von Horizon Agent aktivieren. Informationen dazu finden Sie in den Dokumenten *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Ein Horizon-Administrator muss durch Konfiguration von Einstellungen auch festlegen, wie Horizon Client URL-Inhalte vom Clientsystem zu einem Remote-Desktop oder zu einer Remoteanwendung oder wie Horizon Agent URL-Inhalte von einem Remote-Desktop oder einer Remoteanwendung zum Clientcomputer umleitet. Informationen zur Konfiguration finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Unterstützte Desktop-Betriebssysteme

Administratoren erstellen virtuelle Maschinen mit einem Gastbetriebssystem und installieren die Agent-Software auf diesem Gastbetriebssystem. Die Endbenutzer können sich an diesen virtuellen Maschinen von einem Client-Gerät aus anmelden.

Eine Liste unterstützter Windows-Gastbetriebssysteme finden Sie im Dokument *View-Installation*.

Einige Linux-Gastbetriebssysteme werden auch unterstützt, wenn Sie über View Agent 6.1.1 und höher oder Horizon Agent 7.0 und höher verfügen. Informationen zu den Systemanforderungen, zur Konfiguration virtueller Linux-Maschinen für eine Verwendung in Horizon sowie eine Liste unterstützter Funktionen erhalten Sie in *Einrichten von Horizon 6 for Linux-Desktops* und in *Einrichten von Horizon 7 for Linux-Desktops* .

Vorbereiten des Verbindungsservers für Horizon Client

Administratoren müssen bestimmte Aufgaben durchführen, um Endbenutzern die Verbindung zu Remote-Desktops und -Anwendungen zu ermöglichen.

Bevor Endbenutzer eine Verbindung mit dem Verbindungsserver oder einem Sicherheitsserver herstellen und auf einen Remote-Desktop oder eine Remoteanwendung zugreifen können, müssen bestimmte Pool- und Sicherheitseinstellungen konfiguriert werden:

- Wenn Sie Unified Access Gateway verwenden möchten, konfigurieren Sie den Verbindungsserver zur Zusammenarbeit mit Unified Access Gateway. Siehe das Dokument *Bereitstellen und Konfigurieren von Unified Access Gateway*. Unified Access Gateway-Appliances erfüllen dieselbe Rolle, die früher nur Sicherheitsserver übernommen hatten.

- Wenn Sie einen Sicherheitsserver verwenden, stellen Sie sicher, dass Sie die aktuellen Wartungsversionen für einen Verbindungsserver der Version 5.3.x und für einen Sicherheitsserver der Version 5.3.x oder höher verwenden. Weitere Informationen finden Sie im Dokument *View-Installation*.
- Wenn Sie eine sichere Tunnelverbindung für Clientgeräte verwenden möchten und die sichere Verbindung mit einem DNS-Hostnamen für den Verbindungsserver oder einen Sicherheitsserver konfiguriert ist, muss sichergestellt werden, dass das Clientgerät diesen DNS-Namen auflösen kann.

  Wechseln Sie zur Aktivierung oder Deaktivierung der sicheren Tunnelverbindung in Horizon Administrator zum Dialogfeld Horizon-Verbindungsserver-Einstellungen bearbeiten und aktivieren Sie das Kontrollkästchen **Sichere Tunnelverbindung zum Desktop verwenden**.
- Vergewissern Sie sich, dass ein Desktop- oder Anwendungspool erstellt wurde und das Benutzerkonto, das Sie verwenden möchten, über die Rechte zum Zugriff auf diesen Pool verfügt. Informationen dazu finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

  Wichtig Wenn Endbenutzer mit einem hochauflösenden Anzeigegerät arbeiten und die Clienteinstellung „Hochauflösungsmodus“ verwenden, während ihre Remote-Desktops im Vollbildmodus angezeigt werden, müssen Sie jedem Remote-Desktop mit Windows 7 oder höher ausreichend VRAM zuteilen. Die Menge an vRAM ist von der Anzahl der für Endbenutzer konfigurierten Monitore und der Displayauflösung abhängig. Zur Bestimmung der erforderlichen Menge an vRAM finden Sie Informationen im Dokument *Planung der View-Architektur*.
- Für die Verwendung der zweistufigen Authentifizierung für Horizon Client, z. B. der RSA SecurID- oder RADIUS-Authentifizierung, müssen Sie diese Funktion auf dem Verbindungsserver aktivieren. Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Administration von View*.
- Um Sicherheitsinformationen wie Server-URL-Informationen und das Dropdown-Menü **Domäne** in Horizon Client auszublenden, aktivieren Sie in Horizon Administrator die Einstellungen **Serverinformationen in der Kunden-Benutzeroberfläche ausblenden** und **Domänenliste in der Kunden-Benutzeroberfläche ausblenden**. Diese globalen Einstellungen sind in Horizon 7 Version 7.1 und höher verfügbar. Weitere Informationen zur Konfiguration globaler Einstellungen finden Sie im Dokument *Administration von View*.

  Um eine Authentifizierung bei ausgeblendetem Dropdown-Menü **Domäne** durchführen zu können, müssen Benutzer die Domäneninformationen durch Eingabe ihres Benutzernamens im Format ***Domäne**Benutzername*** oder ***Benutzername@Domäne*** in das Textfeld **Benutzername** zur Verfügung stellen.

  Wichtig Wenn Sie die Einstellungen **Serverinformationen in der Kunden-Benutzeroberfläche ausblenden** und **Domänenliste in der Kunden-Benutzeroberfläche ausblenden** aktivieren und die zweistufige Authentifizierung (RSA SecureID oder RADIUS) für die Verbindungsserver-Instanz auswählen, dürfen Sie nicht die Windows-Benutzernamenübereinstimmung erzwingen. Wenn die Windows-Benutzernamenübereinstimmung erzwungen wird, können Benutzer keine Domäneninformationen in das Textfeld „Benutzername“ eingeben und es ist keine Anmeldung mehr möglich. Weitere Informationen finden Sie in den Themen zur zweistufigen Authentifizierung im Dokument *Administration von View*.
- Um Endbenutzern das Speichern ihrer Kennwörter in Horizon Client zu ermöglichen, damit sie ihre Anmeldedaten nicht bei jeder Verbindungsherstellung mit einer Verbindungsserver-Instanz eingeben müssen, konfigurieren Sie Horizon LDAP für diese Funktion auf dem Verbindungsserver-Host.

  Wenn Horizon LDAP entsprechend konfiguriert ist, können Benutzer ihre Kennwörter speichern, wenn der Horizon Client-Zertifikatsprüfungsmodus auf **Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben** oder **Nie mit nicht vertrauenswürdigen Servern verbinden** eingestellt ist und wenn Horizon Client das vom Verbindungsserver übergebene Zertifikat vollständig überprüfen kann. Die Anweisungen dazu finden Sie im *Administration von View*-Dokument.

Installieren von Horizon Client auf einem Mac

Endbenutzer öffnen Horizon Client, um von einem physischen Mac-Computer eine Verbindung zu Remote-Desktops und -anwendungen herstellen zu können. Horizon Client wird auf Mac-Clientsystemen über eine Festplatten-Image-Datei installiert.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „Systemanforderungen für Mac-Clients“, auf Seite 8.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Wenn Sie beabsichtigen, das RDP-Anzeigeprotokoll zur Verbindung mit einem Remote-Desktop zu verwenden, müssen Sie vorab sicherstellen, dass auf dem Mac-Clientsystem der Microsoft Remote-Desktop-Verbindungs-Client für Mac (Version 2.0 oder höher) installiert ist.
- Stellen Sie sicher, dass Sie über die URL für eine Download-Seite verfügen, auf der sich das Horizon Client-Installationsprogramm befindet. Bei dieser URL kann es sich um die VMware Downloads-Seite unter http://www.vmware.com/go/viewclients oder um die URL für eine Verbindungsserver-Instanz handeln.

Vorgehensweise

1 Navigieren Sie auf Ihrem Mac zur URL zum Herunterladen der Horizon Client-Installationsdatei.

  Das Format des Dateinamens ist `VMware-Horizon-Client-`*`y.y.y-xxxxxx`*`.dmg`. Dabei steht *xxxxxx* für die Build-Nummer und *y.y.y* für die Versionsnummer.

2 Klicken Sie zum Öffnen doppelt auf die `.dmg`-Datei und anschließend auf **Akzeptieren**.

  Die Inhalte des Festplatten-Image werden in einem Horizon Client-Finder-Fenster angezeigt.

3 Ziehen Sie im Finder-Fenster das Symbol **VMware Horizon Client** zum Symbol **Anwendungsordner**.

  Wenn Sie nicht als Administrator angemeldet sind, werden Sie nach dem Administrator-Benutzernamen und -Kennwort gefragt.

Weiter

Starten Sie Horizon Client und stellen Sie sicher, dass Sie sich an einem Remote-Desktop bzw. an einer -Remoteanwendung anmelden können. Siehe „Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung“, auf Seite 27.

Upgrade von Horizon Client Online

Sie können Horizon Client so konfigurieren, dass bei jedem Start automatisch eine Prüfung auf aktuelle Updates vorgenommen wird und diese dann automatisch installiert werden. Sie haben auch die Möglichkeit, die Prüfung auf Updates und deren Installation manuell durchzuführen.

Ermittelt Horizon Client eine neue Version, können Sie diese herunterladen und installieren. Wenn Sie dies nicht durchführen, fordert Sie Horizon Client beim nächsten Start dazu auf, die neue Version zu installieren oder zu überspringen. Wenn Sie bei der manuellen Prüfung auf Updates eine neue Version überspringen, erfolgt dies auch bei der automatischen Update-Prüfung.

Vorgehensweise

- Um Horizon Client für eine Prüfung auf Updates und deren Installation bei jedem Neustart zu konfigurieren, wählen Sie **VMware Horizon Client > Einstellungen** aus und aktivieren Sie das Kontrollkästchen **Automatisch auf Updates prüfen**.

  Das Kontrollkästchen **Automatisch auf Updates prüfen** ist standardmäßig aktiviert.

- Um die Prüfung auf Updates und deren Installation manuell durchzuführen, wählen Sie **VMware Horizon Client > Auf Updates prüfen** aus.

Hinzufügen von Horizon Client zu Ihrem Dock

Sie können Horizon Client auf dieselbe Weise wie alle anderen Anwendungen zu Ihrem Dock hinzufügen.

Vorgehensweise

1. Wählen Sie im Ordner **AnwendungenVMware Horizon Client** aus.
2. Ziehen Sie das Symbol **VMware Horizon Client** zum Dock.
3. Wenn Sie das Dock-Symbol so konfigurieren möchten, dass Horizon Client beim Anmelden geöffnet oder das Symbol im Finder angezeigt wird, klicken Sie mit der rechten Maustaste auf das Dock, wählen Sie **Optionen** und dann den entsprechenden Befehl im Kontextmenü aus.

Wenn Sie Horizon Client beenden, verbleibt die Anwendungsverknüpfung im Dock.

Konfigurieren der Zertifikatsprüfungen für Endbenutzer

Administratoren können den Zertifikatüberprüfungsmodus so konfigurieren, dass beispielsweise immer die vollständige Überprüfung durchgeführt wird.

Die Zertifikatsprüfung wird für SSL-Verbindungen zwischen dem Verbindungsserver und Horizon Client durchgeführt. Die Administratoren können den Überprüfungsmodus so konfigurieren, dass eine der folgenden Strategien verwendet wird:

- Die Endbenutzer wählen selbst den Überprüfungsmodus. In der restlichen Liste werden die drei Überprüfungsmodi beschrieben.
- (Keine Überprüfung) Es werden keine Zertifikatsprüfungen durchgeführt.
- (Warnen) Die Endbenutzer werden gewarnt, wenn der Server ein selbstsigniertes Zertifikat vorlegt. Die Benutzer können dann selbst entscheiden, ob sie diesen Verbindungstyp zulassen.
- (Volle Sicherheit) Es wird eine vollständige Überprüfung durchgeführt. Die Verbindungen, für die diese Prüfung nicht erfolgreich verläuft, werden abgelehnt.

Einzelheiten zu den verschiedenen Arten der durchgeführten Überprüfungen finden Sie unter „Festlegen des Zertifikatsprüfungsmodus für Horizon Client“, auf Seite 26.

Sie können den Überprüfungsmodus so einstellen, dass er von den Endbenutzern nicht geändert werden kann. Legen Sie den Schlüssel „Security Mode“ in der Datei `/Library/Preferences/com.vmware.horizon.plist` auf den Mac-Clients auf einen der folgenden Werte fest:

- **`1`** implementiert `Never connect to untrusted servers`.
- **`2`** implementiert `Warn before connecting to untrusted servers`.
- **`3`** implementiert `Do not verify server identity certificates`.

Konfigurieren erweiterter TLS-/SSL-Optionen

Sie können die Sicherheitsprotokolle und kryptografischen Algorithmen auswählen, die zum Verschlüsseln der Kommunikation zwischen Horizon Client und Horizon Servern und zwischen Horizon Client und dem Agenten im Remote-Desktop verwendet werden.

Diese Sicherheitsoptionen werden auch verwendet, um den USB-Kanal (Kommunikation zwischen dem USB-Plug-In und dem Agenten auf dem Remote-Desktop) zu verschlüsseln.

TLSv1.0, TLSv1.1 und TLSv1.2 sind standardmäßig aktiviert. SSL v2.0 und 3.0 werden nicht unterstützt. Die standardmäßige Verschlüsselungszeichenfolge lautet „!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA +AESGCM:kECDH+AES:ECDH+AES:RSA+AES“.

Hinweis Wenn TLS v1.0 und RC4 deaktiviert sind, ist die USB-Umleitung nicht wirksam, wenn Benutzer mit Windows XP-Remote-Desktops verbunden sind. Bitte beachten Sie, dass bei Aktivierung dieser Funktion durch die Aktivierung von TLS v1.0 und RC4 Sicherheitsrisiken entstehen können.

Wenn Sie ein Sicherheitsprotokoll für Horizon Client konfigurieren, das auf dem Horizon Server, mit dem sich der Client verbindet, nicht aktiviert ist, tritt einen TLS-/SSL-Fehler auf und die Verbindung schlägt fehl.

Wichtig Mindestens eine der von Ihnen in Horizon Client aktivierten Protokollversionen muss auf dem Remote-Desktop aktiviert werden. Andernfalls können USB-Geräte nicht auf den Remote-Desktop umgeleitet werden.

Informationen zum Konfigurieren der Sicherheitsprotokolle, die von Verbindungsserver-Instanzen akzeptiert werden, finden Sie im Dokument *View-Sicherheit*.

Vorgehensweise

1 Wählen Sie **VMware Horizon Client > Einstellungen** aus der Menüleiste aus, klicken Sie auf **Sicherheit** und dann auf **Erweitert**.

2 Zum Aktivieren oder Deaktivieren eines Sicherheitsprotokolls aktivieren Sie das Kontrollkästchen neben dem Namen des Sicherheitsprotokolls.

3 Um die Schlüsselsteuerzeichenfolge zu ändern, ersetzen Sie die Standardzeichenfolge.

4 (Optional) Falls Sie die Standardeinstellungen wiederherstellen müssen, klicken Sie auf **Standardeinstellung wiederherstellen**.

5 Klicken Sie auf **Bestätigen**, um Ihre Änderungen zu speichern.

Die Änderungen werden wirksam, wenn Sie das nächste Mal eine Verbindung zum Server herstellen.

Konfigurieren der Erfassungswerte für Protokolldateien

Horizon Client generiert Protokolldateien im `~/Library/Logs/VMware Horizon Client`-Verzeichnis auf dem Mac-Client. Administratoren können auf einem Mac-Client die maximale Anzahl an Protokolldateien sowie die maximale Anzahl an Tagen konfigurieren, die Protokolldateien aufbewahrt werden sollen: Dazu werden in der Datei `/Library/Preferences/com.vmware.horizon.plist` Schlüssel festgelegt.

Tabelle 1-1. plist-Schlüssel für das Erfassen von Protokolldateien

Schlüssel	Beschreibung
MaxDebugLogs	Die maximale Anzahl von Protokolldateien. Der Maximalwert ist 100.
MaxDaysToKeepLogs	Die maximale Anzahl von Tagen, die Protokolldateien aufbewahrt werden sollen. Für diesen Wert gibt es keinen Grenzwert.

Dateien, die diesen Kriterien nicht entsprechen, werden gelöscht, wenn Sie Horizon Client starten.

Wenn der Schlüssel MaxDebugLogs bzw. MaxDaysToKeepLogs in der Datei `com.vmware.horizon.plist` nicht festgelegt ist, beträgt die Standardanzahl der Protokolldateien 5 und die Standardanzahl an Tagen zum Beibehalten der Protokolldateien 7.

Konfigurieren der VMware Blast-Optionen

Sie können die Optionen für die H.264-Decodierung und für die Netzwerkbedingung für Remote-Desktop- und -anwendungssitzungen konfigurieren, die das VMware Blast-Anzeigeprotokoll verwenden.

Die Option für die Netzwerkbedingung lässt sich nach der Anmeldung bei einem Server nicht mehr ändern. Die H.264-Decodierung können Sie vor und nach der Anmeldung bei einem Server konfigurieren.

Voraussetzungen

Diese Funktion erfordert Horizon Agent 7.0 oder höher.

Vorgehensweise

1 Wählen Sie **VMware Horizon Client > Einstellungen** aus der Menüleiste aus und klicken Sie auf **VMware Blast**.

2 Konfigurieren Sie die Optionen für das Decodieren und die Netzwerkbedingung.

Option	Aktion
H.264-Decodierung zulassen	Sie können diese Option vor oder nach der Herstellung einer Verbindung mit dem Verbindungsserver konfigurieren, um die H.264-Decodierung in Horizon Client aktivieren. Ist diese Option ausgewählt (Standardeinstellung), verwendet Horizon Client die H.264-Decodierung, wenn der Agent die H.264-Software- oder -Hardwarecodierung unterstützt. Unterstützt der Agent die H.264-Software- oder -Hardwarecodierung nicht, verwendet Horizon Client die JPG/PNG-Decodierung. Deaktivieren Sie diese Option, um die JPG/PNG-Decodierung zu verwenden.
Netzwerkstatus auswählen, um optimale Funktion zu gewährleisten	Sie können diese Option nur vor der Herstellung einer Verbindung mit dem Verbindungsserver konfigurieren. Wählen Sie eine der folgenden Optionen für die Netzwerkbedingung aus: ■ **Hervorragend** – Horizon Client verwendet nur das TCP-Netzwerk. Diese Option ist am besten für eine LAN-Umgebung geeignet. ■ **Normal (Standard)** – Horizon Client arbeitet im gemischten Modus. Im gemischten Modus verwendet Horizon Client das TCP-Netzwerk für die Herstellung einer Verbindung mit dem Server und das Protokoll Blast Extreme Adaptive Transport (BEAT), wenn der Agent und das Blast Security Gateway (bei Aktivierung) eine BEAT-Konnektivität unterstützen. Diese Option ist die Standardeinstellung. ■ **Schlecht** – Horizon Client verwendet nur das BEAT-Netzwerk, wenn BEAT Tunnel Server auf dem Server aktiviert ist. Ist dies nicht der Fall, wird in den gemischten Modus gewechselt. **Hinweis** In Horizon 7 Version 7.1 und früher wird BEAT Tunnel Server von den Instanzen des Verbindungsservers und des Sicherheitsservers nicht unterstützt. Unified Access Gateway 2.9 und höher unterstützt BEAT Tunnel Server. Blast Security Gateway für Verbindungsserver- und Sicherheitsserver-Instanzen unterstützt nicht das BEAT-Netzwerk.

3 Schließen Sie das Dialogfeld „Einstellungen“.

Änderungen für H.264 werden wirksam, wenn das nächste Mal ein Benutzer eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herstellt und das VMware Blast-Anzeigeprotokoll auswählt. Ihre Änderungen haben keinen Einfluss auf vorhandene VMware Blast-Sitzungen.

Durch VMware gesammelte Horizon Client -Daten

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

VMware sammelt die Daten auf den Clients zur Priorisierung der Hardware- und Softwarekompatibilität. Wenn sich ein Administrator Ihres Unternehmens 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 Horizon Client-Informationen werden erst an den Verbindungsserver und dann an VMware gesendet, zusammen mit den Daten der Verbindungsserver-Instanzen, Desktop-Pools und Remote-Desktops.

Auch wenn die Informationen bei der Übertragung an den Verbindungsserver verschlüsselt werden, werden die Informationen des Clientsystems unverschlüsselt in einem benutzerspezifischen Verzeichnis protokolliert. Die Protokolle enthalten jedoch keine personen- oder unternehmensbezogenen Informationen.

Der Administrator, der die Installation des Verbindungsservers durchführt, kann während der Ausführung des Installations-Assistenten für den Verbindungsserver entscheiden, ob am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit teilgenommen wird. Nach der Installation kann ein Administrator eine entsprechende Option in Horizon Administrator festlegen.

Tabelle 1-2. Von den Horizon Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Unternehmen, das die Horizon Client-Anwendung hergestellt hat	Nein	VMware
Produktname	Nein	VMware Horizon Client
Client-Produktversion	Nein	(Das Format lautet *x.x.x-yyyyyy*, wobei *x.x.x* für die Client-Versionsnummer und *yyyyyy* für die Build-Nummer steht.)
Client-Binärarchitektur	Nein	Beispiele hierfür sind: ■ i386 ■ x86_64 ■ arm
Client-Build-Name	Nein	Beispiele hierfür sind: ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
Host-Betriebssystem	Nein	Beispiele hierfür sind: ■ Windows 8.1 ■ Windows 7, Service Pack 1 für 64 Bit (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)

Tabelle 1-2. Von den Horizon Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit (Fortsetzung)

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Host-Betriebssystemkernel	Nein	Beispiele hierfür sind: ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ unbekannt (für Windows Store)
Host-Betriebssystemarchitektur	Nein	Beispiele hierfür sind: ■ x86_64 ■ i386 ■ armv71 ■ ARM
Hostsystem-Modell	Nein	Beispiele hierfür sind: ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Hostsystem-CPU	Nein	Beispiele hierfür sind: ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ unbekannt (für iPad)
Anzahl der Cores bzw. Kerne im Prozessor des Hostsystems	Nein	Beispiel: 4
MB Arbeitsspeicher auf dem Hostsystem	Nein	Beispiele hierfür sind: ■ 4096 ■ unbekannt (für Windows Store)
Anzahl der angeschlossenen USB-Geräte	Nein	2 (Die Umleitung von USB-Geräten wird nur für Linux-, Windows- und Mac-Clients unterstützt.)
Maximale Anzahl gleichzeitiger USB-Geräteverbindungen	Nein	2
Hersteller-ID des USB-Geräts	Nein	Beispiele hierfür sind: ■ Kingston ■ NEC ■ Nokia ■ Wacom
Produkt-ID des USB-Geräts	Nein	Beispiele hierfür sind: ■ DataTraveler ■ Gamepad ■ Speicherlaufwerk ■ Kabellose Maus
USB-Gerätefamilie	Nein	Beispiele hierfür sind: ■ Sicherheit ■ Eingabegeräte ■ Bildverarbeitung
Nutzungszähler für das USB-Gerät	Nein	(Gibt an, wie oft das Gerät gemeinsam genutzt wurde)

Verwenden von URIs zur Konfiguration von Horizon Client

2

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 Horizon Client, zur Verbindung mit einem Server oder zum Öffnen 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 Verbindungsservers
- Portnummer für den Verbindungsserver
- Active Directory-Benutzername
- Domänenname
- Desktop- oder Anwendungsanzeigename
- Fenstergröße
- Aktionen, darunter „Zurücksetzen“, „Abmelden“ und „Sitzung starten“
- Anzeigeprotokoll
- Optionen zur Umleitung von USB-Geräten

Verwenden Sie zur Generierung eines URI das URI-Schema `vmware-view` mit Horizon Client-spezifischen Pfad- und Abfragekomponenten.

Hinweis Sie können URIs zum Start von Horizon Client nur dann verwenden, wenn die Clientsoftware bereits auf den Clientcomputern installiert ist.

Dieses Kapitel behandelt die folgenden Themen:

Syntax für die Erstellung von vmware-view-URIs

Die Syntax umfasst das URI-Schema `vmware-view`, einen Pfadauszug zur Angabe des Desktops oder der Anwendung sowie optional eine Abfrage zur Angabe der Desktop- bzw. Anwendungsaktionen oder Konfigurationsoptionen.

URI-Spezifikation

Verwenden Sie zum Generieren von URIs für den Start von Horizon Client die folgende Syntax:

`vmware-view://[`*`authority-part`*`][/`*`path-part`*`][?`*`query-part`*`]`

Das einzig erforderliche Element ist das URI-Schema `vmware-view`. Für einige Versionen bestimmter Clientbetriebssysteme muss für den Namen des Schemas die Groß- und Kleinschreibung beachtet werden. Verwenden Sie daher `vmware-view`.

Wichtig In allen Abschnitten 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/.

authority-part

Gibt die Serveradresse und optional einen Benutzernamen, eine nicht standardmäßige Portnummer oder beides an. Unterstriche (_) werden in Servernamen nicht unterstützt. Die Servernamen müssen der DNS-Syntax entsprechen.

Verwenden Sie zur Angabe eines Benutzernamens die folgende Syntax:

`user1@`*`server-address`*

Sie können keine UPN-Adresse angeben, auch keine Domäne. Zur Angabe des Domänennamens können Sie den Abfrageteil `domainName` im URI verwenden.

Verwenden Sie zur Angabe einer Portnummer die folgende Syntax:

`server-address``:`*`port-number`*

path-part

Gibt den Desktop oder die Anwendung an. Verwenden Sie den Anzeigenamen des Desktops oder der Anwendung. Dieser Name wurde in Horizon Administrator beim Erstellen des Desktop- oder Anwendungspools angegeben. Weist der Anzeigename ein Leerzeichen auf, müssen Sie den Codierungsmechanismus **`%20`** verwenden, um das Leerzeichen darzustellen.

query-part

Gibt die zu verwendenden Konfigurationsoptionen oder die durchzuführenden Desktop- oder Anwendungsaktionen 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...`*`]`

Unterstützte Abfragen

In diesem Abschnitt werden die Abfragen aufgeführt, die für diesen Horizon Client-Typ 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*.

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. Wenn Sie die Aktion `browse` verwenden und einen Desktop oder eine Anwendung angeben, wird der Desktop oder die Anwendung in der Liste der verfügbaren Elemente hervorgehoben.
`start-session`	Öffnet 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 bzw. die angegebene Anwendung herunter und startet ihn bzw. sie neu. Nicht gespeicherte Daten gehen verloren. Das Zurücksetzen eines Remote-Desktops entspricht dem Betätigen der Reset-Taste auf einem physischen PC.
`restart`	Fährt den angegebenen Desktop herunter und startet ihn neu. Der Neustart eines Remote-Desktops entspricht dem Neustart des Windows-Betriebssystems. In der Regel wird der Benutzer dabei vom Betriebssystem aufgefordert, alle nicht gespeicherten Daten zu speichern, bevor der Neustart erfolgt.
`logoff`	Meldet den Benutzer vom Gastbetriebssystem auf dem Remote-Desktop ab. Wenn Sie eine Anwendung angeben, wird die Aktion ignoriert oder der Endbenutzer sieht die Warnmeldung „Ungültige URI-Aktion“.

args

Gibt Befehlszeilenargumente zum Hinzufügen beim Start einer Remoteanwendung an. Verwenden Sie die Syntax `args=`*Wert*, wobei *Wert* eine Zeichenfolge sein muss. Verwenden Sie für die folgenden Zeichen die Prozentkodierung:

- Für einen Doppelpunkt (:) verwenden Sie **`%3A`**.
- Für einen umgekehrten Schrägstrich (\) verwenden Sie **`%5C`**.
- Für ein Leerzeichen ( ) verwenden Sie **`%20`**.
- Für ein doppeltes Anführungszeichen (") verwenden Sie **`%22`**

Um beispielsweise den Dateinamen `"My new file.txt"` für die Notepad++-Anwendung anzugeben, verwenden Sie **`%22My%20new%20file.txt%22`**.

appProtocol

Gültige Werte für Remoteanwendungen sind **`PCOIP`** und **`BLAST`**. Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax **`appProtocol=PCOIP`**.

connectUSBOnInsert

Verbindet ein USB-Gerät beim Anschließen des Geräts mit dem im Vordergrund angezeigten virtuellen Desktop. Diese Abfrage wird bedingungslos festgelegt, wenn Sie die Abfrage `unattended` angeben. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf **`start-session`** setzen oder ohne die Abfrage `action` arbeiten. Gültige Werte sind **`true`** und **`false`**. Ein Beispiel für die Syntax ist etwa **`connectUSBOnInsert=true`**.

connectUSBOnStartup

Leitet alle aktuell mit dem Clientsystem verbundenen USB-Geräte an den Desktop um. Diese Abfrage wird bedingungslos festgelegt, wenn Sie die Abfrage `unattended` angeben. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf **`start-session`** setzen oder ohne die Abfrage `action` arbeiten. Gültige Werte sind **`true`** und **`false`**. Ein Beispiel für die Syntax ist etwa **`connectUSBOnStartup=true`**.

desktopLayout

Legt die Größe des Fensters für die Anzeige eines Remote-Desktops fest. Zur Verwendung dieser Abfrage müssen Sie die Abfrage `action` auf **`start-session`** setzen oder ohne die Abfrage `action` arbeiten.

Tabelle 2-2. Gültige Werte für desktopLayout-Abfrage

Wert	Beschreibung
`fullscreen`	Vollbild auf allen angeschlossenen externen Monitoren. Dieser Wert ist der Standardwert.
`windowLarge`	Großes Fenster.
`windowSmall`	Kleines Fenster.
*W*x*H*	Benutzerdefinierte Auflösung, bei der Sie die Breite mal Höhe in Pixel angeben. Ein Beispiel für die Syntax ist etwa **`desktopLayout=1280x800`**.

desktopProtocol

Gültige Werte für Remote-Desktops sind **`RDP`**, **`PCOIP`** und **`BLAST`**. Zur Angabe von PCoIP verwenden Sie beispielsweise die Syntax **`desktopProtocol=PCOIP`**.

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.

filePath

Gibt den Pfad zur Datei im lokalen System an, die Sie mit einer Remoteanwendung öffnen möchten. Sie können den kompletten oder den relativen Pfad verwenden, z. B. `~/Benutzername/test%20file.txt`. Verwenden Sie für die folgenden Zeichen die Prozentkodierung:

- Für einen Doppelpunkt (:) verwenden Sie **`%3A`**.
- Für einen umgekehrten Schrägstrich (\) verwenden Sie **`%5C`**.
- Für ein Leerzeichen ( ) verwenden Sie **`%20`**.

So haben Sie z. B. die Möglichkeit, für den Dateipfad `/Users/Benutzername/test file.txt` die Kodierung **`/User/Benutzername/test%20file.txt`** zu verwenden.

Beispiele für vmware-view-URIs

Sie können Hypertext-Links oder Schaltflächen mit dem URI-Schema `vmware-view` 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 öffnen.

URI-Syntaxbeispiele

Nach jedem URI-Beispiel finden Sie eine Beschreibung, was der Endbenutzer nach Anklicken des URI-Links sieht.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server 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.

Hinweis Die Standardvorgaben für das Anzeigeprotokoll und die Fenstergröße werden verwendet. Das Standardanzeigeprotokoll ist PCoIP. Die Standardfenstergröße ist Vollbild.

---

2 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

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

3 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Im Anmeldefeld wird das Textfeld **Benutzername** mit dem Namen **fred** gefüllt. Der Benutzer muss den Domänennamen und das Kennwort eingeben. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **Finance Desktop** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet. Die Verbindung nutzt das PCoIP-Anzeigeprotokoll.

4 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. In das Anmeldefeld muss der Benutzer den Benutzernamen, den Domänennamen und das Kennwort eingeben. Nach einer erfolgreichen Anmeldung wird vom Client eine Verbindung mit der Anwendung hergestellt, deren Anzeigename als **Berechnung** dargestellt wird. Die Verbindung nutzt das VMware Blast-Anzeigeprotokoll.

5 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Im Anmeldefeld wird das Textfeld **Benutzername** mit dem Namen **fred** und das Textfeld **Domäne** mit **mycompany** gefüllt. Der Benutzer muss das Kennwort eingeben. Nach einer erfolgreichen Anmeldung stellt der Client eine Verbindung zum Desktop her, dessen Anzeigename als **Finance Desktop** angezeigt wird. Der Benutzer ist dann beim Gast-Betriebssystem angemeldet.

6 `vmware-view://view.mycompany.com/`

Horizon Client startet und der Benutzer wird zur Anmeldeaufforderung für die Verbindung mit dem Server `view.mycompany.com` geleitet.

7 `vmware-view://view.mycompany.com/Primary%20Desktop?action=reset`

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

Hinweis Diese Aktion ist nur möglich, wenn ein Horizon-Administrator die Funktion zum Zurücksetzen eines Desktops für den Desktop aktiviert hat.

8 `vmware-view://view.mycompany.com/Primary%20Desktop?action=restart`

Horizon Client startet und stellt eine Verbindung zum `view.mycompany.com`-Server her. Das Anmeldefeld fordert den Benutzer zur Eingabe von Benutzernamen, Domänennamen und Kennwort auf. Nach einer erfolgreichen Anmeldung zeigt Horizon Client ein Dialogfeld an, in dem der Benutzer aufgefordert wird, den Neustart für „Primary Desktop“ zu bestätigen.

Hinweis Diese Aktion ist nur möglich, wenn ein Horizon-Administrator die Funktion zum Neustart eines Desktops für den Desktop aktiviert hat.

9 `vmware-view://`

Horizon Client startet und der Benutzer wird zu der Seite geleitet, auf der die Adresse eines Servers eingegeben werden kann.

10 `vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22`

Startet My Notepad++ auf dem Server 10.10.10.10 und übergibt das Argument `My new file.txt` an den Befehl zum Start der Anwendung. Der Dateiname ist in doppelte Anführungszeichen gesetzt, da er Leerzeichen enthält.

11 `vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt`

Startet Notepad++ 12 auf dem Server 10.10.10.10 und übergibt das Argument `a.text b.txt` an den Befehl zum Start der Anwendung. Da dieses Argument nicht in Anführungszeichen gesetzt ist, trennt ein Leerzeichen die Dateinamen und die beiden Dateien werden gesondert in Notepad++ geöffnet.

Hinweis Anwendungen können sich in der Umsetzung von Befehlszeilenargumenten unterscheiden. Wenn Sie beispielsweise das Argument `a.txt b.txt` an Wordpad übergeben, öffnet Wordpad nur eine Datei, `a.txt`.

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="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test
Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Verwalten der Remote-Desktop- und Anwendungsverbindungen

3

Mit Horizon Client können Sie eine Verbindung zu einem Verbindungsserver oder Sicherheitsserver herstellen, sich bei einem Remote-Desktop an- oder abmelden sowie Remoteanwendungen verwenden. Zur Fehlerbehebung können Sie auch Remote-Desktops und -Anwendungen zurücksetzen.

Je nachdem, wie der Administrator die Richtlinien für Remote-Desktops festlegt, können die Endbenutzer viele verschiedene Vorgänge auf ihren Desktops durchführen.

Dieses Kapitel behandelt die folgenden Themen:

- „Neuanordnen von Verknüpfungen“, auf Seite 44

Festlegen des Zertifikatsprüfungsmodus für Horizon Client

Administratoren und manchmal auch Endbenutzer können über eine Konfiguration festlegen, ob Client-Verbindungen abgelehnt werden sollen, wenn bei Zertifikatsüberprüfungen Fehler auftreten.

Die Zertifikatsprüfung wird für SSL-Verbindungen zwischen dem Verbindungsserver und Horizon Client durchgeführt. Die Zertifikatsüberprüfung umfasst die folgenden Checks:

- Ist das Zertifikat für einen anderen Zweck bestimmt als für die Überprüfung der Identität des Absenders und die Verschlüsselung der Serverkommunikation? Mit anderen Worten: Handelt es sich um den korrekten Zertifikattyp?
- Ist das Zertifikat abgelaufen oder erst zukünftig gültig? Mit anderen Worten: Ist das Zertifikat laut Computeruhr gültig?
- Stimmt der allgemeine Name auf dem Zertifikat mit dem Hostnamen des Servers überein, der es sendet? Zu einer fehlenden Übereinstimmung kann es kommen, wenn ein Lastenausgleich Horizon Client an einen Server mit einem Zertifikat umleitet, das nicht mit dem in Horizon Client eingegebenen Hostnamen übereinstimmt. Ein weiterer möglicher Grund für eine fehlende Übereinstimmung ist die Eingabe einer IP-Adresse statt eines Hostnamens im Client.
- Ist das Zertifikat von einer unbekannten oder nicht als vertrauenswürdig eingestuften Zertifizierungsstelle (CA) signiert worden? Selbstsignierte Zertifikate sind ein Typ der nicht als vertrauenswürdig eingestuften CA.

  Um diese Prüfung zu bestehen, muss sich das Stammzertifikat für die Zertifikatvertrauenskette im lokalen Zertifikatspeicher des Geräts befinden.

Hinweis Informationen zur Verteilung eines selbstsignierten Stammzertifikats und dessen Installation auf Mac-Clientsystemen finden Sie auf der Apple-Website im Dokument *Erweiterte Serververwaltung* für den von Ihnen verwendeten Mac-Server.

Neben der Bereitstellung eines Serverzertifikats sendet der Verbindungsserver ebenfalls einen Zertifikat-Fingerabdruck an Horizon Client. Ein Fingerabdruck ist ein Hash-Wert des öffentlichen Schlüssels des Zertifikats und wird als Abkürzung für den öffentlichen Schlüssel verwendet. Wenn der Verbindungsserver keinen Fingerabdruck sendet, wird eine Warnung ausgegeben, dass es sich um eine nicht vertrauenswürdige Verbindung handelt.

Wenn Ihr Administrator dies zulässt, können Sie den Zertifikatsprüfungsmodus festlegen. Wählen Sie **VMware Horizon Client > Einstellungen** aus der Menüleiste aus. Sie haben drei Auswahlmöglichkeiten:

- **Nie mit nicht vertrauenswürdigen Servern verbinden**. Sollte eine beliebige der Zertifikatsprüfungen fehlschlagen, kann der Client keine Verbindung mit dem Server herstellen. Die nicht bestandenen Prüfungen werden in einer Fehlermeldung aufgelistet.
- **Warnung vor Verbindung mit nicht vertrauenswürdigen Servern ausgeben**. Wenn eine Zertifikatsprüfung fehlschlägt, weil der Server ein selbstsigniertes Zertifikat verwendet, können Sie auf **Weiter** klicken, um die Warnung zu ignorieren. Bei selbstsignierten Zertifikaten muss der Zertifikatsname nicht mit dem Servernamen übereinstimmen, den Sie in Horizon Client eingegeben haben.
- **Server-Identitätszertifikate nicht überprüfen**. Mit dieser Einstellung werden Zertifikate nicht überprüft.

Ist der Zertifikatsprüfungsmodus auf **Warnen** gesetzt, können Sie immer noch eine Verbindung mit einer Verbindungsserver-Instanz herstellen, die ein selbstsigniertes Zertifikat verwendet.

Installiert ein Administrator später ein Sicherheitszertifikat von einer vertrauenswürdigen Zertifikatsautorität, sodass alle Zertifikatsüberprüfungen bei der Verbindungsherstellung bestanden werden, wird diese vertrauenswürdige Verbindung für diesen speziellen Server vorgemerkt. Legt dieser Server in Zukunft wieder ein selbstsigniertes Zertifikat vor, schlägt die Verbindung fehl. Nachdem ein bestimmter Server ein vollständig überprüfbares Zertifikat vorgelegt hat, muss er dies auch in Zukunft immer so handhaben.

Konfigurieren von Horizon Client für die Auswahl eines Smartcard-Zertifikats

Sie können Horizon Client durch Festlegen einer Einstellung so konfigurieren, dass ein lokales Zertifikat oder das Zertifikat auf einer Smartcard ausgewählt wird, wenn Sie sich bei einem Server authentifizieren. Wenn diese Einstellung nicht festgelegt ist (Standardwert), müssen Sie manuell ein Zertifikat auswählen.

Voraussetzungen

Damit diese Einstellung wirksam wird, muss die Smartcard-Authentifizierung auf dem Server konfiguriert sein und nur ein Zertifikat darf in Ihrem Clientsystem oder auf Ihrer Smartcard verfügbar sein. Wenn mehrere Zertifikate vorhanden sind, werden Sie von Horizon Client stets aufgefordert, ein Zertifikat auszuwählen, unabhängig von der tatsächlichen Einstellung.

Vorgehensweise

1 Wählen Sie vor der Verbindungsherstellung mit einem Server **VMware Horizon Client > Einstellungen** in der Menüleiste aus.

2 Klicken Sie im Dialogfeld „Einstellungen“ auf **Allgemein**.

3 Wählen Sie **Zertifikat automatisch auswählen** aus.

4 Schließen Sie das Dialogfeld „Einstellungen“.

Ihre Änderungen werden mit dem Schließen des Dialogfelds wirksam.

Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung

Nachdem Sie eine Verbindung mit einem Server hergestellt haben, können Sie die Remote-Desktops und -anwendungen öffnen, für deren Verwendung Sie autorisiert sind.

Bevor Endbenutzer auf Remote-Desktops und -anwendungen zugreifen, sollten Sie testen, ob Sie über das Clientsystem eine Verbindung mit einem Remote-Desktop oder einer Remoteanwendung herstellen können.

Voraussetzungen

- Besorgen Sie sich die Anmeldedaten, etwa einen Benutzernamen und das zugehörige Kennwort, den RSA SecurID-Benutzernamen und -Passcode, den RADIUS-Authentifizierungsbenutzernamen und -Passcode oder die Smartcard-PIN.
- Besorgen Sie sich den NETBIOS-Domänennamen für die Anmeldung. Beispielsweise ist es sinnvoller, `MeineFirma` als `MeineFirma.com` zu verwenden.
- Führen Sie die unter „Vorbereiten des Verbindungsservers für Horizon Client“, auf Seite 11 beschriebenen administrativen Aufgaben aus.

- Wenn Sie sich außerhalb des Firmennetzwerks befinden und für den Zugriff auf den Remote-Desktop oder auf die Remoteanwendung keinen Sicherheitsserver verwenden, müssen Sie sicherstellen, dass Ihr Clientgerät für die Verwendung einer VPN-Verbindung konfiguriert ist. Aktivieren Sie diese Verbindung.

  Wichtig In den meisten Fällen ist es empfehlenswert, einen Sicherheitsserver anstelle eines VPN zu verwenden.

- Stellen Sie sicher, dass Sie über den vollqualifizierten Domänennamen (FQDN) des Servers verfügen, der Zugriff auf den Remote-Desktop oder die Remoteanwendung gewährt. Unterstriche (_) werden in Servernamen nicht unterstützt. Wenn es sich nicht um Port 443 handelt, benötigen Sie auch die Portnummer.
- Wenn Sie beabsichtigen, das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem Remote-Desktop zu verwenden, müssen Sie sicherstellen, dass die Gruppenrichtlinieneinstellung AllowDirectRDP des Agenten aktiviert ist.
- Konfigurieren Sie den Zertifikatsprüfungsmodus für das SSL-Zertifikat des Servers. Siehe „Festlegen des Zertifikatsprüfungsmodus für Horizon Client“, auf Seite 26.
- Wenn Sie die Smartcard-Authentifizierung verwenden, konfigurieren Sie Horizon Client so, dass automatisch ein lokales Zertifikat oder das Zertifikat auf Ihrer Smartcard verwendet wird. Siehe „Konfigurieren von Horizon Client für die Auswahl eines Smartcard-Zertifikats“, auf Seite 27.
- Vergewissern Sie sich, sofern die Endbenutzer zur Verwendung des Microsoft RDP-Anzeigeprotokolls berechtigt sind, dass das Clientsystem über den Microsoft Remote-Desktop-Verbindungs-Client für Mac, Version 2.0 oder höher, verfügt. Dieser Client steht auf der Microsoft-Website zum Download zur Verfügung.
- Wenn Sie eine Authentifizierung über Touch ID planen, müssen Sie der Touch-Einstellung auf Ihrem Mac mindestens einen Fingerabdruck hinzufügen. Die Touch ID-Authentifizierung ist nur verfügbar, wenn die biometrische Authentifizierung auf dem Server aktiviert ist. Sämtliche Touch ID-Authentifizierungsanforderungen finden Sie unter „Anforderungen für Authentifizierung über Touch ID“, auf Seite 10.

Vorgehensweise

1 Sollte eine VPN-Verbindung erforderlich sein, müssen Sie das VPN aktivieren.

2 Doppelklicken Sie im **Anwendungen**-Ordner auf **VMware Horizon Client**.

3 Klicken Sie auf **Weiter**, um die USB- und Druckdienste für Remote-Desktops zu starten, oder klicken Sie auf **Abbrechen**, um Horizon Client ohne USB- und Druckdienste für Remote-Desktops zu verwenden.

   Wenn Sie auf **Weiter** klicken, müssen Sie Informationen zur Systemanmeldung eingeben. Wenn Sie auf **Abbrechen** klicken, können Sie die USB- und Druckdienste für Remote-Desktops später aktivieren.

   Hinweis Die Aufforderung zum Starten der USB- und Druckdienste für Remote-Desktops wird beim ersten Start von Horizon Client angezeigt. Sie erscheint nicht erneut, unabhängig davon, ob Sie auf **Abbrechen** oder **Weiter** klicken.

4 Stellen Sie eine Verbindung mit einem Server her.

Option	Beschreibung
Verbindung mit einem neuen Server herstellen	Klicken Sie auf das Symbol **Neuer Server** im Startfenster von Horizon Client. Geben Sie dann den Servernamen und die Portnummer (wenn erforderlich) ein und klicken Sie auf **Fortfahren**. Ein Beispiel für die Verwendung eines nicht standardmäßigen Ports ist view.company.com:1443.
Verbindung mit einem vorhandenen Server herstellen	Doppelklicken Sie auf die Serververknüpfung im Horizon Client-Startfenster.

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

6 Wenn Sie zur Eingabe von Benutzername und Kennwort aufgefordert werden, geben Sie die Active Directory-Anmeldedaten ein.

   a Geben Sie den Benutzernamen und das Kennwort eines Benutzers ein, der berechtigt ist, mindestens einen Desktop- oder Anwendungspool zu benutzen.

   b Wählen Sie eine Domäne aus.

   Wenn das Dropdown-Menü **Domäne** ausgeblendet ist, müssen Sie den Benutzernamen in der Form ***Benutzername@Domäne*** oder ***Domäne\Benutzername*** eingeben.

   c (Optional) Aktivieren Sie das Kontrollkästchen **Dieses Kennwort speichern**, sofern der Administrator diese Funktion aktiviert hat und das Serverzertifikat vollständig überprüft werden kann.

   d (Optional) Aktivieren Sie das Kontrollkästchen **Touch ID aktivieren**, um die Touch ID-Authentifizierung zu aktivieren.

   Wenn die Touch ID aktiviert ist und Sie sich zum ersten Mal anmelden, werden Ihre Active Directory-Anmeldedaten sicher auf Ihrem Mac für die zukünftige Verwendung gespeichert.

   e Klicken Sie auf **Anmelden**.

   Es wird eventuell eine Meldung eingeblendet, die Sie bestätigen müssen, bevor das Anmeldedialogfeld angezeigt wird.

7 Wenn die Sicherheitsanzeige des Desktops rot angezeigt und eine Warnung ausgegeben wird, reagieren Sie auf die Eingabeaufforderung.

Normalerweise bedeutet diese Warnung, dass der Verbindungsserver keinen Zertifikat-Fingerabdruck an den Client gesendet hat. Ein Fingerabdruck ist ein Hash-Wert des öffentlichen Schlüssels des Zertifikats und wird als Abkürzung für den öffentlichen Schlüssel verwendet.

8 Wenn Sie zur Touch ID-Authentifizierung aufgefordert werden, setzen Sie Ihren Finger auf den Touch ID-Sensor.

9 (Optional) Wenn mehrere Anzeigeprotokolle für einen Remote-Desktop oder eine Remoteanwendung konfiguriert sind, müssen Sie das Protokoll auswählen, das verwendet werden soll.

VMware Blast stellt eine verbesserte Akkulaufzeit zur Verfügung und bietet das beste Protokoll für Benutzer von High-End-3D- und mobilen Geräten. Das Standardanzeigeprotokoll ist **PCoIP**.

Option	Beschreibung
Anzeigeprotokoll für einen Remote-Desktop auswählen	Wählen Sie den Namen des Remote-Desktops aus, halten Sie die Steuerungstaste gedrückt und klicken Sie und wählen Sie das Anzeigeprotokoll aus dem Kontextmenü aus. Alternativ haben Sie die Möglichkeit, **Einstellungen** aus dem Kontextmenü aufzurufen und das Anzeigeprotokoll aus dem Dropdown-Menü **Verbinden über** im Dialogfeld „Einstellungen“ auszuwählen.
Anzeigeprotokoll für eine Remoteanwendung auswählen	Wählen Sie den Namen der Remoteanwendung aus, halten Sie die Steuerungstaste gedrückt und klicken Sie und rufen Sie **Einstellungen** aus dem Kontextmenü auf. Wählen Sie das Anzeigeprotokoll aus dem Dropdown-Menü **Bevorzugtes Protokoll** im Dialogfeld „Einstellungen“ aus.

10 Doppelklicken Sie auf einen Remote-Desktop oder eine Remoteanwendung, um die Verbindung herzustellen.

Wenn Sie eine Verbindung mit einem sitzungsbasierten Remote-Desktop auf einem Microsoft RDS-Host herstellen und für den Desktop bereits die Verwendung eines anderen Anzeigeprotokolls festgelegt ist, kann die Verbindung nicht sofort hergestellt werden. Sie werden aufgefordert, entweder das festgelegte Protokoll zu verwenden oder sich vom Remote-Betriebssystem abzumelden, damit eine Verbindung unter Verwendung des von Ihnen ausgewählten Protokolls hergestellt werden kann.

Hinweis Wenn Sie zur Verwendung nur eines Remote-Desktops auf dem Server berechtigt sind, stellt Horizon Client automatisch eine Verbindung mit diesem Desktop her.

Nachdem die Verbindung hergestellt wurde, wird das Clientfenster angezeigt.

Wenn ein Administrator die Funktion der Clientlaufwerksumleitung aktiviert hat, wird eventuell das Dialogfeld „Freigabe“ eingeblendet. In diesem Dialogfeld können Sie den Zugriff auf Dateien Ihres lokalen Systems freigeben oder unterbinden. Weitere Informationen finden Sie unter „Freigegebener Zugriff auf lokale Ordner und Laufwerke“, auf Seite 31.

Wenn ein Administrator die Funktion der URL-Inhaltsumleitung auf dem Server konfiguriert hat, müssen Sie eventuell auf bestimmte Eingabeaufforderungen reagieren. Weitere Informationen finden Sie unter „Anklicken von URL-Links zum Öffnen außerhalb von Horizon Client“, auf Seite 33.

Wenn Horizon Client keine Verbindung mit dem Remote-Desktop oder der Remoteanwendung herstellen kann, führen Sie die folgenden Aufgaben aus:

- Legen Sie fest, ob der Verbindungsserver dahingehend konfiguriert werden soll, SSL nicht zu verwenden. Horizon Client erfordert SSL-Verbindungen. Prüfen Sie, ob die globale Einstellung in Horizon Administrator für das Kontrollkästchen **SSL für Client-Verbindungen verwenden** deaktiviert ist. Ist dies der Fall, müssen Sie entweder das Kontrollkästchen markieren, sodass SSL verwendet wird, oder Ihre Umgebung so einrichten, dass die Clients eine Verbindung zu einem HTTPS-fähigen Lastenausgleich oder einem anderen Zwischengerät herstellen können, das zur Herstellung einer HTTP-Verbindung zum Verbindungsserver konfiguriert ist.
- Stellen Sie eine ordnungsgemäße Funktionsweise des Sicherheitszertifikats für den Verbindungsserver sicher. Wenn dies nicht zutrifft, wird in Horizon Administrator möglicherweise angezeigt, dass View Agent oder Horizon Agent in Desktops nicht erreichbar ist.
- Stellen Sie sicher, dass die für die Verbindungsserver-Instanz festgelegten Kennzeichen Verbindungen von diesem Benutzer erlauben. Siehe das Dokument *Administration von View*.

- Stellen Sie sicher, dass der Benutzer zum Zugriff auf den Desktop oder die Anwendung berechtigt ist. Weitere Erläuterungen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Wenn Sie das RDP-Anzeigeprotokoll zur Verbindungsherstellung mit einem Remote-Desktop verwenden, müssen Sie bestätigen, dass der Clientcomputer Remote-Desktop-Verbindungen zulässt.

Freigegebener Zugriff auf lokale Ordner und Laufwerke

Sie können Horizon Client zur Freigabe von Ordnern und Laufwerken auf Ihren lokalen Systemen für Remote-Desktops und Remoteanwendungen konfigurieren. Zu Laufwerken können auch zugeordnete Laufwerke und USB-Speichergeräte gehören. Diese Funktion wird als Clientlaufwerksumleitung bezeichnet.

In einem Windows-Remote-Desktop werden freigegebene Ordner und Laufwerke im Abschnitt **Geräte und Laufwerke** im Ordner **Dieser PC** oder im Abschnitt **Andere** im Ordner **Computer** je nach verwendetem Windows-Betriebssystem angezeigt. In einer Remoteanwendung (z. B. Editor) können Sie zu einer Datei in einem freigegeben Ordner oder auf einem freigegebenem Laufwerk wechseln und diese öffnen. Die für die Freigabe ausgewählten Ordner und Laufwerke erscheinen im Dateisystem als Netzwerklaufwerke mit dem Namensformat ***Name*** **unter** ***COMPUTERNAME***.

Um die Einstellungen für die Clientlaufwerksumleitung zu konfigurieren, müssen Sie nicht mit einem Remote-Desktop oder mit einer Remoteanwendung verbunden sein. Diese Einstellungen gelten für Ihre gesamten Remote-Desktops und Remoteanwendungen. Das bedeutet, dass lokale Clientordner nicht nur für einen Remote-Desktop oder eine Remoteanwendung freigegeben werden können. Die konfigurierte Freigabe gilt immer für alle Remote-Desktops oder Remoteanwendungen.

Sie können die Funktion zum Öffnen von lokalen Dateien mit Remoteanwendungen direkt aus Ihrem lokalen Dateisystem aktivieren. Wenn Sie eine lokale Datei auswählen, die Steuerungstaste gedrückt halten und klicken, sind im Menü **Öffnen mit** die verfügbaren Remoteanwendungen aufgeführt. Sie können eine lokale Datei auch durch Ziehen und Ablegen im Fenster der Remoteanwendung oder im Dock-Symbol öffnen. Wenn eine Remoteanwendung als Standardanwendung für Dateien mit einer bestimmten Dateierweiterung festgelegt wurde, werden alle Dateien Ihres lokalen Dateisystems mit dieser Dateierweiterung mit dem Server, bei dem Sie angemeldet sind, registriert. Sie können auch die Möglichkeit zur Ausführung von Remoteanwendungen aus dem Ordner „Anwendungen“ aktivieren.

Hinweis Es lassen sich mit einer Remoteanwendung keine Dateien öffnen, deren Namen Zeichen enthalten, die im Windows-System nicht gültig sind. Beispielsweise können Sie mit dem Editor keine Datei mit dem Namen `test2<.txt` öffnen.

Die Konfiguration des Browsers auf dem Clientsystem für die Verwendung eines Proxy-Servers kann die Leistung der Clientlaufwerksumleitung reduzieren, wenn für die Verbindungsserver-Instanz der sichere Tunnel aktiviert ist. Für eine optimale Leistung der Clientlaufwerksumleitung konfigurieren Sie den Browser so, dass kein Proxy-Server verwendet wird oder dass die LAN-Einstellungen automatisch ermittelt werden.

Voraussetzungen

Um Ordner und Laufwerke für einen Remote-Desktop oder eine Remoteanwendung freizugeben, müssen Sie die Funktion der Clientlaufwerksumleitung aktivieren. Diese Aufgabe beinhaltet die Installation von View Agent 6.1.1 oder höher oder von Horizon Agent 7.0 oder höher und die Aktivierung der Agentenoption **Clientlaufwerksumleitung**. Außerdem besteht die Möglichkeit, Richtlinien zur Steuerung des Verhaltens der Laufwerksumleitung festzulegen. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Vorgehensweise

1 Öffnen Sie das Dialogfeld „Einstellungen“ mit dem Bereich „Freigabe“.

Option	Beschreibung
Im Fenster für die Desktop- und Anwendungsauswahl	Wählen Sie **VMware Horizon Client > Einstellungen** aus und klicken Sie auf **Freigabe**.
Im bei der Verbindung mit einem Desktop oder mit einer Anwendung eingeblendeten Dialogfeld „Freigabe“	Klicken Sie im Dialogfeld auf den Link **Einstellungen > Freigabe**.
Aus einem Desktop-Betriebssystem heraus	Wählen Sie **VMware Horizon Client > Einstellungen** aus der Menüleiste aus und klicken Sie auf **Freigabe**.

2 Konfigurieren Sie die Einstellungen für die Clientlaufwerksumleitung.

Option	Aktion
Freigeben eines bestimmten Ordners oder Laufwerks für Remote-Desktops und Remoteanwendungen	Klicken Sie auf die Schaltfläche mit dem Pluszeichen (+), wechseln Sie zum Ordner oder Laufwerk, der/das freigegeben werden soll, und klicken Sie auf **OK**. **Hinweis** Sie können keinen Ordner auf einem USB-Gerät freigeben, das bereits mit einem Remote-Desktop oder mit einer Remoteanwendung über die USB-Umleitungsfunktion verbunden ist.
Freigabe für einen bestimmten Ordner oder ein bestimmtes Laufwerk aufheben	Wählen Sie den Ordner oder das Laufwerk in der Ordnerliste aus und klicken Sie auf die Schaltfläche mit dem Minuszeichen (-).
Erlauben Sie Remote-Desktops und Remoteanwendungen den Zugriff auf Dateien in Ihrem Benutzerordner	Aktivieren Sie das Kontrollkästchen **Zugriff auf *Benutzerordner* erlauben**.
Geben Sie die USB-Speichergeräte für Remote-Desktops und -anwendungen frei.	Aktivieren Sie das Kontrollkästchen **Zugriff auf Wechselmedien erlauben**. Die Funktion der Clientlaufwerksumleitung gibt alle USB-Speichergeräte in Ihrem Clientsystem und alle über FireWire und Thunderbolt verbundenen externe Laufwerke frei. Sie müssen kein bestimmtes Laufwerk für die Freigabe auswählen. **Hinweis** USB-Speichergeräte, die bereits über die Funktion zur USB-Umleitung mit einem Remote-Desktop oder mit einer Remoteanwendung verbunden sind, werden nicht freigegeben. Wenn dieses Kontrollkästchen deaktiviert ist, können Sie mit der Funktion zur USB-Umleitung USB-Speichergeräte mit Remote-Desktops und Remoteanwendungen verbinden.
Dialogfeld „Freigabe“ beim Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung nicht anzeigen	Aktivieren Sie das Kontrollkästchen**Dialogfeld bei der Verbindung mit einem Desktop oder einer Anwendung nicht anzeigen**. Wenn dieses Kontrollkästchen deaktiviert ist, erscheint das Dialogfeld „Freigabe“, wenn Sie nach der Verbindung mit einem Server zum ersten Mal eine Verbindung mit einem Desktop oder einer Anwendung herstellen. Melden Sie sich beispielsweise bei einem Server an und stellen Sie eine Verbindung zu einem Desktop her, wird das Dialogfeld „Freigabe“ eingeblendet. Wenn Sie dann eine Verbindung zu einem anderen Desktop oder zu einer anderen Anwendung herstellen, wird das Dialogfeld nicht mehr angezeigt. Um das Dialogfeld wieder einzublenden, müssen Sie die Verbindung zum Server trennen und sich erneut anmelden.

3 Konfigurieren Sie Einstellungen für Remoteanwendungen.

   a Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf das Zahnradsymbol **Einstellungen** und wählen Sie **Anwendungen** im linken Bereich aus.

   b Wählen Sie **Lokale Dateien in gehosteten Anwendungen öffnen** aus, um die Möglichkeit des Öffnens lokaler Dateien mit Remoteanwendungen aus dem lokalen Dateisystem zu aktivieren.

   c Wählen Sie **Gehostete Anwendungen von Ihrem lokalen Anwendungsordner ausführen** aus, um die Möglichkeit der Ausführung von Remoteanwendungen aus dem Anwendungsordner auf Ihrem Clientsystem zu aktivieren.

Weiter

Stellen Sie sicher, dass die freigegebenen Ordner im Remote-Desktop oder in der Remoteanwendung erscheinen.

- Öffnen Sie in einem Windows-Remote-Desktop den Datei-Explorer und wechseln Sie dann zum Abschnitt **Geräte und Laufwerke** im Ordner **Dieser PC** oder öffnen Sie Windows Explorer und wechseln Sie dann zum Abschnitt **Andere** im Ordner **Computer**.
- Wählen Sie gegebenenfalls in einer Remoteanwendung **Datei > Öffnen** oder **Datei > Speichern unter** aus und wechseln Sie zum Ordner oder Laufwerk, das im Dateisystem als das Netzwerklaufwerk mit dem Namensformat ***Ordnername* auf *COMPUTERNAME*** erscheint.

Anklicken von URL-Links zum Öffnen außerhalb von Horizon Client

Ein Administrator kann URL-Links so konfigurieren, dass diese durch Klicken in einem Remote-Desktop oder in einer Remoteanwendung im Standardbrowser auf Ihrem Clientsystem geöffnet werden. Ein Link kann zu einer Webseite, einer Telefonnummer, einer E-Mail oder zu einer anderen Art von Links führen. Diese Funktion wird als URL-Inhaltsumleitung bezeichnet.

Ein Administrator kann außerdem URL-Links konfigurieren, die, wenn Sie auf Ihrem Clientsystem in einem Browser oder einer Anwendung darauf klicken, in einem Remotedesktop oder einer Remoteanwendung geöffnet werden. Falls Horizon Client in diesem Szenario noch nicht geöffnet ist, erfolgt der Start und Sie werden zur Anmeldung aufgefordert.

Ein Administrator kann die URL-Inhaltsumleitung aus Sicherheitsgründen einrichten. Wenn Sie sich z. B. in Ihrem Unternehmensnetzwerk befinden und auf einen Link klicken, der auf eine URL verweist, die sich außerhalb des Netzwerks befindet, ist es sicherer, wenn der Link in einer Remoteanwendung geöffnet wird. Ein Administrator kann konfigurieren, welche Anwendung den Link öffnet.

Beim ersten Start von Horizon Client und beim ersten Herstellen einer Verbindung mit einem Server, auf dem die Funktion der URL-Inhaltsumleitung konfiguriert ist, werden Sie, wenn Sie auf einen Link für die Umleitung klicken, von Horizon Client aufgefordert, die Anwendung VMware Horizon URL Filter zu öffnen. Klicken Sie auf **Öffnen**, um die URL-Inhaltsumleitung zu aktivieren.

Je nachdem, wie die Funktion der URL-Inhaltsumleitung konfiguriert ist, wird von Horizon Client eventuell eine Warnmeldung eingeblendet, die Sie zur Änderung Ihres Standardwebbrowsers in „VMware Horizon URL Filter“ auffordert. Klicken Sie in diesem Fall auf die Schaltfläche **„VMware Horizon URL Filter“ verwenden**, um „VMware Horizon URL Filter“ als Standardbrowser zu verwenden. Diese Eingabeaufforderung wird dann nicht mehr angezeigt, bis Sie Ihren Standardbrowser nach dem Anklicken von **„VMware Horizon URL Filter“ verwenden** wieder ändern.

Horizon Client blendet eventuell auch eine Warnmeldung ein, die Sie zur Auswahl einer Anwendung auffordert, wenn Sie auf eine URL klicken. In diesem Fall klicken Sie auf **Anwendung auswählen**, um nach einer Anwendung auf Ihrem Clientsystem zu suchen, oder auf **Im App Store suchen**, um eine neue Anwendung zu suchen und gegebenenfalls zu installieren. Wenn Sie auf **Abbrechen** klicken, wird die URL nicht geöffnet.

Jedes Unternehmen konfiguriert seine eigenen URL-Umleitungsrichtlinien. Bei Fragen, wie die Funktion der URL-Inhaltsumleitung in Ihrer Firma gehandhabt wird, wenden Sie sich an Ihren Systemadministrator.

Öffnen eines zuletzt verwendeten Remote-Desktops oder einer zuletzt verwendeten Remoteanwendung

Sie können zuletzt verwendete Remote-Desktops und -anwendungen in Horizon Client öffnen.

Zuletzt verwendete Remote-Desktops und Remoteanwendungen werden in der Reihenfolge dargestellt, in der sie geöffnet wurden. Wenn Sie beim Öffnen eines zuletzt verwendeten Desktop oder einer zuletzt verwendeten Anwendung noch nicht mit dem Server verbunden sind, wird der Serveranmeldebildschirm eingeblendet, in den Sie Ihre Anmeldedaten eingeben müssen.

Voraussetzungen

Zur Verwendung dieser Funktion muss zuvor ein Remote-Desktop oder eine Remoteanwendung geöffnet worden sein. Wenn Sie einen zuletzt verwendeten Desktop oder eine zuletzt verwendete Anwendung aus dem Dock öffnen möchten, muss sich VMware Horizon Client im Dock befinden. Siehe „Hinzufügen von Horizon Client zu Ihrem Dock“, auf Seite 14.

Vorgehensweise

- Um einen Remote-Desktop oder eine Remoteanwendung aus dem Dock zu öffnen, klicken Sie bei gedrückter Ctrl-Taste auf **VMware Horizon Client** und wählen Sie den Remote-Desktop oder die Remoteanwendung aus dem Menü aus.
- Um einen Remote-Desktop oder eine Remoteanwendung aus dem Menü **Datei** zu öffnen, starten Sie Horizon Client, wählen Sie **Datei > Letzte öffnen** und dann den Remote-Desktop oder die Remoteanwendung aus.

Herstellen einer Verbindung mit einem Server beim Start von Horizon Client

Die Einstellung **Beim Start immer verbinden** wird standardmäßig für den ersten Server, zu dem Sie mit Horizon Client eine Verbindung herstellen, aktiviert. Wenn diese Einstellung für einen Server aktiviert ist, stellt Horizon Client stets eine Verbindung mit diesem Server her, wenn Sie Horizon Client starten.

Um dieses Verhalten für einen Server zu deaktivieren, wählen Sie im Horizon Client-Startfenster die Serververknüpfung aus, halten Sie auf der Apple-Tastatur die Ctrl-Taste gedrückt und deaktivieren Sie die Einstellung **Beim Start immer verbinden**. Wenn im Horizon Client-Startfenster weitere Serververknüpfungen vorhanden sind, können Sie die Einstellung **Beim Start immer verbinden** für einen anderen Server aktivieren.

Die Einstellung **Beim Start immer verbinden** kann jeweils immer nur für einen Server aktiviert werden.

Konfigurieren von Horizon Client für das Löschen von Benutzername und -domäne

Standardmäßig speichert Horizon Client den Benutzernamen und die Domäne bei der Anmeldung bei einem Server zum Herstellen einer Verbindung mit einem Remote-Desktop oder einer Remoteanwendung. Zur Erhöhung der Sicherheit können Sie Horizon Client so konfigurieren, dass dabei Benutzername und Domäne des Servers nicht gespeichert werden.

Vorgehensweise

1. Wählen Sie **VMware Horizon Client > Einstellungen** aus der Menüleiste aus.
2. Klicken Sie im Dialogfeld „Einstellungen“ auf **Allgemein**.
3. Deaktivieren Sie **Benutzer- und Domänenname speichern**.

4 Schließen Sie das Dialogfeld „Einstellungen“.

Ihre Änderungen werden mit dem Schließen des Dialogfelds wirksam.

Ausblenden des VMware Horizon Client -Fensters

Sie können das VMware Horizon Client-Fenster nach dem Öffnen eines Remote-Desktops oder einer Remoteanwendung ausblenden.

Außerdem können Sie mit einer speziellen Voreinstellung festlegen, dass das VMware Horizon Client-Fenster nach dem Öffnen eines Remote-Desktops oder einer Remoteanwendung immer ausgeblendet wird.

Vorgehensweise

- Zum Ausblenden des VMware Horizon Client-Fensters nach dem Öffnen eines Remote-Desktops oder einer Remoteanwendung klicken Sie in der Ecke des VMware Horizon Client-Fensters auf die Schaltfläche **Schließen**.

  Das Symbol VMware Horizon Client verbleibt im Dock.

- Um die Voreinstellung so festzulegen, dass das VMware Horizon Client-Fenster nach dem Öffnen eines Remote-Desktops oder einer Remoteanwendung immer ausgeblendet wird, führen Sie diese Schritte aus, bevor Sie die Verbindung zu einem Server herstellen.

  a Wählen Sie **VMware Horizon Client > Einstellungen** in der Menüleiste aus und klicken Sie im Dialogfeld „Einstellungen“ auf **Allgemein**.

  b Wählen Sie **Clientfenster nach Desktop-/Anwendungsstart ausblenden**.

  c Schließen Sie das Dialogfeld „Einstellungen“.

  Ihre Änderungen werden mit dem Schließen des Dialogfelds wirksam.

- Wenn Sie das ausgeblendete VMware Horizon Client-Fenster wieder anzeigen möchten, wählen Sie **Fenster > Auswahlfenster öffnen** in der Menüleiste aus oder klicken Sie mit der rechten Maustaste auf das VMware Horizon Client-Symbol im Dock und wählen Sie **Alle Fenster anzeigen** aus.

Konfigurieren von Tastenkombinationszuordnungen

Sie können durch die Konfiguration von Tastenkombinationszuordnungen festlegen, wie Remote-Desktops und Remoteanwendungen Apple-Tastenkombinationen interpretieren.

Beim Erstellen einer Tastenkombinationszuordnung ordnen Sie eine Apple-Tastenkombination einer Windows-Tastenkombination oder Aktion zu. Eine Tastenkombination besteht aus einer oder mehreren Zusatztasten wie z. B. der Strg-Taste/Ctrl-Taste oder der Umschalttaste sowie aus einem Tastencode. Bei einem Tastencode kann es sich um eine beliebige Taste auf Ihrer Tastatur mit Ausnahme der Zusatztasten handeln. Wenn Sie eine zugeordnete Tastenkombination auf Ihrer Apple-Tastatur drücken, wird die entsprechende Windows-Tastenkombination oder Aktion im Remote-Desktop oder der Remoteanwendung ausgeführt.

Voraussetzungen

Weitere Informationen zum Zuordnen einer Betriebssystem-Tastenkombination finden Sie unter „Überlegungen beim Zuordnen von Betriebssystem-Tastenkombinationen“, auf Seite 37.

Vorgehensweise

1 Wählen Sie **VMware Horizon Client > Einstellungen** aus und klicken Sie auf **Tastatur und Maus**.

2 Wählen Sie das Register **Tastenzuordnungen** aus.

3 Konfigurieren Sie die Tastenkombinationszuordnungen.

Option	Aktion
Löschen einer Tastenkombinationszuordnung	Wählen Sie die Zuordnung aus, die gelöscht werden soll, und klicken Sie auf die Schaltfläche mit dem Minuszeichen (-).
Hinzufügen einer Tastenkombinationszuordnung	a Klicken Sie auf die Schaltfläche mit dem Pluszeichen (+). b Geben Sie die Apple-Tastenkombinationssequenz an, indem Sie auf eine oder mehrere Zusatztasten klicken und einen Tastencode in das Textfeld eingeben. Sie können auch über das Dropdown-Menü eine Taste auswählen. Im Feld **Von:** wird die von Ihnen erstellte Tastenkombination angezeigt. c Geben Sie die entsprechende Windows-Tastenkombinationssequenz an, indem Sie auf eine oder mehrere Zusatztasten klicken und einen Tastencode in das Textfeld eingeben. Sie können auch über das Dropdown-Menü eine Taste auswählen. Im Feld **Zu:** wird die von Ihnen erstellte Tastenkombination angezeigt. d Klicken Sie auf **OK**, um Ihre Änderungen zu speichern. Die Tastenkombinationszuordnung ist standardmäßig aktiviert (das Kontrollkästchen **Ein** neben der Tastenkombinationszuordnung ist dann aktiviert).
Ändern einer Tastenkombinationszuordnung	Doppelklicken Sie auf die Zuordnung und nehmen Sie Änderungen vor. ■ Um die Apple-Tastenkombinationssequenz zu ändern, klicken Sie auf eine oder mehrere Zusatztasten und geben Sie einen Tastencode in das Textfeld ein. Sie können auch über das Dropdown-Menü eine Taste auswählen. ■ Um die entsprechende Windows-Tastenkombinationssequenz zu ändern, klicken Sie auf eine oder mehrere Zusatztasten und geben Sie einen Tastencode in das Textfeld ein. Sie können auch über das Dropdown-Menü eine Taste auswählen. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
Deaktivieren einer Tastenkombinationszuordnung	Deaktivieren Sie das Kontrollkästchen **Ein** neben der betreffenden Tastenkombinationszuordnung. Wenn Sie eine Tastenkombinationszuordnung deaktivieren, sendet Horizon Client die Apple-Tastenkombination nicht an den Remote-Desktop oder die Remoteanwendung.
Aktivieren oder deaktivieren sprachspezifischer Tastenzuordnungen	Aktivieren oder deaktivieren Sie das Kontrollkästchen **Sprachspezifische Tastenzuordnungen aktivieren**. Das Kontrollkästchen ist standardmäßig aktiviert.
Wiederherstellen der Standardzuordnungen	Klicken Sie auf **Standardeinstellungen wiederherstellen**. Änderungen, die Sie an den standardmäßigen Tastenkombinationszuordnungen vorgenommen haben, werden gelöscht, und die Standardzuordnungen werden wiederhergestellt.

4 Schließen Sie das Dialogfeld „Einstellungen“.

Die Änderungen der Tastenkombinationszuordnung sind sofort wirksam. Sie müssen geöffnete Remote-Desktops oder Remoteanwendungen nicht neu starten, damit die Änderungen wirksam werden.

Überlegungen beim Zuordnen von Betriebssystem-Tastenkombinationen

Sowohl für Mac als auch für Windows gibt es standardmäßige Tastenkombinationen. Beispielsweise sind Befehlstaste+Tab und Befehlstaste+Leertaste gängige Tastenkombinationen bei Mac-Systemen, und Strg+Esc und Alt+Eingabe sind gängige Tastenkombinationen bei Windows-Systemen. Wenn Sie versuchen, eine dieser Betriebssystem-Tastenkombinationen in Horizon Client zuzuordnen, kann das zu einem unvorhersehbaren Verhalten der Tastenkombination auf Ihrem Mac-Clientsystem und im Remote-Desktop oder der Remoteanwendung führen.

- Beim Zuordnen einer Tastenkombination hängt das Verhalten der Tastenkombination auf Ihrem Mac-Clientsystem davon ab, wie die Tastenkombination vom Betriebssystem verwaltet wird. Beispielsweise löst die Tastenkombination eventuell eine Aktion im Betriebssystem aus und Horizon Client reagiert möglicherweise nicht auf die Tastenkombination. Alternativ kann die Tastenkombination eine Aktion sowohl im Betriebssystem als auch in Horizon Client auslösen.
- Bevor Sie eine Mac-Tastenkombination in Horizon Client zuordnen, müssen Sie die Tastenkombination in den Systemeinstellungen auf Ihrem Mac-Clientsystem deaktivieren. Nicht alle Mac-Tastenkombinationen können deaktiviert werden.
- Wenn Sie eine Windows-Tastenkombination in Horizon Client zuordnen, wird die zugeordnete Aktion bei Verwendung der Tastenkombination im Remote-Desktop oder der Remoteanwendung ausgelöst.
- Für Remoteanwendungen werden Windows-Tastenkombinationen, die die Windows-Taste enthalten, standardmäßig deaktiviert und nicht im Dialogfeld „Tastatur-Einstellungen“ von Horizon Client angezeigt. Wenn Sie eine Zuordnung für eine dieser deaktivierten Tastenkombinationen erstellen, wird die Tastenkombination im Dialogfeld „Tastatur-Einstellungen“ angezeigt.

Eine Aufstellung der standardmäßigen Mac-Tastenkombinationen finden Sie auf der Apple Support-Website (http://support.apple.com). Eine Aufstellung der standardmäßigen Windows-Tastenkombinationen finden Sie auf der Microsoft Windows-Website (http://windows.microsoft.com).

Konfigurieren von Maustastenzuordnungen

Sie können ein Apple-Mausgerät mit einer einzigen Taste so konfigurieren, dass mit dieser Taste ein Klick mit der rechten oder mittleren Taste an Remote-Desktops und -anwendungen gesendet wird. Sie haben die Möglichkeit, die standardmäßigen Maustastenzuordnungen zu verändern, zu aktivieren oder zu deaktivieren. Es können keine neuen Maustastenzuordnungen erstellt oder die standardmäßigen Maustastenzuordnungen gelöscht werden.

Vorgehensweise

1 Wählen Sie **VMware Horizon Client > Einstellungen** aus und klicken Sie auf **Tastatur und Maus**.

2 Wählen Sie das Register **Maus-Tastenkürzel** aus.

3 Ändern Sie die Maustastenzuordnungen.

Option	Aktion
Ändern einer Maustastenzuordnung	Doppelklicken Sie auf die Zuordnung und nehmen Sie Änderungen vor. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
Deaktivieren einer Maustastenzuordnung	Deaktivieren Sie das Kontrollkästchen **Ein** neben der betreffenden Maustastenzuordnung. Wenn Sie eine Maustastenzuordnung deaktivieren, sendet Horizon Client die Apple-Maustastenzuordnung nicht an den Remote-Desktop oder die Remoteanwendung.

Option	Aktion
Aktivieren einer Maustastenzuordnung	Aktivieren Sie das Kontrollkästchen **Ein** neben der betreffenden Maustastenzuordnung. Wenn Sie eine Maustastenzuordnung aktivieren, sendet Horizon Client die Apple-Maustastenzuordnung an den Remote-Desktop oder die Remoteanwendung.
Wiederherstellen der Standardeinstellungen	Klicken Sie auf **Standardeinstellungen wiederherstellen**. Änderungen, die Sie an den standardmäßigen Maustastenzuordnungen vorgenommen haben, werden gelöscht, und die Standardzuordnungen werden wiederhergestellt.

4 Schließen Sie das Dialogfeld „Einstellungen“.

Die Änderungen der Maustastenzuordnung sind sofort wirksam. Sie müssen geöffnete Remote-Desktops oder Remoteanwendungen nicht neu starten, damit die Änderungen wirksam werden.

Konfigurieren von Horizon Client -Tastenkürzeln

Horizon Client verfügt über voreingestellte Tastenkürzel für häufig verwendete Windows-Aktionen wie z. B. Vollbildmodus ein-/ausschalten, Beenden, Anwendung ausblenden, Fenster vorwärts blättern und Fenster rückwärts blättern. Dazu gehört auch ein voreingestelltes Tastenkürzel für das Ein-/Ausschalten des Exklusivmodus. Sie können diese Standardtastenkürzel aktivieren oder deaktivieren. Darüber hinaus haben Sie die Möglichkeit, neue Tastenkürzel zu erstellen oder Standardtastenkürzel zu löschen.

Vorgehensweise

1 Wählen Sie **VMware Horizon Client > Einstellungen** aus und klicken Sie auf **Tastatur und Maus**.

2 Wählen Sie das Register **Horizon-Tastenkürzel** aus.

3 Konfigurieren Sie die Standardtastenkürzel.

Option	Aktion
Aktivieren eines Tastenkürzels	Aktivieren Sie das Kontrollkästchen **Ein** neben dem betreffenden Tastenkürzel. Wenn Sie ein Tastenkürzel aktivieren, sendet Horizon Client das Tastenkürzel nicht an den Remote-Desktop oder die Remoteanwendung.
Deaktivieren eines Tastenkürzels	Deaktivieren Sie das Kontrollkästchen **Ein** neben dem betreffenden Tastenkürzel. Wenn Sie ein Tastenkürzel deaktivieren, sendet Horizon Client das Tastenkürzel an den Remote-Desktop oder die Remoteanwendung. **Hinweis** Das Verhalten des Tastenkürzels auf dem Remote-Desktop oder in der Remoteanwendung kann variieren.
Wiederherstellen der Standardeinstellungen	Klicken Sie auf **Standardeinstellungen wiederherstellen**. Damit werden alle von Ihnen vorgenommenen Änderungen rückgängig gemacht und die Standardeinstellungen wiederhergestellt.

4 Schließen Sie das Dialogfeld „Einstellungen“.

Ihre Änderungen werden sofort wirksam. Sie müssen geöffnete Remote-Desktops oder Remoteanwendungen nicht neu starten, damit die Änderungen wirksam werden.

Suchen nach Desktops oder Anwendungen

Nachdem Sie eine Verbindung mit einem Server hergestellt haben, werden die auf diesem Server verfügbaren Desktops und Anwendungen im Fenster für die Desktop- und Anwendungsauswahl angezeigt. Sie können nach einem bestimmten Desktop oder einer bestimmten Anwendung suchen, indem Sie eine Eingabe im Fenster vornehmen.

Wenn Sie mit der Eingabe beginnen, hebt Horizon Client den ersten übereinstimmenden Desktop- oder Anwendungsnamen hervor. Drücken Sie die Eingabetaste, um eine Verbindung mit einem hervorgehobenen Desktop oder einer hervorgehobenen Anwendung herzustellen. Wenn Sie die Eingabe fortsetzen, nachdem die erste Übereinstimmung gefunden wurde, sucht Horizon Client weiterhin nach übereinstimmenden Desktops und Anwendungen. Für den Fall, dass Horizon Client mehrere übereinstimmende Desktops oder Anwendungen findet, können Sie durch Drücken der Tabulatortaste zur nächsten Übereinstimmung wechseln. Falls Sie zwei Sekunden lang keine Eingabe vornehmen und dann erneut Text eingeben, geht Horizon Client davon aus, dass Sie eine neue Suche starten.

Auswählen eines Remote-Desktops oder einer Remoteanwendung als Favorit

Sie können Remote-Desktops und -Anwendungen als Favoriten auswählen. Favoriten sind durch ein Sternchen gekennzeichnet. Mithilfe des Sternchens können Sie schnell die Favoriten-Desktops und -anwendungen finden. Die Auswahl der Favoriten wird gespeichert, auch nachdem Sie sich vom Server abgemeldet haben.

Voraussetzungen

Besorgen Sie sich die Anmeldeinformationen, die Sie zum Herstellen der Verbindung mit dem Server benötigen, z. B. einen Benutzernamen und ein Kennwort oder eine RSA SecureID und einen Passcode.

Vorgehensweise

1 Doppelklicken Sie im Startfenster von Horizon Client auf das Serversymbol.

2 Geben Sie auf Aufforderung entweder Ihren RSA-Benutzernamen und den Passcode oder Ihren Active Directory-Benutzernamen und das entsprechende Kennwort oder beides ein.

3 Führen Sie die folgenden Schritte aus, um einen Desktop oder eine Anwendung als Favorit auszuwählen oder die entsprechende Auswahl aufzuheben.

Option	Beschreibung
Favorit auswählen	Wählen Sie die Desktop- oder Anwendungsverknüpfung aus, klicken Sie mit gedrückter Strg-Taste und wählen Sie im Kontextmenü **Als Favorit markieren** aus. In der oberen rechten Ecke der Desktop- oder Anwendungsverknüpfung wird ein Sternchen angezeigt.
Die Auswahl eines Favoriten aufheben	Wählen Sie die Desktop- bzw. Anwendungsverknüpfung aus, klicken Sie mit gedrückter Strg-Taste und heben Sie im Kontextmenü die Auswahl **Als Favorit markieren** auf. In der oberen rechten Ecke der Desktop- oder Anwendungsverknüpfung wird kein Sternchen mehr angezeigt.

4 (Optional) Wenn nur Favoriten-Desktops oder -anwendungen angezeigt werden sollen, klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf die Schaltfläche **Favoriten** (Sternchensymbol).

Sie können erneut auf die Schaltfläche **Favoriten** klicken, um alle verfügbaren Desktops und Anwendungen anzuzeigen.

Wechseln zwischen Desktops oder Anwendungen

Wenn Sie mit einem Remote-Desktop verbunden sind, können Sie zu einem anderen Desktop wechseln. Sie können auch eine Verbindung mit Remoteanwendungen herstellen, während Sie mit einem Remote-Desktop verbunden sind.

Vorgehensweise

- Wählen Sie einen Remote-Desktop oder eine Remoteanwendung auf demselben oder einem anderen Server aus.

Option	Aktion
Einen anderen Desktop oder eine andere Anwendung auf demselben Server auswählen	Führen Sie einen der folgenden Schritte aus: ■ Um den aktuellen Desktop beizubehalten und zusätzlich eine Verbindung mit einem anderen Remote-Desktop herzustellen, wählen Sie in der Menüleiste **Fenster > VMware Horizon Client** aus und doppelklicken Sie auf die Verknüpfung für den anderen Desktop. Der Desktop wird in einem neuen Fenster geöffnet, sodass mehrere Desktops geöffnet sind. Sie können über das Menü **Fenster** in der Menüleiste zwischen Desktops wechseln. ■ Um den aktuellen Desktop zu schließen und eine Verbindung mit einem anderen Desktop herzustellen, wählen Sie in der Menüleiste **Verbindung > Verbindung trennen** aus und doppelklicken Sie auf die Verknüpfung für den anderen Desktop. ■ Doppelklicken Sie zum Öffnen einer anderen Anwendung auf die Verknüpfung für die andere Anwendung. Die Anwendung wird in einem neuen Fenster geöffnet. Es können mehrere Anwendungen geöffnet sein, und Sie können durch Klicken in einem Anwendungsfenster zwischen diesen Anwendungen wechseln.
Einen anderen Desktop oder eine andere Anwendung auf einem anderen Server auswählen	Wenn Sie zur Verwendung mehrerer Desktops oder Anwendungen berechtigt sind und das Fenster für die Desktop- und Anwendungsauswahl geöffnet ist, klicken Sie auf die Schaltfläche **Verbindung zum Server trennen** auf der linken Seite der Symbolleiste im Fenster für die Desktop- und Anwendungsauswahl und trennen Sie die Verbindung mit dem Server. Wenn Sie zur Verwendung nur eines Desktops oder nur einer Anwendung berechtigt sind, ist das Fenster für die Desktop- und Anwendungsauswahl nicht geöffnet. Sie können in der Menüleiste auf **Datei > Verbindung zum Server trennen** klicken und dann eine Verbindung mit einem anderen Server herstellen.

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.

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+Delete drücken und anschließend auf **Abmelden** klicken.

Hinweis Die Eingabe der Windows-Tastenkombination Strg+Alt+Entf wird für Remote-Desktops nicht unterstützt. Wählen Sie, um dieselben Resultate wie bei einer Betätigung von Strg+Alt+Entf zu erzielen, in der Menüleiste die Optionen **Verbindung > Strg+Alt+Entf senden** aus.

Alternativ können Sie auch die Tastenkombination Fn+Steuerungstaste+Option+Entfernen auf einer Apple-Tastatur betätigen.

Vorgehensweise

- Trennen Sie die Verbindung mit einem Remote-Desktop, ohne sich abzumelden.

Option	Aktion
Verbindung trennen und Horizon Client beenden	a Klicken Sie auf die Schaltfläche **Schließen** in der Ecke des Fensters oder wählen Sie **Datei > Schließen** in der Menüleiste aus. b Wählen Sie **VMware Horizon Client > VMware Horizon Client beenden** in der Menüleiste aus.
Verbindung trennen und Horizon Client geöffnet lassen	Klicken Sie auf die Schaltfläche **Trennen** in der Symbolleiste oder wählen Sie **Verbindung > Trennen** in der Menüleiste aus.

Hinweis Der 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 angehalten.

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

Option	Aktion
Aus dem Desktop-Betriebssystem heraus	Melden Sie sich über das Windows-**Start**-Menü ab.
Über die Menüleiste	Wählen Sie in der Menüleiste **Verbindung > Abmelden** aus. Bei Verwendung dieser Option werden alle Dateien, die auf dem Remote-Desktop geöffnet sind, ohne vorheriges Speichern geschlossen.

- Trennen Sie die Verbindung mit einer Remoteanwendung.

Option	Aktion
Die Verbindung mit dem Server trennen und die Anwendung geöffnet lassen	Führen Sie einen der folgenden Schritte aus: ■ Klicken Sie auf der linken Seite der Symbolleiste im Fenster für die Desktop- und Anwendungsauswahl auf die Schaltfläche **Verbindung zum Server trennen**. ■ Wählen Sie **Datei > Verbindung zum Server trennen** in der Menüleiste aus.
Die Anwendung schließen und die Verbindung mit dem Server trennen	a Beenden Sie die Anwendung auf die übliche Weise. Klicken Sie beispielsweise in der Ecke des Anwendungsfensters auf die Schaltfläche **Schließen**. b Klicken Sie auf der linken Seite der Symbolleiste im Fenster für die Desktop- und Anwendungsauswahl auf die Schaltfläche **Verbindung zum Server trennen** oder wählen Sie in der Menüleiste **Datei > Verbindung zum Server trennen** aus.

- Melden Sie sich 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.

Option	Aktion
Aus dem Startfenster	a Doppelklicken Sie auf die Server-Verknüpfung und geben Sie die Anmeldeinformationen an. Zu diesen Anmeldeinformationen zählen möglicherweise die RSA SecurID-Anmeldeinformationen und die Anmeldeinformationen zur Anmeldung am Desktop. b Wählen Sie zuerst den Desktop und anschließend in der Menüleiste **Verbindung > Abmelden** aus.
Im Fenster für die Desktop- und Anwendungsauswahl	Wählen Sie zuerst den Desktop und anschließend in der Menüleiste **Verbindung > Abmelden** aus.

Verwenden einer Touch Bar in Horizon Client

Wenn Ihr Mac über eine Touch Bar verfügt, können Sie mit dieser Horizon Client bedienen.

Mit der Touch Bar können Sie einen neuen Server hinzufügen und die Verbindung mit einem Server trennen. Wenn Sie über eine Verbindung mit einem Remote-Desktop verfügen, können Sie mit der Touch Bar den Desktop trennen, abmelden, neu starten und zurücksetzen, die Tastenkombination Strg+Alt+Entf zum Desktop senden, den Vollbildmodus aufrufen und beenden und das Fenster für die Desktop- und Anwendungsauswahl in den Vordergrund setzen. Die Funktionen zum Abmelden, Zurücksetzen und Neustarten sind nur verfügbar, wenn sie von einem Administrator aktiviert wurden.

Die Touch Bar ist nicht für Fenster von Remoteanwendungen verfügbar. Wenn sich der Remote-Desktop im Exklusivmodus befindet, ist es nicht möglich, mit der Touch Bar den Vollbildmodus aufzurufen und zu beenden sowie das Fenster für die Desktop- und Anwendungsauswahl in den Vordergrund setzen.

Automatische Verbindungsherstellung mit einem Remote-Desktop

Sie können einen Server so konfigurieren, dass automatisch ein Remote-Desktop geöffnet wird, wenn Sie eine Verbindung mit einem Server herstellen.

Wenn Sie zur Verwendung nur eines Remote-Desktops auf einem Server berechtigt sind, öffnet Horizon Client diesen Desktop, wenn Sie eine Verbindung mit dem Server herstellen.

Hinweis Sie können einen Server nicht so konfigurieren, dass automatisch eine Remoteanwendung geöffnet wird.

Voraussetzungen

Besorgen Sie sich die Anmeldedaten zur Herstellung einer Verbindung mit dem Server, so etwa den Benutzernamen und das Kennwort, den RSA SecurID-Benutzernamen und -Passcode, den RADIUS-Authentifizierungsbenutzernamen und -Passcode oder die Smartcard-PIN.

Vorgehensweise

1. Doppelklicken Sie im Startfenster von Horizon Client auf das Serversymbol.
2. Geben Sie, wenn Sie dazu aufgefordert werden, Ihre Anmeldedaten ein.
3. Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf die Schaltfläche **Einstellungen** (Zahnradsymbol).
4. Wählen Sie im linken Fensterbereich des Dialogfelds „Einstellungen“ einen Desktop-Pool aus.
5. Wählen Sie **Verbindung mit diesem Desktop automatisch herstellen** aus.

6 Schließen Sie das Dialogfeld „Einstellungen“, um Ihre Einstellungen zu speichern.

Wenn Sie das nächste Mal eine Verbindung mit dem Server herstellen, wird der Remote-Desktop von Horizon Client automatisch geöffnet.

Konfigurieren des Neuverbindungsverhaltens für Remoteanwendungen

Wenn ein Benutzer die Verbindung mit einem Server trennt, ohne eine Remoteanwendung zu schließen, wird der Benutzer von Horizon Client gefragt, ob diese Anwendung bei der nächsten Verbindungsherstellung zum Server erneut geöffnet werden soll. Dieses Verhalten können Sie ändern, indem Sie die Einstellung „Neuverbindungsverhalten“ in Horizon Client bearbeiten.

Voraussetzungen

Besorgen Sie sich die Anmeldedaten, die Sie zum Herstellen der Verbindung mit dem Server benötigen, z. B. einen Benutzernamen und ein Kennwort oder einen RSA SecurID-Benutzernamen und einen Passcode.

Vorgehensweise

1 Doppelklicken Sie im Startfenster von Horizon Client auf das Serversymbol.

2 Geben Sie, wenn Sie dazu aufgefordert werden, Ihre Anmeldedaten ein.

3 Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf die Schaltfläche **Einstellungen** (Zahnradsymbol).

4 Wählen Sie im linken Fensterbereich des Dialogfelds „Einstellungen“ die Option **Anwendungen** aus.

5 Wählen Sie eine Option für das Neuverbindungsverhalten von Anwendungen aus.

Diese Optionen bestimmen das Verhalten von Horizon Client, wenn ein Benutzer eine Verbindung mit dem Server herstellt und noch Remoteanwendungen ausgeführt werden.

Option	Beschreibung
Vor Neuverbindung zum Öffnen von Anwendungen fragen	Horizon Client zeigt die Meldung **Es werden eine oder mehrere Remoteanwendungen ausgeführt. Möchten Sie sie jetzt öffnen?** . Die Benutzer können darauf reagieren, indem Sie auf **Mit Anwendungen neu verbinden** oder **Nicht jetzt** klicken. Alternativ können Sie das Kontrollkästchen **Diese Meldung nicht erneut anzeigen** aktivieren, um diese Meldung in Zukunft nicht mehr anzuzeigen. Diese Einstellung ist standardmäßig aktiviert.
Neuverbindung zum Öffnen von Anwendungen automatisch herstellen	Ausgeführte Anwendungen werden von Horizon Client sofort erneut geöffnet. **Hinweis** Diese Einstellung aktiviert auch die Funktion des Vorabstarts der Anwendung in Horizon Client.
Vor Neuverbindung nicht fragen und nicht automatisch neu verbinden	Horizon Client fragt die Benutzer nicht, ob ausgeführte Anwendungen erneut geöffnet werden sollen, und ausgeführte Anwendungen werden auch nicht erneut geöffnet. Diese Einstellung hat dieselben Auswirkungen wie das Kontrollkästchen **Diese Meldung nicht erneut anzeigen**.

Die neue Einstellung wird wirksam, wenn Sie das nächste Mal eine Verbindung mit dem Server herstellen.

Aktivieren der Funktion des Vorabstarts der Anwendung in Horizon Client

Ein Administrator hat die Möglichkeit, eine Remoteanwendung so zu konfigurieren, dass eine Anwendungssitzung gestartet wird, bevor ein Benutzer die Anwendung in Horizon Client öffnet. Wenn eine Remoteanwendung vorab gestartet wird, wird diese in Horizon Client schneller geöffnet. Um diese Funktion verwenden zu können, muss sie in Horizon Client aktiviert werden.

Voraussetzungen

- Aktivieren Sie die Funktion des Vorabstarts für den Anwendungspool auf dem Server. Informationen hierzu finden Sie im Dokument *Administration von View*.
- Besorgen Sie sich die Anmeldedaten für den Server, z. B. einen Benutzernamen und ein Kennwort oder einen RSA SecurID-Benutzernamen und einen Passcode.

Vorgehensweise

1. Doppelklicken Sie im Startfenster von Horizon Client auf das Serversymbol.
2. Geben Sie, wenn Sie dazu aufgefordert werden, Ihre Anmeldedaten ein.
3. Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf die Schaltfläche **Einstellungen** (Zahnradsymbol).
4. Wählen Sie im linken Fensterbereich des Dialogfelds „Einstellungen“ die Option **Anwendungen** aus.
5. Wählen Sie unter „Neuverbindungsverhalten“ die Einstellung **Neuverbindung zum Öffnen von Anwendungen automatisch herstellen** aus.

Die neue Einstellung wird wirksam, wenn Sie das nächste Mal eine Verbindung mit dem Server herstellen.

Entfernen einer View Server-Verknüpfung aus dem Startfenster

Nach der Verbindungsherstellung mit einer Serverinstanz wird eine Serververknüpfung im Horizon Client-Startfenster gespeichert.

Sie können eine Serververknüpfung durch Auswahl der Verknüpfung und Betätigen der Löschtaste oder durch einen Strg-Klick/Rechtsklick auf die Verknüpfung im Startfenster und Auswahl von **Löschen** entfernen.

Sie können die Remote-Desktop- oder Remote-Anwendungsverknüpfungen nicht entfernen, die nach der Verbindungsherstellung mit einem Server angezeigt werden.

Neuanordnen von Verknüpfungen

Sie können Server-, Remote-Desktop- und Remoteanwendungsverknüpfungen neu anordnen.

Bei jeder Verbindungsherstellung mit einer Serverinstanz speichert Horizon Client eine Serververknüpfung im Startfenster. Diese Serververknüpfungen können Sie neu anordnen, indem Sie eine Verknüpfung auswählen und an eine neue Position im Startfenster ziehen.

Nachdem Sie eine Verbindung mit einem Server hergestellt haben, werden die auf diesem Server verfügbaren Desktops und Anwendungen im Fenster für die Desktop- und Anwendungsauswahl angezeigt. Desktop-Verknüpfungen werden vor Anwendungsverknüpfungen angezeigt. Desktop-Verknüpfungen und Anwendungsverknüpfungen werden alphabetisch angeordnet, und die Anordnung kann nicht geändert werden. In der Ansicht „Favoriten“ (nachdem Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf die Schaltfläche **Favoriten** geklickt haben) können Sie die Desktop- und Anwendungsverknüpfungen neu anordnen, indem Sie eine Verknüpfung auswählen und an eine neue Position im Fenster ziehen.

Verwenden von Microsoft Windows-Desktops oder -Anwendungen auf einem Mac

4

Horizon Client für Mac unterstützt verschiedene Funktionen.

Dieses Kapitel behandelt die folgenden Themen:

Funktionsunterstützungs-Matrix für Mac

Einige Funktionen werden auf manchen Horizon Client-Typen unterstützt, auf anderen nicht.

Tabelle 4-1. Auf Windows-Desktops für Mac-Clients unterstützte Funktionen

Funktion	Windows 10-Desktop	Windows 8.x-Desktop	Windows 7-Desktop	Windows Vista-Desktop	Windows XP-Desktop	Windows Server 2008/2012 R2- oder Windows Server 2016-Desktop
RSA SecurID oder RADIUS	X	X	X	Begrenzt	Begrenzt	X
Einmaliges Anmelden	X	X	X	Begrenzt	Begrenzt	X
PCoIP-Anzeigeprotokoll	X	X	X	Begrenzt	Begrenzt	X
RDP-Anzeigeprotokoll	X	X	X	Begrenzt	Begrenzt	X
VMware Blast-Anzeigeprotokoll	X	X	X			X
USB-Umleitung	X	X	X	Begrenzt	Begrenzt	X

Tabelle 4-1. Auf Windows-Desktops für Mac-Clients unterstützte Funktionen (Fortsetzung)

Funktion	Windows 10-Desktop	Windows 8.x-Desktop	Windows 7-Desktop	Windows Vista-Desktop	Windows XP-Desktop	Windows Server 2008/2012 R2- oder Windows Server 2016-Desktop
Clientlaufwerksumleitung	X	X	X			X
Echtzeit-Audio/Video (RTAV)	X	X	X	Begrenzt	Begrenzt	X
Wyse MMR						
Windows 7 MMR						
Virtuelles Drucken	X	X	X	Begrenzt	Begrenzt	X
Standortbasierter Druck	X	X	X	Begrenzt	Begrenzt	X
Smartcards	X	X	X	Begrenzt	Begrenzt	X
Mehrere Monitore	X	X	X	Begrenzt	Begrenzt	X

Windows 10-Desktops erfordern View Agent 6.2 oder höher oder Horizon Agent 7.0 oder höher. Windows Server 2012 R2-Desktops erfordern View Agent 6.1 oder höher oder Horizon Agent 7.0 oder höher. Windows Server 2016-Desktops erfordern Horizon Agent 7.0.2 oder höher.

Wichtig Windows XP- und Windows Vista-Desktops werden von View Agent 6.1 und höher und von Horizon Agent 7.0 oder höher nicht unterstützt. View Agent 6.0.2 ist die letzte Version, die diese Gastbetriebssysteme unterstützt. Kunden, die über einen Vertrag mit Microsoft über erweiterten Support für Windows XP und Windows Vista sowie über einen Vertrag mit VMware über erweiterten Support für diese Gastbetriebssysteme verfügen, können View Agent 6.0.2 ihrer Windows XP- und Windows Vista-Desktops mit Verbindungsserver 6.1 bereitstellen.

Weitere Erläuterungen zu diesen Funktionen finden Sie im Dokument *Planung der View-Architektur*.

Funktionsunterstützung für veröffentlichte Desktops auf RDS-Hosts

RDS-Hosts sind Server-Computer, auf denen Windows-Remotedesktopdienste und View Agent oder Horizon Agent installiert sind. Mehrere Benutzer können gleichzeitig über Desktop-Sitzungen auf einem RDS-Host verfügen. Ein RDS-Host kann ein physischer Computer oder eine virtuelle Maschine sein.

Hinweis Die folgende Tabelle enthält nur Zeilen für die unterstützten Funktionen. Wenn im Text Mindestversionen von View Agent festgelegt sind, gilt die Angabe „und höher“ auch für Horizon Agent 7.0.x und höher.

Tabelle 4-2. Unterstützte Funktionen für RDS-Hosts mit installiertem View Agent 6.0.x oder höher oder mit Horizon Agent 7.0.x oder höher

Funktion	Windows Server 2008 R2 RDS-Host	Windows Server 2012 RDS-Host	Windows Server 2016 RDS-Host
RSA SecurID oder RADIUS	X	X	Horizon Agent 7.0.2 und höher
Smartcard	View Agent 6.1 und höher	View Agent 6.1 und höher	Horizon Agent 7.0.2 und höher
Einmaliges Anmelden	X	X	Horizon Agent 7.0.2 und höher

Tabelle 4-2. Unterstützte Funktionen für RDS-Hosts mit installiertem View Agent 6.0.x oder höher oder mit Horizon Agent 7.0.x oder höher (Fortsetzung)

Funktion	Windows Server 2008 R2 RDS-Host	Windows Server 2012 RDS-Host	Windows Server 2016 RDS-Host
PCoIP-Anzeigeprotokoll	X	X	Horizon Agent 7.0.2 und höher
VMware Blast-Anzeigeprotokoll	Horizon Agent 7.0 und höher	Horizon Agent 7.0 und höher	Horizon Agent 7.0.2 und höher
HTML Access	View Agent 6.0.2 und höher (nur virtuelle Maschine)	View Agent 6.0.2 und höher (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher
USB-Umleitung (nur USB-Speichergeräte)		View Agent 6.1 und höher	Horizon Agent 7.0.2 und höher
Clientlaufwerksumleitung	View Agent 6.1.1 und höher	View Agent 6.1.1 und höher	Horizon Agent 7.0.2 und höher
Virtueller Druck (für Desktop-Clients)	View Agent 6.0.1 und höher (nur virtuelle Maschine)	View Agent 6.0.1 und höher (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher (nur virtuelle Maschine)
Standortbasierter Druck	View Agent 6.0.1 und höher (nur virtuelle Maschine)	View Agent 6.0.1 und höher (nur virtuelle Maschine)	Horizon Agent 7.0.2 und höher (nur virtuelle Maschine)
Mehrere Monitore (für Desktop-Clients)	X	X	Horizon Agent 7.0.2 und höher
Unity Touch (für mobile und Chrome OS-Clients)	X	X	Horizon Agent 7.0.2 und höher
Echtzeit-Audio/Video (RTAV)	Horizon Agent 7.0.2 und höher	Horizon Agent 7.0.2 und höher	Horizon Agent 7.0.3 und höher

Informationen darüber, welche Editionen bzw. Service Packs der einzelnen Gastbetriebssysteme unterstützt werden, finden Sie im Dokument *View-Installation*.

Einschränkungen für Sonderfunktionen

Für bestimmte Funktionen, die auf Windows-Desktops für Horizon Client für Mac unterstützt werden, gelten spezielle Einschränkungen.

Tabelle 4-3. Anforderungen für Sonderfunktionen

Funktion	Anforderungen
RDP-Verbindung mit einem Windows 8.1-Desktop oder höher	Siehe VMware KB-Artikel unter http://kb.vmware.com/kb/2059786.
Echtzeit-Audio/Video	Siehe „Systemanforderungen für Echtzeit-Audio/Video“, auf Seite 8.
Virtuelles und standortbasiertes Drucken für Windows Server 2008 R2-Desktops, veröffentlichte Desktops (auf RDS-Hosts virtueller Maschinen) und veröffentlichte Anwendungen	Horizon 6.0.1 (mit View) und Server höherer Version.

Tabelle 4-3. Anforderungen für Sonderfunktionen (Fortsetzung)

Funktion	Anforderungen
Smartcards	Für sitzungsbasierte Desktops auf RDS-Hosts: View Agent 6.1 und höher.
Clientlaufwerksumleitung	View Agent 6.1.1 und höher oder Horizon Agent 7.0 und höher.

Hinweis Mit Horizon Client haben Sie nicht nur auf Remote-Desktops, sondern auch auf Windows-basierte Remoteanwendungen sicheren Zugriff. Durch die Auswahl einer Anwendung in Horizon Client wird ein Fenster für diese Anwendung auf dem lokalen Clientgerät geöffnet, und das Erscheinungsbild und das Verhalten der Anwendung entspricht einer lokal installierten Anwendung.

Remoteanwendungen können Sie nur verwenden, wenn Sie mit Verbindungsserver 6.0 oder höher verbunden sind. Einzelheiten zu den unterstützten Betriebssystemen für den RDS-Host, der veröffentlichte Anwendungen und veröffentlichte Desktops bereitstellt, finden Sie im Dokument *View-Installation*.

Funktionsunterstützung für Linux-Desktops

Einige Linux-Gastbetriebssysteme werden unterstützt, wenn Sie über View Agent 6.1.1 und höher oder Horizon Agent 7.0 und höher verfügen. Im Dokument *Einrichten von Horizon 6 for Linux-Desktops* oder *Einrichten von Horizon 7 for Linux-Desktops* finden Sie eine Liste unterstützter Linux-Betriebssysteme sowie Informationen zu den unterstützten Funktionen.

Internationalisierung

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

Monitore und Bildschirmauflösung

Wenn Sie das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwenden, können Sie einen Remote-Desktop auf mehrere Monitore erweitern. Wenn Sie einen Mac mit Retina-Display besitzen, können Sie den Remote-Desktop in voller Auflösung sehen.

Verwendung mehrerer Monitore

Mit dem VMware Blast- oder dem PCoIP-Anzeigeprotokoll wird eine Bildschirmauflösung von 4K (3840 x 2160) für den Remote-Desktop unterstützt. Die Anzahl der unterstützten 4K-Bildschirme hängt von der Hardwareversion der virtuellen Maschine des Desktops und der Windows-Version ab.

Hardwareversion	Windows-Version	Anzahl der unterstützten 4K-Bildschirme
10 (ESXi 5.5.x-kompatibel)	7, 8, 8.x, 10	1
11 (ESXi 6.0-kompatibel)	7 (3D-Rendern-Funktion deaktiviert und Windows Aero deaktiviert)	3
11	7 (3D-Rendern-Funktion aktiviert)	1
11	8, 8.x, 10	1

Auf dem Remote-Desktop muss View Agent 6.2 oder höher oder Horizon Agent 7.0 oder höher installiert sein. Für eine optimale Leistung muss die virtuelle Maschine mindestens über 2 GB RAM und 2 vCPUs verfügen. Diese Funktion kann gute Netzwerkbedingungen erfordern, wie eine Bandbreite von 1000 Mbit/s mit niedriger Netzwerklatenz und geringen Paketverlusten.

Verwenden des Vollbildmodus mit mehreren Monitoren

Wenn ein Remote-Desktop-Fenster geöffnet ist, können Sie mit der Menüoption **Fenster > Vollbild aufrufen** oder mit den Erweiterungspfeilen rechts oben im Desktop-Fenster den Remote-Desktop auf mehrere Monitore erweitern. Es besteht die Möglichkeit, den Remote-Desktop mit der Menüoption **Fenster > Im Vollbildmodus einzelnen Monitor verwenden** vollständig nur auf einem Monitor darzustellen. Mit dieser Option muss für die Monitore nicht der gleiche Modus gelten. Wenn Sie zum Beispiel einen Laptop verwenden, der mit einem externen Monitor verbunden ist, kann sich der externe Monitor sowohl im Quer- als auch im Hochformat befinden.

Sie können nach der Herstellung einer Verbindung mit einem Server und vor dem Öffnen eines Remote-Desktops eine Vollbildoption aus dem Dialogfeld „Einstellungen“ auswählen. Klicken Sie dazu auf die Schaltfläche **Einstellungen** (Zahnradsymbol) rechts oben im Auswahlfenster für Desktops und Anwendungen, wählen Sie den Remote-Desktop und dann eine Vollbildoption aus dem Dropdown-Menü **Vollbild** aus.

Verwenden von Remote-Desktops in einer geteilten Darstellung (Split View)

Mit einer geteilten Darstellung, die in El Capitan (10.11) und höheren Betriebssystemen unterstützt wird, können Sie auf Ihrem Mac-Bildschirm zwei Anwendungen vollständig anzeigen, ohne Fenster manuell verschieben oder deren Größe ändern zu müssen. Sie können Split View mit Remote-Desktops im Vollbildmodus (**Vollbildmodus** oder **Einzelansicht im Vollbildmodus**) verwenden.

Verwenden eines hochauflösenden Mac mit Retina-Display

Wenn Sie das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwenden, unterstützt Horizon Client für Clientsysteme mit Retina-Display auch sehr hohe Auflösungen. Nachdem Sie die Verbindung mit einem Remote-Desktop hergestellt haben, wählen Sie das Menüelement **Verbindung > Auflösung > Volle Auflösung** aus. Dieses Menüelement wird nur dann angezeigt, wenn das Clientsystem ein Retina-Display unterstützt.

Wenn Sie **Volle Auflösung** verwenden, erscheinen die Symbole auf dem Remote-Desktop kleiner, aber die Anzeige ist schärfer.

Verwenden des Exklusivmodus

Der Exklusivmodus entspricht dem Vollbildmodus, da dabei der Remote-Desktop den gesamten Bildschirm ausfüllt. Anders als im Vollbildmodus werden im Exklusivmodus die VMware Horizon Client-Menüleiste und das -Dock aber nicht angezeigt, wenn Sie Ihren Cursor an den Bildschirmrand bewegen.

Um den Exklusivmodus aufzurufen, öffnen Sie einen Remote-Desktop im Fenstermodus, halten Sie die Optionstaste gedrückt und wählen Sie **Fenster > Exklusivmodus aufrufen** aus.

Befindet sich ein Remote-Desktop im Fenstermodus, können Sie den Exklusivmodus auch durch Drücken von Befehl-Ctrl-Option-F aufrufen. Um den Exklusivmodus zu beenden, drücken Sie Befehl-Ctrl-Option-F erneut.

Hinweis Wenn Sie die Optionstaste nicht gedrückt halten, wird statt der Menüoption **Exklusivmodus aufrufen** die Option **Vollbild aufrufen** angezeigt. Wenn sich der Remote-Desktop im Vollbildmodus befindet, steht die Menüoption **Exklusivmodus aufrufen** nicht zur Verfügung.

Verwenden des Exklusivmodus mit mehreren Monitoren

Um den Exklusivmodus mit zwei Monitoren zu verwenden, wählen Sie, bevor Sie den Remote-Desktop öffnen, **Alle Monitore verwenden** aus dem Dialogfeld „Einstellungen“ aus. Anschließend öffnen Sie den Desktop und rufen Sie den Exklusivmodus auf. Um den Exklusivmodus mit einem Monitor zu verwenden, wählen Sie, bevor Sie den Remote-Desktop öffnen, **Einzelnen Monitor verwenden** aus dem Dialogfeld „Einstellungen“ aus. Stellen Sie dann eine Verbindung mit dem Desktop her und rufen Sie den Exklusivmodus auf.

Um das Dialogfeld „Einstellungen“ zu öffnen, klicken Sie auf die Schaltfläche **Einstellungen** (Zahnradsymbol) rechts oben im Fenster für Desktops und Anwendungen, wählen Sie den Remote-Desktop und dann eine Option aus dem Dropdown-Menü **Vollbild** aus.

Verbinden von USB-Geräten

Sie können lokal angeschlossene USB-Geräte, zum Beispiel Thumb-Flashlaufwerke, Kameras oder Drucker, von einem Remote-Desktop aus verwenden. Diese Funktion wird als USB-Umleitung bezeichnet.

Bei Aktivierung dieser Funktion stehen die meisten USB-Geräte, die an das lokale Clientsystem angeschlossen sind, in einem Menü in Horizon Client zur Verfügung. Über das Menü können Sie die Geräte verbinden oder deren Verbindung trennen.

Mit View Agent 6.1 oder höher oder mit Horizon Agent 7.0 oder höher können Sie auch lokal angeschlossene USB-Thumb-Flashlaufwerke und Festplatten für die Verwendung in veröffentlichten Desktops und Anwendungen auf RDS-Hosts umleiten. Andere Arten von USB-Geräten, einschließlich anderer Arten von Speichergeräten (z. B. Sicherheitsspeicherlaufwerke und USB-CD-ROM-Laufwerke), werden in veröffentlichten Desktops und Anwendungen nicht unterstützt. Auf dem Server, der den veröffentlichten Desktop bzw. die veröffentlichte Anwendung hostet, muss Windows Server 2012 oder höher ausgeführt werden.

Wenn Sie die Funktion der Clientlaufwerksumleitung zur Freigabe eines USB-Speichergeräts oder eines Ordners auf einem USB-Speichergerät verwenden, können Sie mit der USB-Umleitungsfunktion das Gerät nicht zu einem Remote-Desktop oder zu einer Remoteanwendung umleiten, da das Gerät bereits freigegeben ist.

Bei der Verwendung von USB-Geräten mit Remote-Desktops gelten folgende Einschränkungen:

- Beim Zugriff auf ein USB-Gerät von einem Menü in Horizon Client und Verwendung des Geräts in einem Remote-Desktop können Sie nicht auf dem lokalen Computer auf das Gerät zugreifen.
- Zu den USB-Geräten, die nicht im Menü angezeigt werden, aber auf dem Remote-Desktop verfügbar sind, zählen Eingabegeräte (Human Interface Devices) wie zum Beispiel Tastaturen und Zeigegeräte. Der Remote-Desktop und der lokale Computer verwenden diese Geräte gleichzeitig. Die Interaktion mit diesen Geräten kann aufgrund der Netzwerklatenz manchmal recht langsam sein.
- Große USB-Festplattenlaufwerke können erst nach mehreren Minuten auf dem Desktop angezeigt werden.
- Manche USB-Geräte erfordern bestimmte Treiber. Wenn der erforderliche Treiber nicht bereits auf dem Remote-Desktop installiert ist, werden Sie möglicherweise bei Verbindung des USB-Geräts mit dem Remote-Desktop zu Installation dieses Treibers aufgefordert.
- Wenn Sie USB-Geräte verbinden möchten, die MTP-Treiber verwenden, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets, müssen Sie Horizon Client so konfigurieren, dass die USB-Geräte automatisch mit Ihrem Remote-Desktop verbunden werden. Anderenfalls wird das USB-Gerät beim Versuch der manuellen Umleitung über ein Menüelement erst umgeleitet, nachdem Sie das Gerät getrennt und neu verbunden haben.
- Webcams werden für die USB-Umleitung nicht unterstützt.
- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz.

Sie können USB-Geräte sowohl manuell als auch automatisch mit einem Remote-Desktop verbinden.

Hinweis Leiten Sie keinesfalls USB-Ethernet-Verbindungen an den Remote-Desktop um. Ihr Remote-Desktop kann sich mit dem Netzwerk verbinden, wenn Ihr lokales System verbunden ist. Wenn Sie Ihren Remote-Desktop zur automatischen Verbindung von USB-Geräten konfiguriert haben, können Sie eine Ausnahme hinzufügen, um Ihre Ethernet-Verbindung auszuschließen. Siehe „Konfigurieren der USB-Umleitung auf einem Mac-Client“, auf Seite 53.

Voraussetzungen

- Um USB-Geräte mit einem Remote-Desktop verwenden zu können, muss ein Horizon-Administrator die USB-Funktion für den Remote-Desktop aktivieren.

  Diese Aufgabe schließt die Installation der Komponente **USB-Umleitung** des Agenten ein und kann auch die Erstellung von Einstellungsrichtlinien hinsichtlich der USB-Umleitung umfassen. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

- Beim erstmaligen Anschlussversuch eines USB-Geräts müssen Sie das Administrator-Kennwort eingeben. Horizon Client fordert Sie zur Eingabe des Kennworts auf.

  Einige der für die USB-Umleitung erforderlichen Komponenten, die durch Horizon Client installiert werden, müssen konfiguriert werden. Für die Konfiguration dieser Komponenten sind Administratorberechtigungen erforderlich.

Vorgehensweise

- Verbinden Sie das USB-Gerät manuell mit einem Remote-Desktop.

  a Bei erstmaliger Verwendung der USB-Funktion klicken Sie in der VMware Horizon Client-Menüleiste auf **Verbindung > USB > Remote-USB-Dienste starten**. Geben Sie auf Aufforderung das Administratorkennwort an.

  b Schließen Sie das USB-Gerät an Ihr lokales Clientsystem an.

  c Klicken Sie in der VMware Horizon Client-Menüleiste auf **Verbindung > USB > Verbindung mit Desktop herstellen und USB-Geräte auflisten**.

  d Stellen Sie eine Verbindung mit einem Remote-Desktop her, um eine Liste der verbundenen USB-Geräte anzuzeigen und ein USB-Gerät auszuwählen.

  Das Gerät wird manuell vom lokalen System an den Remote-Desktop umgeleitet.

- Schließen Sie das USB-Gerät an eine gehostete Remoteanwendung an.

  a Bei erstmaliger Verwendung der USB-Funktion klicken Sie in der VMware Horizon Client-Menüleiste auf **Verbindung > USB > Remote-USB-Dienste starten**. Geben Sie auf Aufforderung das Administratorkennwort an.

  b Schließen Sie das USB-Gerät an.

  c Öffnen Sie die Remoteanwendung.

  d Klicken Sie in der oberen rechten Ecke des Fensters für die Desktop- und Anwendungsauswahl auf die Schaltfläche **Einstellungen** (Zahnradsymbol).

  e Wählen Sie im linken Fensterbereich des Dialogfelds „Einstellungen“ die Option **Anwendungen** aus.

  f Klicken Sie oben im rechten Fensterbereich des Dialogfelds „Einstellungen“ auf **USB**.

  Die verfügbaren USB-Geräte werden im linken Bereich angezeigt.

  g Wählen Sie ein USB-Gerät aus und klicken Sie auf **Gerät verbinden**.

  Wenn ein USB-Gerät bereits mit einem Remote-Desktop oder mit einer Remoteanwendung verbunden ist, müssen Sie diese Verbindung trennen, bevor Sie das USB-Gerät auswählen können.

h Wählen Sie eine Remoteanwendung aus und klicken Sie auf **Fortfahren**.

Sie können jede ausgeführte Anwendung auf dem RDS-Host auswählen. Nach der Auswahl einer Remoteanwendung lässt sich das USB-Gerät mit der Remoteanwendung benutzen.

i Wenn die Remoteanwendung nicht mehr verwendet wird, öffnen Sie das Dialogfeld „Einstellungen“ erneut, wählen **USB** und dann **Verbindung trennen**, um das USB-Gerät und die Remoteanwendung voneinander zu trennen.

Sie können nun das USB-Gerät mit Ihrem lokalen Clientsystem, mit einem Remote-Desktop oder mit einer anderen Remoteanwendung verwenden.

- Konfigurieren Sie Horizon Client dahingehend, dass USB-Geräte automatisch mit dem Remote-Desktop verbunden werden, wenn Sie diese an das lokale System anschließen.

  Mit der Funktion zur automatischen Verbindung haben Sie die Möglichkeit, Geräte mit MTP-Treibern zu verbinden, so zum Beispiel Android-basierte Samsung-Smartphones und -Tablets.

  a Bevor Sie das USB-Gerät anschließen, starten Sie Horizon Client und stellen Sie die Verbindung mit einem Remote-Desktop her.

  b Bei erstmaliger Verwendung der USB-Funktion klicken Sie in der VMware Horizon Client-Menüleiste auf **Verbindung > USB > Remote-USB-Dienste starten**. Geben Sie auf Aufforderung das Administratorkennwort an.

  c Klicken Sie in der VMware Horizon Client-Menüleiste auf **Verbindung > USB > Nach Einführung automatisch verbinden**.

  d Schließen Sie das USB-Gerät an.

  USB-Geräte, die Sie nach dem Start von Horizon Client an Ihr lokales System anschließen, werden an den Remote-Desktop umgeleitet.

- Konfigurieren Sie Horizon Client zur automatischen Verbindung von USB-Geräten mit dem Remote-Desktop, wenn Horizon Client gestartet wird.

  a Bei erstmaliger Verwendung der USB-Funktion klicken Sie in der VMware Horizon Client-Menüleiste auf **Verbindung > USB > Remote-USB-Dienste starten**. Geben Sie auf Aufforderung das Administratorkennwort an.

  b Klicken Sie in der VMware Horizon Client-Menüleiste auf **Verbindung > USB > Beim Start automatisch verbinden**.

  c Schließen Sie das USB-Gerät an und starten Sie Horizon Client neu.

  USB-Geräte, die Sie beim Start von Horizon Client an Ihr lokales System anschließen, werden an den Remote-Desktop umgeleitet.

Das USB-Gerät wird auf dem Desktop angezeigt. Es kann dabei bis zu 20 Sekunden dauern, bis das USB-Gerät auf dem Desktop eingeblendet wird. Bei erstmaliger Verbindung von Gerät und Desktop werden Sie eventuell dazu aufgefordert, bestimmte Treiber zu installieren.

Wird das USB-Gerät auch nach mehreren Minuten nicht auf dem Desktop angezeigt, sollten Sie die Verbindung trennen und das Gerät anschließend neu mit dem Clientcomputer verbinden.

Weiter

Bei Problemen mit der USB-Umleitung finden Sie weitere Informationen im Kapitel über die Behebung von Problemen bei der USB-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Konfigurieren der USB-Umleitung auf einem Mac-Client

Administratoren können das Clientsystem zur Angabe der USB-Geräte konfigurieren, die an einen Remote-Desktop umgeleitet werden können.

Zum Erreichen der folgenden Ziele können Sie sowohl für View Agent oder Horizon Agent auf dem Remote-Desktop als auch für Horizon Client auf dem lokalen System einzelne USB-Richtlinien konfigurieren:

- Legen Sie bestimmte Einschränkungen für die USB-Gerättypen fest, die Horizon Client zur Umleitung bereitstellt.
- Veranlassen Sie, dass View Agent oder Horizon Agent das Weiterleiten bestimmter USB-Geräte von einem Clientcomputer aus verhindert.
- Geben Sie an, ob Horizon Client USB-Verbundgeräte für die Umleitung in separate Komponenten aufschlüsseln soll.

  USB-Verbundgeräte bestehen aus einer Kombination von zwei oder mehr Geräten, so zum Beispiel einem Videoeingabegerät und einem Speichergerät.

Die Konfigurationseinstellungen auf dem Client können mit den entsprechenden, für View Agent oder Horizon Agent auf dem Remote-Desktop festgelegten Richtlinien zusammengeführt oder von diesen überschrieben werden. Informationen zur Zusammenarbeit der USB-Einstellungen auf dem Client mit den View Agent- oder Horizon Agent-USB-Richtlinien finden Sie in den Abschnitten über die Verwendung von Richtlinien zur Steuerung der USB-Umleitung im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Verwenden von Regeln einer vorherigen Horizon Client -Version

In früheren Horizon Client-Versionen mussten Sie zur Konfiguration von USB-Filterungs- und Aufschlüsselungsregeln Sudo verwenden. Mithilfe des im Folgenden dargestellten Vorgangs können Sie Regeln, die Sudo verwenden, auf neue Regeln verschieben, die Sudo nicht verwenden.

1 Öffnen Sie auf dem Mac-Client Terminal (`/Applications/Utilities/Terminal.app`) und führen Sie den folgenden Befehl aus:

```
sudo defaults export com.vmware.viewusb /tmp/usb.plist
```

2 Öffnen Sie ein Terminal-Fenster (drücken Sie die Tastenkombination Befehlstaste+N) und führen Sie den folgenden Befehl aus:

```
defaults import com.vmware.viewusb /tmp/usb.plist
```

3 Führen Sie im ersten Terminal-Fenster den folgenden Befehl aus:

```
sudo rm –rf /tmp/usb.plist
```

4 Schließen Sie beide Terminal-Fenster.

Aktualisieren Sie jetzt die Regeln. Verwenden Sie dazu `defaults write com.vmware.viewusb` *`property value`*.

Syntax zur Konfiguration der USB-Umleitung

Sie können Filter- und Aufschlüsselungsregeln konfigurieren, um USB-Geräte-Typen von der Umleitung an einen Remote-Desktop auszuschließen oder sie einzuschließen. Konfigurieren Sie auf einem Mac-Client die USB-Funktionalität, indem Sie Terminal (`/Applications/Utilities/Terminal.app`) verwenden und einen Befehl als „Root“ ausführen.

- Zur Auflistung der Regeln:

  ```
  # defaults read domain
  ```

Beispiel:

```
# defaults read com.vmware.viewusb
```

- Zum Entfernen einer Regel:

  ```
  # defaults delete domain property
  ```

  Beispiel:

  ```
  # defaults delete com.vmware.viewusb ExcludeVidPid
  ```

- Zum Festlegen oder Ersetzen einer Filterregel:

  ```
  # defaults write domain property value
  ```

  Beispiel:

  ```
  # defaults write com.vmware.viewusb ExcludeVidPid vid-1234_pid-5678
  ```

  Wichtig Manche Konfigurationsparameter erfordern für ein USB-Gerät die VID (Hersteller-ID) und die PID (Produkt-ID). Die korrekte VID und PID finden Sie, indem Sie im Internet nach dem Produktnamen plus `VID` und `PID` suchen. Alternativ können Sie nach Anschluss des USB-Geräts an das lokale System bei Ausführung von Horizon Client auch in der USB-Protokolldatei nachsehen. Weitere Informationen finden Sie unter „Aktivieren der Protokollierung für die USB-Umleitung“, auf Seite 58.

- So stellen Sie eine Aufschlüsselungsregel für ein Verbundgerät ein bzw. ersetzen sie:

  ```
  # defaults write domain property value
  ```

  Beispiel:

  ```
  # defaults write com.vmware.viewusb AllowAutoDeviceSplitting true
  # defaults write com.vmware.viewusb SplitExcludeVidPid vid-03f0_Pid-2a12
  # defaults write com.vmware.viewusb SplitVidPid "'vid-0911_Pid-149a(exintf:03)'"
  # defaults write com.vmware.viewusb IncludeVidPid vid-0911_Pid-149a
  ```

  USB-Verbundgeräte bestehen aus einer Kombination von zwei oder mehr Geräten, so zum Beispiel einem Videoeingabegerät und einem Speichergerät. Die erste Zeile in diesem Beispiel aktiviert die automatische Aufschlüsselung von Verbundgeräten. Die zweite Zeile schließt das angegebene USB-Verbundgerät (`Vid-03f0_Pid-2a12`) von der Aufschlüsselung aus.

  Die dritte Zeile weist Horizon Client dazu an, die Komponenten eines anderen Verbundgeräts (`Vid-0911_Pid-149a`) als separate Geräte zu behandeln, die folgende Komponente jedoch von der Umleitung auszuschließen: Die Komponente, deren Schnittstellennummer 03 lautet. Diese Komponente wird lokal beibehalten.

  Da dieses Verbundgerät eine Komponente enthält, die im Regelfall standardmäßig ausgeschlossen wird, z. B. eine Maus oder eine Tastatur, ist die vierte Zeile notwendig, damit andere Komponenten des Verbundgeräts `Vid-0911_Pid-149a` an den Remote-Desktop umgeleitet werden können.

  Die ersten drei Eigenschaften beziehen sich auf die Aufschlüsselung. Die letzte Eigenschaft bezieht sich auf das Filtern. Filtereigenschaften werden vor den Aufschlüsselungseigenschaften verarbeitet.

Beispiel: Ausschließen eines USB-Ethernet-Geräts

Zu den USB-Geräten, die Sie von der Umleitung ausschließen sollten, zählen beispielsweise auch USB-Ethernet-Geräte. Ihr Mac nutzt möglicherweise ein USB-Ethernet-Gerät für die Verbindung des Netzwerks des Mac-Clientsystems mit einem Remote-Desktop. Wenn Sie das USB-Ethernet-Gerät umleiten, verliert Ihr lokales Clientsystem die Verbindung zum Netzwerk und zum Remote-Desktop.

Wenn Sie dieses Gerät dauerhaft aus dem USB-Verbindungsmenü ausblenden möchten oder Sie Ihren Remote-Desktop so eingerichtet haben, dass USB-Geräte automatisch verbunden werden, können Sie eine Ausnahme hinzufügen, um Ihre Ethernet-Verbindung auszuschließen.

```
defaults write com.vmware.viewusb ExcludeVidPid vid–xxxx_pid–yyyy
```

In diesem Beispiel steht *xxxx* für die Hersteller-ID und *yyyy* für die Produkt-ID des USB-Ethernet-Adapters.

Eigenschaften der USB-Umleitung

Bei der Erstellung von Filterregeln können Sie die Eigenschaften der USB-Umleitung verwenden.

Tabelle 4-4. Konfigurationseigenschaften für die USB-Umleitung

Name und Eigenschaft der Richtlinie	Beschreibung
Autom. Gerätesplitten zulassen Eigenschaft: `AllowAutoDeviceSplitting`	Lässt das automatische Splitten von Composite USB-Geräten zu. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
Exclude Vid/Pid Device From Split (Vid/Pid-Gerät vom Splitten ausschließen) Eigenschaft: `SplitExcludeVidPid`	Schließt ein Composite USB-Gerät vom Splitten aus, das durch Anbieter- und Produkt-IDs angegeben ist. Das Format der Einstellung lautet `vid–`*xxx1*`_pid–`*yyy1*`[;vid–`*xxx2*`_pid–`*yyy2*`]`... Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid–0781_pid–55**`** Der Standardwert ist nicht definiert.
Split Vid/Pid Device (Vid/Pid-Gerät splitten) Eigenschaft: `SplitVidPid`	Behandelt die Komponenten eines Composite USB-Gerätes, die durch Anbieter- und Produkt-IDs angegeben sind, als separate Geräte. Das Format der Einstellung ist `vid–`*xxxx*`_pid–`*yyyy*`([exintf:`*zz*`[;exintf:`*ww*`]])[;...]` Sie können das Stichwort `exintf` verwenden, um Komponenten durch Angabe ihrer Schnittstellennummer von der Umleitung auszuschließen. Sie müssen hexadezimale ID-Nummern und dezimale Schnittstellennummern einschließlich der 0 am Anfang angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid–0781_pid–554c(exintf:01;exintf:02)`** **Hinweis** Enthält das Verbundgerät Komponenten, die automatisch ausgeschlossen werden, z. B. Maus- und Tastaturkomponenten, dann schließt Horizon die Komponenten, die Sie nicht ausdrücklich ausgeschlossen haben, nicht automatisch ein. Sie müssen eine Filterrichtlinie wie z. B. `Include Vid/Pid Device` angeben, um diese Komponenten einzuschließen. Der Standardwert ist nicht definiert.
Allow Audio Input Devices (Audioeingabegeräte zulassen) Eigenschaft: `AllowAudioIn`	Lässt zu, dass Audioeingabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.
Allow Audio Output Devices (Audioausgabegeräte zulassen) Eigenschaft: `AllowAudioOut`	Lässt zu, dass Audioausgabegeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
HID zulassen Eigenschaft: `AllowHID`	Ermöglicht die Umleitung anderer Eingabegeräte neben Tastaturen und Mäusen. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.
Allow HIDBootable (HIDBootable zulassen) Eigenschaft: `AllowHIDBootable`	Ermöglicht die Umleitung anderer Eingabegeräte neben Tastaturen und Mäusen, die zur Startzeit verfügbar sind (auch bezeichnet als „startfähige Eingabegeräte“). Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.

Tabelle 4-4. Konfigurationseigenschaften für die USB-Umleitung (Fortsetzung)

Name und Eigenschaft der Richtlinie	Beschreibung
Ausfallsicherung der Dienstbeschreibung zulassen Eigenschaft: `AllowDevDescFailsafe`	Ermöglicht die Umleitung der Geräte, auch wenn Horizon Client die Konfigurations-/Gerätebeschreibungen nicht abrufen kann. Um ein Gerät trotz Fehler in der Konfiguration/Beschreibung zuzulassen, muss dieses in den Filter „Include“ eingeschlossen werden, zum Beispiel in `IncludeVidPid` oder `IncludePath`. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
Allow Keyboard and Mouse Devices (Tastatur- und Mausgeräte zulassen) Eigenschaft: `AllowKeyboardMouse`	Lässt zu, dass Tastaturen mit eingebauten Zeigegeräten (Maus, Trackball oder Touchpad) umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
Allow Smart Cards (SmartCards zulassen) Eigenschaft: `AllowSmartcard`	Lässt zu, dass SmartCard-Geräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
Allow Video Devices (Videogeräte zulassen) Eigenschaft: `AllowVideo`	Lässt zu, dass Videogeräte umgeleitet werden. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`true`** ist.
Disable Remote Configuration Download (Remote-Konfigurations-Download deaktivieren) Eigenschaft: `DisableRemoteConfig`	Deaktiviert die Verwendung der View Agent- oder Horizon Agent-Einstellungen beim Durchführen der USB-Gerätefilterung. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
Exclude All Devices (Alle Geräte ausschließen) Eigenschaft: `ExcludeAllDevices`	Schließt alle USB-Geräte von der Umleitung aus. Wenn für diese Einstellung **`true`** festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn für diese Einstellung **`false`** festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zu verhindern, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn Sie den Wert von `Exclude All Devices` in View Agent oder Horizon Agent auf **`true`** setzen und diese Einstellung an Horizon Client weitergegeben wird, überschreibt die View Agent- oder Horizon Agent-Einstellung die Horizon Client-Einstellung. Der Standardwert ist nicht definiert, was gleichbedeutend mit **`false`** ist.
Exclude Device Family (Gerätefamilie ausschließen) Eigenschaft: `ExcludeFamily`	Schließt Gerätefamilien von der Umleitung aus. Das Format der Einstellung lautet *Familienname_1*[`;`*Familienname_2*]... Beispiel: **`bluetooth;smart-card`** Der Standardwert ist nicht definiert. **Hinweis** Wenn Sie das automatische Gerätesplitten aktiviert haben, prüft Horizon die Gerätefamilie jeder Schnittstelle eines Composite USB-Gerätes, um zu entscheiden, welche Schnittstelle ausgeschlossen werden sollte. Wenn Sie das automatische Gerätesplitten deaktiviert haben, prüft Horizon die Gerätefamilie des gesamten Composite USB-Gerätes.
Exclude Vid/Pid Device (Vid/Pid-Gerät ausschließen) Eigenschaft: `ExcludeVidPid`	Schließt Geräte mit einer angegebenen Anbieter- oder Produkt-ID von der Umleitung aus. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (`*`) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0781_pid-****;vid-0561_pid-554c`** Der Standardwert ist nicht definiert.

Tabelle 4-4. Konfigurationseigenschaften für die USB-Umleitung (Fortsetzung)

Name und Eigenschaft der Richtlinie	Beschreibung
Exclude Path (Pfad ausschließen) Eigenschaft: `ExcludePath`	Schließt Geräte an angegebenen Hub- oder Portpfaden von der Umleitung aus. Das Format der Einstellung lautet `bus-`*x1*`[/`*y1*`]..._port-`*z1*`[;bus-`*x2*`[/`*y2*`]..._port-`*z2*`]...` Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** Der Standardwert ist nicht definiert.
Include Device Family (Gerätefamilie einschließen) Eigenschaft: `IncludeFamily`	Bestimmt Gerätefamilien, die umgeleitet werden können. Das Format der Einstellung lautet *Familienname_1*`[;`*Familienname_2*`]...` Beispiel: **`storage`** Der Standardwert ist nicht definiert.
Include Path (Pfad einschließen) Eigenschaft: `IncludePath`	Schließt Geräte an angegebenen Hub- oder Portpfaden in die Umleitung ein. Das Format der Einstellung lautet `bus-`*x1*`[/`*y1*`]..._port-`*z1*`[;bus-`*x2*`[/`*y2*`]..._port-`*z2*`]...` Bus- und Portnummern müssen im hexadezimalen Format angegeben werden. Sie können das Platzhalterzeichen nicht in Pfaden verwenden. Beispiel: **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** Der Standardwert ist nicht definiert.
Include Vid/Pid Device (Vid/Pid-Gerät einschließen) Eigenschaft: `IncludeVidPid`	Bestimmt Geräte mit einer angegebenen Anbieter- und Produkt-ID, die umgeleitet werden können. Das Format der Einstellung lautet `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (**`*`**) anstelle einzelner Ziffern in einer ID verwenden. Beispiel: **`vid-0561_pid-554c`** Der Standardwert ist nicht definiert.

USB-Gerätefamilien

Beim Erstellen von USB-Filterregeln für Horizon Client oder View Agent oder Horizon Agent können Sie eine bestimmte Familie angeben.

Hinweis Einige Geräte zeigen keine Gerätefamilie an.

Tabelle 4-5. USB-Gerätefamilien

Gerätefamilien-name	Beschreibung
`audio`	Ein Audioeingabe- oder Audioausgabegerät beliebigen Typs.
`audio-in`	Audioeingabegeräte, z. B. Mikrofone.
`audio-out`	Audioausgabegeräte, z. B. Lautsprecher und Kopfhörer.
`bluetooth`	Per Bluetooth verbundene Geräte.
`comm`	Kommunikationsgeräte wie Modems und kabelgebundene Netzwerkadapter.
`hid`	Eingabegeräte (Human Interface Devices) außer Tastaturen und Zeigegeräten.
`hid-bootable`	Eingabegeräte (Human Interface Devices), die beim Start verfügbar sind, außer Tastaturen und Zeigegeräte.
`imaging`	Bildverarbeitungsgeräte, z. B. Scanner.
`keyboard`	Tastaturgerät.
`mouse`	Zeigegerät, z. B. eine Maus.
`other`	Familie nicht angegeben.
`pda`	PDA (Personal Digital Assistant)

Tabelle 4-5. USB-Gerätefamilien (Fortsetzung)

Gerätefamilien-name	Beschreibung
`physical`	Force-Feedback-Geräte, z. B. Force-Feedback-Joysticks.
`printer`	Druckergeräte.
`security`	Sicherheitsgeräte, z. B. Fingerabdruckleser.
`smart-card`	SmartCard-Geräte.
`storage`	Massenspeichergeräte wie z. B. Flash-Laufwerke und externe Festplattenlaufwerke.
`unknown`	Familie nicht bekannt.
`vendor`	Geräte mit herstellerspezifischen Funktionen.
`video`	Videoeingabegeräte.
`wireless`	Drahtlose Netzwerkadapter.
`wusb`	Drahtlose USB-Geräte.

Aktivieren der Protokollierung für die USB-Umleitung

Zur Fehlerbehebung und Ermittlung der Produkt- und Hersteller-IDs verschiedener Geräte, die Sie an das Clientsystem anschließen, können Sie die USB-Protokolle verwenden.

Vorgehensweise

1 Öffnen Sie in einem Texteditor die Datei `config` im Verzeichnis `~/Library/Preferences/VMware Fusion/` auf Ihrem Mac-Clientsystem.

2 Fügen Sie zur Festlegung der Protokollierungsebene für die USB-Umleitung der Datei `config` den Parameter `view-usbd.logLevel` hinzu.

Beispiel:

```
#[or info, debug, error]. Info level by default.
view-usbd.logLevel=trace
```

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

Mit der Echtzeit-Audio/Video-Funktion können Sie die Webcam oder das Mikrofon Ihres lokalen Computers 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.

Informationen zur Einrichtung der Echtzeit-Audio/Video-Funktion sowie zur Konfiguration der Frame-Rate und der Bildauflösung in einem Remote-Desktop finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*. Informationen zum Konfigurieren dieser Einstellungen auf Clientsystemen finden Sie im VMware KB-Artikel *Festlegen von Frame-Raten und Auflösung für Echtzeit-Audio/Video auf Horizon View Clients* unter http://kb.vmware.com/kb/2053644.

Auf der Website http://labs.vmware.com/flings/real-time-audio-video-test-application können Sie eine Testanwendung herunterladen, mit der überprüft wird, ob die Echtzeit-Audio/Video-Funktion ordnungsgemäß installiert ist und fehlerfrei arbeitet. Diese Testanwendung ist als VMware-Fling verfügbar, weshalb kein technischer Support besteht.

In diesen Fällen können Sie Ihre Webcam verwenden

Wenn ein Horizon-Administrator die Echtzeit-Audio/Video-Funktion konfiguriert hat und Sie das PCoIP-Anzeigeprotokoll oder das VMware Blast-Anzeigeprotokoll verwenden, kann eine integrierte oder an Ihren lokalen Computer angeschlossene Webcam auf Ihrem Desktop verwendet werden. Sie können die Webcam in Konferenzanwendungen wie z. B. Skype, Webex oder Google Hangouts verwenden.

Bei der Einrichtung einer Anwendung wie Skype, Webex oder Google Hangouts auf Ihrem Remote-Desktop können Sie Ein- und Ausgabegeräte aus Menüs in der Anwendung auswählen. Für VM-Desktops können Sie das virtuelle VMware-Mikrofon und die virtuelle VMware-Webcam auswählen. Für veröffentlichte Desktops können Sie ein Remoteaudiogerät und die virtuelle VMware-Webcam auswählen.

Bei vielen Anwendungen kann diese Funktion ohne die Auswahl eines Eingabegeräts genutzt werden.

Wenn die Webcam zurzeit von Ihrem lokalen Computer genutzt wird, kann sie gleichzeitig vom Remote-Desktop verwendet werden. Genauso kann die Webcam vom lokalen Computer verwendet werden, wenn sie zurzeit vom Remote-Desktop genutzt wird.

Hinweis Wenn Sie eine USB-Webcam verwenden, verbinden Sie diese nicht über das Menü **Verbindung > USB** in Horizon Client. Dies würde dazu führen, dass die USB-Umleitung für das Gerät aktiviert wird und die Leistung für einen Videochat nicht ausreicht.

Wenn mehr als eine Webcam an Ihren lokalen Computer angeschlossen ist, können Sie eine bevorzugte Webcam konfigurieren, die auf Ihrem Remote-Desktop verwendet wird.

Auswählen eines Standardmikrofons auf einem Mac-Clientsystem

Wenn Sie auf Ihrem Clientsystem über mehrere Mikrofone verfügen, wird nur eines davon auf Ihrem Remote-Desktop verwendet. Zur Festlegung, welches Mikrofon standardmäßig auf dem Remote-Desktop verwendet werden soll, können Sie die „Systemeinstellungen“ auf Ihrem Clientsystem verwenden.

Mit der Echtzeit-Audio/Video-Funktion arbeiten Audioeingabe- und Audioausgabegeräte ohne Verwendung der USB-Umleitung ordnungsgemäß, und die erforderliche Netzwerkbandbreite wird erheblich verringert. Analoge Audioeingabegeräte werden ebenfalls unterstützt.

Dieses Verfahren beschreibt die Auswahl eines Mikrofons über die Benutzeroberfläche des Clientsystems. Administratoren können mithilfe der Mac-Standardwerte auch ein bevorzugtes Mikrofon konfigurieren. Siehe „Konfigurieren einer bevorzugten Webcam oder eines bevorzugten Mikrofons auf einem Mac-Clientsystem“, auf Seite 61.

Wichtig Wenn Sie ein USB-Mikrofon verwenden, verbinden Sie dieses nicht über das Menü **Verbindung > USB** in Horizon Client. In diesem Fall würde das Gerät über die USB-Umleitung umgeleitet, sodass die Echtzeit-Audio/Video-Funktion nicht genutzt werden kann.

Voraussetzungen

- Stellen Sie sicher, dass ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Stellen Sie sicher, dass das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll für Ihre Remote-Desktops verwendet wird.

Vorgehensweise

1. Wählen Sie auf Ihrem Clientsystem **Apple-Menü > Systemeinstellungen** und klicken Sie auf **Ton**.
2. Öffnen Sie den Eingabebereich der Toneinstellungen.
3. Wählen Sie das bevorzugte Mikrofon aus.

Wenn Sie das nächste Mal eine Verbindung zu einem Remote-Desktop herstellen und einen Anruf starten, verwendet der Desktop das von Ihnen auf dem Clientsystem ausgewählte Standardmikrofon.

Konfigurieren von Echtzeit-Audio/Video auf einem Mac-Client

Sie können Einstellungen für Echtzeit-Audio/Video mithilfe der Mac-Standardsystemwerte über die Befehlszeile konfigurieren. Mit den Standardsystemwerten können Sie benutzerdefinierte Mac-Standardwerte mithilfe von Terminal (`/Applications/Utilities/Terminal.app`) lesen, schreiben und löschen.

Mac-Standardwerte gehören zu Domänen. Domänen entsprechen in der Regel einzelnen Anwendungen. Die Domäne für die Echtzeit-Audio/Video-Funktion lautet com.vmware.rtav.

Syntax zur Konfiguration von Echtzeit-Audio/Video

Für die Konfiguration der Echtzeit-Audio/Video-Funktion können Sie die folgenden Befehle verwenden.

Tabelle 4-6. Befehlssyntax für die Konfiguration von Echtzeit-Audio/Video

Befehl	Beschreibung
`defaults write com.vmware.rtav scrWCamId "`*webcam-userid*`"`	Legt die bevorzugte Webcam für die Verwendung auf Remote-Desktops fest. Wenn dieser Wert nicht festgelegt ist, wird die Webcam automatisch durch die Systemauflistung ausgewählt. Sie können jede Webcam angeben, die an das Clientsystem angeschlossen (oder in dieses integriert) ist.
`defaults write com.vmware.rtav srcAudioInId "`*audio-device-userid*`"`	Legt das bevorzugte Mikrofon (Audioeingabegerät) für die Verwendung auf Remote-Desktops fest. Wenn dieser Wert nicht festgelegt ist, verwenden Remote-Desktops das Standard-Aufzeichnungsgerät auf dem Clientsystem. Sie können jedes Mikrofon angeben, das an das Clientsystem angeschlossen (oder in dieses integriert) ist.
`defaults write com.vmware.rtav srcWCamFrameWidth` *pixels*	Legt die Bildbreite fest. Hierfür wird standardmäßig ein hartcodierter Wert von 320 Pixeln verwendet. Die Bildbreite können Sie auf jeden Pixelwert ändern.
`defaults write com.vmware.rtav srcWCamFrameHeight` *pixels*	Legt die Bildhöhe fest. Hierfür wird standardmäßig ein hartcodierter Wert von 240 Pixeln verwendet. Die Bildhöhe können Sie auf jeden Pixelwert ändern.
`defaults write com.vmware.rtav srcWCamFrameRate` *fps*	Legt die Framerate fest. Standardmäßig wird der Wert 15 F/s verwendet. Die Framerate können Sie auf jeden Wert ändern.
`defaults write com.vmware.rtav LogLevel "`*level*`"`	Legt die Protokollierungsebene der Protokolldatei für Audio-Video in Echtzeit (`~/Library/Logs/VMware/vmware-RTAV-`*`pid`*`.log`) fest. Als Protokollierungsebene können Sie „trace“ oder „debug“ festlegen.
`defaults write com.vmware.rtav IsDisabled` *value*	Bestimmt, ob Echtzeit-Audio/Video aktiviert oder deaktiviert ist. Echtzeit-Audio/Video ist standardmäßig aktiviert. (Dieser Wert ist nicht aktiv.) Legen Sie „true“ fest, um Echtzeit-Audio/Video auf dem Client zu deaktivieren.
`defaults read com.vmware.rtav`	Zeigt Einstellungen für die Konfiguration von Echtzeit-Audio/Video an.
`defaults delete com.vmware.rtav` *setting*	Löscht eine Einstellung für die Konfiguration von Echtzeit-Audio/Video. Beispiel: `defaults delete com.vmware.rtav srcWCamFrameWidth`

Hinweis Sie können für die Framerate einen Wert zwischen 1 F/s und maximal 25 F/s sowie eine Auflösung von maximal 1920x1080 einstellen. Eine hohe Auflösung in Kombination mit einer schnellen Framerate wird möglicherweise nicht auf allen Geräten oder in allen Umgebungen unterstützt.

Konfigurieren einer bevorzugten Webcam oder eines bevorzugten Mikrofons auf einem Mac-Clientsystem

Wenn Sie die Echtzeit-Audio/Video-Funktion einsetzen und auf Ihrem Clientsystem über mehrere Webcams oder Mikrofone verfügen, kann nur eine Webcam oder ein Mikrofon auf Ihrem Remote-Desktop verwendet werden. Die bevorzugte Webcam und das bevorzugte Mikrofon legen Sie mithilfe der Mac-Standardwerte über die Befehlszeile fest.

Mit der Echtzeit-Audio/Video-Funktion arbeiten Webcams, Audioeingabe- und Audioausgabegeräte ohne USB-Umleitung ordnungsgemäß, und die erforderliche Netzwerkbandbreite wird erheblich verringert. Analoge Audioeingabegeräte werden ebenfalls unterstützt.

In den meisten Umgebungen muss kein bevorzugtes Mikrofon bzw. keine bevorzugte Webcam konfiguriert werden. Wenn Sie kein bevorzugtes Mikrofon festlegen, verwenden Remote-Desktops das standardmäßige Audiogerät, das in den Systemeinstellungen des Clientsystems festgelegt ist. Siehe

„Auswählen eines Standardmikrofons auf einem Mac-Clientsystem“, auf Seite 59. Wenn Sie keine bevorzugte Webcam konfigurieren, wählt der Remote-Desktop die Webcam anhand der Auflistung aus.

Voraussetzungen

- Stellen Sie beim Konfigurieren einer bevorzugten USB-Webcam sicher, dass die Webcam auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Stellen Sie beim Konfigurieren eines bevorzugten USB-Mikrofons oder eines sonstigen Mikrofontyps sicher, dass das Mikrofon auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Stellen Sie sicher, dass das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll für Ihre Remote-Desktops verwendet wird.

Vorgehensweise

1 Starten Sie auf Ihrem Mac-Clientsystem eine Webcam- oder Mikrofonanwendung, um eine Auflistung der Kamera- oder Audiogeräte in der Echtzeit-Audio/Video-Protokolldatei auszulösen.

   a Schließen Sie die Webcam oder das Audiogerät an.

   b Doppelklicken Sie im Ordner **Anwendungen** auf **VMware Horizon Client**, um Horizon Client zu starten.

   c Starten Sie einen Anruf und beenden Sie ihn dann.

2 Suchen Sie in der Echtzeit-Audio/Video-Protokolldatei nach Protokolleinträgen für die Webcam oder das Mikrofon.

   a Öffnen Sie die Echtzeit-Audio/Video-Protokolldatei in einem Text-Editor.

   Die Audio-Video-Protokolldatei in Echtzeit heißt `~/Library/Logs/VMware/vmware-RTAV-`*`pid`*`.log`, wobei *pid* die Prozess-ID der aktuellen Sitzung ist.

   b Suchen Sie in der Echtzeit-Audio/Video-Protokolldatei nach Einträgen für die angeschlossenen Webcams oder Mikrofone.

   Das folgende Beispiel veranschaulicht Webcam-Einträge in der Echtzeit-Audio/Video-Protokolldatei:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
1 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=FaceTime HD Camera (Built-in)   UserId=FaceTime HD Camera (Built-
in)#0xfa20000005ac8509   SystemId=0xfa20000005ac8509
```

Das folgende Beispiel veranschaulicht Mikrofon-Einträge in der Echtzeit-Audio/Video-Protokolldatei:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int AVCaptureEnumerateAudioDevi-
ces(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- 2 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- Index=255   Name=Built-in Microphone   UserId=Built-in Microphone#AppleHDAEngineInput:1B,
0,1,0:1   SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- Index=255   Name=Built-in Input   UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

3 Suchen Sie in der Echtzeit-Audio/Video-Protokolldatei nach der bevorzugten Webcam oder dem bevorzugten Mikrofon und notieren Sie sich die zugehörige Benutzer-ID.

   Die Benutzer-ID wird in der Protokolldatei nach der Zeichenfolge „UserId=“ aufgeführt. Beispielsweise lautet die Benutzer-ID der internen FaceTime-Kamera „FaceTime HD Camera (Built-in)“, und die Benutzer-ID des internen Mikrofons lautet „Built-in Microphone“.

4 Legen Sie in Terminal (`/Applications/Utilities/Terminal.app`) mithilfe des Befehls `defaults write` die bevorzugte Webcam bzw. das bevorzugte Mikrofon fest.

Option	Aktion
Bevorzugte Webcam festlegen	Geben Sie **`defaults write com.vmware.rtav srcWCamId "`*`Webcam-Benutzer-ID`*`"`** ein, wobei *Webcam-Benutzer-ID* für die Benutzer-ID der bevorzugten Webcam steht, die Sie anhand der Echtzeit-Audio/Video-Protokolldatei ermittelt haben. Beispiel: `defaults write com.vmware.rtav srcWCamId "HD Webcam C525”`
Bevorzugtes Mikrofon festlegen	Geben Sie **`defaults write com.vmware.rtav srcAudioInId "`*`Audiogerät-Benutzer-ID`*`"`**, ein, wobei *Audiogerät-Benutzer-ID* für die Benutzer-ID des bevorzugten Mikrofons steht, die Sie anhand der Echtzeit-Audio/Video-Protokolldatei ermittelt haben. Beispiel: `defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"`

5 (Optional) Überprüfen Sie mithilfe des Befehls `defaults read` Ihre Änderungen an der Echtzeit-Audio/Video-Funktion.

   Beispiel: **`defaults read com.vmware.rtav`**

   Mit diesem Befehl werden alle Einstellungen für Echtzeit-Audio/Video aufgeführt.

Wenn Sie das nächste Mal eine Verbindung zu einem Remote-Desktop herstellen und einen Anruf starten, verwendet der Desktop soweit verfügbar die bevorzugte Webcam bzw. das bevorzugte Mikrofon, die bzw. das Sie konfiguriert haben. Falls die bevorzugte Webcam oder das bevorzugte Mikrofon nicht verfügbar ist, kann der Remote-Desktop eine andere verfügbare Webcam oder ein anderes verfügbares Mikrofon verwenden.

Kopieren und Einfügen von Text und Bildern

Sie können standardmäßig Text von Ihrem Clientsystem auf einen Remote-Desktop oder in eine Remoteanwendung kopieren und einfügen. Wenn ein Horizon-Administrator die Funktion aktiviert, können Sie auch Text zwischen einem Remote-Desktop oder einer Remoteanwendung und Ihrem Clientsystem oder zwischen zwei Remote-Desktops oder -anwendungen kopieren und einfügen.

Zu den unterstützten Dateiformaten gehören Text, Bilder und RTF (Rich Text Format). Hierfür gelten allerdings einige Einschränkungen.

Horizon-Administratoren haben die Möglichkeit, das Kopieren/Einfügen durch entsprechende Konfiguration der Gruppenrichtlinieneinstellungen zu aktivieren, die Horizon Agent zugeordnet sind. Je nach installierter Version von Horizon Server und Agent können Administratoren auch mit Gruppenrichtlinien Zwischenablageformate für das Kopieren/Einfügen beschränken oder das Kopieren/Einfügen auf Remote-Desktops mithilfe von intelligenten Richtlinien steuern. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Wenn Sie formatierten Text kopieren, handelt es sich bei den Daten teilweise um Text und teilweise um Formatierungsinformationen. Wenn Sie daher eine große Menge an formatiertem Text oder Text und ein Bild kopieren, kann es beim Einfügen dazu kommen, dass Sie den einfachen Text ganz oder teilweise sehen, nicht aber die Formatierung oder das Bild. Dies liegt daran, dass die drei Arten von Daten separat gespeichert werden können. Je nach Art des Dokuments, von dem aus Sie kopieren, können Bilder möglicherweise als Bilder oder als RTF-Daten gespeichert werden.

Beträgt die Gesamtmenge von Text und RTF weniger als die maximale Größe der Zwischenablage, wird der formatierte Text eingefügt. Es ist häufig der Fall, dass die RTF-Daten nicht gekürzt werden können, sodass die RTF-Daten verworfen und nur der reine Text eingefügt wird, sollten Text und Formatierung zusammen mehr als die maximale Größe der Zwischenablage umfassen.

Sollten Sie nicht in der Lage sein, den gesamten formatierten Text und die von Ihnen ausgewählten Bilder einzufügen, versuchen Sie geringere Teilmengen zu speichern und einzufügen.

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

Konfigurieren der Größe des Zwischenablagespeichers für den Client

Sie können die Größe des Zwischenablagespeichers für den Client durch Erstellen einer Datei namens `config` im Verzeichnis `%HomeDir%/Library/Preferences/VMware Horizon View/` auf Ihrem Mac-Client-System konfigurieren.

Um die Größe des Zwischenablagespeichers für den Client festzulegen, fügen Sie der Datei `config` die nachfolgend aufgeführten Parameter hinzu.

```
mksvchan.clipboardSize=Wert
```

Wert stellt die Größe des Zwischenablagespeichers für den Client in Kilobytes (KB) dar. Die zulässigen Eingaben für dieses Feld reichen von 512 KB (Minimum) bis 16384 KB (Maximum). Wenn Sie 0 oder keinen Wert eingeben, gilt die Standardgröße des Zwischenablagespeichers für den Client von 8192 KB (8 MB).

Ein hoher Wert für die Größe des Zwischenablagespeichers kann sich je nach verwendetem Netzwerk negativ auf die Leistung auswirken. VMware empfiehlt für die maximale Größe des Zwischenablagespeichers einen Wert von 16 MB.

Verwenden von Remoteanwendungen

Sie können in Remoteanwendungen viele Mac-Funktionen verwenden.

- Wenn Sie eine Remoteanwendung ausführen, wird ihr Symbol im Dock angezeigt. Sie können eine minimierte Remoteanwendung maximieren, indem Sie auf ihr Symbol im Dock klicken.
- Über das Kontextmenü einer Remoteanwendung können Sie sie im Dock behalten, sie öffnen und beenden. Wenn Sie **Im Dock behalten** auswählen, verbleibt das Symbol der Remoteanwendung auch dann im Dock, wenn Sie alle Anwendungsfenster schließen.
- Sie können eine Remoteanwendung öffnen, indem Sie auf ihr Symbol im Dock klicken.
- Sie können lokale Dateien in Remoteanwendungen öffnen und Remoteanwendungen aus dem Anwendungsordner auf Ihrem Clientsystem ausführen. Erläuterungen zu diesen Funktionen finden Sie unter „Freigegebener Zugriff auf lokale Ordner und Laufwerke“, auf Seite 31.

- Blinkende Windows-Taskleistenelemente werden an Horizon Client weitergeleitet. Wenn es sich bei der Remoteanwendung beispielsweise um einen IM-Client handelt und Sie eine neue Nachricht erhalten, wird ein blinkender roter Punkt als Symbol für den IM-Client im Dock angezeigt.
- Sie können über die Menüleiste die Spracheingabe starten und eine Remoteanwendung minimieren oder vergrößern.
- Sie können mit der Funktion „Exposé“ geöffnete Remoteanwendungen anzeigen und durch Drücken von Befehl+Tabulator zwischen geöffneten Remoteanwendungen wechseln.
- Sie können Mac-Standard-Tastenkombinationen zum Interagieren mit Remoteanwendungen verwenden. Beispielsweise können Sie die Befehlstaste+W drücken, um ein einzelnes Anwendungsfenster zu schließen, und die Befehlstaste+S, um die aktuelle Datei zu speichern. Sie können auch mit Mac-Standard-Tastenkombinationen Text zwischen Ihren Mac-Anwendungen und Remoteanwendungen kopieren, ausschneiden und einfügen. Sie können die Tastenkombinationszuordnungen anpassen. Siehe „Konfigurieren von Tastenkombinationszuordnungen“, auf Seite 35.
- Wenn eine Remoteanwendung ein Element in der Windows-Taskleiste erstellt, wird dieses Element auf Ihrem Mac-Clientsystem im Infobereich auf der Menüleiste angezeigt. Sie können auf Ihrem Mac mit diesem Element im Infobereich genau so wie über die Taskleiste auf einem Windows-System interagieren.

Hinweis Wenn Sie auf Ihrem Mac erneut auf ein umgeleitetes Taskleistenelement im Infobereich klicken, wird das Kontextmenü nicht ausgeblendet.

Verwenden eines lokalen IMEs mit Remoteanwendungen

Wenn Sie nicht englische Tastaturen und Gebietsschemata verwenden, können Sie einen auf Ihrem lokalen System installierten IME (Eingabemethoden-Editor) dazu nutzen, nicht englische Zeichen an eine gehostete Remoteanwendung zu senden.

Sie haben auch die Möglichkeit, mit dem Menü **Eingabe** in der Menüleiste Ihres Mac oder mit Tastenkombinationen zu einem anderen IME zu wechseln. Es besteht keine Notwendigkeit, einen IME auf dem Remote-RDS-Host zu installieren.

Hinweis Auf einem Mac wird ein IME als eine Eingabequelle behandelt.

Bei Deaktivierung dieser Funktion wird der lokale IME verwendet. Sofern auf dem RDS-Host, auf dem die Remoteanwendung installiert ist, ein IME installiert und konfiguriert ist, wird dieser Remote-IME ignoriert.

Voraussetzungen

- Stellen Sie sicher, dass einer oder mehrere IMEs auf dem Clientsystem installiert sind.
- Stellen Sie sicher, dass View Agent 6.1.1 oder höher oder Horizon Agent 7.0 oder höher auf dem RDS-Host installiert ist.

Vorgehensweise

1. Halten Sie im Fenster für die Desktop- und Anwendungsauswahl von Horizon Client die Steuerungstaste gedrückt, klicken Sie auf eine Remoteanwendung und wählen Sie **Einstellungen** aus.
2. Aktivieren Sie im anschließend angezeigten Bereich „Remoteanwendungen“ das Kontrollkästchen **Den lokalen IME auf gehostete Anwendungen erweitern**.
3. Verwenden Sie den lokalen IME so, wie Sie jede andere lokal installierte Anwendung verwenden würden.

Das Menü **Eingabe** erscheint in der Menüleiste auf Ihrem Mac-Clientsystem. Wenn Sie eine Remoteanwendung verwenden, können Sie mithilfe des Menüs **Eingabe** oder von Tastenkombinationen zu einer anderen Sprache oder zu einem anderen IME wechseln. Tastenkombinationen für bestimmte Aktionen wie Befehlstaste-C zum Kopieren oder Befehlstaste-V zum Einfügen funktionieren weiterhin korrekt.

Speichern von Dokumenten in einer Remoteanwendung

Sie können mit bestimmten Remoteanwendungen, z. B. Microsoft Word oder WordPad, Dokumente erstellen und speichern. Der Speicherort für diese Dokumente hängt von der Netzwerkumgebung Ihres Unternehmens ab. Beispielsweise können die Dokumente in einer Basisfreigabe gespeichert werden, die auf Ihrem lokalen Computer gemountet wird.

Administratoren können anhand einer ADMX-Vorlagendatei eine Gruppenrichtlinie zur Angabe des Speicherorts für Dokumente einrichten. Hierbei handelt es sich um die Richtlinie **Basisverzeichnis für Remote-Desktop-Dienste-Benutzer festlegen**. Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Drucken über einen Remote-Desktop oder über eine Remoteanwendung

Sie können von einem Remote-Desktop aus Dokumente auf einem virtuellen Drucker oder einem USB-Drucker ausdrucken, der mit Ihrem Clientcomputer verbunden ist. Die virtuelle Druckfunktion und das Drucken mit USB-Umleitung können ohne Konflikte gemeinsam eingesetzt werden.

Sie können die virtuelle Druckfunktion mit den folgenden Typen von Remote-Desktops und -anwendungen verwenden:

- Remote-Desktops, auf denen Windows Server-Betriebssysteme ausgeführt werden
- Sitzungsbasierte Desktops (auf RDS-Hosts von virtuellen Maschinen)
- Gehostete Remoteanwendungen

Aktivieren der virtuellen Druckfunktion in Horizon Client

Wenn Sie das VMware Blast-Anzeigeprotokoll oder das PCoIP-Anzeigeprotokoll verwenden, können Sie für Ihren lokalen Computer konfigurierte Drucker von einem Remote-Desktop aus oder aus einer Remoteanwendung heraus verwenden. Um die virtuelle Druckfunktion verwenden zu können, müssen Sie keine Druckertreiber auf dem Remote-Desktop installieren.

Sie können den virtuellen Druck beim ersten Start von Horizon Client aktivieren. Klicken Sie auf **Weiter**, wenn Horizon Client Sie zum Starten der USB- und Druckdienste für Remote-Desktops auffordert, und geben Sie Ihre Systemanmeldeinformationen ein.

Wenn Sie den virtuellen Druck nicht beim ersten Start von Horizon Client aktivieren, können Sie das Menü **Verbindung** dazu verwenden, die Funktion für den virtuellen Druck später zu aktivieren.

- Zum Aktivieren der virtuellen Druckfunktion vor der Verbindungsherstellung mit einem Remote-Desktop oder einer Remoteanwendung wählen Sie **Verbindung > Druckdienste starten** im Menü **VMware Horizon Client** aus. Klicken Sie auf **Fortfahren** und geben Sie Ihre Systemanmeldedaten ein.
- Zum Aktivieren der virtuellen Druckfunktion nach der Verbindungsherstellung mit einem Remote-Desktop wählen Sie **Verbindung > Druckdienste starten** im Menü **VMware Horizon Client** aus. Klicken Sie auf **Fortfahren**, geben Sie Ihre Systemanmeldeinformationen ein und stellen Sie erneut eine Verbindung mit dem Desktop oder der Anwendung her. Wenn Sie die erneute Verbindungsherstellung abbrechen, können Sie **Verbindung > Druckfunktion aktivieren** auswählen. Horizon Client fordert Sie daraufhin zur erneuten Verbindungsherstellung auf.

Wenn die Funktion für den virtuellen Druck aktiviert ist, wird im Menü **Verbindung** der Eintrag **Druckfunktion aktiviert** angezeigt.

Hinweis Wenn Sie Horizon Client auf einem Mac installieren, auf dem zuvor VMware Fusion gestartet wurde, werden die Druckdienste bereits beim Start von Horizon Client aktiviert. Dieses Verhalten tritt auf, da VMware Fusion und Horizon Client einige derselben Dateien verwenden, um das virtuelle Drucken zu implementieren.

Festlegen von Voreinstellungen für die virtuelle Druckfunktion auf einem Remote-Desktop

Die virtuelle Druckfunktion ermöglicht Endbenutzern das Verwenden von lokalen oder Netzwerkdruckern auf einem Remote-Desktop, ohne dass im Remote-Desktop zusätzliche Druckertreiber installiert werden müssen. Für jeden Drucker, der über diese Funktion zur Verfügung steht, können Sie Voreinstellungen für Datenkomprimierung, Druckqualität, doppelseitigen Druck, Farbe usw. festlegen.

Nachdem dem lokalen Computer ein Drucker hinzugefügt wurde, fügt Horizon Client diesen Drucker der Liste der verfügbaren Drucker auf dem Remote-Desktop hinzu. Keine weitere Konfiguration ist erforderlich. Benutzer mit Administratorrechten können weiterhin Druckertreiber auf dem Remote-Desktop installieren, ohne einen Konflikt mit der virtuellen Druckfunktion zu verursachen.

Wichtig Diese Funktion steht für die folgenden Druckertypen nicht zur Verfügung:

- USB-Drucker, die die USB-Umleitungsfunktion zur Verbindung mit einem virtuellen USB-Port im Remote-Desktop verwenden

  Sie müssen den USB-Drucker im Remote-Desktop trennen, um die virtuelle Druckfunktion verwenden zu können.

- Die Windows-Funktion für die Ausgabe in einer Datei

  Das Kontrollkästchen **Ausgabe in Datei** im Dialogfeld „Drucken“ kann nicht ausgewählt werden. Ein Druckertreiber, über den eine Datei erstellt wird, kann verwendet werden. Beispielsweise können Sie einen PDF-Writer zum Drucken einer PDF-Datei verwenden.

Dieses Verfahren beschreibt die Schritte auf einem Remote-Desktop mit einem Windows 7- oder Windows 8.x-Betriebssystem (Desktop). Die Vorgehensweise ähnelt derjenigen für Windows Server 2008 und Windows Server 2012, ist aber nicht identisch.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Druckfunktion des Agenten auf dem Remote-Desktop installiert ist. Stellen Sie sicher, dass im Dateisystem des Remote-Desktops der folgende Ordner vorhanden ist: `C:\Program–me\Common Files\ThinPrint`.

Zur Anwendung der virtuellen Druckfunktion muss diese in Horizon Administrator für den Remote-Desktop aktiviert werden. Diese Aufgabe beinhaltet die Aktivierung der Option **Virtueller Druck** im Agenteninstallationsprogramm. Außerdem können Richtlinien für das Verhalten der virtuellen Druckfunktion eingerichtet werden. Weitere Informationen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Vorgehensweise

1 Klicken Sie auf einem Remote-Desktop unter Windows 7 oder Windows 8.x auf **Start > Geräte und Drucker**.

2 Klicken Sie im Fenster „Geräte und Drucker“ mit der rechten Maustaste auf den Standarddrucker und wählen Sie aus dem Kontextmenü **Druckereigenschaften** und dann den Drucker aus.

   Virtuelle Drucker werden auf Einzelplatz-Desktops mit einer virtuellen Maschine in der Form <*Druckername*> und auf veröffentlichten Desktops von RDS-Hosts in der Form <*Druckername*>(<*Sitzungs_ID*>) angezeigt, wenn View Agent 6.2 oder höher oder Horizon Agent 7.0 oder höher installiert ist. Wenn View Agent 6.1 oder früher im Remote-Desktop installiert ist, werden virtuelle Drucker als <*printer_name*>#:<*number*> angezeigt.

3 Klicken Sie im Fenster mit den Druckereigenschaften auf die Registerkarte **Geräteeinstellungen** und geben Sie die zu verwendenden Einstellungen an.

4 Klicken Sie auf der Registerkarte **Allgemein** auf **Einstellungen** und geben Sie die zu verwendenden Einstellungen an.

5 Klicken Sie im Dialogfeld mit den Druckeinstellungen auf die verschiedenen Registerkarten und geben Sie an, welche Einstellungen verwendet werden sollen.

   Für die erweiterte Einstellung **Seitenanpassung** empfiehlt VMware, die Standardeinstellungen beizubehalten.

6 Klicken Sie auf **OK**.

Verwenden von USB-Druckern

In einer Horizon-Umgebung können virtuelle Drucker und umgeleitete USB-Drucker konfliktfrei zusammen eingesetzt werden.

Ein USB-Drucker ist ein Drucker, der an einen USB-Port auf dem lokalen Clientsystem angeschlossen ist. Zum Senden von Druckaufträgen an einen USB-Drucker können Sie entweder die USB-Umleitungsfunktion oder die virtuelle Druckfunktion verwenden. Der USB-Druck ist gelegentlich schneller als der virtuelle Druck, abhängig von den Netzwerkbedingungen.

- Sie können die USB-Umleitungsfunktion zum Anschließen eines USB-Druckers an einen virtuellen USB-Port auf dem Remote-Desktop verwenden, sofern die erforderlichen Treiber auf dem Remote-Desktop installiert sind.

  Wenn Sie diese Umleitungsfunktion verwenden, ist der Drucker nicht länger logisch an den physischen USB-Port auf dem Client angeschlossen. Aus diesem Grund wird der USB-Drucker nicht mehr in der Liste der lokalen Drucker angezeigt. Dies bedeutet auch, dass Sie über den USB-Drucker auf dem Remote-Desktop drucken können, nicht jedoch über die lokale Clientmaschine.

  Auf dem Remote-Desktop werden umgeleitete USB-Drucker als <*Druckername*> angezeigt.

  Informationen zur Verbindungsherstellung mit einem USB-Drucker finden Sie unter „Verbinden von USB-Geräten“, auf Seite 50.

- Auf einigen Clients können Sie alternativ die virtuelle Druckfunktion nutzen, um Druckaufträge an einen USB-Drucker zu senden. Wenn Sie die virtuelle Druckfunktion verwenden, können Sie sowohl über den Remote-Desktop als auch über den lokalen Client auf dem USB-Drucker drucken, und es ist nicht erforderlich, Druckertreiber auf dem Remote-Desktop zu installieren.

PCoIP-Client-Bildcache

Bei der PCoIP-Client-Bildzwischenspeicherung wird der Bildinhalt auf dem Client gespeichert, um erneute Übertragungen zu vermeiden. Durch diese Funktion wird die Bandbreitenauslastung reduziert.

Der PCoIP-Bildcache erfasst die räumliche sowie zeitliche Redundanz. Wenn Sie beispielsweise in einem PDF-Dokument einen Bildlauf nach unten durchführen, wird unten im Fenster neuer Inhalt angezeigt, während oben im Fenster der älteste Inhalt nicht mehr angezeigt wird. Der restliche Inhalt bleibt unverändert und wird nach oben verschoben. Der PCoIP-Bildcache kann räumliche und zeitliche Redundanz erkennen.

Da es sich während des Bildlaufs bei den an das Client-Gerät gesendeten Anzeigeinformationen in erster Linie um eine Abfolge von Cache-Indizes handelt, lassen sich durch die Verwendung eines Bildcaches deutliche Bandbreiteneinsparungen erzielen. Dieser effiziente Bildlauf hat sowohl bei LAN- als auch WAN-Verbindungen Vorteile.

- Bei LAN-Verbindungen mit relativ uneingeschränkter Bandbreite führt die clientseitige Bildzwischenspeicherung zu deutlichen Bandbreiteneinsparungen.
- Um bei WAN-Verbindungen innerhalb der Bandbreiteneinschränkungen zu bleiben, nimmt die Bildlaufleistung ohne clientseitige Zwischenspeicherung ab. Bei WAN-Verbindungen führt die clientseitige Zwischenspeicherung zu einer Einsparung von Bandbreite und stellt einen reibungslosen, äußerst schnellen Bildlauf sicher.

Mithilfe der clientseitigen Zwischenspeicherung speichert der Client Teile der Anzeige, die zuvor übertragen wurden. Die Cachegröße beträgt 250 MB.

Fehlerbehebung für Horizon Client 5

Sie können die meisten Probleme mit Horizon Client lösen, indem Sie den Desktop neu starten oder zurücksetzen oder die VMware Horizon Client-Anwendung neu installieren.

Dieses Kapitel behandelt die folgenden Themen:

Neustarten eines Remote-Desktops

Eventuell muss ein Remote-Desktop neu gestartet werden, wenn das Desktop-Betriebssystem nicht mehr reagiert. Der Neustart eines Remote-Desktops entspricht dem Neustart des Windows-Betriebssystems. In der Regel werden Sie dabei vom Desktop-Betriebssystem aufgefordert, alle nicht gespeicherten Daten zu speichern, bevor der Neustart erfolgt.

Sie können einen Remote-Desktop nur dann neu starten, wenn ein Horizon-Administrator die Funktion zum Neustart eines Desktops für den Desktop aktiviert hat.

Informationen zur Aktivierung der Funktion zum Neustart eines Desktops finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Vorgehensweise

- Wählen Sie im Fenster für die Desktop- und Anwendungsauswahl den Namen des Remote-Desktops aus, halten Sie die Strg-Taste gedrückt und klicken Sie und wählen Sie **Neu starten** aus dem Kontextmenü aus.

Das Betriebssystem im Remote-Desktop wird neu gestartet und Horizon Client wird getrennt bzw. vom Desktop abgemeldet.

Weiter

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

Wenn das Problem durch den Neustart des Remote-Desktops nicht behoben werden kann, müssen Sie den Remote-Desktop eventuell zurücksetzen. Siehe „Zurücksetzen eines Remote-Desktops oder von Remoteanwendungen“, auf Seite 70.

Zurücksetzen eines Remote-Desktops oder von Remoteanwendungen

Sie müssen einen Remote-Desktop eventuell zurücksetzen, wenn das Betriebssystem nicht mehr reagiert und der Neustart des Remote-Desktops das Problem nicht löst. Durch das Zurücksetzen von Remoteanwendungen werden alle geöffneten Anwendungen beendet.

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 geschlossen und nicht gespeichert.

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

Sie können einen Remote-Desktop nur zurücksetzen, wenn ein Horizon-Administrator die Funktion zum Zurücksetzen eines Desktops für den Desktop aktiviert hat.

Informationen zur Aktivierung der Funktion zum Zurücksetzen eines Desktops finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Vorgehensweise

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

Option	Aktion
Einen Remote-Desktop im Fenster für die Desktop- und Anwendungsauswahl zurücksetzen	Wählen Sie den Namen des Remote-Desktops aus, halten Sie die Strg-Taste gedrückt und klicken Sie und wählen Sie **Zurücksetzen** aus dem Kontextmenü aus.
Remoteanwendungen im Fenster für die Desktop- und Anwendungsauswahl zurücksetzen	Klicken Sie in der oberen rechten Ecke des Fensters auf die Schaltfläche **Einstellungen** (Zahnradsymbol), wählen Sie im linken Fensterbereich **Anwendungen** aus, klicken Sie auf **Zurücksetzen** und dann auf **Weiter**.

Wenn Sie einen Remote-Desktop zurücksetzen, wird das Betriebssystem im Remote-Desktop neu gestartet und Horizon Client getrennt bzw. vom Desktop abgemeldet. Wenn Sie Remoteanwendungen zurücksetzen, werden diese beendet.

Weiter

Warten Sie eine Weile, bis das System gestartet wurde, und versuchen Sie anschließend erneut, eine Verbindung mit dem Remote-Desktop oder der Remoteanwendung herzustellen.

Deinstallieren von Horizon Client

Manchmal können Sie Probleme mit Horizon Client einfach dadurch beheben, dass Sie die Horizon Client-Anwendung deinstallieren und anschließend neu installieren.

Die Vorgehensweise beim Deinstallieren von Horizon Client entspricht der Vorgehensweise bei der Deinstallation anderer Anwendungen.

Ziehen Sie die **VMware Horizon Client**-Anwendung vom Ordner **Anwendungen** zum **Papierkorb** und leeren Sie diesen.

Nachdem Sie die Deinstallation durchgeführt haben, können Sie die Anwendung von neuem installieren.

Siehe „Installieren von Horizon Client auf einem Mac“, auf Seite 13.

Herstellen einer Verbindung mit einem Server im Workspace ONE -Modus

Wenn Sie mit Horizon Client keine direkte Verbindung mit einem Server herstellen können oder wenn Ihre Desktop- und Anwendungsberechtigungen in Horizon Client nicht angezeigt werden, kann eventuell der Workspace ONE-Modus auf dem Server aktiviert werden.

Problem

- Wenn Sie versuchen, eine direkte Verbindung mit dem Server über Horizon Client herzustellen, werden Sie von Horizon Client zum Workspace ONE-Portal umgeleitet.
- Wenn Sie einen Desktop oder eine Anwendung über einen URI oder eine Verknüpfung öffnen oder wenn Sie eine lokale Datei über die Dateiverknüpfung öffnen, leitet die Anforderung Sie zum Workspace ONE-Portal zur Authentifizierung weiter.
- Nach dem Öffnen eines Desktops oder einer Anwendung über Workspace ONE und dem Start von Horizon Client werden andere berechtigte Remote-Desktops oder -anwendungen in Horizon Client nicht angezeigt oder können nicht geöffnet werden.

Ursache

Ab Horizon 7 Version 7.2 hat ein Administrator die Möglichkeit, den Workspace ONE-Modus auf einer Verbindungsserver-Instanz zu aktivieren. Dies ist das Standardverhalten, wenn der Workspace ONE-Modus auf einer Verbindungsserver-Instanz aktiviert ist.

Lösung

Verwenden Sie Workspace ONE, um eine Verbindung mit einem Workspace ONE-aktivierten Server herzustellen und um auf Ihre Remote-Desktops und -anwendungen zuzugreifen.

Index