# Verwaltung von Horizon Cloud für gehostete Infrastruktur

VMware Horizon Cloud Service
Horizon Cloud with Hosted Infrastructure 17.2

vmware®

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

https://docs.vmware.com/de/

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

# Informationen zur Verwaltung von Horizon Cloud für gehostete Infrastruktur

1

Dieses Handbuch enthält Informationen zur Erstellung, Bereitstellung und Verwaltung virtueller Desktops und Anwendungen mithilfe von Horizon Cloud.

## Zielgruppe

Dieses Dokument ist für erfahrene IT-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und den Vorgängen von Datencentern vertraut sind.

## VMware Technical Publications – Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter http://www.vmware.com/support/pubs.

# Horizon Cloud-Verwaltungskonsole 2

Die Horizon Cloud-Verwaltungskonsole ist die Schnittstelle zur Mandantenverwaltung für Horizon Cloud.

Die Themen in diesem Abschnitt bieten allgemeine Informationen zur Verwaltungskonsole.

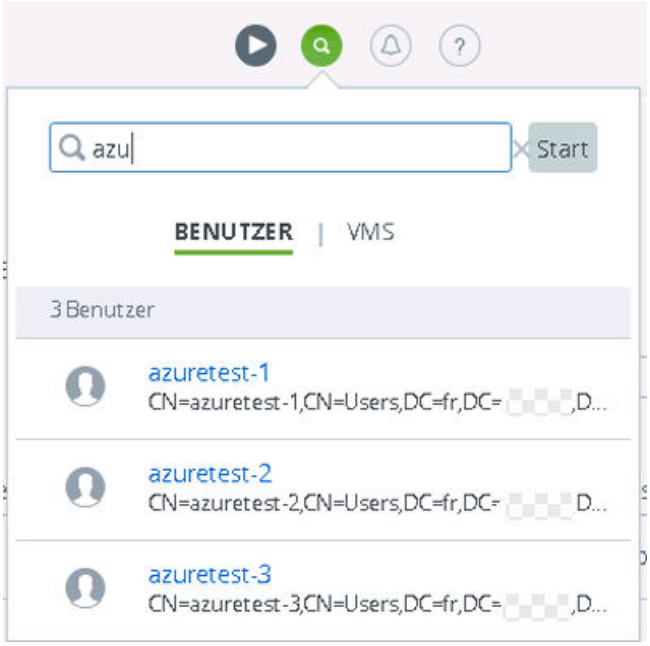
Dieses Kapitel behandelt die folgenden Themen:



## Verwenden der Suchfunktion der Konsole

Verwenden Sie die Suchfunktion der Horizon Cloud-Verwaltungskonsole, um Ihre Umgebung nach einem bestimmten Benutzer oder einer bestimmten virtuellen Maschine (VM) anhand des Namens zu durchsuchen.

Öffnen Sie das Suchfeld, indem Sie auf das Lupensymbol () oben in der Verwaltungskonsole klicken. Anschließend können Sie auswählen, ob Benutzer oder VMs durchsucht werden sollen. Wenn Sie mindestens drei (3) Zeichen in das Suchfeld eingegeben haben, werden die Namen, die mit diesen Zeichen beginnen, angezeigt. Sie können weitere Zeichen eingeben, um die Ergebnisse einzugrenzen.



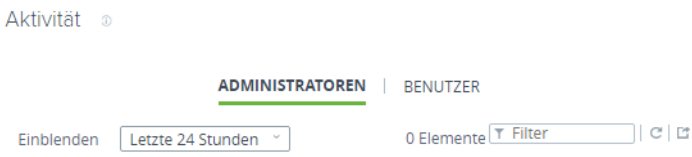

**Hinweis** Beim Durchsuchen der VMs können Sie nach RDS-Server-VMs in Farmen und nach VDI-Desktop-VMs suchen.

Wenn der gesuchte Benutzer bzw. die gesuchte VM angezeigt wird, klicken Sie auf das Ergebnis, um weitere Informationen zur VM bzw. zum Benutzer zu erhalten. Welcher Bildschirm angezeigt wird, hängt davon ab, ob Sie auf eine VM oder einen Benutzer geklickt haben:

- Für einen Benutzer wird die Karte des Benutzers angezeigt. Weitere Informationen finden Sie unter Die Benutzerkarte in der Horizon Cloud-Verwaltungskonsole.
- Für eine VM wird ein Bildschirm angezeigt, auf der Sie die VM sehen können. Wenn Sie in der Ergebnisliste beispielsweise auf VM klicken, bei der es sich um eine RDS-Server-VM in einer Farm handelt, wird die Registerkarte „Server“ der Detailseite dieser Farm angezeigt.

## Verwenden des Filterfelds in der Verwaltungskonsole

Bestimmte Seiten in der Horizon Cloud-Verwaltungskonsole enthalten ein Filterfeld zum Filtern der Informationen, die auf den Seiten angezeigt werden.



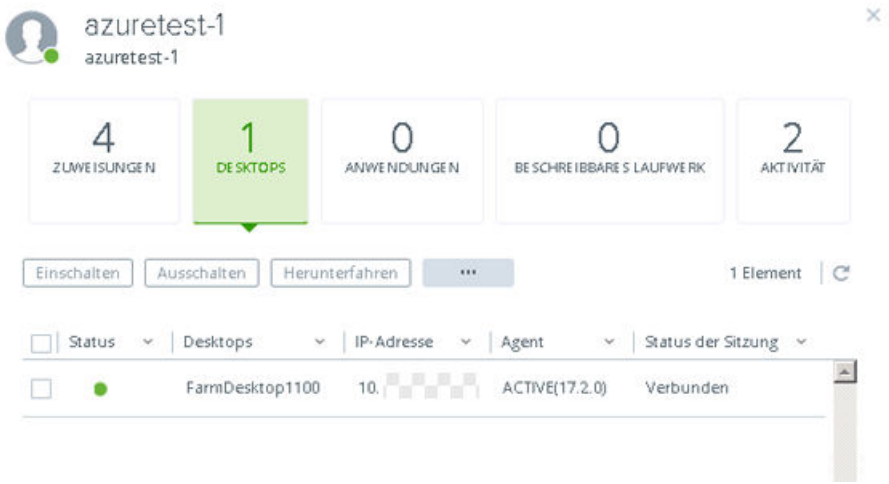
Wenn eine Seite ein Filterfeld enthält und Sie Zeichen in das Feld eingeben, wird nur die Teilmenge der Datensätze angezeigt, die Zeichen gemäß diesem Muster enthalten.

**Hinweis** Der Abgleich des Musters und das Filtern der auf der Seite angezeigten Datensätze wird gestartet, sobald Sie drei (3) Zeichen in das Feld „Filter“ eingegeben haben.

# Die Benutzerkarte in der Horizon Cloud - Verwaltungskonsole

Verwenden Sie die Benutzerkartenfunktion der Horizon Cloud-Verwaltungskonsole als Dashboard, um mit den Ressourcen eines bestimmten Benutzers (z. B. den Zuweisungen des Benutzers) zu arbeiten.

Verwenden Sie die Suchfunktion der Verwaltungskonsole, um die Karte für einen bestimmten Benutzer anzuzeigen. Weitere Informationen zur Suche nach einem Benutzer finden Sie unter Verwenden der Suchfunktion der Konsole. Wenn Sie in den Suchergebnissen auf einen Benutzer klicken, wird die Karte des Benutzers angezeigt.




Verwenden Sie die Registerkarten am oberen Rand der Benutzerkarte, um mit den Objekten in Ihrer Umgebung zu arbeiten, die mit dem Benutzer zusammenhängen.

| Registerkarten für die Benutzerkarte | Beschreibung |
|---|---|
| **Zuweisungen** | Listet Zuweisungen des Benutzers auf.<br>**Hinweis** Wenn ein Benutzer über eine Berechtigung für eine dedizierte VDI-Desktop-Zuweisung verfügt, den Desktop aber bisher noch nicht gestartet hat, wird diese Zuweisung auf der Registerkarte **Zuweisungen** angezeigt. Nach dem ersten Start des Desktops durch den Benutzer wird diese dann aus der Liste auf der Registerkarte **Zuweisungen** entfernt und auf der Registerkarte **Desktops** angezeigt. |
| **Desktops** | Listet die aktiven Desktop-Sitzungen des Benutzers auf.<br>Wenn bei einer dedizierten VDI-Desktop-Zuweisung der Benutzer den berechtigten dedizierten VDI-Desktop zum ersten Mal startet, wird der Desktop diesem Benutzer dauerhaft zugewiesen. Nach der ersten Verwendung enthält die Registerkarte **Desktops** immer die berechtigten dedizierten VDI-Desktops des Benutzers, auch wenn der Benutzer nicht über eine aktive Sitzung für diese Desktops verfügt. |

| Registerkarten für die Benutzerkarte | Beschreibung |
|---|---|
| **Anwendungen** | Listen die berechtigten nativen und Remoteanwendungen des Benutzers auf. |
| **Beschreibbares Laufwerk** | Listet die berechtigten beschreibbaren Laufwerke des Benutzers auf. |
| **Aktivität** | Zeigt die Aktivität des Benutzers für ausgewählte Zeiträume an. |

# In der Verwaltungskonsole verwendete Begriffe

Die Horizon Cloud-Verwaltungskonsole ersetzt das Enterprise Center. Einige in der Benutzeroberfläche verwendeten Begriffe unterscheiden sich dabei.

In der folgenden Tabelle werden einige Enterprise Center-Begriffe und ihre Entsprechungen in der Horizon Cloud-Verwaltungskonsole aufgeführt.

| Enterprise Center | Horizon Cloud-Verwaltungskonsole |
|---|---|
| Desktop-Manager | Pod |
| Benutzeraktivität | Aktivität |
| Aufgabe und Ereignisse | Aktivität |
| Pool | Zuweisung |
| Sitzungsbasierter Pool (nur Desktop) | Sitzungs-Desktop-Zuweisung |
| Sitzungsbasierter Pool (nur Anwendung) | Remoteanwendungszuweisung |
| Statischer Pool | Dedizierte Desktop-Zuweisung |
| Dynamischer Pool | Flexible Desktop-Zuweisung |
| Zugeordnet | Zugewiesener Benutzer |
| Dynamische Poolaktualisierung | Aktualisierungen starten |
| Golden Image | Image |
| Versiegeltes Golden Image | Veröffentlichtes Image |
| Unversiegeltes Golden Image | Offline-Image |

# Assistent für erste Schritte

3

Der Assistent für erste Schritte wird standardmäßig mit den für die Einrichtung Ihres Horizon Cloud-System erforderlichen Aufgaben angezeigt, wenn Sie die Benutzeroberfläche öffnen. Der Assistent bietet eine allgemeine Übersicht über die bereits erledigten und noch ausstehenden Aufgaben. Sie können jederzeit auf diese Seite zugreifen, indem Sie oben auf der Seite auf das Symbol „Abspielen“ klicken.

Es wird empfohlen, die Aufgaben in der angegebenen Reihenfolge auszuführen.

**Hinweis** Wenn Sie sich zum ersten Mal anmelden, müssen Sie, um das System verwenden zu können, zuerst Active Directory registrieren. Weitere Erläuterungen finden Sie nachfolgend unter „Allgemeine Einrichtung“.

| Abschnitt | Beschreibung |
|---|---|
| Allgemeine Einrichtung | Umfasst Aufgaben im Zusammenhang mit allgemeinen Einstellungen.<br>■ Active Directory<br>■ So fügen Sie die erste AD-Domäne hinzu:<br>a Klicken Sie unter „Active Directory“ auf die Schaltfläche **Hinzufügen**.<br>b Führen Sie die Schritte unter Registrieren Sie Ihre erste Active Directory-Domäne aus.<br>■ So bearbeiten Sie die AD-Domäne:<br>a Klicken Sie unter „Active Directory“ auf die Schaltfläche **Bearbeiten**.<br>b Führen Sie die Schritte unter Bearbeiten einer Active Directory-Domäne aus.<br>■ Rollen und Berechtigungen<br>Zur Bearbeitung von Rollen und Berechtigungen führen Sie folgende Schritte aus:<br>a Klicken Sie unter „Rollen und Berechtigungen“ auf die Schaltfläche **Bearbeiten**.<br>b Folgen Sie den unter Bearbeiten von Rollen und Berechtigungen beschriebenen Schritten.<br>■ Benutzersitzungsinformationen<br>Mit dieser Funktion können vom Cloudüberwachungsdienst (Cloud Monitoring Service, CMS) Benutzer- und Domänendaten für Berichte auf der Seite „Berichte“ verwendet werden. Wenn die Funktion deaktiviert ist, sind die folgenden Elemente nicht verfügbar:<br>■ Die Funktion „Eindeutige Benutzerzusammenfassung“ des Berichts „Auslastung“<br>■ Der Bericht „Sitzungsverlauf“<br>a Klicken Sie unter „Benutzersitzungsinformationen“ auf die Schaltfläche **Bearbeiten**.<br>b Damit die Funktion aktiviert bleibt, behalten Sie die Standardeinstellung („JA“) bei und klicken Sie auf **Speichern**. Um die Funktion zu deaktivieren, wechseln Sie die Einstellung auf „NEIN“ und klicken Sie auf **Speichern**.<br>Sie können diese Einstellung jederzeit zurücksetzen und ändern, entweder im Assistenten für erste Schritte oder in den allgemeinen Einstellungen.<br>**Hinweis** Die Agenten in den virtuellen Maschinen (RDSH und VDI) benötigen einen ausgehenden Internetzugriff, um Daten an Horizon Cloud senden zu können. |
| Desktop-Zuweisung | Beinhaltet Aufgaben zur Erstellung von Desktop-Zuweisungen.<br>■ Zur Erstellung eines Image führen Sie folgende Schritte aus:<br>■ Klicken Sie unter „Image erstellen“ auf die Schaltfläche **Neu**.<br>■ Folgen Sie den unter Erstellen eines Images beschriebenen Schritten.<br>■ Zur Erstellung einer Desktop-Zuweisung führen Sie folgende Schritte aus:<br>■ Klicken Sie unter „Neue Desktop-Zuweisung erstellen“ auf die Schaltfläche **Neu**.<br>■ Folgen Sie den unter Erstellen einer dedizierten oder flexiblen VDI-Desktop-Zuweisung oder Erstellen einer Zuweisung eines RDSH-Sitzungs-Desktops beschriebenen Schritten, je nachdem welchen Typ von Desktop-Zuweisung Sie erstellen möchten. Weitere Informationen finden Sie unter Zuweisungstypen. |
| Anwendungszuweisung | Beinhaltet Aufgaben zur Erstellung von Anwendungszuweisungen.<br>■ Zur Erstellung eines RDSH-Image führen Sie folgende Schritte aus:<br>■ Klicken Sie unter „RDSH-Image erstellen“ auf die Schaltfläche **Konfigurieren**.<br>■ Folgen Sie den Schritten im Abschnitt „RDSH-Image erstellen“.<br>■ Zur Erstellung einer Anwendungsfarm führen Sie folgende Schritte aus:<br>■ Klicken Sie unter „Anwendungsfarm erstellen“ auf die Schaltfläche **Neu**. |

| Abschnitt | Beschreibung |
| --- | --- |
| | ■ Folgen Sie den unter Erstellen einer Farm beschriebenen Schritten.<br>■ Zur Überprüfung des Anwendungsbestands führen Sie folgende Schritte aus:<br>■ Klicken Sie unter „Anwendungsbestand“ auf die Schaltfläche **Start**.<br>■ Überprüfen und bearbeiten Sie die Anwendungen auf der Seite „Anwendungen“ wie unter Kapitel 7 Anwendungen beschrieben.<br>■ Zur Erstellung einer neuen Anwendungszuweisung führen Sie folgende Schritte aus:<br>■ Klicken Sie unter „Neue Anwendungszuweisung erstellen“ auf die Schaltfläche **Neu**.<br>■ Folgen Sie den unter Erstellen einer Anwendungszuweisung beschriebenen Schritten. |

Verwenden Sie den Schieberegler am unteren Rand der Seite, um anzugeben, ob die Seite „Erste Schritte“ beim Starten angezeigt werden soll.

# Programm zur Verbesserung der Benutzerfreundlichkeit beitreten oder verlassen

4

Das VMware-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) stellt Informationen bereit, mit deren Hilfe Produkte und Services verbessert, Probleme gelöst und Sie bei der optimalen Bereitstellung und Verwendung von VMware-Produkten beraten werden.

Horizon Cloud nimmt am VMware-CEIP teil. Informationen zu den über CEIP gesammelten Daten und zur Verwendung dieser Daten durch VMware finden Sie im Trust & Assurance Center unter http://www.vmware.com/trustvmware/ceip.html.

Das CEIP wird angezeigt, wenn Sie Horizon Cloud nach dem Hinzufügen einer Domäne erstmalig starten. Sie müssen dann eine Auswahl vornehmen. Sie können Ihre Auswahl danach jederzeit ändern.

### Vorgehensweise

1. Starten Sie die Horizon Cloud-Verwaltungskonsole.
2. Wählen Sie **Hilfe > CEIP** aus.
3. Bewegen Sie den Schieberegler neben „Programm zur Verbesserung der Benutzerfreundlichkeit beitreten“ auf „Nein“, um CEIP zu verlassen, oder auf „Ja“, um dem Programm beizutreten. Die Standardeinstellung lautet „Ja“.
4. Klicken Sie auf **Speichern**.

# Überwachen

5

Verwenden Sie das Symbol „Überwachen“, um auf Desktop-Informationen, Administrator- und Benutzeraktivitäten zuzugreifen, Detailberichte zur Benutzer- und Desktop-Zuordnung anzuzeigen und Benachrichtigungen zu prüfen.

Das Symbol „Überwachen“ bietet vier Auswahlmöglichkeiten.

| | |
|---|---|
| Dashboard | Zeigt Details zu Desktopverbindungen, Verbindungsstatus und Kapazitätszuordnungen an. |
| Aktivität | Zeigt Aktivitätsdetails für Administratoren und Benutzer an. |
| Berichte | Liefert Zuordnungsdetails für Benutzer und Desktops |
| Benachrichtigungen | Zeigt eine Liste der aktuellen Benachrichtigungen an. |

Dieses Kapitel behandelt die folgenden Themen:



## Die Seite „Dashboard“

Diese Seite ist über das Symbol **Überwachen** verfügbar. Sie zeigt Informationen über die gesamte Umgebung an.

Die Informationen werden immer nach einigen Minuten aktualisiert. Eine Meldung zeigt die verbleibende Zeit bis zur nächsten Aktualisierung an. Sie können die Seite auch manuell aktualisieren.

| Kategorie | Beschreibung |
|---|---|
| Kapazität | Die zugeteilte Kapazität. Um detaillierte Informationen einzublenden, zeigen Sie auf die Grafik, und klicken Sie auf **Mehr**.<br><br>**Hinweis** Wenn Sie über mehrere Desktop-Modelle verfügen, gibt der hier angezeigte Wert den prozentualen Anteil der zugeteilten Modelle an der Gesamtkapazität aller Desktop-Modelle an. Wenn beispielsweise DM-1 50 von 100 Desktop-Modellen (50 %) und DM-2 0 von 25 Desktop-Modellen (0 %) zugeteilt werden, werden insgesamt 50 von 125 Desktop-Modellen zugeteilt. Der angezeigte Wert beträgt dann 40 %. Um die Informationen für die einzelnen Desktop-Modelle anzuzeigen, zeigen Sie auf die Grafik und klicken Sie auf **Weiter**. |
| Auslastung | Die Nutzung der zugeteilten RDS-Desktops und Remoteanwendungen Um den Nutzungsbericht einzublenden, zeigen Sie auf die Grafik, und klicken Sie auf **Mehr**.<br><br>**Hinweis** Die Daten für diesen Bericht werden zu jeder vollen Stunde, jedoch nicht im Verlauf einer Stunde aktualisiert. Beispielsweise sind die Benutzeraktivitäten von 14:01 Uhr bis 14:59 Uhr erst im Bericht von 15:00 Uhr enthalten. |
| Aktivität | Desktop, Anwendung und Spitzenaktivität. Klicken Sie auf die Bezeichnungen, um die angezeigte Informationen zu filtern.<br><br>**Hinweis** Die Daten für diesen Bericht werden zu jeder vollen Stunde, jedoch nicht im Verlauf einer Stunde aktualisiert. Beispielsweise sind die Benutzeraktivitäten von 14:01 Uhr bis 14:59 Uhr erst im Bericht von 15:00 Uhr enthalten. |
| Führender Ort nach Benutzern | Gibt die Nutzung entsprechend Ihrer benannten Speicherorte an. |

# Seite „Aktivität“

Die Seite „Aktivität“ zeigt Daten zu aktuellen und früheren Ereignissen im System.

Die Seite „Aktivität“ erreichen Sie über das Symbol „Überwachen“. Sie können folgende Aufgaben ausführen.

- Den Anzeigefilter verwenden, um nur Ereignisse in einem bestimmten Zeitraum anzuzeigen.
- Die Gesamtzahl der Ereignisse anzeigen.
- Ereignisse über das Feld „Filter“ filtern.
- Die Liste aktualisieren.
- In der Liste enthaltene Information mit der Exportfunktion im .xlsx-Format herunterladen.

Die Seite „Aktivität“ enthält Registerkarten für Administrator- und Benutzerereignisse.

## Administratorereignisse

Die Registerkarte „Administrator“ zeigt Administratorereignisse mit Informationen für die einzelnen Aktionen an. Erweitern Sie ein Ereignis, um die Details und Teilaufgaben für das Ereignis anzuzeigen.

| Spalte | Beschreibung |
|---|---|
| Beschreibung | Details zum Ereignis. |
| Durchgeführt (in Prozent) | Aktueller Prozentsatz des Ereignisabschlusses. |
| Status | „Erfolgreich“ zeigt an, dass ein Ereignis vollständig ausgeführt wurde. „Fehler“ zeigt an, dass ein Ereignis entweder teilweise oder gar nicht ausgeführt wurde. |
| Uhrzeit | Zeitpunkt, zu dem das Ereignis protokolliert wurde. |

## Benutzerereignisse

Die Registerkarte „Benutzer“ zeigt Benutzerereignisse mit Informationen für die einzelnen Ereignisse an.

| Spalte | Beschreibung |
|---|---|
| Beschreibung | Details zum Ereignis. |
| Uhrzeit | Zeitpunkt, zu dem das Ereignis protokolliert wurde. |

# Seite „Berichte“

Verwenden Sie die Seite „Berichte“, um auf verschiedene Berichte zu Desktop- und Anwendungssitzungen der Endbenutzer zuzugreifen.

**Wichtig** Die Berichte Desktop-Zustand, Auslastung, Sitzungsverlauf und Parallelität enthalten erst eine Stunde nach dem Aktivieren der Überwachung der Benutzersitzungsinformationen die aktuellen Benutzerdaten.

Wählen Sie **Überwachen > Berichte** aus, um die Seite „Berichte“ zu öffnen, auf der Sie detaillierte Informationen für die folgenden Kategorien anzeigen können. Sie können diese Seite auch manuell aktualisieren, Ihre Suche filtern und Daten in ein Microsoft Excel-Arbeitsblatt exportieren.

**Hinweis** Wenn Sie die Überwachung der Benutzersitzungsinformationen zu Nutzung, Trends und historischen Analysen deaktiviert haben, sind die mit diesem Datentyp verknüpften Berichte deaktiviert und werden auf der Seite „Berichte“ nicht angezeigt. Wenn die Überwachungsfunktion deaktiviert ist, werden die Benutzersitzungsinformationen für einen begrenzten Zeitraum gesammelt und auf den Benutzernamen wird ein Hash angewendet, um Echtzeitverwaltung zu aktivieren und historische und aggregierte Ansichten dieser Benutzerinformationen zu deaktivieren. Das heißt, Berichte, die normalerweise solche historischen und aggregierten Ansichten enthalten (z. B. Bericht „Sitzungsverlauf“), sind nicht verfügbar.

Die Umschaltoption **Benutzersitzungsinformationen aktivieren** zum Aktivieren oder Deaktivieren der Überwachung der Benutzersitzungsinformationen befindet sich auf der Seite „Allgemeine Einstellungen“ (**Einstellungen > Allgemeine Einstellungen**).

| Berichtstyp | Details |
|---|---|
| Benutzerzuordnung | Anzeige der Details und Sortieren nach verschiedenen Kategorien, z. B. Benutzername, Domäne, Desktopname, Desktopmodell, Farm und Zuordnungstyp (Benutzer oder Gruppe)<br><br>**Hinweis** In diesem Bericht werden nur Daten von Benutzer berücksichtigt, die über mindestens eine direkte Desktop-Zuweisung verfügen. In der Verwaltungskonsole können Sie beim Erstellen einer Desktop-Zuweisung einzelnen Benutzer oder Benutzergruppen auswählen. Wenn ein Benutzer über mindestens einer Zuweisung als einzelner Benutzer und über keine, eine oder mehrere Zuweisungen im Rahmen der zugewiesenen Gruppe verfügt, enthält dieser Bericht alle Desktop-Zuweisungen des Benutzers.<br>Wenn jedoch alle Desktop-Zuweisungen des Benutzers im Rahmen der Gruppe bestehen, sind die Zuweisungen des Benutzers nicht in diesem Bericht enthalten. |
| Desktopzuordnung | Anzeige der Details und Sortieren nach verschiedenen Kategorien, z. B. Desktopname, Modell, Zuweisungsname, Typ, Farm, aktiver Benutzer, zugeordnete Benutzer und zugeordnete Benutzergruppen |
| Desktop-Zustand | Zeigen Sie eine Liste der Desktops an, die nach Zuweisung oder Fehlerstatus gefiltert werden kann. Klicken Sie auf einen Desktop, um den Bericht anzuzeigen.<br>■ Für RDS-Desktops enthält der Bericht CPU-Auslastung in %, Arbeitsspeicher-Auslastung in %, Festplatten-IOPS und aktiv/getrennte Sitzungen.<br>■ Für VDI-Desktops enthält der Bericht CPU-Auslastung in %, Arbeitsspeicher-Auslastung in %, Festplatten-IOPS, Dauer, Bandbreite und Latenz. |
| Auslastung | Zeigen Sie Diagramme für Benutzer- und Sitzungstrends, Protokoll- und Clientnutzung, Zugriffstyp (intern oder extern), Sitzungsdauer und Diensttyp an. Kann nach Zuweisung und Zeitraum gefiltert werden.<br><br>**Hinweis** Wenn für Ihre Umgebung **Benutzersitzungsinformationen aktivieren** deaktiviert ist, ist die Berichtfunktion „Eindeutige Benutzerzusammenfassung“ nicht verfügbar. Die Einstellung **Benutzersitzungsinformationen aktivieren** wird auf der Seite „Allgemeine Einstellungen“ festgelegt. |
| Sitzungsverlauf | Zeigen Sie Sitzungsinformationen nach Benutzer an, einschließlich Uhrzeit der letzten Anmeldung, Sitzungsdauer, wöchentliche durchschnittliche Nutzung und durchschnittliche Sitzungsdauer. Kann nach Zeitraum gefiltert werden.<br><br>**Hinweis** Dieser Bericht ist nicht verfügbar, wenn **Benutzersitzungsinformationen aktivieren** für Ihre Umgebung auf der Seite „Allgemeine Einstellungen“ deaktiviert ist. |
| Parallelität | Zeigen Sie Daten für Kapazität, Anzahl der gleichzeitigen Benutzer, Spitzenparallelität und verwendete Anwendungen pro Zuweisung an. Kann nach Zeitraum gefiltert werden. |
| URL-Konfigurationen | Zeigen Sie Informationen zu kürzlich konfigurierten URL-Umleitungen an. Weitere Informationen finden Sie unter Erstellen einer Konfiguration für die URL-Weiterleitung. |

# Seite „Benachrichtigungen“

Auf der Seite „Benachrichtigungen“ finden Sie Informationen zu Systembenachrichtigungen.

Die Seite „Benachrichtigungen“ erreichen Sie über das Symbol „Überwachen“. Sie können folgende Aufgaben ausführen.

- Benachrichtigungen nur für einen bestimmten Zeitraum über den Anzeigefilter abrufen
- Die Gesamtzahl der Benachrichtigungen abrufen
- Benachrichtigungen über das Feld „Filter“ filtern
- Die Liste aktualisieren.
- In der Liste enthaltene Information mit der Exportfunktion im .xlsx-Format herunterladen.

Die Seite „Benachrichtigungen“ zeigt zusätzliche Informationen zu Benachrichtigungen.

| Spalte | Beschreibung |
|---|---|
| Typ | Der Typ der Benachrichtigung geht aus dem Symbol hervor.<br>■ Blaues „i“ – Information<br>■ Gelbes „!“ – Warnung<br>■ Rotes „x“ – Schwerwiegendes Problem |
| Benachrichtigung | Text der Benachrichtigung |
| Status | Status der Benachrichtigung (z. B. „Aktiv“ oder „Abgelehnt“) |
| Datum | Datum der Benachrichtigung |

**Hinweis** Mit dem Benachrichtigungssymbol (Glocke) oben auf der Seite in der Benutzeroberfläche können Sie die Benachrichtigungen auch im verkürzten Listenformat abrufen. Wenn Sie auf eine Benachrichtigung doppelklicken, wird sie auf der Seite „Benachrichtigungen“ angezeigt. Mit „Alle Benachrichtigungen anzeigen“ gelangen Sie zur Seite „Benachrichtigungen“ mit allen Einträgen.

# Zuweisungen

6

Auf der Seite „Zuweisungen“ können Sie Zuweisungen erstellen, bearbeiten und löschen sowie die Agent-Software für dedizierte Desktop-Zuweisungen aktualisieren.

Klicken Sie auf das Symbol „Zuweisen“. Die Seite „Zuweisungen“ wird geöffnet; hier können Sie die nachfolgenden Aktionen durchführen.

| Aktion | Beschreibung |
|---|---|
| Neu | Erstellen Sie eine neue Anwendungs- oder Desktop-Zuweisung. |
| Bearbeiten | Wählen Sie eine Zuweisung aus, um Änderungen vorzunehmen oder weitere Details, wie Übersichts- und Sitzungsinformationen, anzuzeigen. |
| URL-Weiterleitung | Erstellen Sie eine neue Zuweisung für eine Konfiguration der URL-Weiterleitung. |
| Aktualisieren des Agent | Aktualisieren Sie Agenten für dedizierte Desktop-Zuweisungen. |
| Offline schalten | Schalten Sie bestimmte Arten von Desktop-Zuweisungen für die Wartung offline. |
| Löschen | Löschen einer Zuweisung. |
| Wiederherstellen | Stellen Sie Desktops wieder her, bei denen im Zuge einer vorangegangen Image-Aktualisierung ein Fehler aufgetreten ist. |
| Online schalten | Schalten Sie eine Desktop-Zuweisung, die offline ist, wieder online. |

Wenn Sie auf eine Zuweisung in der Liste klicken, wird eine Detailseite mit Übersichtsinformationen für die Zuweisung geöffnet. Für einige Zuweisungstypen werden zusätzlich zur Registerkarte „Übersicht“ weitere Registerkarten angezeigt:

- Desktops – wird für dedizierte und flexible Desktop-Zuweisungen angezeigt. Siehe Verwalten von Desktops in einer dedizierter oder flexiblen Desktop-Zuweisung.
- Systemaktivität und Benutzeraktivität – wird für dedizierte und flexible Desktop-Zuweisungen angezeigt. Siehe Anzeigen der System- oder Benutzeraktivität für Zuweisungen.
- Sitzungen – wird für native Anwendungszuweisungen angezeigt Siehe Anzeigen der System- oder Benutzeraktivität für Zuweisungen.

In den nachfolgenden Themen finden Sie weitere Informationen zu den Daten auf der Seite „Zuweisungen“:

- Zuweisungstypen – beschreibt die Werte in der Spalte „Typ“.

- Werte für „Kapazität“ und „Benutzer“ für VDI-Desktop-Zuweisungen – beschreibt die Werte in den Spalten „Kapazität“ und „Benutzer“.

Dieses Kapitel behandelt die folgenden Themen:



# Zuweisungstypen

Es gibt verschiedene Zuweisungstypen, wie in der folgenden Tabelle beschrieben. Der Typ jeder Zuweisung wird in der Spalte „Typ“ der Zuweisungsliste angezeigt.

| Typ | Beschreibung |
| --- | --- |
| Anwendung | Verwenden Sie Anwendungszuweisungen zur Zuweisung von Windows-Anwendungen zu Gruppen. Siehe Erstellen einer Anwendungszuweisung.<br>Der angezeigte Typ kann wie folgt lauten: .<br>■ Remoteanwendungen – die Zuweisung umfasst Anwendungen von Servern in RDSH-Farmen.<br>■ Native Anwendung – die Zuweisung umfasst AppStacks. |
| Desktops | Verwenden Sie Desktop-Zuweisungen zur Zuweisung von dedizierten, flexiblen oder RDSH-basierten virtuellen Desktops und Sitzungen zu Benutzern und Gruppen. Siehe Erstellen einer dedizierten oder flexiblen VDI-Desktop-Zuweisung und Erstellen einer Zuweisung eines RDSH-Sitzungs-Desktops.<br>Der angezeigte Typ kann wie folgt lauten:<br>■ Dedizierter Desktop – Traditional Clone<br>■ Dedizierter Desktop – Instant Clone<br>**Hinweis** Dedizierter Desktop – Instant Clone-Zuweisungen können nur in bestimmten ungewöhnlichen Konfigurationen erstellt werden und sind nicht empfohlen. Wenden Sie sich zunächst an Ihren VMware-Vertreter, wenn Sie diese Art von Zuweisung erstellen möchten, um zu erfahren, ob Sie dies tun können.<br>■ Flexibler Desktop – Traditional Clone<br>■ Flexibler Desktop – Instant Clone<br>■ Sitzungs-Desktop<br>**Hinweis** Da ein Sitzungs-Desktop standardmäßig das herkömmliche Klonen verwendet, wird in der Spalte „Typ“ der Seite „Zuweisungen“ für solche Zuweisungen „Sitzungs-Desktop“ angezeigt.<br>Die Definitionen lauten wie folgt.<br>■ Dedizierter Desktop – Bei einer dedizierten Desktop-Zuweisung ist jedem Benutzer ein spezieller Remote-Desktop zugewiesen und der Benutzer kehrt bei jeder Anmeldung zum selben Desktop zurück. Für dedizierte Zuweisungen ist eine Beziehung zwischen einem Desktop und einem Benutzer erforderlich. Die Größe sollte sich an |

| Typ | Beschreibung |
|---|---|
| | der gesamten Benutzerpopulation orientieren. Dedizierte Desktop-Zuweisungen dienen hauptsächlich dazu sicherzustellen, dass der Hostname der Desktop-VM zwischen den Sitzungen immer gleich bleibt. Bei manchen Software-Paketen ist eine solche Nutzung möglicherweise für die Lizenzierung erforderlich.<br>■ Flexibler Desktop: Bei einer flexiblen Desktop-Zuweisung erhält ein Benutzer unter Umständen bei jeder Anmeldung eine andere VM mit einem anderen Computer- und/oder Hostnamen. Bei flexiblen Desktop-Zuweisungen können Sie Desktops erstellen, die von Benutzern dynamisch, d. h. wechselweise verwendet werden. Die Zahl sollte sich an der maximalen Anzahl gleichzeitiger Benutzer orientieren.<br>■ Sitzungs-Desktop – In einer Sitzungs-Desktop-Zuweisung wird eine über RDSH veröffentlichte Desktop-Erfahrung für mehrere Benutzer freigegeben (Terminaldienste).<br>■ Traditional Clone und Instant Clone – Klontypen für Desktops. Der Klontyp kann beim Erstellen eines Images ausgewählt werden. Das ausgewählte Image zum Erstellen eines Desktops bestimmt den Klontyp des Desktops. Siehe Erstellen eines Images.<br>Hinweis:<br>■ Einem Desktop können mehrere Benutzer zugewiesen werden, er kann jedoch nur von jeweils einem Benutzer verwendet werden.<br>■ Desktops in flexiblen Desktop-Zuweisungen bieten keine Persistenz. Sie können die Persistenz im Rahmen einer Anwendungszuweisung konfigurieren.<br>■ Verwenden Sie nach Möglichkeit flexible Desktop-Zuweisungen, da sie kostengünstiger sind als dedizierte Desktop-Zuweisungen und für einzelne Benutzer keine dedizierten VM-Ressourcen bereitgestellt werden müssen. |
| Konfiguration der URL-Weiterleitung | Verwenden Sie diese Zuweisungen zur Zuweisung von Regeln zur URL-Handhabung an Benutzer. Siehe Erstellen einer Konfiguration für die URL-Weiterleitung. |

# Werte für „Kapazität“ und „Benutzer“ für VDI-Desktop-Zuweisungen

Für dedizierte und flexible VDI-Desktop-Zuweisungen werden die in den entsprechenden Spalten auf der Seite „Zuweisungen“ angezeigten Werte für Kapazität und Benutzer wie nachfolgend beschrieben berechnet.

| Wert | Beschreibung |
|---|---|
| Kapazität | Dieser Wert gibt die Anzahl an Desktops in dieser dedizierten oder flexiblen Desktop-Zuweisung wieder. |
| Benutzer oder Benutzergruppen | Anzahl der Benutzer oder Benutzergruppen, die derzeit der Zuweisung zugeordnet ist. Die tatsächlich angezeigte Anzahl hängt davon ab, ob die Zuweisung einer Reihe von einzelnen Benutzern, einer oder mehreren Gruppen oder einer Kombination von beidem zugeordnet ist. |

**Hinweis** Für Desktop- und Anwendungszuweisungen wird in der Spalte „Kapazität“ der Seite „Zuweisung“ standardmäßig „NV“ angezeigt.

# Erstellen einer Anwendungszuweisung

Eine Anwendungszuweisung kann auf der Seite „Zuweisungen“ erstellt werden.

### Vorgehensweise

1 Klicken Sie auf das Symbol **Zuweisen**.

Die Seite „Zuweisungen“ wird angezeigt.

2 Klicken Sie auf **Neu**.

3 Klicken Sie auf die Schaltfläche **Erste Schritte** unter „Anwendungen“.

4 Wählen Sie auf der Registerkarte „Definition“ einen Zuweisungstyp aus.

| Option | Beschreibung |
|---|---|
| **Remote** | Die Zuweisung umfasst Anwendungen aus Ihren RDSH-Farmen. |
| **Nativ** | Die Zuweisung umfasst AppStacks. |

**Hinweis** Die Felder auf dieser Registerkarte sind abhängig vom jeweils ausgewählten Typ.

5 Wenn Sie die Option „Nativ“ gewählt haben, füllen Sie die Felder gemäß den nachfolgenden Anweisungen aus, klicken Sie auf **Weiter** und fahren Sie mit Schritt 9 fort.

| Feld | Beschreibung |
|---|---|
| **Zuweisungsname** | Eindeutiger Name für die Zuweisung |
| **Betriebssystem** | Wählen Sie im Dropdown-Menü das passende Betriebssystem aus. Dieses Betriebssystem muss mit dem Betriebssystem übereinstimmen, das für das Erfassen der Anwendungen verwendet wird. |
| **Präfix für Computername** | (Optional) Geben Sie ein Präfix ein. Durch die Angabe eines Präfix wird der Zugriff auf Anwendungszuweisungen auf autorisierte Benutzer eingeschränkt, die sich bei einer Desktop-Zuweisung anmelden, deren Name mit demselben Präfix beginnt. Wenn Sie für diese Option keine Angabe vornehmen, können alle autorisierten Benutzer auf die neue Anwendungszuweisung zugreifen, ohne dass berücksichtigt wird, bei welchen Desktop-Zuweisungen sie angemeldet sind. |

6 Wenn Sie „Remote“ ausgewählt haben, geben Sie einen eindeutigen Namen für die Zuweisung ein und setzen Sie den Vorgang mit dem nächsten Schritt fort.

7 Wählen Sie auf der Registerkarte „Anwendungen“ die Remoteanwendungen bzw. die AppStacks aus, die in die Zuweisung aufgenommen werden sollen, und klicken Sie auf **Weiter**.

Der Inhalt der angezeigten Liste hängt davon ab, ob Sie in den vorherigen Schritten als Anwendungstyp **Remote** oder **Nativ** ausgewählt haben. Wenn Sie **Remote** als Anwendungstyp festgelegt haben, können die Anwendungen, die Sie hier auswählen, aus verschiedenen Farmen stammen.

8 Beginnen Sie auf der Registerkarte „Benutzer“ mit der Eingabe des Namens eines Benutzers oder einer Gruppe im Textfeld und klicken Sie dann auf den Namen in der Liste, um ihn auszuwählen.

9 (Optional) Wiederholen Sie den vorherigen Schritt für die Auswahl zusätzlicher Benutzer oder Gruppen.

10 Klicken Sie auf **Weiter**.

11 Prüfen Sie auf der Registerkarte „Übersicht“ die darauf angezeigten Informationen und klicken Sie auf **Absenden**, sofern sie richtig sind. Falls nicht, klicken Sie auf **Zurück**, um zu den vorherigen Registerkarten zurückzukehren, und bearbeiten Sie Ihre Informationen.

# Erstellen einer dedizierten oder flexiblen VDI-Desktop-Zuweisung

VDI-Desktop-Zuweisungen können über die Seite „Zuweisungen“ erstellt werden.

Mit diesen Schritten können Sie Ihren Endbenutzern einen dedizierten oder flexiblen VDI-Desktop zuweisen. Erläuterungen der Schritte zur Zuweisung eines sitzungsbasierten RDSH-Desktops finden Sie unter Erstellen einer Zuweisung eines RDSH-Sitzungs-Desktops.

### Vorgehensweise

1 Klicken Sie auf das Symbol **Zuweisen**.

Die Seite „Zuweisungen“ wird angezeigt.

2 Klicken Sie auf **Neu**.

3 Klicken Sie auf die Schaltfläche **Erste Schritte** unter „Desktops“.

Die Schaltfläche „Desktops zuweisen“ wird angezeigt.

4 Wählen Sie zur Erstellung einer Zuweisung für einen VDI-Desktop entweder „Zugeordnet“ (für dediziert) oder „Flexibel“ aus. Informationen zu den Desktop-Zuweisungstypen finden Sie unter Zuweisungstypen. Erläuterungen der Schritte zum Erstellen eines sitzungsbasierten Desktops finden Sie unter Erstellen einer Zuweisung eines RDSH-Sitzungs-Desktops.

**Hinweis** Die tatsächlich auf dem Bildschirm angezeigten Felder sind abhängig vom zu erstellenden Desktop-Zuweisungstyp. Die Abweichungen werden in den folgenden Schritten notiert.

5 Geben Sie Informationen für „Feste Attribute“ ein.

| Option | Beschreibung |
|---|---|
| **Pod** | Diese Option wird nur angezeigt, wenn das Datencenter mit mehreren Pods konfiguriert ist. Sie können Zuweisungen nur anhand von Images im selben Pod erstellen. |
| **Desktop-Modell** | Wählen Sie das Modell in der Dropdown-Liste aus. |
| **Domäne** | [nur Traditional Clone-Images] Wählen Sie eine Domäne in der Dropdown-Liste aus. |
| **Domäne beitreten** | [nur Traditional Clone-Images] Behalten Sie die Standardeinstellung („Ja“) bei. |

6 Geben Sie Informationen für die angezeigten flexiblen Attribute ein.

| Option | Beschreibung |
|---|---|
| **Image** | Wählen Sie ein Image aus der Liste aus.<br>■ In der Liste wird das Akronym für den Imagetyp am Anfang des Imagenamens angezeigt. So steht beispielsweise „[IC]-Image1“ für ein Instant Clone-Image, während „[TC]-Image 2“ ein Traditional Clone-Image darstellt.<br>■ Bei dedizierten Desktop-Zuweisungen werden Instant-Clone-Images für die meisten Benutzer nicht angezeigt. Es wird nicht empfohlen, solche Zuweisungen zu erstellen. Wenn Sie dies dennoch tun möchten, wenden Sie sich zunächst an Ihren VMware-Vertreter, um sicherzustellen, dass die Konfigurationen Ihres Systems dies zulassen.<br>■ Für dedizierte und flexible Desktop-Zuweisungen werden rollenfähige RDSH-Images nicht aufgeführt, da Benutzer keinen Grund haben, dedizierte oder flexible Desktop-Zuweisungen aus diesen Images zu erstellen. Rollenfähige RDSH-Images werden für Sitzungs-Desktop-Zuweisungen verwendet. |
| **Zuweisungsname** | Ein eindeutiger Name für die neue Zuweisung. |
| **Standardprotokoll** | Wählen Sie Blast (HTML Access) oder PCoIP aus. |
| **Bevorzugter Client-Typ** | Wählen Sie Browser oder Horizon Client aus. |
| **Kapazität** | Anzahl der in der Zuweisung erforderlichen Desktops. |

7 Erweitern Sie unter „Flexible Attribute“ die Option „Erweiterte Eigenschaften“ und geben Sie die erforderlichen Informationen ein.

| Option | Beschreibung |
|---|---|
| **VM-Namen** | Name für alle virtuellen Maschinen oder Gast-Desktops in dieser Zuweisung, an den eine Zahl angehängt wird, z. B. „win7-1“, „win7-2“ oder „win7-Floating“ Der Name muss mit einem Buchstaben beginnen und darf nur Buchstaben, Bindestriche und Ziffern enthalten. Dieser Wert wird anhand des Zuweisungsnamens vorab ausgefüllt. |
| **Computer-OE** | Active Directory-Organisationseinheit, in der VMs vorhanden sind. Z. B. OU=NestedOrgName,OU=RootOrgName,DC=DomainComponent,DC=eng usw. Die Einträge müssen durch Komma getrennt sein und zwischen den Einträgen dürfen keine Leerzeichen stehen. Weitere Informationen zu Active Directory finden Sie unter Mit verschachtelten Organisationseinheiten arbeiten. |
| **Anmeldeskript ein Mal ausführen** | (Optional) Speicherort der Skripts, die nach Abschluss der Systemvorbereitung ausgeführt werden sollen. |

| Option | Beschreibung |
|---|---|
| **Intervall für Zeitüberschreitung der Sitzung** | Der Zeitüberschreitungswert für Endbenutzersitzungen auf Desktops. Der Standardwert ist sieben Tage (10.080 Minuten). Der Höchstwert von 99.999 Minuten entspricht ca. 69 Tagen.<br><br>**Hinweis** Wenn bis zum Ablauf des Zeitüberschreitungsintervalls keine Benutzeraktivität stattfindet, erscheint eine Meldung, dass der Benutzer abgemeldet wird, sofern er nicht innerhalb der nächsten 30 Sekunden auf **OK** klickt. Im Falle einer solchen Abmeldung gehen alle nicht gespeicherten Dokumente verloren.<br><br>Wenn Sie einen Zeitüberschreitungswert für dedizierte Desktops zuweisen, können Sie den Höchstwert selbst festlegen. Wenn Sie für flexible Desktops ein großes Zeitüberschreitungsintervall festgelegt haben, werden die Desktops bei Nichtverwendung nicht so schnell zurückgesetzt. Diese Konfiguration führt möglicherweise dazu, dass der Pool der verfügbaren Desktops ausgeht und den Benutzern Fehlermeldungen angezeigt werden. |
| **Hotplug aktiviert** | Diese Einstellung aktiviert/deaktiviert die Hotplug-Funktionalität für Desktops in einer Zuweisung. Wenn hierfür „Nein“ festgelegt ist (Standardeinstellung), werden keine Netzwerkadapter im Bereich „Schnelles Hinzufügen/Entfernen“ angezeigt. Damit wird der Gefahr vorgebeugt, dass Benutzer ihre virtuellen Maschinen in einen instabilen Zustand versetzen. |

8 Klicken Sie auf **Weiter**.

9 Wählen Sie ein Image aus der Liste aus.

In der Liste wird das Akronym für den im Image verwendeten Klontyp am Anfang des Imagenamens angezeigt. So steht beispielsweise „[IC]-Image1“ für ein Instant Clone-Image, während „[TC]-Image 2“ ein Traditional Clone-Image darstellt.

10 Klicken Sie auf **Weiter**.

11 Beginnen Sie auf der Seite für die Active Directory-Suche mit der Eingabe eines Benutzer- oder Gruppennamens aus Active Directory.

12 Wählen Sie einen Benutzer oder eine Gruppe aus der Liste aus.

13 (Optional) Suchen Sie nach zusätzlichen Benutzern oder Gruppen, wählen Sie diese aus und klicken Sie auf **Weiter**.

Wenn Sie einen dedizierten Desktop mehr als einem Benutzer zuweisen, wird eine Warnmeldung angezeigt, die rückfragt, ob dies die gewünschte Konfiguration ist. Diese Konfiguration wird unterstützt, jedoch teilen sich die Benutzer den Desktop und er kann immer nur durch einen Benutzer verwendet werden.

14 Prüfen Sie auf der Übersichtsseite, ob die angezeigten Informationen richtig sind, und klicken Sie auf **Übernehmen**.

15 Klicken Sie zum Anzeigen der neuen Zuweisung auf das Symbol **Zuweisen**.

# Erstellen einer Zuweisung eines RDSH-Sitzungs-Desktops

Sie können Zuweisungen von Sitzungs-Desktops auf der Seite „Zuweisungen“ erstellen.

Allgemeine Informationen zu Desktop-Zuweisungen finden Sie unter Zuweisungstypen.

### Voraussetzungen

Stellen Sie sicher, dass die folgende Voraussetzungen gegeben sind:

- Auf der Seite „Farmen“ ist mindestens eine Farm vom Typ „Remote-Desktops“ aufgeführt. Es können für eine Sitzungs-Desktop-Zuweisung nur Farmen verwendet werden, die für die Bereitstellung von Remote-Desktops konfiguriert sind.
- Die verwendete Farm befindet sich in dem Knoten, von dem Sie Sitzungs-Desktops bereitstellen möchten.
- Die Farm wird noch keiner Zuweisung verwendet. Eine für die Bereitstellung von Remote-Desktops konfigurierte Farm kann nur einer Sitzungs-Desktop-Zuweisung verwendet werden. Um zu festzustellen, ob die gewünschte Farm bereits in einer Sitzungs-Desktop-Zuweisung verwendet wird, überprüfen Sie, ob die Farm in der Spalte „Farmen“ der Seite „Zuweisung“ enthalten ist. Ist dies der Fall, wird sie bereits in einer anderen Sitzungs-Desktop-Zuweisung verwendet. Sie müssen dann eine neue Farm erstellen.

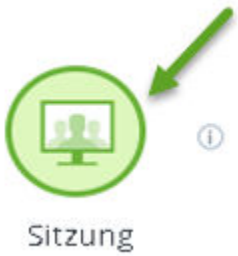
### Vorgehensweise

1 Starten Sie den Workflow „Neue Zuweisung“ durch Klicken auf **Zuweisen** und **Neu**.

2 Klicken Sie im Startbildschirm „Neue Zuweisung“ auf das Symbol „Desktops“.


Das Fenster „Neue Desktop-Zuweisung“ wird mit dem ersten Schritt des Assistenten geöffnet.

3 Klicken Sie im Schritt „Definition“ des Assistenten auf **Sitzung**.



4 Schließen Sie die Auswahl im Schritt „Definition“ ab und klicken Sie auf **Weiter**.

| Option | Beschreibung |
|---|---|
| **Pod** | Diese Option wird nur angezeigt, wenn Ihr Datencenter mit mehreren Pods konfiguriert ist. Pods enthalten bestimmte zuweisbare Images und Servermodellkapazitäten für Zuweisungen. Sie können Zuweisungen nur anhand von Images im selben Pod erstellen. |
| **Farm** | Wählen Sie die Farm mit dem konfigurierten RDS-fähigen Image, die Sie an die Endbenutzer zuweisen möchten.<br>Zur Auswahl stehen nur Farmen im ausgewählten Knoten zur Verfügung, die noch nicht für vorhandene Sitzungs-Desktop-Zuweisungen verwendet werden. |
| **Zuweisungsname** | Geben Sie einen Anzeigenamen für diese Zuweisung ein. Die Endbenutzer sehen diesen Namen, wenn sie auf ihren zugewiesenen Desktop zugreifen. Wenn ein Endbenutzer beispielsweise Horizon Client öffnet, um zu einem zugewiesenen Desktop zu wechseln, wird dieser Name in Horizon Client angezeigt.<br>Der Name darf nur Buchstaben, Bindestriche und Ziffern enthalten. Leerzeichen sind nicht zulässig. Der Name darf nicht mit einem nicht alphabetischen Zeichen beginnen. |

5 Suchen Sie im Schritt „Benutzer“ nach Benutzern und Gruppen in Ihren registrierten Active Directory-Domänen, wählen Sie diejenigen aus, die diese Sitzungs-Desktop-Zuweisung erhalten sollen, und klicken Sie auf **Weiter**.

6 Überprüfen Sie im Schritt „Zusammenfassung“ die Konfiguration und klicken Sie auf **Übernehmen**.

Die Serverinstanzen der Farm werden nun automatisch konfiguriert, um Sitzungs-Desktops für die ausgewählten Benutzer bereitzustellen. Auf der Seite „Zuweisungen“ zeigt die Spalte „Status“ den aktuellen Fortschritt an.

# Bearbeiten einer Zuweisung

Sie können Zuweisungseinstellungen wie Kapazität und zugewiesene Benutzer ändern.

### Vorgehensweise

1 Wählen Sie auf der Seite „Zuweisungen“ die zu bearbeitende Zuweisung aus, und klicken Sie auf **Bearbeiten**.

2 Nehmen Sie Änderungen vor, und klicken Sie auf **Senden**.

**Hinweis** Wenn Sie die Kapazität einer Desktop-Zuweisung bearbeiten, spiegelt sich die Änderung erst nach einigen Minuten im System wider.

Anweisungen zum Ausfüllen der Felder im Assistenten finden Sie im Thema über das Erstellen des Zuweisungstyps, den Sie bearbeiten (in Erstellen einer Anwendungszuweisung oder Erstellen einer dedizierten oder flexiblen VDI-Desktop-Zuweisung).

# Erstellen einer Konfiguration für die URL-Weiterleitung

Mit diesen Konfigurationen definieren Sie in Horizon Cloud Regeln zur URL-Handhabung, mit denen Horizon Client die URLs des Clientcomputers des Endbenutzers zu einem Desktop oder einer Anwendung in Ihrer Horizon Cloud-Umgebung umleitet. Mit der Konfiguration einer URL-Weiterleitung legen Sie für Horizon Client fest, welche URLs nicht vom lokalen Benutzersystem geöffnet, sondern von einem Ihrer dem Endbenutzer zugewiesenen Horizon Cloud-Desktops oder -Anwendungen geöffnet werden sollen.

**Hinweis** Die Horizon Cloud-Verwaltungskonsole enthält eine Benutzeroberfläche zur Konfiguration der Client-zu-Agent-URL-Umleitung. Um die Agent-zu-Client-URL-Umleitung zu konfigurieren, verwenden Sie Gruppenrichtlinieneinstellungen wie in Konfigurieren der Agent-zu-Client-Umleitung beschrieben. Im Folgenden werden die Schritte zur Konfiguration der Client-zu-Agent-URL-Umleitung beschrieben.

Horizon Client ruft die einem Endbenutzer zugewiesenen Konfigurationen der URL-Weiterleitung ab, wenn sich der Benutzer bei Horizon Client auf seinem lokalen Gerät anmeldet. Wenn dieser Benutzer dann versucht, einen Link in einem lokalen Dokument oder einer lokalen Datei zu öffnen und dieser Link der URL-Musterregel in der Konfiguration entspricht, bestimmt Horizon Client den zu verwendenden entsprechenden Handler. Die festgelegten Handler öffnen den dem Benutzer zugewiesenen Desktop oder die zugewiesene Anwendung zur Verarbeitung des URL-Link, wie in der Konfiguration der URL-Weiterleitung festgelegt. Wenn der Handler der URL-Weiterleitung die Verwendung eines Desktops festlegt, wird die URL von der Standardanwendung des Desktops für das angegebene Protokoll des Link verarbeitet. Wenn der Handler der URL-Weiterleitung die Verwendung einer Anwendung festlegt, wird die URL von der dem Benutzer zugewiesenen Anwendung verarbeitet. Wenn der Benutzer über keine Berechtigung für den im Handler festgelegten Desktop oder für die angegebene Anwendung verfügt, zeigt Horizon Client eine Meldung an, außer Sie haben für den Handler unter **Genaue Übereinstimmung** die Einstellung **Nein** gewählt.

Wenn für **Genaue Übereinstimmung** die Einstellung **Nein** festgelegt ist, wird die zu verwendende Ressource auf der Basis des folgenden Fallback-Verhaltens ermittelt:

1. Die Benutzerzuweisungen werden mithilfe eines Teilzeichenfolgenabgleichs der für den Handler angegebenen Zielressource ermittelt. Wenn eine Zuweisung gefunden wird, die mit der Teilzeichenfolge übereinstimmt, wird mit diesem zugewiesenen Desktop oder mit dieser zugewiesenen Anwendung der Link geöffnet.
2. Wenn für die Option **Ressourcentyp** des Handler die Einstellung **Anwendung** festgelegt ist und wenn keine Übereinstimmung mit einer Teilzeichenfolge vorhanden ist, werden die Anwendungszuweisungen des Benutzers nach einer zugewiesenen Anwendung durchsucht, mit der sich das im Feld **Schema** des Handler angegebene Protokoll verarbeiten lässt.

   **Hinweis** Dieser Schritt im Fallback-Verhalten gilt nur für Anwendungen. Wenn für **Ressourcentyp** die Einstellung **Desktops** festgelegt ist, wird dieser Schritt übersprungen.

3 Wenn in den Zuweisungen des Benutzers keine Ressource ermittelt werden kann, die in der Lage ist, das Protokoll zu verarbeiten kann, zeigt Horizon Client eine entsprechende Meldung an.

**Wichtig** Der Horizon Client des Benutzers muss mit der Option `URL_FILTERING_ENABLED=1` installiert worden sein, damit der Client die Funktion der URL-Weiterleitung ausführen kann. Weitere Informationen finden Sie im Thema Installieren von Horizon Client für Windows mit der Funktion der URL-Inhaltsumleitung in der Dokumentation zu VMware Horizon 7.

Wenn Ihre Umgebung in VMware Identity Manager™ integriert ist, muss für den Benutzer mindestens eine Anwendung mit Horizon Client geöffnet sein, bevor die URL-Weiterleitung für diesen Benutzer verwendet werden kann. Durch Öffnen mindestens einer Anwendung mit der Option **In Client öffnen** wird die dem Benutzer zugewiesene Konfiguration der URL-Weiterleitung in die Registrierung des Clientgeräts geladen, aus der Horizon Client die Konfigurationswerte abrufen kann.

Einem Benutzer können mehrere Konfigurationen der URL-Weiterleitung zugewiesen werden. Für die entsprechenden Konfigurationen muss dazu die Umschaltoption **Aktiv** auf „Ja“ festgelegt sein. Um potenzielle Konflikte zwischen den Regeln verschiedener Konfigurationen zu vermeiden, wenn der Benutzer sich bei Horizon Client anmeldet, gilt Folgendes:

- Es wird tatsächlich nur eine Konfiguration verwendet, auch wenn dieser Benutzer über mehrere aktive zugewiesene Konfigurationen verfügt.
- Es wird diejenige Konfiguration der URL-Weiterleitung verwendet, die alphabetisch die erste für den Benutzer ist.

### Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie mit der Verwaltungskonsole Konfigurationen für eine URL-Weiterleitung erstellen:

- Horizon Agent im von der Farm verwendeten Basis-Image wurde mit dem Parameter `URL_FILTERING_ENABLED=1` in der Befehlszeile installiert.
- Ihre Horizon Cloud-Bestandsliste enthält die Sitzungs-Desktops und Remoteanwendungen, die Sie in der Konfiguration verwenden möchten.

### Vorgehensweise

1 Klicken Sie auf der Seite „Zuweisungen“ auf **URL-Weiterleitung**.

Mit diesem ersten Schritt wird der Assistent „Neue Konfiguration der URL-Weiterleitung“ geöffnet.

2 Konfigurieren Sie im Abschnitt „Allgemeine Einstellungen“ des Schritts „Definition“ die allgemeinen Einstellungen und führen Sie dann einen Bildlauf zum Abschnitt „Regeln“ durch.

| Option | Beschreibung |
|---|---|
| **Name** | Geben Sie einen Anzeigenamen für diese Konfiguration ein. |
| **Aktiv** | Wählen Sie **Ja** aus, um diese Konfiguration zu aktivieren. |
| **Beschreibung** | Geben Sie optional eine Beschreibung für die Konfiguration ein. |

3 Erstellen Sie im Abschnitt „Regeln“ eine Liste der URL-Muster für diese Konfiguration, nach der Horizon Client URLs aus dem Clientsystem umleiten soll.

   a Geben Sie im Feld **URL-Muster** in Anführungszeichen eine Zeichenfolge für das Muster der URLs ein, die umgeleitet werden sollen.

   Dabei muss das Protokollpräfix wie z. B. `https://` enthalten sein. Sie können mit Platzhalterzeichen ein URL-Muster für eine Gruppe von URLs angeben.

   Beispiel:

   - Wenn Sie "`http://google.*`" eingeben, werden alle URLs, die den Text `google` enthalten, umgeleitet.
   - Wenn Sie `.*` (Punkt Stern) eingeben, werden alle URLs umgeleitet.
   - Wenn Sie "`mailto://.*.example.com`" eingeben, werden alle URLs, die den Text `mailto://.*.example.com` enthalten, umgeleitet.

   b Klicken Sie auf **Hinzufügen**, um das URL-Muster der Liste der Regeln hinzuzufügen.

   a Wiederholen Sie die Schritte, um weitere URL-Muster zur Ermittlung von URLs hinzuzufügen.

4 Klicken Sie auf **Weiter** , um mit dem nächsten Assistentenschritt fortzufahren.

5 Definieren Sie im Schritt „Konfiguration“ einen Satz von Handlern, mit denen die Zielbestandsressource zur Verarbeitung verschiedener Protokolle festgelegt wird.

   Ein Handler definiert, welcher berechtigte Desktop oder welche berechtigte Anwendung das angegebene Protokoll verarbeitet. Wenn beispielsweise ein Benutzer ein Microsoft Word-Dokument mit einem `mailto`-Hypertext-Link öffnet und der Benutzer auf diesen Link im Dokument klickt, definiert der Handler, welche berechtigte Anwendung die Anforderung verarbeiten soll, z. B. Microsoft Outlook oder Mozilla Thunderbird.

   a Klicken Sie auf **Neu**.

   b Konfigurieren Sie im Fenster „Handler“ die Einstellungen und klicken Sie auf **Speichern**.

| Option | Beschreibung |
|---|---|
| **Name** | Geben Sie einen Namen für diesen Handler ein. |
| **Schema** | Geben Sie das Protokoll ein, auf das dieser Handler angewendet wird, z. B. `http`, `https`, `mailto`, `callto` etc. |
| **Ressourcentyp** | Legen Sie fest, ob ein Desktop oder eine Anwendung das angegebene Protokoll verarbeiten soll. |
| **Zielressource** | Geben Sie in Ihre Horizon Cloud-Bestandsliste den Namen der Zielressource ein, die das im Feld **Schema** angegebene Protokoll verarbeiten soll. |
| **Genaue Übereinstimmung** | Wählen Sie **Ja**, um eine exakte Übereinstimmung zwischen dem im Feld **Zielressource** angegebenen Namen und den Namen der verfügbaren berechtigten Sitzungs-Desktops oder Remoteanwendungen des Benutzers zu erzwingen.<br>Wählen Sie **Nein**, wenn das Fallback-Verhalten verwendet werden soll, wenn ein Endbenutzer über keine Zuweisung für eine Ressource mit dem im Feld **Zielressource** angegebenen exakten Namen verfügt.<br>Angenommen, für **Ressourcentyp** ist die Einstellung **Anwendungen** festgelegt und Microsoft Outlook ist als Zielressource zur Verarbeitung des `mailto`-Protokolls angegeben, wobei der Benutzer aber über keine Zuweisung für Microsoft Outlook-Anwendungen verfügt. Wenn dann für **Genaue Übereinstimmung** die Einstellung **Nein** gewählt wurde, wird nach einer diesem Benutzer zugewiesenen kompatiblen Anwendung gesucht, um das `mailto`-Protokoll zu verarbeiten, z. B. Mozilla Thunderbird. |

   c Wiederholen Sie die Schritte, um weitere Handler hinzuzufügen.

6 Klicken Sie auf **Weiter**, um mit dem nächsten Assistentenschritt fortzufahren.

7 Suchen Sie nach den Benutzern und Gruppen für diese Zuweisung der URL-Weiterleitung, wählen Sie diese aus und klicken Sie auf „Weiter“.

8 Überprüfen Sie die zusammengefassten Informationen und klicken Sie auf **Übernehmen**.

## Grundlegendes zur URL-Inhaltsumleitung

Allgemein ausgedrückt, unterstützt die Funktion der URL-Inhaltsumleitung die Umleitung von einem Remote-Desktop bzw. von einer Remoteanwendung zu einem Client und umgekehrt.

Die Umleitung von einem Remote-Desktop oder einer Remoteanwendung zu einem Client wird als „Agent-zu-Client-Umleitung“ bezeichnet. Die Umleitung von einem Client zu einem Remote-Desktop oder zu einer Remoteanwendung wird „Client-zu-Agent-Umleitung“ genannt.

| | |
|---|---|
| **Agent-zu-Client-Umleitung** | Bei der Agent-zu-Client-Umleitung sendet Horizon Agent die URL an Horizon Client. Dort wird auf dem Clientcomputer die Standardanwendung für das Protokoll der URL geöffnet. Ausführliche Informationen zur Konfiguration der Agent-zu-Client-Umleitung in Horizon Cloud finden Sie unter Konfigurieren der Agent-zu-Client-Umleitung. |
| **Client-zu-Agent-Umleitung** | Bei der Client-zu-Agent-Umleitung öffnet Horizon Client einen Remote-Desktop oder eine Remoteanwendung, den bzw. die Sie für die Verarbeitung der URL festgelegt haben. Ausführliche Informationen zur Konfiguration der Client-zu-Agent-Umleitung in Horizon Cloud finden Sie unter Erstellen einer Konfiguration für die URL-Weiterleitung. |

Es lassen sich URLs von einem Remote-Desktop oder von einer Remoteanwendung zum Client und URLs von einem Client zu einem Remote-Desktop oder zu einer Remoteanwendung umleiten. Sie können eine beliebige Anzahl von Protokollen inklusive HTTP, HTTPS, mailto und callto umleiten.

## Konfigurieren der Agent-zu-Client-Umleitung

Bei der Agent-zu-Client-Umleitung sendet Horizon Agent die URL an Horizon Client. Dort wird die Standardanwendung für das Protokoll der URL geöffnet.

Für die Aktivierung der Agent-zu-Client-Umleitung müssen Sie die nachfolgend aufgeführten Konfigurationsaufgaben durchführen.

- Stellen Sie sicher, dass die Funktion der URL-Inhaltsumleitung in Horizon Agent in der Master-Image-VM wie im Abschnitt zu den Voraussetzungen in Erstellen einer Konfiguration für die URL-Weiterleitung beschrieben aktiviert ist.
- Wenden Sie die Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung auf Ihre Remote-Desktops und -anwendungen an. Siehe Hinzufügen der ADMX-Vorlage für die URL-Inhaltsumleitung zu einem GPO.
- Konfigurieren Sie die Gruppenrichtlinieneinstellungen, um für jedes Protokoll festzulegen, wie Horizon Agent die URL umleiten soll. Siehe Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung.

### Hinzufügen der ADMX-Vorlage für die URL-Inhaltsumleitung zu einem GPO

Die ADMX-Vorlagendatei `urlRedirection.admx` für die URL-Inhaltsumleitung enthält Einstellungen, mit denen Sie festlegen können, ob ein URL-Link auf dem Client (Agent-zu-Client-Umleitung) oder auf einem Remote-Desktop bzw. in einer Remoteanwendung (Client-zu-Agent-Umleitung) geöffnet wird.

Um die Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung auf Ihre Remote-Desktops und -anwendungen anzuwenden, fügen Sie den GPOs auf Ihrem Active Directory-Server die ADMX-Vorlagendatei hinzu. Für Regeln zu URL-Links, auf die in Remote-Desktops oder -anwendungen geklickt wird, müssen die GPOs mit der Organisationseinheit, die die virtuellen Desktops und RDS-Hosts enthält, verknüpft werden.

Sie können die Gruppenrichtlinieneinstellungen auch auf ein GPO anwenden, das mit der Organisationseinheit verknüpft ist, in der sich Ihre Windows-Clientcomputer befinden. Für die Konfiguration der Client-zu-Agent-Umleitung wird aber die Verwendung des `vdmutil`-Befehlszeilendienstprogramms empfohlen. Da MacOS keine GPOs unterstützt, müssen Sie für Mac-Clients `vmdutil` verwenden.

### Voraussetzungen

- Stellen Sie sicher, dass die Funktion der URL-Inhaltsumleitung bei der Installation von Horizon Agent in der Master-Image-VM wie in Erstellen einer Konfiguration für die URL-Weiterleitung beschrieben installiert wird.
- Stellen Sie sicher, dass Active Directory-GPOs für die Gruppenrichtlinieneinstellungen zur URL-Inhaltsumleitung erstellt wurden.
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienverwaltungs-Editor“ auf Ihrem Active Directory-Server installiert sind.

### Vorgehensweise

1. Laden Sie die Horizon 7-GPO-Bundle-ZIP-Datei von der VMware-Download-Website unter my.vmware.com/web/vmware/downloads herunter.

   Der Name der Datei lautet allgemein `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`, wobei *x.x.x* die Version und *yyyyyyy* die Build-Nummer darstellt. Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für das Produkt bereitstellen, sind in dieser Datei verfügbar.

2. Extrahieren Sie diese ZIP-Datei und kopieren Sie die ADMX-Datei der URL-Inhaltsumleitung auf Ihren Active Directory-Server.

   a. Kopieren Sie die Datei `urlRedirection.admx` in den Ordner `C:\Windows\PolicyDefinitions\`.

   b. Kopieren Sie die Sprachressourcendatei `urlRedirection.adml` in den entsprechenden Unterordner des Ordners `C:\Windows\PolicyDefinitions`.

      So kopieren Sie beispielsweise für das Gebietsschema EN die Datei `urlRedirection.adml` in den Ordner `C:\Windows\PolicyDefinitions\en-US`.

3. Öffnen Sie auf Ihrem Active Directory-Server den Editor zur Gruppenrichtlinienverwaltung.

   Die Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung werden in **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware Horizon-URL-Umleitung** installiert.

### Weiter

Konfigurieren Sie die Gruppenrichtlinieneinstellungen auf Ihrem Active Directory-Server. Eine Beschreibung der Einstellungen finden Sie unter Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung.

## Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung

Die Vorlagendatei für die URL-Inhaltsumleitung enthält Gruppenrichtlinieneinstellungen, mit denen Sie Regeln zur Konfiguration der Agent-zu-Client-Umleitung für Ihre Horizon Cloud-Umgebung erstellen können. In der Vorlagendatei sind ausschließlich Einstellungen für die Computerkonfiguration enthalten. Alle Einstellungen befinden sich im Ordner **VMware Horizon URL Redirection** im Gruppenrichtlinienverwaltungs-Editor.

**Wichtig** Auch wenn die Vorlagendatei für die URL-Inhaltsumleitung Gruppenrichtlinieneinstellungen zur Client-zu-Agent-Umleitung enthält, sollten Sie keine Gruppenrichtlinieneinstellungen zur Konfiguration der Client-zu-Agent-Umleitung in Horizon Cloud verwenden. In Horizon Cloud verwenden Sie die Verwaltungskonsole zum Erstellen von Regeln für die Client-zu-Agent-Umleitung. Sie erstellen Regeln für die Client-zu-Agent-Umleitung beim Anlegen einer URL-Umleitungszuweisung in der Verwaltungskonsole. Ausführliche Anweisungen dazu finden Sie unter Erstellen einer Konfiguration für die URL-Weiterleitung.

In der folgenden Tabelle werden die in der Vorlagendatei für die URL-Inhaltsumleitung verfügbaren Gruppenrichtlinieneinstellungen beschrieben.

**Tabelle 6-1. Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung**

| Einstellung | Eigenschaften |
|---|---|
| `IE Policy: Prevent users from changing URL Redirection plugin loading behavior` | Legt fest, ob Benutzer die Funktion der URL-Inhaltsumleitung deaktivieren können.<br>Diese Einstellung ist standardmäßig nicht konfiguriert. |
| `IE Policy: Automatically enable URL Redirection plugin` | Legt fest, ob neu installierte Internet Explorer-Plug-Ins automatisch aktiviert werden.<br>Diese Einstellung ist standardmäßig nicht konfiguriert. |
| `Url Redirection Enabled` | Legt fest, ob die URL-Inhaltsumleitung aktiviert wird. Sie können mit dieser Einstellung die Funktion der URL-Inhaltsumleitung deaktivieren, auch wenn diese Funktion auf dem Client oder Agent installiert wurde.<br>Diese Einstellung ist standardmäßig nicht konfiguriert. |

**Tabelle 6-1. Gruppenrichtlinieneinstellungen für die URL-Inhaltsumleitung (Fortsetzung)**

| Einstellung | Eigenschaften |
|---|---|
| `Url Redirection Protocol 'http'` | Legt für alle URLs, die das HTTP-Protokoll verwenden, fest, welche URLs umgeleitet werden. Diese Einstellung verfügt über die folgenden Optionen:<br>■ **brokerHostname** – IP-Adresse oder vollqualifizierter Name des Verbindungsserver-Hosts für die Umleitung von URLs auf einen Remote-Desktop oder eine Remoteanwendung.<br>■ **remoteItem** – Anzeigename des Remote-Desktop- oder Remoteanwendungspools, der die in **agentRules** angegebenen URLs verarbeiten kann.<br>■ **clientRules** – die URLs, die zum Client umgeleitet werden sollen. Wenn Sie beispielsweise für **clientRules** den Wert `.*.mycompany.com` festlegen, werden alle URLs mit der Zeichenfolge `mycompany.com` zum Windows-basierten Client umgeleitet und dort in einem Standardbrowser geöffnet.<br>■ **agentRules** – die URLs, die zum in **remoteItem** angegebenen Remote-Desktop oder zur dort angegebenen Remoteanwendung umgeleitet werden sollen. Wenn Sie beispielsweise für **agentRules** den Wert `.*.mycompany.com` festlegen, werden alle URLs, die `mycompany.com` enthalten, zum Remote-Desktop bzw. zur Remoteanwendung umgeleitet.<br>Wenn Sie Agentregeln erstellen, müssen Sie mit der Option **brokerHostname** auch die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Verbindungsserver-Hosts und mit der Option **remoteItem** den Anzeigenamen des Desktop- oder Anwendungspools festlegen.<br>**Hinweis** Für die Konfiguration von Clientregeln wird die Verwendung des `vdmutil`-Befehlszeilendienstprogramms empfohlen.<br>Diese Einstellung ist standardmäßig aktiviert. |
| `Url Redirection Protocol '[...]'` | Sie können diese Einstellung für jedes Protokoll außer HTTP, also für HTTPS, email oder callto verwenden.<br>Die Optionen entsprechen jenen für `Url Redirection Protocol 'http'`.<br>Wenn Sie keine anderen Protokolle konfigurieren müssen, können Sie diesen Eintrag vor dem Hinzufügen der Vorlagendatei für die URL-Inhaltsumleitung zu Active Directory löschen oder auskommentieren.<br>Als Best Practice wird empfohlen, die gleichen Umleitungseinstellungen für die HTTP- und HTTPS-Protokolle zu konfigurieren. Wenn ein Benutzer die URL dann teilweise in Internet Explorer eingibt, z. B. in der Form `mycompany.com`, und diese Site automatisch von HTTP nach HTTPS umgeleitet wird, wird die Funktion der URL-Inhaltsumleitung wie erforderlich ausgeführt. Wenn Sie in diesem Beispiel eine Regel für HTTPS, aber nicht die gleiche Umleitungseinstellung für HTTP festlegen, wird die vom Benutzer eingegebene Teil-URL nicht umgeleitet.<br>Diese Einstellung ist standardmäßig nicht konfiguriert. |

# Zuweisungsmodus bearbeiten

Mit der Einstellung „Zuweisungsmodus bearbeiten“ können Sie Zuweisungen zu Wartungszwecken offline nehmen und danach wieder online stellen. Durch das Einstellen einer Zuweisung auf den Offline-Modus können sich Benutzer nicht bei den Zuweisungs-Desktops/-Anwendungen anmelden. Mit dieser Einstellung haben Sie auch die Möglichkeit, einen benutzerdefinierten Wartungshinweis für die Zuweisung hinzuzufügen.

Sie können mit der Einstellung „Zuweisungsmodus bearbeiten“ die folgenden Aufgaben ausführen.

- Eine Zuweisung offline nehmen:
  a Wählen Sie die Zuweisung auf der Seite „Zuweisungen“ aus und klicken Sie oben auf der Seite auf die Schaltfläche **Zuweisungsmodus bearbeiten**.

    Das Dialogfeld „Zuweisungsmodus bearbeiten“ wird angezeigt.

  b Ändern Sie den Zuweisungsmodus in „Offline“.

  c Klicken Sie auf **Speichern**.
- Eine Zuweisung online stellen:
  a Wählen Sie die Zuweisung auf der Seite „Zuweisungen“ aus und klicken Sie oben auf der Seite auf die Schaltfläche **Zuweisungsmodus bearbeiten**.

    Das Dialogfeld „Zuweisungsmodus bearbeiten“ wird angezeigt.

  b Ändern Sie den Zuweisungsmodus in „Online“.

  c Klicken Sie auf **Speichern**.

# Aktualisieren von Agenten für eine Zuweisung

Mit der Funktion zur Aktualisierung der Agent-Software können Sie Agenten für Zuweisungen der Art „Dedizierter Desktop – Traditional Clone“ aktualisieren.

**Hinweis** Sie haben auch die Möglichkeit, die Agent-Software für eine Zuweisung der Art „Dedizierter Desktop – Instant Clone“ zu aktualisieren. Dazu aktualisieren Sie das Image und geben die Änderungen an die Zuweisung weiter. Dieser Vorgang ist unter Agentensoftware für Image aktualisieren beschrieben.

Mit der Funktion zur Agentenaktualisierung werden alle Agenten in einer Zuweisung in einem einzigen Arbeitsgang automatisch aktualisiert.

- Das System nimmt regelmäßig Kontakt zum VMware CDS-Software-Distributionsnetzwerk auf und lädt die Agentenaktualisierungen automatisch in eine Dateifreigabe herunter, die Sie auf einem lokalen Computer eingerichtet haben. Die Aktualisierungsdateien werden dann automatisch in das System importiert und für die Zuweisungen bereitgestellt.
- Die Verfügbarkeit von Aktualisierungen wird auf der Seite „Zuweisungen“ angezeigt; hier können Sie die Aktualisierungen auf die Zuweisungen anwenden. Wenn Sie die Aktualisierung für eine Zuweisung starten, werden alle VMs in dieser Zuweisung gleichzeitig aktualisiert.

- Ihr VMware-Vertreter kann auf Wunsch den Zeitraum zwischen den Suchvorgängen nach neuen Agenten sowie die Wartezeit für Suchvorgänge nach dem Start der Mandanten ändern.

### Voraussetzungen

- Sie müssen eine Agenten-Dateifreigabe erstellt und diese Horizon Cloud hinzugefügt haben. Beim Erstellen der Dateifreigabe wählen Sie also den Dateifreigabetyp „Agenten“. Die Agenten-Dateifreigaben dienen lediglich zum Importieren von Agenten-Aktualisierungsdateien. Siehe Verwalten von Dateifreigaben.
- Die Zuweisung muss bereits über DaaS Agent 16.6.0.4408091 oder höher verfügen, um eine DaaS Agent-Aktualisierung durchführen zu können.
- Die Zuweisung muss bereits über Horizon Agent 7.0.3.4612900 oder höher verfügen, um eine Horizon Agent-Aktualisierung durchführen zu können.

### Vorgehensweise

1 Klicken Sie auf **Zuweisen**.

Die Seite „Zuweisungen“ wird angezeigt, wobei ein blauer Punkt neben dem Namen der jeweiligen Zuweisung angezeigt wird, für die Agentenaktualisierungen zur Verfügung stehen.

- Wenn Sie mit der Maus auf einen blauen Punkt zeigen, wird ein Popup-Fenster mit einer Meldung geöffnet, dass Agentenaktualisierungen für diese Zuweisung bereitstehen.
- Standardmäßig werden die jeweils aktuellen Versionen der einzelnen Agenten ausgewählt. Sie können jedoch die verschiedenen Dropdown-Listen öffnen und alle verfügbaren Versionen betrachten.

2 Aktivieren Sie das Kontrollkästchen für mindestens eine Zuweisung. Wenn Sie mehrere Zuweisungen auswählen, können Sie alle Zuweisungen gleichzeitig auf gemeinsame Agentenversionen aktualisieren.

3 Klicken Sie auf **Agent-Software aktualisieren**.

Das Dialogfeld „Agentenaktualisierung“ wird angezeigt.

4 Wählen Sie auf der Registerkarte „Software“ den bzw. die zu aktualisierenden Agent(en) aus und klicken Sie auf **Weiter**.

5 Aktivieren Sie auf der Registerkarte „Vereinbarungen“ jeweils das Kontrollkästchen **Zustimmen** für die zu akzeptierenden Vereinbarungen und klicken Sie auf **Weiter**. Bei allen Elementen, bei denen Sie der Vereinbarung nicht zugestimmt haben, wird die Aktualisierung übersprungen.

6 (Optional) Fügen Sie auf der Registerkarte „Befehlszeile“ Befehlszeilenoptionen hinzu. Details hinsichtlich Befehlszeilenoptionen finden Sie in der Dokumentation für den relevanten Agenten.

**Hinweis** Für DaaS Agent sind derzeit keine Befehlszeilenoptionen verfügbar.

7 Klicken Sie auf **Fertigstellen**.

Oben auf der Seite wird eine Meldung angezeigt, die angibt, dass die Aktualisierung gestartet wurde.

Hinweis:

- Desktops werden in Batches zu maximal 30 Stück aktualisiert. Wenn die Zuweisung maximal 30 Desktops umfasst, werden alle Desktops in der Zuweisung gemeinsam aktualisiert. Ihr VMware-Vertreter kann die Batch-Größe nach Bedarf anpassen.
- Wenn ein Desktop über eine aktive Sitzung verfügt, wird der Benutzer fünf Minuten vor der Aktualisierung gewarnt.
- Wenn ein Benutzer versucht, sich bei einem Desktop anzumelden, der aktualisiert wird, ist die Anmeldung fehlerhaft und dem Benutzer wird eine Meldung angezeigt, die besagt, dass der Desktop nicht verfügbar ist.

Sie können den Fortschritt der Aktualisierungsaufgabe anzeigen, indem Sie **Überwachen > Aktivität** auswählen. Die Aufgabenbeschreibung gibt den Agenten, der aktualisiert wird, und die Zuweisung an, anhand derer die Aktualisierung durchgeführt wird. Ist die Aufgabe nicht binnen 24 Stunden erfolgreich, schlägt der Vorgang fehl.

# Zuweisung löschen

Wenn Sie Zuweisungen nicht mehr benötigen, können Sie sie löschen.

### Voraussetzungen

Eine Zuweisung kann nur dann gelöscht werden, wenn sie keine virtuellen Computer enthält.

- Zum Löschen einer dedizierten Desktop-Zuweisung müssen Sie zunächst die virtuellen Maschinen auf der Seite „Zuweisung“ löschen.
- Zum Löschen einer flexiblen Desktop-Zuweisung müssen Sie zunächst die Zuweisungsgröße auf null festlegen.

### Vorgehensweise

1. Wählen Sie die zu löschende Zuweisung aus, und klicken Sie auf **Löschen**.
2. Klicken Sie im Bestätigungsdialogfeld auf **Löschen**, um die Zuweisung dauerhaft zu löschen.

# Zuweisung wiederherstellen

Sie können Desktops wiederherstellen, bei denen während eines vorherigen Image-Updates ein Fehler aufgetreten ist.

### Vorgehensweise

1. Wählen Sie die wiederherzustellende Zuweisung aus.
2. Klicken Sie auf **Wiederherstellen**.

# Verwalten von Desktops in einer dedizierter oder flexiblen Desktop-Zuweisung

Sie können Desktops in dedizierten und flexiblen Desktop-Zuweisungen verwalten.

**Hinweis** Bei Sitzungs-Desktop-Zuweisungen werden die Zuweisungen nur für das Erteilen von Zugriffsberechtigungen für den RDS-basierten Desktop und nicht für die Verwaltung von Desktops verwendet. Für die Verwaltung von Sitzungs-Desktops verwalten Sie die Server und Sitzungen in der zugrunde liegenden Farm. Siehe Verwalten von Farmen in Horizon Cloud.

### Vorgehensweise

1 Klicken Sie auf das Symbol **Zuweisen**.

Die Seite „Zuweisungen“ wird angezeigt.

2 Klicken Sie in der Liste auf den Namen einer Zuweisung.

Die Seite mit den Zuweisungsdetails wird geöffnet.

3 Klicken Sie oben auf der Seite auf **Desktops**.

Die Registerkarte „Desktops“ wird geöffnet und zeigt eine Liste der Desktops für die Zuweisung. Mit den Steuerungen oben rechts auf der Seite können Sie die Liste filtern, aktualisieren und exportieren.

Über die Schaltflächen oben auf der Seite können Sie die nachfolgenden Aktionen durchführen.

**Hinweis** Diese Aktionen sind nur dann verfügbar, wenn der Desktop-Status grün ist.

| Option | Beschreibung |
|---|---|
| Herunterfahren | Fährt den/die Desktop(s) herunter.<br>■ Sie können mehrere Desktops gleichzeitig auswählen.<br>■ Sie können nur VMs herunterfahren, die keine aktiven Benutzersitzungen haben. |
| Neu starten | Führt einen unterbrechungsfreien Neustart der VM(s) durch. Sie können mehrere Desktops gleichzeitig auswählen.<br>Wenn dies nicht funktioniert, ist es unter Umständen erforderlich, die Menüoption „Zurücksetzen“ zu nutzen (siehe unten). |
| Zuweisen | [Nur dedizierte Desktop-Zuweisungen] Weist dedizierten Desktop einem bestimmten Benutzer zu. Klicken Sie auf die Schaltfläche und suchen Sie dann im Active Directory nach dem Benutzer. |

Sie können die folgenden Aktionen durchführen, indem Sie auf die Schaltfläche „. . .“ klicken und eine Auswahl aus dem Dropdown-Menü vornehmen.

| | |
|---|---|
| Umbenennen | [Nur dedizierte Desktop-Zuweisungen] Benennt den ausgewählten Desktop um. |
| Zuweisung aufheben | [Nur dedizierte Desktop-Zuweisungen] Hebt die Zuweisung des ausgewählten Desktops an den Benutzer auf. |
| Löschen | [Nur dedizierte Desktop-Zuweisungen] Löscht den ausgewählten Desktop. |

| | |
|---|---|
| Anhalten | Hält den/die ausgewählten Desktop(s) an. Sie können mehrere Desktops gleichzeitig auswählen. |
| Fortsetzen | Setzt den Betrieb des/der ausgewählten Desktop(s) fort. Sie können mehrere Desktops gleichzeitig auswählen. |
| Einschalten | [Nur Traditional Clone-Zuweisungen] Ausgewählte(r) Desktop(s) wird/werden eingeschaltet. Sie können mehrere Desktops gleichzeitig auswählen. |
| Ausschalten | [Nur Traditional Clone-Zuweisungen] Ausgewählte(r) Desktop(s) wird/werden ausgeschaltet. Sie können mehrere Desktops gleichzeitig auswählen. |
| Zurücksetzen | Führt einen Hard Reset der VM(s) durch. Sie können mehrere Server gleichzeitig auswählen.<br>Wenn eine VM hängt, ist es empfehlenswert, zuerst einen Neustart durchzuführen (siehe oben). |
| Abmelden | Aktuell verbundener Benutzer wird beim ausgewählten Desktop abgemeldet. |
| Trennen | Aktuell verbundener Benutzer wird vom ausgewählten Desktop getrennt. |
| Konsole starten | Öffnet eine Konsole für den ausgewählten Desktop. Diese Option ist deaktiviert, wenn die virtuelle Maschine ausgeschaltet oder wenn mehr als eine VM ausgewählt ist. |
| Neu erstellen | [Nur flexible Desktop-Zuweisungen] Löscht den ausgewählten Desktop und erstellt ihn neu. Nutzen Sie diese Option für Desktop-VMs, die beschädigt wurden oder anderweitig nicht betriebsbereit sind. |
| In Image konvertieren | Konvertiert den ausgewählten Desktop in ein Image.<br>**Hinweis** Wenn eine VM derzeit als Appliance fungiert, können Sie sie nicht in ein Image konvertieren. |

# Anzeigen der System- oder Benutzeraktivität für Zuweisungen

Sie können auf der Detailseite einer Zuweisung die System- oder Benutzeraktivität für dedizierte und flexible Desktop-Zuweisungen anzeigen. Außerdem haben Sie die Möglichkeit, die Sitzungsaktivität für eine native Anwendungszuweisung anzuzeigen.

Mit diesen Schritten können Sie die System- oder Benutzeraktivität für dedizierte und flexible Desktop-Zuweisungen sowie die Sitzungsaktivität für native Anwendungszuweisungen anzeigen. Für Sitzungs-Desktop-Zuweisungen entnehmen Sie die System- und Benutzeraktivität der Detailseite der zugrunde liegenden Farm. Weitere Informationen dazu finden Sie unter Verwalten von Farmen in Horizon Cloud.

### Vorgehensweise

1 Klicken Sie auf das Symbol **Zuweisen**.

Die Seite „Zuweisungen“ wird angezeigt.

2 Klicken Sie in der Liste auf den Namen einer Zuweisung.

Die Seite mit den Zuweisungsdetails wird geöffnet.

3 Klicken Sie auf die entsprechende Option, je nachdem, ob es sich um eine dedizierte Desktop-Zuweisung, eine flexible Desktop-Zuweisung oder um eine native Anwendungszuweisung handelt.

   - Klicken Sie für eine dedizierte oder flexible Desktop-Zuweisung auf **System** oder **Benutzeraktivität**. Die Registerkarte „Aktivität“ wird geöffnet und zeigt eine Liste der letzten Aktivitäten für die Zuweisung an. Über das Dropdown-Menü passen Sie den Zeitrahmen für die Liste an, über die Steuerungen oben rechts auf der Seite können Sie die Liste filtern, aktualisieren und exportieren.
   - Klicken Sie für eine native Anwendungszuweisung auf **Sitzungen**.

# Mit verschachtelten Organisationseinheiten arbeiten

Fügen Sie Desktops zu einer verschachtelten Organisationseinheit (OE) hinzu.

Wenn Sie eine Desktop-Zuweisung erstellen, können Sie im Feld „Computer-OE“ eine Domänenorganisationseinheit angeben. Sie können keine verschachtelte OE angeben. Sie müssen die Informationen der verschachtelten OE ermitteln und dann manuell in das Feld „Computer-OE“ eingeben.

### Vorgehensweise

1 Öffnen Sie **Active Directory-Benutzer und -Computer**.

2 Wählen Sie **Ansicht > Erweiterte Funktionen (Aktivierte erweiterte Funktionen)** aus.

3 Navigieren Sie zu der Organisationseinheit, in die die Desktops platziert werden sollen.

4 Klicken Sie mit der rechten Maustaste und wählen Sie **Eigenschaften**.

5 Klicken Sie auf **Attribut-Editor** und wählen Sie „Distinguished Name“ aus.

6 Klicken Sie auf **Anzeigen**.

7 Geben Sie auf der Seite „Desktop-Zuweisung“ im Feld „Computer-OE“ die Distinguished Name-Information ein.

   Es ist nur der Teil `OU=` der Zeichenfolge erforderlich. Der Teil `DC=` ist optional.

# Anwendungen

7

Die Seite „Anwendungen“ zeigt eine Liste aller zuweisbaren Anwendungen.

Zum Öffnen der Seite „Anwendungen“ klicken Sie auf das Symbol **Bestand** und wählen Sie **Anwendungen**.

Es gibt drei Anwendungstypen:

- Native Anwendungen werden in AppStacks importiert. Die Importfunktion befindet sich nicht auf der Seite „Anwendungen“. Siehe Importieren von Anwendungen mithilfe von App Volumes.

  Wenn mehrere Anwendungen gemeinsam als AppStack manuell werden, wird der AppStack als einzelnes Element in der Anwendungsliste aufgeführt, wobei die Zahl neben dem Symbol die Anzahl der im AppStack enthaltenen Anwendungen angibt. Wenn Sie mit der Maus auf den Namen in der Spalte „Anwendungen“ zeigen, wird eine Liste der Anwendungen im AppStack angezeigt (bis zu 10 Einträge).
- Remoteanwendungen werden von einer RDS-Farm importiert. Sie fügen dem RDS-Image Benutzeranwendungen von Drittanbietern zu, bevor Sie dieses Image für Horizon Cloud veröffentlichen. Um Ihrer Anwendungsbestandsliste Anwendungen aus Farmen hinzuzufügen, können Sie entweder Ihre Farmen automatisch durchsuchen oder Anwendungen aus der Farm manuell hinzufügen.
- Benutzerdefinierte Anwendungen sind Anwendungen auf den Servern der RDS-Farmen, die Sie der Bestandsliste manuell hinzufügen. Dazu verwenden Sie die Schaltfläche **Neu** auf der Seite „Anwendungen“ und die Option **Manuell von Farm**. Obwohl die automatische Methode empfohlen wird, kann die manuelle Methode in manchen Situationen hilfreich sein, z. B. für das Hinzufügen von Anwendungen, die von der Befehlszeile aus aufgerufen werden oder in einem Windows-Betriebssystem nicht automatisch erkannt werden.

Auf der Seite „Anwendungen“ stehen die nachfolgenden Aktionen zur Auswahl.

| | |
|---|---|
| Neu | Fügen Sie eine Remote- oder benutzerdefinierte Anwendung hinzu. |
| Bearbeiten | Wählen Sie eine Anwendung aus, um Änderungen vorzunehmen. |
| Löschen | Löschen Sie eine Anwendung. |
| Umbenennen | Benennen Sie eine Anwendung um. |

Dieses Kapitel behandelt die folgenden Themen:



# Importieren neuer Anwendungen aus einer RDSH-Farm mithilfe von „Automatisch auf Farm suchen“

Um Remoteanwendungen für Benutzerzuweisungen bereitzustellen, müssen Sie die Anwendungen aus einer RDSH-Anwendungsfarm importieren.

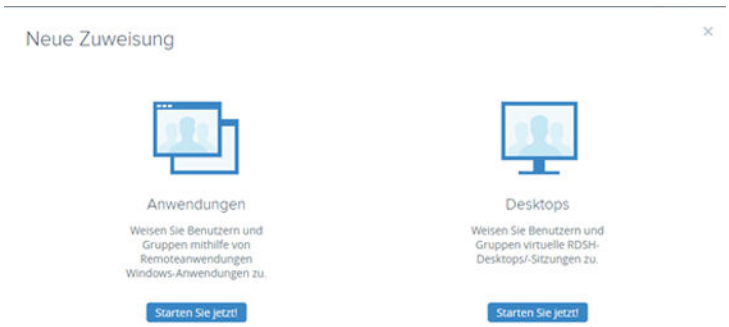
Wenn Ihre Umgebung mehrere Anwendungsfarmen enthält, wiederholen Sie diese Schritte, um die jeweils gewünschten Anwendungen aus den Farmen zu importieren.

### Voraussetzungen

Stellen Sie unter **Bestand > Farmen** sicher, dass in Ihrer Bestandsliste mindestens eine Anwendungsfarm verfügbar ist.

### Vorgehensweise

1 Klicken Sie auf der Seite „Anwendungen“ auf **Neu**.




2 Klicken Sie im Startbildschirm auf **Automatisch auf Farm suchen**.

Der erste Schritt des Assistenten wird geöffnet.

3 Wählen Sie die Anwendungsfarm aus, und klicken Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

   Wenn Sie auf **Weiter** klicken, wird die ausgewählte Farm nach Anwendungen durchsucht. Die gefundenen Anwendungen werden zur Auswahl angezeigt.

4 Wählen Sie die Anwendungen aus, die Sie zu Ihrem Anwendungskatalog hinzufügen möchten.

   Dieser Schritt des Assistenten zeigt die Anwendungen an, die bei der automatischen Suche im RDS-fähigen Windows Server-Betriebssystem gefunden wurden, das für die RDS-Server der Farm verwendet wird.

5 Klicken Sie auf **Weiter**, um mit dem nächsten Assistentenschritt fortzufahren.

6 (Optional) Passen Sie die konfigurierbaren Optionen für die ausgewählten Anwendungen ggf. an, und klicken Sie auf **Weiter**, um mit dem nächsten Assistentenschritt fortzufahren.

7 Überprüfen Sie die Zusammenfassung und klicken Sie auf **Übernehmen**.

Die ausgewählten Anwendungen werden zum Anwendungskatalog in Ihrem Horizon Cloud-Bestand hinzugefügt.

#### Weiter

Wiederholen Sie die Schritte, um Anwendungen aus Ihren anderen Farmen zu importieren.

## Manuelles Hinzufügen benutzerdefinierter Anwendungen aus einer RDSH-Farm

Einige Anwendungen werden beim Durchsuchen der Farm nicht automatisch erkannt. Sie können diese Anwendungen manuell zu Ihrem Horizon Cloud-Anwendungskatalog hinzufügen.

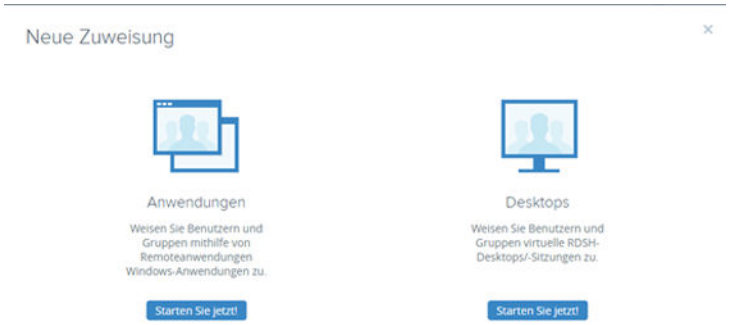
Wenn Sie über mehrere solcher Anwendungen verfügen, wiederholen Sie diese Schritte, um die gewünschten Anwendungen hinzuzufügen.

#### Voraussetzungen

Stellen Sie unter **Bestand > Farmen** sicher, dass in Ihrer Bestandsliste mindestens eine Anwendungsfarm verfügbar ist.

#### Vorgehensweise

1 Klicken Sie auf der Seite „Anwendungen“ auf **Neu**.




2 Klicken Sie im Startbildschirm auf **Manuell von Farm**.

3 Geben Sie im Abschnitt „Eigenschaften“ die folgenden Werte ein.

| Option | Beschreibung |
|---|---|
| **Name** | Eindeutiger Name für die Anwendung |
| **Anzeigename** | Name der Anwendung, der angezeigt wird, wenn Endbenutzer die Anwendung in ihren Clients öffnen, z. B. in Horizon Client oder Workspace ONE. |
| **Pod** | Diese Option wird nur angezeigt, wenn Ihr Datencenter mit mehreren Pods konfiguriert ist. Wählen Sie einen Pod aus, um die in der Liste **Farm** angezeigten Farmen zu filtern. |
| **Farm** | Wählen Sie die Farm aus, die über die RDSH-Server-VM verfügt, aus der Sie die Anwendung hinzufügen möchten. |
| **Anwendungspfad** | Geben Sie den Pfad der Anwendung im Betriebssystem der RDSH-Server-VM an. |
| **Symboldatei** | Optional: Laden Sie eine PNG-Datei (32 x 32 Pixel) herunter, die als Symbol der Anwendung verwendet werden soll. |

4 Legen Sie im Abschnitt „Erweiterte Eigenschaften“ die folgenden optionalen Einstellungen fest.

| Option | Beschreibung |
|---|---|
| **Verfügbare Anwendung in der Farm** | Wählen Sie **Ja**, damit das System den Anwendungspfad überprüft. Wenn die Anwendung nicht in der Farm unter diesem Pfad vorhanden ist, wählen Sie **Nein**, damit das System nicht nach der Anwendung sucht. Wenn eine Anwendung beispielsweise im lokalen Verzeichnis auf der Server-VM gespeichert ist, wählen Sie **Nein** aus, damit das System nicht versucht, die Anwendung dort zu finden. |
| **Version** | Optional: Versionsnummer der Anwendung |
| **Herausgeber** | Optional: Herausgeber der Anwendung |
| **Startordner** | Geben Sie den Speicherort im Windows-Betriebssystem der RDS-Server-VM an, den die Remoteanwendung als Startordner verwenden soll.<br>**Hinweis** Wenn Sie unter **Anwendungspfad** eine LNK-Datei angeben, die ein eigenes Startverzeichnis angibt, wird der hier angegebene Speicherort nicht verwendet. |
| **Parameter** | Geben Sie die Befehlszeilenparameter an, die beim Starten der Remoteanwendung verwendet werden sollen. |

5 Klicken Sie auf **Übernehmen**.

Ein Eintrag für die Anwendung wird auf der Seite „Anwendungen“ hinzugefügt.

### Weiter

Wiederholen Sie die Schritte für alle Anwendungen, die Sie aus Ihren anderen Farmen hinzufügen möchten.

# Bearbeiten einer Anwendung

Mit dem folgenden Verfahren können Sie eine Anwendung bearbeiten.

### Vorgehensweise

1 Wählen Sie eine Anwendung auf der Anwendungsseite aus und klicken Sie oben auf der Seite auf die Schaltfläche **Bearbeiten**.

Das Dialogfeld „Bearbeiten Sie die Anwendung“ wird angezeigt.

2 Bearbeiten Sie die Informationen wie unten beschrieben.

**Hinweis** Einige Elemente können nicht bearbeitet werden.

| Feld | Beschreibung |
|---|---|
| **Name** | Eindeutiger Name für die Anwendung |
| **Anzeigename** | Name der Anwendung, der angezeigt wird, wenn Endbenutzer die Anwendung in ihren Clients öffnen, z. B. in Horizon Client oder im Browser mit Horizon HTML Access. |
| **Pod** | Diese Option wird nur angezeigt, wenn Ihr Datencenter mit mehreren Pods konfiguriert ist. Zeigt den Namen des Pods an, in dem die Farm enthalten ist. |
| **Farm** | Der Farm, die beim Hinzufügen der Anwendung zu Ihren Bestand angegeben wurde. |
| **Anwendungspfad** | Speicherort der ausführbaren Anwendungsdatei auf der VM (z. B. „Z:\Customapps\app.exe“) oder UNC-spezifizierter Pfad (z. B. „\\fileserver.accounting.com\vol1\software\app.exe“) |
| **Symboldatei** | PNG-Datei (32 x 32 Pixel), die als Symbol für die Anwendung verwendet wird. [optional] Klicken Sie auf „Datei auswählen“, um zu einer Datei zu navigieren. |
| **Verfügbare Anwendung in der Farm** | Diese Option gibt wieder, was beim Hinzufügen der Anwendung zu Ihrem Bestand festgelegt wurde. |
| **Version** | Versionsnummer der Anwendung [optional] |
| **Herausgeber** | Herausgeber der Anwendung [optional] |
| **Startordner** | Geben Sie den Speicherort im Windows-Betriebssystem der RDS-Server-VM an, den die Remoteanwendung als Startordner verwenden soll.<br>**Hinweis** Wenn Sie unter **Anwendungspfad** eine LNK-Datei angeben, die ein eigenes Startverzeichnis angibt, wird der hier angegebene Speicherort nicht verwendet. |
| **Parameter** | Geben Sie die Befehlszeilenparameter an, die beim Starten der Remoteanwendung verwendet werden sollen. |

3 Klicken Sie auf **Speichern**.

# Löschen einer Anwendung

Mit dem folgenden Verfahren können Sie eine Anwendung löschen.

### Vorgehensweise

1 Wählen Sie eine Anwendung auf der Anwendungsseite aus und klicken Sie oben auf der Seite auf die Schaltfläche „Löschen“.

Das Bestätigungsdialogfeld wird angezeigt.

2 Klicken Sie zum Bestätigen des Löschvorgangs auf **OK**.

# Umbenennen einer Anwendung

Mit dem folgenden Verfahren benennen Sie eine Anwendung um.

### Vorgehensweise

1 Wählen Sie auf der Seite „Anwendungen“ eine Anwendung aus und klicken Sie oben auf der Seite auf die Schaltfläche **Umbenennen**.

Das Dialogfeld „Umbenennen“ wird geöffnet.

2 Geben Sie den neuen Namen ein und klicken Sie auf **Speichern**.

Der neue Anwendungsname wird in der Liste aufgeführt.

# Ausblenden einer Anwendung

Mit dem folgenden Verfahren können Sie eine Anwendung auf der Seite „Anwendungen“ ausblenden (deaktivieren).

**Hinweis** Die Anwendung wird dabei nicht aus dem System gelöscht, sondern nur deaktiviert. Die Anwendung wird aus der Liste der sichtbaren (aktivierten) in die Liste der ausgeblendeten (deaktivierten) Anwendungen verschoben. Anwendungen können nur über die Funktion „Löschen“ gelöscht werden.

### Vorgehensweise

1 Wählen Sie auf der Seite „Anwendungen“ eine Anwendung aus.

2 Klicken Sie oben auf der Seite auf die Schaltfläche **Ausblenden**.

Die Anwendung wird deaktiviert und in die Liste der ausgeblendeten Anwendungen verschoben.

# Einblenden einer Anwendung

Mit dem nachfolgenden Verfahren können Sie eine Anwendung auf der Seite „Anwendungen“ einblenden (aktivieren).

**Vorgehensweise**

1 Wählen Sie oben in der Anwendungsliste im Anzeigefilter die Option „Ausgeblendet“ .

Die Liste der sichtbaren (aktivierten) Anwendungen wird durch die Liste der ausgeblendeten (deaktivierten) Anwendungen ersetzt.

2 Wählen Sie die Anwendung aus und klicken Sie auf **Einblenden**.

Die Anwendung wird wieder aktiviert und in die Liste der sichtbaren (aktivierten) Anwendungen verschoben.

# Importieren von Anwendungen mithilfe von App Volumes

VMware App Volumes™ ist ein integriertes und vereinheitlichtes Anwendungsbereitstellungs- und Endbenutzerverwaltungssystem für Horizon® und virtuelle Umgebungen. Sie können die AppCapture-Komponente von App Volumes verwenden, um AppStacks für die Verteilung von Anwendungen an Benutzer zu erstellen.

Hinweis:

- Ihr VMware-Vertreter muss die Integration von App Volumes für Sie aktivieren, bevor Sie mit dieser Funktion arbeiten können.
- App Volumes wird für dedizierte Desktops – Traditional Clone-Zuweisungen nicht unterstützt. App Volumes kann nur mit Instant Clone-Zuweisungen verwendet werden.

Dieser Vorgang besteht aus drei Schritten:

- Erstellen eines AppStacks mithilfe von AppCapture
- Kopieren des AppStacks in eine Anwendungsdateifreigabe
- Importieren Sie den AppStack in Horizon Cloud.

Die ersten beiden Schritte werden auf einem separaten Computer ausgeführt, also außerhalb der Benutzeroberfläche.

## Erstellen eines AppStacks mithilfe von AppCapture

Erstellen Sie mit dem AppCapture-Tool einen AppStack auf einem separat verwalteten Computer, auf dem sich die Anwendungen befinden, die für die Zuweisungen erfasst werden sollen.

- Um einen AppStack mithilfe von AppCapture zu erstellen, gehen Sie vor wie in Verwalten von Anwendungen zur Bereitstellung mit AppCapture erläutert.
- Kopieren Sie den fertigen AppStack in die Dateifreigabe. Siehe Kopieren eines AppStacks zu einer Dateifreigabe.

### Verwalten von Anwendungen zur Bereitstellung mit AppCapture

Mit AppCapture erstellen Sie AppStacks zum Bereitstellen von Anwendungen für Benutzer.

Bevor Sie Benutzern Anwendungen zuweisen können, müssen Sie diese Anwendungen erfassen und in AppStacks packen. Dazu verwenden Sie das AppCapture-Dienstprogramm. Dann müssen Sie die AppStacks manuell in eine Dateifreigabe kopieren.

### AppCapture -Systemanforderungen

Beachten Sie die folgenden AppCapture-Mindestanforderungen für Windows-Plattformen.

### AppCapture -Systemanforderungen

Um AppCapture installieren und ausführen zu können, müssen Sie sicherstellen, dass Ihr System die im Folgenden aufgeführten Systemanforderungen erfüllt.

- Betriebssystem: AppCapture funktioniert auf Windows 7- und Windows 10-Plattformen, auf sowohl x86- (32-Bit) als auch 64-Bit-Computern: auf physischen, Workstations oder ESX VMs.
- Festplattenspeicher: Die benötigte Menge an Festplattenspeicher richtet sich nach Anzahl und Größe der Anwendungen, die Sie bereitstellen. Stellen Sie sicher, dass Ihr System über ausreichend Festplattenspeicher für alle AppStacks verfügt, die Sie erstellen.
- AppCapture Client: Um AppCapture Client verwenden zu können, das mit AppCapture installiert wird, muss .Net 4.6.1 auf Ihrem System installiert sein.

### Installieren Sie AppCapture

Mit dem Dienstprogramm AppCapture packen Sie Anwendungen zum Kopieren in eine Dateifreigabe.

#### Voraussetzungen

- Bereiten Sie eine neue Windows-Maschine mit deaktivierter Benutzerzugriffssteuerung (User Access Control, UAC) vor. Erläuterungen zur Deaktivierung der UAC finden Sie unter http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#ITC=windows-7.
- App Volumes Agent darf nicht auf der virtuellen Maschine installiert sein, auf der AppCapture installiert werden soll. Wenn App Volumes Agent auf der Maschine installiert ist, erstellen Sie einen Snapshot der Maschine, schließen Sie sie und deinstallieren Sie den Agenten.

#### Vorgehensweise

1. Melden Sie sich als Administrator bei der Maschine an, auf der AppCapture installiert werden soll.
2. Laden Sie das Installationsprogramm („`VMware-appvolumes-appcapture-<buildnumber>.exe`“) für AppCapture von der VMware-Downloadseite herunter.
3. Doppelklicken Sie auf das Installationsprogramm und installieren Sie AppCapture gemäß den Anweisungen auf dem Bildschirm.
4. Nach dem Neustart der Maschine überprüfen Sie, ob `AppCapture.exe` im Verzeichnis `C:\Program Files(x86) \VMware\AppCapture` installiert ist.

#### Weiter

- Der UEM-Anwendungsprofiler wird zusammen mit dem Dienstprogramm AppCapture installiert. Sie können AppStacks mit dem UEM-Anwendungsprofiler personalisieren.

- Bei der Installation von AppCapture wird auch die Benutzeroberfläche von AppCapture installiert. Mit AppCapture Client erstellen und verwalten Sie App Bundles. Siehe Verwenden von AppCapture Client.

### Verwenden von AppCapture

Bevor Sie Anwendungen zu Benutzern zuweisen können, müssen Sie die Anwendungen in AppStacks packen. Ein AppStack ist eine Sammlung von Dateien, Ordnern, Registrierungen und Metadaten, die in `.vhd`- oder `.vmdk`-Dateien gespeichert sind. Der AppStack ist mit einer `.json`-Datei verknüpft.

Mit AppCapture erstellen und verwalten Sie AppStacks. Bei AppCapture handelt es sich um ein eigenständiges Dienstprogramm, das Sie außerhalb von App Volumes ausführen. Sie können AppCapture entweder über die Befehlszeile aus AppCapture GUI oder über Microsoft PowerShell ausführen.

Zum Erstellen von AppStacks auf einer virtuellen Maschine verwenden Sie das AppCapture-Dienstprogramm.

App Volumes verwendet nur .vmdk-Dateien. Sie können auch .vhd-Dateien verwenden, um Anwendungen auf einem physischen Computer mit anderen VMware-Produkten zu installieren.

### AppCapture und UEM-Anwendungsprofiler

Sie können einen AppStack mit erfassten Anwendungen personalisieren, ohne tatsächlich eine Zuweisung vorzunehmen.

Die Personalisierung erfolgt mit dem UEM-Anwendungsprofiler (im Installationsprogramm für AppCapture enthalten). Mit dem Befehl `AppCapture.exe` und der Option `/personalize` öffnen Sie das Fenster des UEM-Anwendungsprofilers. Sie können die zu personalisierenden Anwendungen auswählen und die Einstellungen speichern.

Weitere Informationen zur Option `/personalize` finden Sie unter Befehlszeilenoptionen für AppCapture.

### Ausführen von AppCapture von der Befehlszeile

Sie können AppCapture von einer Befehlszeile aus ausführen.

**Hinweis** Die Anwendungen müssen aus demselben Betriebssystem erfasst werden, unter dem diese Anwendungen bereitgestellt sind. Wenn die Benutzer beispielsweise mit einem Win7x64-Betriebssystem arbeiten, müssen Sie die Anwendungen mithilfe eines ähnlichen oder identischen Basisbetriebssystem-Win7x64-Images erfassen.

#### Voraussetzungen

1 Sie müssen AppCapture als Administrator ausführen.

2 Überprüfen Sie, dass die Benutzerkontensteuerung (User Account Control , UAC) in Windows deaktiviert ist. Informationen zur UAC-Deaktivierung finden Sie unter http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#1TC=windows-7.

3 Überprüfen Sie, dass der CLI-Befehl `AppCapture.exe` unter `C:\Program Files (x86)\VMware\AppCapture` (64-Bit-Computer) bzw. `C:\Program Files\VMware\AppCapture` (32-Bit-Computer) installiert ist.

4 Informationen zu den Optionen des `AppCapture.exe`-Befehls finden Sie unter Befehlszeilenoptionen für AppCapture.

### Vorgehensweise

1 Fertigen Sie einen Snapshot des Systems an.

   Sie können das System nach der Erfassungssitzung zum Snapshot wiederherstellen.

2 Öffnen Sie ein Konsolenfenster.

3 Führen Sie den folgenden `AppCapture.exe`-Befehl aus: **`AppCapture.exe /n`** *your_appstack_name*.

   Drücken Sie an dieser Stelle nicht die Eingabetaste.

   Die AppStack-Festplatte der virtuellen Maschine steht in der Regel in weniger als einer Minute zur Verfügung.

4 Minimieren Sie das AppCapture-Fenster, und führen Sie die herkömmliche Windows-Installation aus, um alle Anwendungsinstallationsprogramme aufzunehmen.

   a Akzeptieren Sie die vollständige Installation aller Anwendungen auf der Festplatte C:. Die Installationsaktivität wird zur virtuellen Ausgabefestplatte weitergeleitet.

   b Wenn ein Installationsprogramm einen Neustart erfordert, müssen Sie warten, bis der Neustart abgeschlossen ist.

   c Wenn diese Funktion verfügbar ist, können Sie auch ThinApp-MSI-Pakete ausführen. Diese Pakete werden mit demselben Verfahren wie andere MSI-Anwendungspakete installiert. Weitere Informationen zum Erstellen von ThinApp-MSI-Paketen finden Sie in der aktuellen ThinApp-Dokumentation.

5 Schließen Sie die Erstellung der virtuellen Festplatte ab.

   a Nachdem alle Installationsprogramme ausgeführt wurden, die in diesem AppStack erfasst werden müssen, kehren Sie zum Konsolenfenster zurück.

   b Drücken Sie die **Eingabe**-Taste, um einen Neustart einzuleiten und die Erstellung der virtuellen Festplatte abzuschließen.

      Nach dem Neustart sehen Sie den neuen AppStacks mit Anwendungen.

   c Überprüfen Sie, ob neue VHD- und VMDK-Dateien unter `C:\ProgramData\VMware\AppCapture\appvhds` vorliegen.

6 Rufen Sie die Anwendungen in der VHD-Datei und den VMDK-Dateien mit dem Befehl `AppCapture.exe` ab. VHD-Dateien: **`AppCapture.exe /list`** *Name_meines_AppStacks.vhd*; VMDK-Dateien: **`AppCapture.exe /list`** *Name_meines_AppStacks.vmdk*

7 Kopieren Sie den AppStacks, den Sie erstellt haben, in eine Staging-Dateifreigabe Ihrer Wahl.

8 Stellen Sie das System zum Snapshot wieder her, den Sie erfasst haben, bevor Sie die erste Erfassungssitzung gestartet haben.

9 Kopieren Sie die AppStacks von der Staging-Dateifreigabe in Ihr System.

### Befehlszeilenoptionen für AppCapture

Mit den Befehlszeilenoptionen für AppCapture erstellen und verwalten Sie AppStacks.

Optionen des Befehls `AppCapture.exe`

Die Optionen `/meta`, `/vhd` und `/vmdk` sind nützlich, falls Sie versehentlich eine JSON-, VHD- oder VMDK-Datei gelöscht haben. Falls eine JSON-Datei gelöscht wurde, kann App Volumes den AppStack nicht lesen.

Mit dem Befehl `/personalize` personalisieren Sie einen AppStack.

Der `AppCapture.exe`-Befehl akzeptiert die folgenden Optionen:

**Tabelle 7-1. Befehlszeilenoptionen für `AppCapture.exe`**

| Aufgabe | Option |
|---|---|
| Anzeigen von Hilfe für den Befehl `AppCapture.exe`. | `/?` |
| Angeben eines Namens für den AppStack-Autor. Wenn der Name mindestens ein Leerzeichen enthält, muss er in Klammern eingeschlossen sein.<br>Beispiel: **`AppCapture.exe /n /a (IT Admin)`** | `/a` |
| Angeben einer AppStack-Beschreibung.<br>Beispiel:<br>**`Dieser Datenträger enthält die Anwendungssuite XYZ.`** | `/d` |
| Auflisten des Inhalts der JSON-, VHD- und VMDK-Dateien im AppStack. Wenn Sie nicht das Standardverzeichnis verwenden, müssen Sie das Verzeichnis angeben, in dem sich die Dateien befinden.<br>Beispiel: **`AppCapture.exe /list`** ***`Dateipfad`*** | `/list` |
| Erzeugen einer `JSON`-Datei unter Verwendung einer VMDK-Datei als Eingabe. Wenn Sie nicht das Standardverzeichnis verwenden, müssen Sie das Verzeichnis angeben, in dem sich die VMDK-Datei befindet.<br>Beispiel: **`AppCapture.exe /meta`** ***`appStackPfad`***. | `/meta` |
| Erstellen eines AppStack.<br>Beispiel: **`AppCapture.exe /n`** | `/n` |
| Angeben eines Ausgabeverzeichnisses für die AppStack-Dateien. Das Standardverzeichnis ist `C:\ProgramData\VMware\AppCapture\appvhds`.<br>Sie können diese Option mit der `/s`-Option verwenden, um einen AppStack aus einem vorhandenen AppStack zu erstellen. Siehe Aktualisieren eines AppStack von der Befehlszeile aus.<br>Beispiel:<br>**`AppCapture.exe /s`** ***`oldAppStackDir`*** **`/o`** ***`newAppStackDir`*** | `/o` |

**Tabelle 7-1. Befehlszeilenoptionen für `AppCapture.exe` (Fortsetzung)**

| Aufgabe | Option |
|---|---|
| Angeben eines Quellverzeichnisses für die AppStack-Dateien. Das Standardverzeichnis ist `C:\ProgramData\VMware\AppCapture\appvhds`.<br>Verwenden Sie diese Option nicht, wenn Sie eine neue Anwendung installieren.<br>Sie können diese Option mit der `/o`-Option verwenden, um einen AppStack aus einem vorhandenen AppStack zu erstellen. Siehe Aktualisieren eines AppStack von der Befehlszeile aus.<br>Beispiel:<br>**`AppCapture.exe /s oldAppStackDir /o newAppStackDir`**<br>Sie können die Option `/s` auch mit `/n` verwenden, um einen alten AppStack durch einen neuen zu aktualisieren. In diesem Beispiel wird die vorhandene *oldAppStack.vhd* AppStack als Basis-AppStack kopiert und dann als *newAppstackName* aktualisiert:<br>**`AppCapture.exe /n newAppstackName /s oldAppStack.vhd /o newAppStackDir`** | `/s` |
| Erstellen einer `.vhd`-Datei aus einer `.vmdk`-Datei. Wenn Sie nicht den Standardpfad verwenden, müssen Sie den Pfad angeben, unter dem sich die `.vhd`-Datei befindet.<br>Beispiel: **`AppCapture.exe /vhd appStackPath.vmdk`** | `/vhd` |
| Erzeugen einer VMDK-Datei unter Verwendung einer VHD-Datei als Eingabe Wenn Sie nicht den Standardpfad verwenden, müssen Sie den Pfad angeben, unter dem sich die `.vhd`-Datei befindet.<br>Beispiel: **`AppCapture.exe /vmdk appStackPath.vhd`**. | `/vmdk` |

**Tabelle 7-1. Befehlszeilenoptionen für `AppCapture.exe` (Fortsetzung)**

| Aufgabe | Option |
|---|---|
| Virtualisieren der Anwendung nach der Bereitstellung zur Vorverifizierung Wenn Sie die Option `/test` ohne weitere Parameter angeben, sollte der AppStack nur ein einziges Anwendungspaket enthalten.<br>Beispiel:<br>**AppCapture.exe /test *bereitgestellter appStack-Pfad*.vhd**<br>Virtualisieren Sie alle Anwendungspakete im AppStack. Beispiel:<br>**AppCapture.exe /test *bereitgestellter appStack-Pfad*.vhd ***<br>Virtualisieren Sie Anwendungspakete, die über ihre entsprechenden GUIDs im AppStack gekennzeichnet sind. Beispiel:<br>**AppCapture.exe /test *bereitgestellter appStack-Pfad*.vhd *GUID1, GUID2 GUIDn*** | `/test <Provisioned AppStackPath>.vhd [* \| GUID]` |
| Möglichkeit für Benutzer zum Personalisieren des Anwendungspakets mithilfe des UEM-Anwendungsprofilers Es werden Konfigurationsdateien mit den Personalisierungseinstellungen erzeugt. Standardmäßig werden die Dateien in demselben Verzeichnis wie die VHD-Datei gespeichert, also im Ordner `UEMConfigFiles\*AppStack*`.<br>Beispiel:<br>**AppCapture.exe /personalize *C:\FinanceApps.vhd*** – Die Personalisierungseinstellungen werden unter `C:\Programme\VMware\AppCapture\appvhds\UEMConfigFiles\FinanceApps` gespeichert.<br>Die Unteroption `/predef` fungiert als optionaler boolescher Schalter für die Option `/personalize`. Mit diesem Schalter erfassen Sie die vordefinierten Einstellungen des angegebenen Anwendungspakets in einer Konfigurationsdatei. Die vordefinierten Einstellungen werden in einer zusätzlichen Konfigurationsdatei erfasst.<br>Beispiel:<br>**AppCapture.exe /personalize *C:\FinanceApps.vhd* /predef** – Die Personalisierungseinstellungen und die vordefinierten Einstellungen werden unter `C:\Programme\VMware\AppCapture\appvhds\UEMConfigFiles\FinanceApps` gespeichert.<br>Mit der Unteroption `/flexconfigname` für den Befehl `/personalize` speichern Sie die Personalisierungseinstellungen unter einem aussagekräftigen Konfigurationsdateinamen.<br>Beispiel:<br>**AppCapture.exe /personalize *C:\FinanceApps.vhd* /flexconfigname *MSOffice2016*** – Die Personalisierungseinstellungen werden unter `C:\Programme\VMware\AppCapture\appvhds\UEMConfigFiles\MSOffice2016` gespeichert. | `/personalize <ProvisionedAppStackPath>.vhd [/predef \| flexconfigname <flexconfigfilename> ]` |

## Zusammenführen von AppStacks

Sie können zwei oder mehr AppStacks von der Befehlszeile aus zusammenführen. Dazu verwenden Sie AppMerge.

Mithilfe von AppMerge führen Sie zwei oder mehr vorhandene AppStacks zu einer Datei zusammen. Als Eingabe für einen AppMerge dienen die VHD-Dateien, die mit einem AppStack verknüpft sind.

**Hinweis** Alle AppStack-Eingabedateien müssen im VHD-Format vorliegen. Sie können einen zusammengeführten Ausgabe-AppStack mit einem anderen Typ erstellen, indem Sie die Optionen `/vhd` und `/vmdk` verwenden.

AppMerge hat die folgende Syntax:

**`AppMerge.exe /o *outputAppStack* /s "*inputAppStack1file*","*inputAppStack2file*", "*inputAppStack3file*",...`**

Beispiel: **Erstellen eines zusammengeführten AppStack**

In diesem Beispiel erstellen Sie eine AppStack-Datei namens `MergedAppstack.vhd` aus den drei vorhandenen AppStack-Dateien `Office.vhd`, `Notepad++.vhd` und `Firefox.vhd`:

**`AppMerge.exe /o C:\MergedAppstack.vhd /s "Office.vhd","Notepad++.vhd","Firefox.vhd"`**

Sie können die Eingabedateipfade, die Ausgabedateipfade und die Dateinamen angeben. In diesem Fall wird angenommen, dass sich die drei Eingabe-AppStacks am AppStack-Standardspeicherort befinden. Der Ausgabe-AppStack wird auf dem Laufwerk C: abgelegt.

Neben den Parametern `/o` und `/s` akzeptiert AppMerge die folgenden Optionen:

- `/df`. Löscht ein spezifisches Anwendungspaket. Nimmt einen vollständigen Pfad einer Datei, die eine einzelne GUID in jeder Zeile enthält, als ihre Argumente.
- `/dl`. Löscht ein spezifisches Anwendungspaket. Nimmt durch Komma getrennte GUIDs als Argumente.
- `/list`. Listet den Inhalt der neu erstellten AppStack-Datei auf.
- `/meta`. Erstellt eine JSON-Datei aus der AppStack-Ausgabedatei
- `/vhd` Erstellt eine AppStack-VHD-Ausgabedatei aus AppStack-VMDK-Eingabedateien
- `/vmdk`. Erstellt eine AppStack-VMDK-Ausgabedatei aus AppStack-VHD-Eingabedateien

Siehe auch Befehlszeilenoptionen für AppCapture.

### Aktualisieren eines AppStack von der Befehlszeile aus

Sie aktualisieren einen AppStack, um Anwendungen hinzuzufügen, vorhandene Anwendungen zu aktualisieren oder Anwendungen aus dem AppStack zu entfernen.

#### Voraussetzungen

Stellen Sie sicher, dass Sie über die richtigen Anmeldedaten verfügen und dass die entsprechenden Voraussetzungen erfüllt sind:

- Führen Sie AppCapture als Administrator aus.
- Erstellen Sie mindestens einen AppStack.

- Deaktivieren Sie die Benachrichtigungen der Benutzerkontensteuerung (User Account Control – UAC) auf dem bereitstellenden Computer. Siehe http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#1TC=windows-7.
- Machen Sie sich mit den Befehlsoptionen vertraut, die für das Aktualisieren eines AppStack gelten. Siehe Befehlszeilenoptionen für AppCapture.

### Vorgehensweise

1 Öffnen Sie die Befehlszeile und navigieren Sie zum AppCapture-Ordner – entweder mit `cd "\Program Files\VMware\AppCapture"` (64-Bit) oder `cd "\Program Files (x86)\VMware\AppCapture"` (32-Bit).

2 Aktualisieren eines AppStack:

   a Führen Sie `AppCapture.exe /n` *`appStackName`* `/s` *`sourceAppStackDir`* aus.

   *sourceAppStackDir* ist der Pfad des AppStack, das Sie aktualisieren möchten.

   Dieses Beispiel verwendet einen vorhandenen AppStack und aktualisiert ihn zu einem neuen Aktualisierungs-AppStack:

   ```
   AppCapture.exe /n AdminUser2.0 /s "C:ProgramData\VMware\AppCapture\appvhds\AdminUser1.0" /o C:\NewFolder
   ```

   Sie können andere Befehlsoptionen einbeziehen, die für das Aktualisieren eines AppStack gelten.

   Der AppStack wird erstellt und an dem von Ihnen angegebenen Speicherort gespeichert oder standardmäßig im `appvhds`-Ordner.

   b Fügen Sie Anwendungen hinzu, aktualisieren Sie vorhandene Anwendungen oder entfernen Sie Anwendungen aus dem AppStack.

| Aufgabe | Aktion |
|---|---|
| **Anwendungen hinzufügen oder vorhandene Anwendungen aktualisieren** | Führen Sie die Installationsprogramme für die Anwendungen aus, die Sie in dem AppStack installieren oder aktualisieren möchten. |
| **(Optional) Anwendungen entfernen** | 1 Navigieren Sie zu **Systemsteuerung > Programme und Features**.<br>2 Wählen Sie die Anwendungen aus, die Sie aus dem AppStack entfernen möchten, und schließen Sie das Deinstallationsverfahren ab. |

3 Nachdem Sie die Anwendungen hinzugefügt oder entfernt haben, navigieren Sie zur Befehlszeile und drücken Sie die **Eingabe**-Taste.

4 Drücken Sie die **Eingabe**-Taste, um einen Neustart auszuführen und das AppStack-Aktualisierungsverfahren abzuschließen.

Nach dem Neustart des Computers werden die JSON-, VHD- und VMDK-Dateien erstellt. Wenn der Anwendungserfassungsprozess abgeschlossen ist, werden die Anwendungen vom Computer entfernt.

## Verwenden von AppCapture mit Microsoft PowerShell

Sie können Microsoft PowerShell-cmdlets verwenden, um Anwendungen zu erfassen, um AppStacks zu erstellen und zu aktualisieren und um gelöschte AppStacks mit AppCapture erneut zu erstellen. Sie können die 32-Bit- oder 64-Bit-PowerShell-Konsole verwenden, um das AppCapture-Modul auszuführen.

Sie können AppCapture von der Befehlszeile aus ausführen, wie es in Ausführen von AppCapture von der Befehlszeile beschrieben ist.

**Hinweis** Sie müssen Anwendungen aus demselben Betriebssystem erfassen, in dem Sie diese bereitstellen. Wenn Benutzer zum Beispiel mit einem Win7x64-Betriebssystem arbeiten, müssen Sie die Anwendungen erfassen, indem Sie ein ähnliches oder identisches Basisbetriebssystem-Win7x64-Image verwenden.

## Ausführen von AppCapture mithilfe von PowerShell

Sie können AppCapture mithilfe von Microsoft PowerShell ausführen.

### Voraussetzungen

Stellen Sie sicher, dass Sie als Administrator angemeldet sind und dass die entsprechenden Voraussetzungen erfüllt sind:

- Führen Sie AppCapture als Administrator aus.
- Deaktivieren Sie die Benutzerkontensteuerung (User Account Control – UAC). Siehe http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#1TC=windows-7
- Machen Sie sich mit denAppCapture-cmdlets vertraut. Siehe PowerShell-Optionen und -Parameter.

### Vorgehensweise

1. Fertigen Sie einen Snapshot des Systems an.

   Sie können das System nach der Erfassungssitzung zum Snapshot wiederherstellen.
2. Öffnen Sie eine 32-Bit- oder 64-Bit-PowerShell-Konsole.
3. Importieren Sie das PowerCLI-Modul mithilfe des **`import-module vmware.appcapture`**-Befehls.

   Dadurch wird das AppCapture-Modul importiert.
4. (Optional) Um eine Liste aller Module anzuzeigen, führen Sie den **`get-module`**-Befehl aus.
5. Führen Sie den Befehl `Start-AVAppCapture -Name` *appStackFile* aus, wobei *appStackFile* der Name der AppStack `.vhd`-Datei ist, die erstellt werden soll.

   Drücken Sie noch nicht die **Eingabe**-Taste.

   *appStackFile*`.vhd` wird erstellt.
6. Verlassen Sie die PowerShell-Konsole und installieren Sie auf diesem Computer alle Anwendungen, die bereitgestellt werden sollen.
7. Nachdem alle Anwendungen installiert wurden, öffnen Sie erneut die PowerShell-Konsole.

8 Drücken Sie die **Eingabe**-Taste.

9 Führen Sie einen Neustart Ihres Computers durch, falls dies erforderlich ist.

Im AppCapture-Konsolenfenster sehen Sie die Speicherorte der AppStack-Dateien `.json`, `.vhd` und `.vmdk`. Standardmäßig werden diese Dateien in `C:\ProgramData\VMware\AppCapture\appvhds` gespeichert.

10 (Optional) Überprüfen Sie die `.json`-, `.vhd`- und `.vmdk`-Dateien in diesem Verzeichnis, um sicherzustellen, dass die Anwendungen in das Paket aufgenommen wurden.

11 Kopieren Sie die AppStacks, die Sie erstellt haben, in eine Staging-Dateifreigabe.

12 Stellen Sie das System zum Snapshot wieder her, den Sie erfasst haben, bevor Sie die erste Erfassungssitzung gestartet haben.

13 Kopieren Sie die AppStacks von der Staging-Dateifreigabe in Ihr System.

PowerShell-Optionen und -Parameter

Sie können verschiedene Optionen verwenden, wenn Sie AppCapture mit Microsoft PowerShell ausführen.

AppCapture -Optionen und -Parameter mit PowerShell

Verwenden Sie die Option `Start-AVAppCapture`, um einen AppStack zu erstellen und ihm Anwendungen hinzuzufügen. Der UEM-Anwendungsprofiler wird zusammen mit dem Dienstprogramm AppCapture installiert und Sie können die AppStacks mit dem Profiler konfigurieren.

**Tabelle 7-2.** `Start-AVAppCapture` **-Optionen**

| **`Start-AVAppCapture`-Parameter** | **Beschreibung** |
|---|---|
| `-Author` *Autorenname* | Angeben eines Autors, der mit diesem AppStack verknüpft ist. |
| *Gemeinsame Parameter* | Verwenden Sie einen oder mehrere gemeinsame Parameter. Die gemeinsamen Parameter sind eine Gruppe von cmdlet-Parametern, die durch Windows PowerShell implementiert werden.<br>`Start-AVAppCapture` unterstützt die folgenden gemeinsamen Parameter:<br>■ Debug<br>■ ErrorAction<br>■ ErrorVariable<br>■ OutBuffer<br>■ OutVariable<br>■ PipelineVariable<br>■ Verbose<br>■ WarningAction<br>■ WarningVariable<br>Weitere Informationen über gemeinsame Parameter finden Sie unter about_CommonParameters. |
| `-Description` *Text* | Angeben einer AppStack-Beschreibung. Wenn die Beschreibung ein Leerzeichen enthält, müssen Sie die Beschreibung in Klammern einschließen, zum Beispiel **`-Description (HR Apps)`**. |

### Tabelle 7-2. `Start-AVAppCapture` -Optionen (Fortsetzung)

| Start-AVAppCapture-Parameter | Beschreibung |
|---|---|
| `-Destination` *Ausgabeverzeichnis* | Angeben eines Ausgabeverzeichnisses für einen AppStack. Standardmäßig werden die AppStacks in `C:\ProgramData\VMware\AppCapture\appvhds` abgelegt. |
| `-Force` | Erstellen eines Ausgabeverzeichnisses, falls es noch nicht vorhanden ist. Sie geben das Ausgabeverzeichnis mit dem Parameter `-Destination` an. |
| `-Name` *vhd-Name* | Angeben eines Namens für die zu erfassenden Anwendungen.<br>Die ausgegebene `.vhd`-Datei wird unter Verwendung des angegebenen Anwendungsnamens benannt. |
| `-Novmdk` | Geben Sie diese Option an, um eine VMDK-Datenträgererstellung nach der Erfassung zu verhindern. |
| `-Path` *Verzeichnispfad* | Angeben eines Pfads zu einem AppStack. Der AppStack wird als Vorlage für die aktuelle Erfassung verwendet.<br>Verwenden Sie diese Option nicht, wenn Sie eine neue Anwendung installieren. |

Mit dem Befehl AppCapture können Sie verschiedene Workflows durchführen.

### Tabelle 7-3. AppCapture -PowerShell-Workflows

| Workflow | Beschreibung |
|---|---|
| `ConvertTo-AVVhdDisk` | Generieren einer `.vhd`-Datei unter Verwendung der `.vmdk`-Datei als Eingabe. |
| `ConvertTo-AVVmdkDisk` | Generieren einer `.vmdk`-Datei unter Verwendung der `.vhd`-Datei als Eingabe. |
| `Export-AVMetadata` | Generieren einer `.json`-Datei unter Verwendung einer `.vhd`- oder `.vmdk`-Datei als Eingabe. |
| `Merge-AVAppDisks` | Zusammenführen von AppStack `.vhd`-Dateien zu einer neuen AppStack `.vhd`-Datei. Zusammenführen von AppStacks beschreibt die Befehlszeilenversion, die ähnlich funktioniert. |
| `Remove-AVApp` | Löschen eines AppStacks von einer Festplatte oder Entfernen bestimmter Anwendungen aus einem AppStack Wenn Sie Anwendungen aus dem AppStack entfernen, muss der AppStack erneut in den App Volumes Manager importiert werden. |
| `Reset-AVConfig` | Löschen der AppCapture-Konfigurationsinformationen vom Computer. |
| `Show-AVDiskDetails` | Auflisten des Inhalts der `.vhd`-Datei, `.json`-Datei oder `.vmdk`-Datei. |
| `Start-AVAppCapture` | Starten des Verfahrens zur Erfassung von Anwendungen. |
| `Start-AVAppUpdate` | Aktualisieren eines AppStack. |

**Tabelle 7-3. AppCapture -PowerShell-Workflows (Fortsetzung)**

| Workflow | Beschreibung |
|---|---|
| `Test-AVAppStack` | Anhängen oder Virtualisieren von Anwendungen nach der Bereitstellung der Anwendung. |
| `Start-AVAppPersonalization` | Anhängen des AppStacks (`.vhd`) und Personalisieren des angegebenen Anwendungspakets mit dem UEM-Anwendungsprofiler |

Die nachfolgenden Beispiele enthalten die Workflow-Dateipfade und die Befehle zum Erreichen der Workflows.

- Starten einer neuen Erfassungssitzung Die Ausgabe wird als VHD-Datei erzeugt und erhält den Namen *AdobeSuite.vhd*. Als Autor wird *John* festgelegt und es wird eine Beschreibung hinzugefügt.

  **Start-AVAppCapture -Name AdobeSuite -Author John -Description "Dieser Datenträger enthält die AdobeSuite-Anwendung"**

- `ConverTo-AVVhdDisk`. Dieses Beispiel generiert eine Ausgabe im `.vhd`-Dateiformat, `Adobe.vhd`, aus einer Quelldatei, `Adobe.vmdk`. Die Ausgabedatei wird in einem anderen Verzeichnis abgelegt als die Quelldatei.

  **ConvertTo-AVVhdDisk -Path "C:\Program Files (x86)\VMware\AppCapture\appvhds\Adobe.vmdk" -Destination "C:\AppCaptures"**

- `Export-AVMetadata`. Dieses Beispiel generiert die Ausgabe-Metadatei `Adobe.json`. Die Datei wird an derselben Stelle generiert wie `Adobe.vhd`:

  **Export-AVMetadata -Path "C:\Program Files (x86)\VMware\AppCapture\appvhds\Adobe.vhd"**

- `Merge-AVAppDisks`. Dieses Beispiel führt alle `.vhd`-Dateien in den Verzeichnissen `.\temp` und `.\appstacks` zusammen und generiert eine `Notepad+Adobe.vhd`-Datei in `C:\temp`.

  **Merge-AVAppDisks -Path .\temp*.vhd .\appstacks*.vhd -Destination c:\temp\Notepad+Adobe.vhd**

- `Remove-AVApp`. Dieses Beispiel löscht die Adobe- und Notepad-Anwendungen vom Eingabedatenträger `Adobe+Notepad.vhd`. Jede Anwendung wird durch ihre eindeutige GUID identifiziert.

  **Remove-AVApp -Path C:\Temp\Adobe+Notepad.vhd -Destination C:\Temp\empty.vhd -Guids GUID1, GUID2**

- `Show-AVDiskDetails`. Dieses Beispiel zeigt die Details aus einer `.json`-Datei an. Die Syntax ist für `.vhd`- und `.vmdk`-Dateien dieselbe:

  **Show-AVDiskDetails -Path "C:\Program Files (x86)\VMware\WEM Capture\appvhds\Adobe.json"**

- `Start-AVAppUdate`. Dieses Beispiel aktualisiert die `AdobeSuite.vhd` durch einen Hotfix. Eine Kopie von `AdobeSuite.vhd` wird erstellt und erhält den Namen `AdobeHotfixUpdate.vhd`. Alle Hotfix-Installationen werden in `AdobeHotfixUpdate.vhd` erfasst:

  **`Start-AVAppUpdate -Name AdobeHotfixUpdate -Path "C:\Program Files (x86)\VMware\AppCapture\appvhds\AdobeSuite.vhd"`**

- `Test-AVAppStack -Path`: Virtualisieren der Anwendung nach der Bereitstellung zur Vorverifizierung Wenn Sie diesen Befehl ohne weitere Parameter angeben, sollte der AppStack nur ein einziges Anwendungspaket enthalten.

  **`Test-AVAppStack -Path C:\Program Files (x86)\VMware\WEMCapture\appvhds\Chrome.vhd`**

  - **`Test-AVAppStack -Path "C:\Program Files (x86)\VMware\WEMCapture\appvhds\HRApps.vhd" -Guids Guid1Guid2..Guid1. GUIDn`**. Mit diesem cmdlet werden Anwendungspakete virtualisiert, die durch die zugehörigen GUIDs im AppStack identifiziert sind.
  - **`Test-AVAppStack -Path "C:\Program Files (x86)\VMware\WEMCapture\appvhds\HRApps.vhd" -Guids "*"`**. Mit diesem cmdlet werden alle Anwendungspakete im AppStack virtualisiert.

- `Start-AVAppPersonalization -Path`. Mit diesem cmdlet wird die VHD-Datei angehängt und die Benutzer erhalten die Möglichkeit, das Anwendungspaket mit dem UEM-Anwendungsprofiler zu personalisieren. Die Personalisierungseinstellungen werden unter `C:\Programme\VMware\AppCapture\appvhds\UEMConfigFiles\Chrome` gespeichert.
  **`Start-AVAppPersonalization -Path "C:\Programme\VMware\AppCapture\appvhds\Chrome.vhd"`**

  - **`Start-AVAppPersonalization -Path "C:\appvhds\Chrome.vhd" -Predef`**. Mit diesem cmdlet wird die VHD-Datei angehängt und die Benutzer erhalten die Möglichkeit, das Anwendungspaket mit dem UEM-Anwendungsprofiler zu personalisieren. Die vordefinierten Einstellungen und die Personalisierungseinstellungen werden unter `C:\Programme\VMware\AppCapture\appvhds\UEMConfigFiles\Chrome` gespeichert.
  - **`Start-AVAppPersonalization -Path "C:\appvhds\Chrome.vhd" -Name Browser1`**. Mit diesem cmdlet wird die VHD-Datei angehängt und die Benutzer erhalten die Möglichkeit, das Anwendungspaket mit dem UEM-Anwendungsprofiler zu personalisieren. Die Dateien mit den Personalisierungseinstellungen werden unter `C:\Programme\VMware\AppCapture\appvhds\UEMConfigFiles\Browser1` gespeichert.

Mit dem Befehl **`get-help`** erhalten Sie Hilfe zu Workflows.

**Tabelle 7-4. AppCapture -PowerShell Workflow – Informationen und Beispiele**

| Befehl | Beschreibung |
|---|---|
| `get-help WorkflowName` | Anzeige allgemeiner Informationen über einen Workflow. |
| `get-help WorkflowName -detailed` | Anzeige detaillierter Informationen über einen Workflow. |
| `get-help WorkflowName -examples` | Anzeigen eines Beispiels für einen Workflow. |
| `get-help WorkflowName -full` | Anzeige technischer Informationen über einen Workflow. |

## Verwenden von AppCapture Client

AppCapture Client enthält eine grafische Benutzeroberfläche, mit denen Sie den AppCapture-Vorgang vereinfachen können.

Mit AppCapture Client können Sie App Bundles erstellen, aktualisieren, zusammenführen und testen. Sie haben auch die Möglichkeit, zusammengeführte AppStacks zu aktualisieren und verschiedene Aktion nach der Erfassung durchzuführen. AppStacks werden in der Benutzeroberfläche als App Bundles bezeichnet.

Wenn Sie die AppCapture-Befehle in der Benutzeroberfläche eingeben, wird die entsprechende Befehlszeichenfolge automatisch generiert. Sie können die Zeichenfolge kopieren und in die Befehlszeile einfügen. Klicken Sie auf **Skript einblenden**, um die generierte Zeichenfolge anzuzeigen.

## Hinzufügen einer Dateifreigabe

Bevor Sie mit AppCapture Client App Bundles erstellen und verwalten können, müssen Sie eine Dateifreigabe hinzufügen.

### Voraussetzungen

- Es wird empfohlen, beim Hinzufügen einer Dateifreigabe eine Remotedateifreigabe zu verwenden.
- Stellen Sie sicher, dass die Dateifreigabe auf der Maschine mithilfe von Domänenanmeldedaten bereitgestellt wird.

### Vorgehensweise

1. Starten Sie AppCapture Client und wechseln Sie zu **Einstellungen > Dateifreigabe**.
2. Wechseln Sie zum Speicherort der Dateifreigabe und wählen Sie diese aus.
3. Klicken Sie auf **Hinzufügen**.

   Das Feld „Name“ wird automatisch ausgefüllt.
4. (Optional) Geben Sie einen Namen für den Autor ein.
5. Klicken Sie auf **Speichern**.

   Anschließend wird die Seite App Bundles eingeblendet.

### Weiter

Sie können jetzt mit dem Erfassen, Aktualisieren und Testen von App Bundlesbeginnen.

## Erstellen eines App Bundle

Erstellen Sie ein App Bundle und erfassen Sie darin Anwendungen mithilfe von AppCapture Client.

**Hinweis** App Bundles können mehr als eine Anwendung enthalten. Um die Funktionen AppToggle und AppMerge allerdings maximal nutzen zu können, wird empfohlen, nur eine Anwendung in App Bundle zu installieren. Siehe Erstellen eines zusammengeführten App Bundle.

### Vorgehensweise

1 Klicken Sie in AppCapture Client auf **APP-BUNDLES**.

2 Klicken Sie auf **Erfassen** und geben Sie die folgenden Informationen ein:

| Option | Beschreibung |
|---|---|
| **Name (erforderlich)** | Der Name des App Bundle. |
| **Beschreibung (optional)** | Eine Beschreibung des App Bundle. |
| **Autor (Optional)** | Der Name der Person, die das App Bundle erstellt hat. Standardmäßig ist der aktuelle Benutzer oder der in den Einstellungen der Anwendung festgelegte Name ausgewählt. |
| **Ziel (schreibgeschützt)** | Hier wird automatisch der ausgewählte Speicherort der Dateifreigabe eingetragen. An diesem Speicherort werden die App Bundle-Dateien, die VHD-Dateien und zugehörige JSON-Dateien erstellt. |

Das generierte Befehlsskript wird am unteren Rand des Bildschirms angezeigt.

3 Klicken Sie auf **Erstellen**.

Der AppCapture-Vorgang wird gestartet. Sie werden aufgefordert, die Anwendungen zu installieren, die in App Bundleerfasst werden sollen. Folgen Sie den Bildschirmanweisungen, um das Erstellen des App Bundleabzuschließen.

### Weiter

Die Erfassung ist erst mit dem Neustart der virtuellen Maschine abgeschlossen. Nach dem Neustart der virtuellen Maschine und dem automatischen Neustart von AppCapture Client wechseln Sie zur Seite **APP-BUNDLES**. Doppelklicken Sie auf das erstellte Paket und prüfen Sie, ob das Paket die darin installierten Anwendungen enthält.

## Aktualisieren eines App Bundle :

Sie können mit AppCapture Client die Informationen in einem App Bundle bearbeiten und aktualisieren sowie neue Anwendungen im Paket installieren.

**Hinweis** Ein App Bundle kann mehrere Anwendungen enthalten. Um allerdings die Dienstprogramme AppToggle und AppMerge optimal nutzen zu können, sollte nur eine Anwendung in App Bundle installiert werden.

### Vorgehensweise

1 Klicken Sie in AppCapture Client auf **APP-BUNDLES**.

2 Wählen Sie das Paket aus, das aktualisiert werden soll.

3 Klicken Sie auf **Aktualisieren** und bearbeiten Sie die erforderlichen Informationen:

| Option | Beschreibung |
|---|---|
| **Neuer Name (erforderlich)** | Der neue Name des App Bundle. Dieser muss sich vom bestehenden Namen unterscheiden. |
| **Beschreibung (optional)** | Eine Beschreibung des App Bundle. |

| Option | Beschreibung |
|---|---|
| **Autor (Optional)** | Der Name der Person, die das App Bundle erstellt hat. Standardmäßig ist der aktuelle Benutzer oder der in den Einstellungen der Anwendung festgelegte Name ausgewählt. |
| **Ziel (schreibgeschützt)** | Hier wird automatisch der Speicherort des App Bundle eingetragen, das Sie aktualisieren möchten. Dieser entspricht dem Speicherort für die Dateifreigabe. |

Das generierte Befehlsskript wird am unteren Rand des Bildschirms angezeigt.

4 Klicken Sie auf **Aktualisieren**.

Sie können dann neue Anwendungen im Paket installieren, wenn Sie dazu aufgefordert werden.

Folgen Sie den Anweisungen auf dem Bildschirm, um die Aktualisierung des App Bundle abzuschließen.

### Erstellen eines zusammengeführten App Bundle

Sie können zwei oder mehr einzelne App Bundles zu einem zusammengeführten App Bundle verbinden.

**Hinweis** Um die Komponente AppToggle optimal nutzen zu können, lassen sich nur einzelne App Bundles in einem AppStack zusammenführen. Ein bereits zusammengeführtes App Bundle kann nicht mit einem anderen App Bundlezusammengeführt werden.

#### Vorgehensweise

1 Klicken Sie in AppCapture Client auf **ZUSAMMENGEFÜHRTE APP-BUNDLES**.

2 Geben Sie die im Folgenden aufgeführten Informationen ein.

| Option | Beschreibung |
|---|---|
| **Name (erforderlich)** | Der Name des Pakets. |
| **Beschreibung** | Eine Beschreibung des Pakets. |
| **Autor** | Der Name der Person oder der Einheit, die das zusammengeführte Paket erstellt hat. Standardmäßig ist der aktuelle Benutzer oder der in den Einstellungen der Anwendung festgelegte Name ausgewählt. |
| **Ziel** | Der Speicherort, an dem das zusammengeführte Paket gespeichert werden soll. |

3 Klicken Sie auf **Hinzufügen**.

Eine Liste der App Bundles, der zusammengeführt werden können, wird angezeigt.

4 Wählen Sie die gewünschten Pakete aus und klicken Sie auf **OK**.

5 Klicken Sie auf **Erstellen**.

Eine Meldung zeigt an, wenn das Zusammenführen abgeschlossen ist. Klicken Sie auf das Protokoll, um die Details der Zusammenführung anzuzeigen.

### Aktualisieren eines zusammengeführten App Bundle

Sie können ein zusammengeführtes Paket durch Hinzufügen oder Löschen von Anwendungen aktualisieren.

### Voraussetzungen

Um das Paket zu aktualisieren, muss ein zusammengeführtes App Bundle vorhanden sein. Siehe Erstellen eines zusammengeführten App Bundle.

### Vorgehensweise

1 Klicken Sie in AppCapture Client auf **Zusammengeführte App-Bundles**.

2 Wählen Sie ein zusammengeführtes Paket aus und klicken Sie auf **Aktualisieren**.

Es wird eine Liste der Pakete angezeigt, die im zusammengeführten Paket enthalten sind.

3 Bearbeiten Sie die erforderliche Informationen:

| Option | Beschreibung |
|---|---|
| **Neuer Name (erforderlich)** | Der neue Name des zusammengeführten App Bundle. Dieser muss sich vom bestehenden Namen unterscheiden. |
| **Beschreibung (optional)** | Eine Beschreibung des App Bundle. |
| **Autor (Optional)** | Der Name der Person, die das App Bundle erstellt hat. Standardmäßig ist der aktuelle Benutzer oder der in den Einstellungen der Anwendung festgelegte Name ausgewählt. |
| **Ziel (schreibgeschützt)** | Hier wird automatisch der Speicherort des App Bundle eingetragen, das Sie aktualisieren möchten. Dieser entspricht dem Speicherort für die Dateifreigabe. |

Das generierte Befehlsskript wird am unteren Rand des Bildschirms angezeigt.

4 Klicken Sie auf **Bearbeiten** und wählen Sie die Anwendung(en) aus, die Sie hinzufügen oder entfernen möchten.

Es wird eine Liste der Anwendungen angezeigt, die im Paket erfasst sind.

5 Klicken Sie auf **OK**.

6 Überprüfen Sie den aktualisierten Inhalt des Pakets und klicken Sie auf **Aktualisieren**.

7 Klicken Sie auf **Ja**, um die Aktualisierung des zusammengeführten Pakets zu bestätigen.

## Testen von App Bundle

Überprüfen Sie mit AppCapture Client, ob Anwendungen erfolgreich in einem App Bundle erfasst wurden und ob das Paket wie erwartet funktioniert.

### Voraussetzungen

Erstellen Sie einen Snapshot der Maschine, bevor Sie den Befehl **Test** ausführen. Ein App Bundle kann nur getestet werden, wenn darin Anwendungen erfasst sind.

### Vorgehensweise

1 Klicken Sie in AppCapture Client eine der folgenden Optionen an:

- **App-Bundles** für das Testen eines einzelnen App Bundle.
- **Zusammengeführte App-Bundles** für das Testen eines zusammengeführten App Bundle.

2 Wählen Sie ein Paket aus der Liste aus und klicken Sie auf **Test**.

Das ausgewählte Paket wird bereitgestellt und von App Volumes überprüft.

### AppCapture-Ordner und -Dateien

AppCapture erstellt verschiedene Dateien und Ordner.

AppCapture erstellt verschiedene Ordner in `C:\ProgramData\VMware\AppCapture\appvhds`.

**Tabelle 7-5. AppCapture -Ordner**

| Ordner | Beschreibung |
|---|---|
| `appvhds` | `.vhd`-, `.json`- und `.vdmk`-Dateien, die generiert werden, wenn Sie mithilfe von AppCapture einen AppStack erstellen. |
| `logs` | Von AppCapture generierte Protokolldatei. Die Protokolldatei trägt den Namen `AppCapture.log` und befindet sich in `C:\ProgramData\VMware\AppCapture\logs`. |
| `modules` | PowerCLI `.dll`-Dateien, die benötigt werden, um PowerCLI-Operationen durchzuführen. |
| `plugins` | VMware Horizon Air-Plug-ins. Plug-ins wandeln den AppStack in das korrekte Format zur Bereitstellung an Endbenutzer um. |
| `templates` | `.vhd`-Dateivorlagen, die als Textbaustein-`.vhd`-Dateien dienen, auf deren Grundlage AppStacks erstellt werden. |

AppCapture erstellt diese Dateien im `appvhds`-Verzeichnis, wenn Sie kein anderes Verzeichnis angeben. Siehe Befehlszeilenoptionen für AppCapture.

**Tabelle 7-6. AppCapture -Dateien**

| Datei | Beschreibung |
|---|---|
| *application*`.vhd` | `.vhd`-Datei, welche die Anwendungsdateien enthält, die Bestandteil des AppStack sind. |
| *application*`.vmdk` | Virtual-Hard-Disk-Datei im VMDK-Format, die von VMware Horizon Air nativ verwendet werden. |
| *application*`.json` | Die `.json`-Datei mit Informationen zu den Anwendungen, die im AppStack erfasst sind. |

## Kopieren eines AppStacks zu einer Dateifreigabe

Nach dem Erstellen Ihres AppStacks müssen Sie ihn in einer Dateifreigabe platzieren.

### Voraussetzungen

Erstellen Sie zunächst eine Dateifreigabe und tragen Sie sie auf der Seite „Infrastruktur“ als Anwendungsdateifreigabe ein.

### Vorgehensweise

1 Öffnen Sie ein Datei-Explorer-Fenster für `\\`*`Freigabe-IP`*`\Freigabename`, wobei der Freigabename der Name Ihrer Anwendungsdateifreigabe ist.

2 Kopieren Sie die .vmdk- und .json-Dateien Ihres AppStacks in dieses Verzeichnis.

AppCapture erstellt zwei Arten von Dateien:

- .vmdk-Dateien zum Einrichten von AppStacks auf virtuellen Maschinen
- .vhd-Dateien zum Einrichten von AppStacks auf physischen Computern

Horizon Cloud verwendet nur .vmdk-Dateien. Sie können jedoch auch .vhd-Dateien verwenden, um Anwendungen auf einem physischen Computer mit anderen VMware-Produkten zu installieren.

### Weiter

Nach dem Hinzufügen des AppStacks zur Dateifreigabe müssen Sie diesen importieren. Siehe Importieren eines AppStacks in Horizon Cloud.

## Importieren eines AppStacks in Horizon Cloud

Nach dem Platzieren eines AppStacks in einer Anwendungsdateifreigabe können Sie diesen in Horizon Cloud importieren.

### Vorgehensweise

1 Navigieren Sie zu **Einstellungen > Infrastruktur**.

2 Klicken Sie auf **Dateifreigabe**.

3 Aktivieren Sie das Kontrollkästchen der Dateifreigabe, die den zu importierenden AppStack enthält.

Sie können jeweils nur aus einer Dateifreigabe importieren.

4 Klicken Sie auf **...** und wählen Sie **Importieren** aus.

## Fehlerbehebung bei App Volumes-Funktionen

Mit Python-Skripts nehmen Sie die Fehlerbehebung bei App Volumes-Funktionen vor.

Für die nachfolgenden Skripts ist Python 2.7.9 (oder höher) erforderlich.

- Abrufen der Zuordnungsdetails für Anwendungszuweisungen

  Das nachfolgende Skript ruft Details zu den Zuweisungen in Ihrer Arbeitsumgebung ab.

  - Syntax:

```
usage: mapping_details.py [-h] [-t TYPE] [-p XMP_PORT] [-o CSV_PATH]
                          [-u SEARCH_USER] [-g SEARCH_GROUP]
                          [-d SEARCH_DOMAIN]
                          xmp_host xmp_domain xmp_user xmp_password

positional arguments:
  xmp_host              XMP host url
  xmp_domain            XMP user domain
  xmp_user              XMP user name
  xmp_password          XMP user password

optional arguments:
```

```
  -h, --help            show this help message and exit
  -t TYPE, --type TYPE  All, AppVolumes, DaaS
  -p XMP_PORT, --port XMP_PORT
                        XMP host port
  -o CSV_PATH, --output CSV_PATH
                        Output csv file path
  -u SEARCH_USER, --user SEARCH_USER
                        Search user name
  -g SEARCH_GROUP, --group SEARCH_GROUP
                        Search group name
  -d SEARCH_DOMAIN, --domain SEARCH_DOMAIN
                        Search domain name
```

- Skriptformat:

```
mapping_details.py <IP/FQDN> <domain> <username> '<password>' -p 8443
```

- Codebeispiel (zum Abrufen aller Zuweisungen):

```
qbi@qbi-vm ~ # mapping_details.py qbi-ubuntu.eng.vmware.com falcon administrator '<password>' -
p 8443
Get assignments successfully.
qbi@qbi-vm ~ # cat assignments.csv
key,user name,assignment,application name,bundle name,package name,assignment type,Os type
MIRAGEDOMAIN\qbi only||Mozilla Firefox (3.0.3),MIRAGEDOMAIN\qbi only,qbi-only-win10-x64,Mozil-
la Firefox (3.0.3),,,Native,Windows 10 (x64)
MIRAGEDOMAIN\qbi only||Adobe Flash Player 21 NPAPI,MIRAGEDOMAIN\qbi only,qbi-only-win10-
x64,Adobe Flash Player 21 NPAPI,,,Native,Windows 10 (x64)
MIRAGEDOMAIN\qbi only||Mozilla Maintenance Service,MIRAGEDOMAIN\qbi only,qbi-only-win10-x64,Mo-
zilla Maintenance Service,,,Native,Windows 10 (x64)
MIRAGEDOMAIN\qbi only||Mozilla Firefox 45.0.1 (x86 en-US),MIRAGEDOMAIN\qbi only,qbi-only-win10-
x64,Mozilla Firefox 45.0.1 (x86 en-US),,,Native,Windows 10 (x64)
MIRAGEDOMAIN\qbi only||Python 2.6.6,MIRAGEDOMAIN\qbi only,qbi-only-win10-x64,Python 2.6.6,,,Na-
tive,Windows 10 (x64)
FALCON\qbi||Adobe Flash Player 21 NPAPI,FALCON\qbi,qbi-win10-x64,Adobe Flash Player 21 NPA-
PI,,,Native,Windows 10 (x64)
FALCON\qbi||Mozilla Maintenance Service,FALCON\qbi,qbi-win10-x64,Mozilla Maintenance Ser-
vice,,,Native,Windows 10 (x64)
FALCON\qbi||Mozilla Firefox 45.0.1 (x86 en-US),FALCON\qbi,qbi-win10-x64,Mozilla Firefox 45.0.1
(x86 en-US),,,Native,Windows 10 (x64)
MIRAGEDOMAIN\qbi||Adobe Flash Player 21 NPAPI,MIRAGEDOMAIN\qbi,qbi-win10-x64,Adobe Flash
Player 21 NPAPI,,,Native,Windows 10 (x64)
MIRAGEDOMAIN\qbi||Mozilla Maintenance Service,MIRAGEDOMAIN\qbi,qbi-win10-x64,Mozilla Mainte-
nance Service,,,Native,Windows 10 (x64)
MIRAGEDOMAIN\qbi||Mozilla Firefox 45.0.1 (x86 en-US),MIRAGEDOMAIN\qbi,qbi-win10-x64,Mozilla Fi-
refox 45.0.1 (x86 en-US),,,Native,Windows 10 (x64)
FALCON\Users||FirefoxWin10x64,FALCON\Users,app-bundle-assignment,Mozilla Firefox (3.0.3),Fire-
foxWin10x64,,Native,Windows 10 (x64)
FALCON\Users||CutePDF Professional 3.7 (Evaluation),FALCON\Users,users-win7,CutePDF Professio-
nal 3.7 (Evaluation),,,Native,Windows 7 (x64)
FALCON\Users||FileZilla Client 3.9.0.6,FALCON\Users,users-win7,FileZilla Client 3.9.0.6,,,Nati-
ve,Windows 7 (x64)
```

```
MIRAGEDOMAIN\Users||CutePDF Professional 3.7 (Evaluation),MIRAGEDOMAIN\Users,users-win7,Cu-
tePDF Professional 3.7 (Evaluation),,,Native,Windows 7 (x64)
MIRAGEDOMAIN\Users||FileZilla Client 3.9.0.6,MIRAGEDOMAIN\Users,users-win7,FileZilla Client
3.9.0.6,,,Native,Windows 7 (x64)
```

- Abrufen von Details zu Fehlern beim Anhängen und Trennen

  Das nachfolgende Skript ruft Details zu Fehlern beim Anhängen und Trennen ab (auch für AppStacks).

  - Syntax:

```
usage: fetch_volume_failures.py [-h] [-t SEARCH_DURATION] [-u SEARCH_USER]
                                [-d SEARCH_DOMAIN] [-s PAGE_SIZE]
                                [-c | -v | -o CSV_PATH]
                                login_host login_domain login_user
                                login_password

positional arguments:
  login_host            Login host url in format hostname<:port>
  login_domain          Login user domain
  login_user            Login user name
  login_password        Login user password

optional arguments:
  -h, --help            show this help message and exit
  -t SEARCH_DURATION, --time SEARCH_DURATION
                        Last1Hour, Last12Hour, Last24Hour, Last72Hour, All
  -u SEARCH_USER, --user SEARCH_USER
                        Search user name
  -d SEARCH_DOMAIN, --domain SEARCH_DOMAIN
                        Search domain name
  -s PAGE_SIZE, --size PAGE_SIZE
                        Size of each page of the results
  -c, --concise         Print results in concise view
  -v, --verbose         Print results in itemed view
  -o CSV_PATH, --output CSV_PATH
                        Output to csv file in given path (default)
```

  - Skriptformat:

```
python fetch_volume_failures.py <IP/FQDN> <domain> <username> '<password>'
```

  - Codebeispiele:

```
python fetch_volume_failures.py 10.111.24.65 falcon administrator '<password>' # output as vo-
lume_failures.csv for last 1 hour
python fetch_volume_failures.py 10.111.24.65 falcon administrator '<password>' -v # show re-
sults of last 1 hour in screen
python fetch_volume_failures.py 10.111.24.65 falcon administrator '<password>' -t Last24Hour #
show last 24 hour result
python fetch_volume_failures.py 10.111.24.65 falcon administrator '<password>' -t All -u hez -
d vmwarem # show all results of hez@vmwarem for last 1 hour
```

Die Fehlerdatensätze umfassen jeweils die folgenden Daten:

- Zeitstempel
- Beschreibbar? – gibt an, ob ein beschreibbares Volume (Y für Ja) oder ein AppStack (N für Nein) vorliegt.

  **Hinweis** Beschreibbare Volumes ist eine Beta-Funktion. Weitere Informationen erhalten Sie von Ihrem VMware-Vertreter.

- Anhängen/Trennen – gibt an, ob ein Fehler beim Anhängen oder beim Trennen vorliegt.
- Benutzer/Domäne – Benutzername und Domäne, bei der der Fehler aufgetreten ist
- Dateispeicherort – Speicherort der Dateien Das Format lautet <Datenzentrum>/<Knoten>/<vCenter>/<Datenspeicher>/<VMDK-Pfad>.
- VM-Speicherort – Speicherort der Dateien Das Format lautet <Datenzentrum>/<Knoten>/<vCenter>/<VM-Name>.

Wenn Fehler beim Anhängen/Trennen auftreten, prüfen Sie Folgendes:

- Ist der Benutzer ein Mitglied der richtigen Gruppe?
- Ist der Agent auf dem Desktop installiert und auf dem neuesten Stand?

Sie können die Fehlerangaben zusammen mit einer Supportanfrage versenden.

**Hinweis** In der Benutzeroberfläche werden außerdem Benachrichtigungen mit grundlegenden Informationen zu diesen Fehlern angezeigt (Anzahl der Fehler und Anzahl der betroffenen Benutzer). Weitere Informationen zu Benachrichtigungen finden Sie unter Seite „Benachrichtigungen“.

# Images

8

Images sind Muster, die Sie zum Erstellen von Zuweisungen verwenden.

**Informationen zu Images**

Images werden anhand von Vorlagen-VMs erstellt, die für die Anforderungen verschiedener Benutzertypen konfiguriert sind. Sie haben folgende Möglichkeiten:

- Empfangen eines von VMware vorab gepackten Images
- Erstellen eines Images anhand einer von VMware empfangenen Vorlage
- Erstellen eines Images anhand Ihrer eigenen Vorlage

**Imagetypen**

Es gibt zwei Imagetypen, wie dies im Folgenden beschrieben wird.

| Imagetyp | Beschreibung |
|---|---|
| Instant Clone | Die NGVC-Technologie von VMware verwendender Imagetyp für die schnelle Erstellung von VMs für eine Zuweisung |
| Traditional Clone | Proprietärer Imagetyp, bei dem Images vollständig geklont werden, wenn Zuweisungen erstellt werden |

Der Imagetyp wird beim ersten Erstellen des Images ausgewählt.

**Die Seite „Images“**

Wählen Sie zum Anzeigen der aktuell in Ihrem System vorhandenen Images **Bestandsliste** > **Images** aus, um die Seite „Images“ anzuzeigen.

Dieses Kapitel behandelt die folgenden Themen:

- Verwalten von Images
- Erstellen eines Images
- Agentensoftware für Image aktualisieren
- Erstellen einer eigenen Vorlage

## Verwalten von Images

Auf der Seite „Images“ werden alle aktuell im System vorhandenen Images aufgeführt. Die Aktionen, die Sie auf dieser Seite durchführen können, werden im Folgenden beschrieben.

Es gibt zwei Möglichkeiten zur Durchführung von Aktionen für Images.

- Aktivieren Sie das Kontrollkästchen für ein Image in der Liste und verwenden Sie die Schaltflächen und Menüoptionen oben auf der Seite wie unten beschrieben.
- Klicken Sie auf ein Image zur Anzeige der Detailseite des Image und verwenden Sie die Schaltflächen und Menüoptionen oben auf dieser Seite. Es sind nur einige der unten aufgeführten Optionen auf der Detailseite des Image in unterschiedlicher Reihenfolge verfügbar.

  Die Detailseite des Image enthält auch Optionen zum Wiederherstellen oder Löschen einer Sicherung. Weitere Informationen finden Sie unten unter „Jetzt sichern“.

Mithilfe der Schaltflächen oben auf der Seite „Images“ können Sie die im Folgenden dargestellten Aktionen durchführen.

| Schaltfläche | Beschreibung |
|---|---|
| Neu | Starten Sie den Image-Erstellungsvorgang. Siehe Erstellen eines Images. |
| Umbenennen | Benennt das ausgewählte Image um |
| Duplizieren | [nur Instant Clone-Images] Erstellt ein Duplikat des ausgewählten Images |
| Aktualisieren des Agent | Aktualisiert Agenten für ein ausgewähltes Image. Siehe Agentensoftware für Image aktualisieren. |

Sie können die folgenden Aktionen durchführen, indem Sie auf die Schaltfläche „. . .“ oben auf der Seite „Images“ klicken und eine Auswahl im Dropdown-Menü durchführen.

| Option | Beschreibung |
|---|---|
| Jetzt sichern | [nur Traditional Clone-Images] Erstellt eine Sicherung des ausgewählten Images<br>■ Nachdem Sie die Sicherung erstellt und benannt haben, wird diese unter „Sicherungen“ auf der Detailseite des Image angezeigt.<br>■ Neben jeder Sicherung auf der Detailseite des Image finden Sie Optionen zum Wiederherstellen und Löschen dieser Sicherung.<br>**Hinweis** Wenn eine zuvor auf der Detailseite des Image angezeigte Sicherung nicht mehr vorhanden ist und Sie diese nicht gelöscht haben, wenden Sie sich an Ihren VMware-Vertreter, um dieses Problem zu beheben. |
| Löschen | Löscht das ausgewählte Image vorübergehend. |
| Veröffentlichen | Veröffentlicht das ausgewählte Image |
| Offline schalten | Schaltet das ausgewählte Image offline Das Image kann dann nicht verwendet werden, um neue Zuweisungen vorzunehmen oder neue Desktops oder Server für bestehende Zuweisungen bereitzustellen. Wenn Sie ein Image offline schalten, müssen Sie es erneut veröffentlichen, damit es wieder für Zuweisungen verfügbar wird. |
| Zu Desktop konvertieren | Konvertiert das ausgewählte Image in einen Desktop. |
| Image zuweisen | [nur Instant Clone-Images] Überträgt Aktualisierungen mithilfe des ausgewählten Images per Push an dedizierte bzw. flexible Desktop-Zuweisungen Wählen Sie die Zuweisung(en) in der Liste aus und klicken Sie zum Übertragen der Aktualisierungen per Push auf **OK**. |
| Konsole starten | Startet eine Konsole für die dem ausgewählten Image zugeordnete virtuelle Maschine. Diese Option ist deaktiviert, wenn die virtuelle Maschine ausgeschaltet oder wenn mehr als ein Image ausgewählt ist. |

| Option | Beschreibung |
|---|---|
| Aktualisierungen starten | Überträgt Aktualisierungen auf Zuweisungen mithilfe des ausgewählten Image.<br>■ Desktop-Images – Klicken Sie auf **Aktualisierungen starten**, wählen Sie die Zuweisung(en) aus der Liste aus und klicken Sie auf **OK** zum Übertragen der Aktualisierungen.<br>**Hinweis** Bevor Sie Aktualisierungen auf Ihre vorhandenen Zuweisungen übertragen, wird empfohlen, zuerst eine Testzuweisung zu erstellen und die Aktualisierungen auf diese zu übertragen. Sie können damit prüfen, ob alle Funktionen wie erwartet ausgeführt werden.<br>■ RDS-Images<br>■ Wenn Sie das Image mithilfe der Funktion „Agent-Software aktualisieren“ aktualisiert haben, klicken Sie auf **Aktualisierungen starten**, wählen Sie die Farm aus der Liste aus und klicken Sie auf **OK**, um die Aktualisierungen zu starten.<br>■ Wenn Sie das Image ohne die Funktion „Agent-Software aktualisieren“ aktualisiert haben, ist keine Aktion erforderlich. Die Aktualisierungen werden automatisch übertragen, wenn Sie ein aktualisiertes Image erneut veröffentlichen. |
| Bootstrap herunterladen | Lädt eine verschlüsselte Bootstrap-Datei zur Bereitstellung Ihrer Images herunter.<br>Sie werden aufgefordert, ein aus 8–20 ASCII-Zeichen bestehendes Kennwort einzugeben, das mindestens einen Kleinbuchstaben, einen Großbuchstaben, eine Ziffer und ein Symbol (!@#$ %^&*) enthält. Verwenden Sie für das Kennwort keine Nicht-ASCII-Zeichen. |
| Kennwort aktualisieren | Erstellt ein neues Standardkennwort für Bootstrapping-Images.<br>Wenn Sie dies nach dem Herunterladen der Bootstrap-Datei, aber vor der Anwendung von Keytool auf die Bootstrap-Datei tun, können die resultierenden Agents nicht miteinander gekoppelt werden. Daher sollte die Bootstrap-Datei nach dem Aktualisieren des Kennworts erneut heruntergeladen werden. |

## Aktualisieren eines Instant Clone-Images

Sie können ein Instant Clone-Image und die auf dem Image basierenden Zuweisungen aktualisieren.

Im Gegensatz zu einem herkömmlichen Clone-Image, das nach dem Veröffentlichen aktualisiert werden kann (offline nehmen, ändern und erneut veröffentlichen), muss ein Instant Clone-Image dupliziert und das neue Image aktualisiert und den relevanten Zuweisungen hinzugefügt werden.

### Vorgehensweise

1 Wählen Sie aus dem Menü **Bestandsliste > Images** aus, um die Seite „Images“ zu öffnen.

2 Aktivieren Sie das Kontrollkästchen für das Image, klicken Sie auf die Schaltfläche „...“, und wählen Sie aus dem Dropdown-Menü die Option **Duplizieren**.

Das System erstellt ein Duplikat des Images.

**Hinweis** Dieser Vorgang kann einige Zeit in Anspruch nehmen, planen Sie daher entsprechend Zeit ein.

3 Nehmen Sie die erforderlichen Änderungen an dem Image-Duplikat vor und veröffentlichen Sie es.

4 Wenn das neue Image veröffentlicht wurde, bearbeiten Sie jeweils die Zuweisungen auf Basis des ursprünglichen Images, damit stattdessen das Duplikat-Image verwendet wird. Siehe Bearbeiten einer Zuweisung.

   Wenn Benutzer sich von ihrer Sitzung abmelden, werden die VMs in jeder Zuordnung mit dem neuen Image synchronisiert.

5 [Optional] Löschen Sie das ursprüngliche Image, indem Sie es auf der Seite „Images“ auswählen, auf die Schaltfläche „...“ klicken und dann aus dem Dropdown-Menü **Löschen** auswählen.

## Automatisches Synchronisieren von Images für mehrere Desktop-Manager

Wenn Sie mehrere Desktop-Manager für einen Mandanten im selben Datenzentrum registriert haben, können Sie mit der Option „Image synchronisieren“ Images automatisch für mehrere Desktop-Manager synchronisieren.

Die Funktion zur Synchronisierung von Images ist standardmäßig deaktiviert. Sie lässt sich für jeden Mandanten durch Ihren VMware-Vertreter aktivieren bzw. deaktivieren.

Wenn die Option „Image synchronisieren“ aktiviert ist, werden die im Folgenden aufgeführten Aktionen automatisch ausgeführt.

- Neue Images für mehrere Desktop-Manager duplizieren, ohne sie manuell klonen und importieren zu müssen.
- Änderungen an Images für mehrere Desktop-Manager synchronisieren, sodass die Änderungen nicht für alle Kopien durchgeführt werden müssen.

Hinweis:

- Images, die vor der Aktivierung der Option „Image synchronisieren“ erstellt wurden, werden nicht automatisch synchronisiert. Sie müssen diese offline schalten und dann erneut für die Synchronisierung veröffentlichen.
- Wenn Sie nach der Synchronisierung von Images die Option deaktivieren, wird für jedes synchronisierte Image in der Liste ein zusätzliches Image mit dem gleichen Namen wie das synchronisierte Image angezeigt.

# Erstellen eines Images

Erstellen eines neuen Images auf der Seite „Images“.

**Hinweis** Dieser Vorgang dauert ca. 30 Minuten. Stellen Sie sicher, dass genügend Zeit für den Abschluss vorhanden ist, bevor Sie den Vorgang beginnen.

### Vorgehensweise

1 Wählen Sie **Bestandsliste > Images** aus.

   Die Seite „Images“ wird angezeigt.

2 Klicken Sie auf **Neu**.

Das Dialogfeld „Neues Image“ wird angezeigt.

3 Geben Sie im Feld „Desktop“ die ersten Buchstaben des Vorlagennamens ein.

Alle Desktops, die in ein Image konvertiert werden können, werden angezeigt. Beachten Sie, dass es nach dem Import der Vorlage rund fünf Minuten dauern kann, bis der Bestand angezeigt wird.

4 Wählen Sie den Desktop-Namen aus, wenn er angezeigt wird.

**Hinweis** Stellen Sie vor der Konvertierung sicher, dass der Desktop eingeschaltet ist.

5 Stellen Sie sicher, dass der Agent-Status in „Aktiv“ geändert wurde, was angibt, dass die Agent-Paarbildung stattgefunden hat. Dies sollte innerhalb von ca. 30 Sekunden passieren.

**Hinweis** Sie müssen die neuesten Agents für eine erfolgreiche Agent-Paarbildung installieren. Wenn Sie ältere Versionen von Agents verwenden, müssen Sie sicherstellen, dass der DaaS-Agent manuell konfiguriert und ein Bootstrapping zur Agent-Kopplung durchgeführt wurde.

6 Wählen Sie für Instant Clone **Ja** aus, um ein Instant Clone-Image zu erstellen. Wählen Sie alternativ **Nein** aus, um ein Traditional Clone-Image zu erstellen. Informationen zu den Arten der Desktop-Zuweisungen finden Sie unter Kapitel 8 Images.

| Option | Beschreibung |
|---|---|
| **Instant Clone** | Die NGVC-Technologie von VMware verwendender Imagetyp für die schnelle Erstellung von VMs für eine Zuweisung<br><br>**Hinweis** Windows Server-Betriebssysteme werden für Instant Clone-Zuweisungen nicht unterstützt, sodass Sie keine Instant Clone-Images anhand von Windows Server-Vorlagen-VMs erstellen sollten. Mit dem installierten Instant Clone Agent kann das Image zwar erstellt und Desktops können bereitgestellt werden, diese werden für die Benutzer jedoch nicht erfolgreich gestartet. |
| **Traditional Clone** | Proprietärer Imagetyp, bei dem Images vollständig geklont werden, wenn Zuweisungen erstellt werden |

7 Geben Sie die erforderlichen Informationen ein, wie dies im Folgenden beschrieben wird.

Der von Ihnen oben ausgewählte Imagetyp wirkt sich auf die angezeigten Felder aus.

| Option | Beschreibung |
|---|---|
| **Image-Name** | Name des neuen Images |
| **Domäne** | [nur Instant Clone] Wählen Sie die Domäne in der Dropdown-Liste aus. |
| **Firmenname** | Der Name Ihres Unternehmens |
| **Zeitzone** | Ihre Zeitzone |

| Option | Beschreibung |
|---|---|
| **Benutzername** | Admin-Benutzer für die erforderliche Desktop-Domäne<br><br>**Hinweis** Dieses Feld wird nur dann für Instant Clone-Images eingeblendet, wenn Ihr VMware-Vertreter die Funktion zur Synchronisation von Images aktiviert hat. |
| **Kennwort/Kennwort bestätigen** | Kennwort für den Administratorbenutzer<br><br>**Hinweis** Dieses Feld wird nur dann für Instant Clone-Images eingeblendet, wenn Ihr VMware-Vertreter die Funktion zur Synchronisation von Images aktiviert hat. |

8 Klicken Sie auf **Veröffentlichen**.

Der Veröffentlichungsprozess dauert etwa 40 Minuten. Falls er erfolgreich abgeschlossen wird, wird die Image-Aufgabe als abgeschlossen angezeigt.

**Hinweis** Stellen Sie die VM nicht mithilfe eines Snapshots wieder her, der vor dem Bootstrapping-Vorgang erstellt wurde. Wenn das Bootstrapping für den Agent bereits durchgeführt wurde, kann dieser nicht mehr ordnungsgemäß kommunizieren.

9 Gehen Sie wie folgt vor, wenn die Veröffentlichung fehlschlägt:

a Wählen Sie **Überwachen > Aktivität** aus und suchen Sie den fehlgeschlagenen Auftrag.

b Beheben Sie das Problem, das den Fehler verursacht hat.

c Wählen Sie **Bestand > Images** aus und aktivieren Sie das Kontrollkästchen neben dem Image.

d Klicken Sie auf **...** und wählen Sie **In Desktop konvertieren** aus.

e Wiederholen Sie die obigen Schritte, um das Image erneut zu veröffentlichen.

# Agentensoftware für Image aktualisieren

Mit der Funktion zur Aktualisierung von Agenten können Sie die Agent-Software für ein Image aktualisieren und Aktualisierungen an Zuweisungen weitergeben.

Mit der Funktion zur Agentenaktualisierung werden alle Agenten in einem Image in einem einzigen Arbeitsgang automatisch aktualisiert.

- Das System nimmt regelmäßig Kontakt zum VMware CDS-Software-Distributionsnetzwerk auf und lädt die Agentenaktualisierungen automatisch in eine Dateifreigabe herunter, die Sie auf einem lokalen Computer eingerichtet haben. Die Aktualisierungsdateien werden dann automatisch in das System importiert und für Images bereitgestellt.
- Die Verfügbarkeit von Aktualisierungen wird auf der Seite „Images“ angezeigt. Hier können Sie die Aktualisierungen auf Images anwenden.
- Ihr VMware-Vertreter kann auf Wunsch den Zeitraum zwischen den Suchvorgängen nach neuen Agenten sowie die Wartezeit für Suchvorgänge nach dem Start der Mandanten ändern.

### Voraussetzungen

- Sie müssen eine Agenten-Dateifreigabe erstellt und diese Horizon Cloud hinzugefügt haben. Beim Erstellen der Dateifreigabe wählen Sie also den Dateifreigabetyp „Agenten“. Die Agenten-Dateifreigaben dienen lediglich zum Importieren von Agenten-Aktualisierungsdateien. Siehe Verwalten von Dateifreigaben.
- Das Image muss bereits über DaaS Agent 16.6.0.4408091 oder höher verfügen, um eine DaaS Agent-Aktualisierung durchführen zu können.
- Das Image muss bereits über Horizon Agent 7.0.3.4612900 oder höher verfügen, um eine Horizon Agent-Aktualisierung durchführen zu können.

### Vorgehensweise

1 Klicken Sie auf **Bestandsliste > Images**.

Die Seite „Images“ wird angezeigt, wobei ein blauer Punkt neben dem Namen der jeweiligen Zuweisung dargestellt wird, für die Agentenaktualisierungen zur Verfügung stehen.

- Wenn Sie mit der Maus auf einen blauen Punkt zeigen, wird ein Popup-Fenster mit einer Meldung geöffnet, dass Agentenaktualisierungen für dieses Image bereitstehen.
- Standardmäßig werden die jeweils aktuellen Versionen der einzelnen Agenten ausgewählt. Sie können jedoch die verschiedenen Dropdown-Listen öffnen und alle verfügbaren Versionen betrachten.

2 Aktivieren Sie das Kontrollkästchen für ein Image. Sie können Agenten immer nur für jeweils ein Image aktualisieren.

3 Klicken Sie auf **Agent aktualisieren**.

Das Dialogfeld „Agentenaktualisierung“ wird angezeigt.

4 Wählen Sie auf der Registerkarte „Software“ den bzw. die zu aktualisierenden Agent(en) aus und klicken Sie auf **Weiter**.

5 Aktivieren Sie auf der Registerkarte „Vereinbarungen“ jeweils das Kontrollkästchen **Zustimmen** für die zu akzeptierenden Vereinbarungen und klicken Sie auf **Weiter**. Bei allen Elementen, bei denen Sie der Vereinbarung nicht zugestimmt haben, wird die Aktualisierung übersprungen.

6 (Optional) Fügen Sie auf der Registerkarte „Befehlszeile“ Befehlszeilenoptionen hinzu. Details hinsichtlich Befehlszeilenoptionen finden Sie in der Dokumentation für den relevanten Agenten.

**Hinweis** Für DaaS Agent sind derzeit keine Befehlszeilenoptionen verfügbar.

7 Klicken Sie auf **Fertigstellen**.

- Oben auf der Seite wird eine Meldung angezeigt, die angibt, dass die Aktualisierung gestartet wurde.
- Das System erstellt einen Klon des Image und aktualisiert die Agenten auf dem Klon-Image.

Hinweis:

- Desktops werden in Batches zu maximal 30 Stück aktualisiert. Wenn die Zuweisung maximal 30 Desktops umfasst, werden alle Desktops in der Zuweisung gemeinsam aktualisiert. Ihr VMware-Vertreter kann die Batch-Größe nach Bedarf anpassen.
- Wenn ein Desktop über eine aktive Sitzung verfügt, wird der Benutzer fünf Minuten vor der Aktualisierung gewarnt.
- Wenn ein Benutzer versucht, sich bei einem Desktop anzumelden, der aktualisiert wird, ist die Anmeldung fehlerhaft und dem Benutzer wird eine Meldung angezeigt, die besagt, dass der Desktop nicht verfügbar ist.

Sie können den Fortschritt der Aktualisierungsaufgabe anzeigen, indem Sie **Überwachen > Aktivität** auswählen. Die Aufgabenbeschreibung gibt den Agenten an, der aktualisiert wird, und die Zuweisung, für die die Aktualisierung durchgeführt wird. Ist die Aufgabe nicht binnen 24 Stunden erfolgreich, schlägt der Vorgang fehl.

8 Starten Sie die Aktualisierungen auf Basis des Klon-Image. Weitere Informationen finden Sie unter Verwalten von Images.

9 (Optional) Löschen Sie das ursprüngliche Image und benennen Sie das Klon-Image in den Namen des ursprünglichen Image um.

# Erstellen einer eigenen Vorlage

Bevor Sie ein Image erstellen können, muss zunächst die Desktop-Vorlage vorbereitet werden.

Das Aufbauen der Vorlage umfasst die folgenden Schritte:

- Installieren und Konfigurieren von Agents
- Einrichten einer direkten Verbindung zu Desktop-VMs (optional)
- Optimieren der Anzeige (optional)

## Installieren und Konfigurieren von Agenten

Die Agenten müssen in einer bestimmten Reihenfolge auf der VM, auf der sich die Vorlage befindet, installiert und konfiguriert werden.

Führen Sie zunächst die Aufgaben unter Vorbereiten der VM, auf der sich die Vorlage befindet, auf die Installation der Agents aus, bevor Sie die Agenten installieren.

### Vorbereiten der VM, auf der sich die Vorlage befindet, auf die Installation der Agents

Führen Sie die nachfolgenden Vorinstallationsschritte aus, bevor Sie die Agent-Software installieren, mit der die Verbindung zu den Desktops hergestellt wird.

### Vorgehensweise

1 Deinstallieren Sie alle Software-Komponenten für andere Protokolle.

**Wichtig:** Sie müssen alle Software-Komponenten für alle anderen Protokolle (z. B. HDX oder RGS) deinstallieren. Wenn Sie die Komponenten für diese anderen Protokolle nicht deinstallieren, wird die Vorlage beschädigt und Sie können Windows nicht mehr starten. Diese Warnung gilt nicht für RDP; die RDP-Komponenten verursachen keine Probleme.

2 Aktualisieren Sie VMware Tools.

3 Prüfen Sie, ob Port 443 bereits von einer anderen Software verwendet wird; falls ja, geben Sie einen nicht standardmäßigen Port an.

4 Die folgenden Ports müssen für den TCP- und/oder den UDP-Datenverkehr geöffnet werden:

| Port(s) | Quelle | Ziel | TCP | UDP |
|---|---|---|---|---|
| 4172 (PCoIP) | Access Point | VM | P | P |
| 443 (View-Kommunikation) | Mandanten-Appliance | VM | P | |
| 32111 (PCoIP) | Access Point | VM | P | |
| 22443 (HTML Access) | Access Point | VM | P | |
| 443 (HTML Access) | Access Point | T/VM | P | |
| 8443 (HTML Access) | Access Point | VM | P | |
| 4172 (PCoIP) | Access Point | VM | P | P |
| 80 (Weiterleitung an 443) | Access Point | T/VM | P | |

### Weiter

Installieren Sie den Horizon Agent. Siehe Installieren des Horizon Agent.

## Installieren des Horizon Agent

Sobald Sie die Vorbereitung abgeschlossen haben, können Sie den Horizon Agent auf der VM installieren, auf der sich die Vorlage befindet.

Bei der Installation des Horizon Agent sind drei Szenarien möglich:

- Installation auf einem Desktop (Windows 7, Windows 8, Windows 8.1, Windows 10)
- Installation auf einem Server (Windows Server 2008 R2, Windows Server 2012 R2) als persönlicher Desktop (kein RDSH)
- Installation auf einem Server (Windows Server 2008 R2, Windows Server 2012 R2) als RDSH-Rolle

**Hinweis** Falls nicht die jeweils aktuelle Version des Horizon Agent installiert ist, können Probleme beim Erstellen von RDS-Pools auftreten. So erhalten Sie beim Erstellen eines neuen RDS-Pools die Möglichkeit, die Option „HTML Access (Blast)“ als Protokoll auszuwählen. Diese Option wird jedoch nicht auf den Pool angewendet, auch wenn sie scheinbar erfolgreich angewendet wurde.

## Installieren des Horizon Agent auf einem Windows-Desktop

Sie können den Horizon Agent auf einem Desktop mit Windows 7, Windows 8, Windows 8.1 oder Windows 10 installieren.

### Vorgehensweise

1. Laden Sie den aktuellen Horizon Agent von der Myvmware-Download-Website herunter. Beachten Sie, dass für 32-Bit- und 64-Bit-Betriebssysteme unterschiedliche Downloads angeboten werden.
2. Doppelklicken Sie auf die Installationsdatei für den Horizon Agent (Dateiname für das 64-Bit-Installationsprogramm: VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe).
3. Führen Sie eine benutzerdefinierte Installation mit den folgenden Optionen aus:
   - Deaktivieren Sie den VMware Horizon View Composer Agent.
   - Aktivieren Sie den VMware Horizon Instant Clone-Agenten.
   - Wählen Sie „vRealize Operations Desktop Agent“ aus.
4. Starten Sie die virtuelle Maschine neu, sobald Sie dazu aufgefordert werden.

### Weiter

- Deaktivieren Sie die schwache Verschlüsselung in SSL und TLS, sodass die Sicherheit beim Arbeiten mit dem Horizon Agent erhöht wird. Bearbeiten Sie hierzu das Gruppenrichtlinienobjekt (GPO) des Active Directory-Servers. Weitere Informationen zur Deaktivierung der schwachen Verschlüsselung in SSL/TLS finden Sie in der entsprechenden Dokumentation zum Horizon Agent, beispielsweise im Dokumentationsset zu VMware Horizon 7.
- Installieren des DaaS Agent

## Installieren des Horizon Agent unter Windows Server als persönlicher Desktop (kein RDSH)

Sie können den Horizon Agent unter Windows Server 2008 R2 oder 2012 R2 als persönlichen Desktop installieren.

### Vorgehensweise

1. Laden Sie den aktuellen Horizon Agent von der VMware-Website (https://my.vmware.com) herunter. Beachten Sie, dass für 32-Bit- und 64-Bit-Betriebssysteme unterschiedliche Downloads angeboten werden.
2. Doppelklicken Sie auf die Installationsdatei für den Horizon Agent (Dateiname für das 64-Bit-Installationsprogramm: VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe).
3. Wählen Sie die Option, mit der der Horizon Agent im Desktop-Modus installiert wird.
4. Führen Sie eine benutzerdefinierte Installation mit den folgenden Optionen aus:
   - Deaktivieren Sie den VMware Horizon View Composer Agent.
   - Wählen Sie „vRealize Operations Desktop Agent“ aus.
5. Starten Sie die virtuelle Maschine neu, sobald Sie dazu aufgefordert werden.

#### Weiter

- Deaktivieren Sie die schwache Verschlüsselung in SSL und TLS, sodass die Sicherheit beim Arbeiten mit dem Horizon Agent erhöht wird. Bearbeiten Sie hierzu das Gruppenrichtlinienobjekt (GPO) des Active Directory-Servers. Weitere Informationen zur Deaktivierung der schwachen Verschlüsselung in SSL/TLS finden Sie in der entsprechenden Dokumentation zum Horizon Agent, beispielsweise im Dokumentationsset zu VMware Horizon 7.
- Installieren des DaaS Agent

### Installieren des Horizon Agent unter Windows Server als RDSH-Rolle

Sie können den Horizon Agent unter Windows Server 2008 R2, 2012 R2 oder 2016 als RDSH-Rolle installieren.

**Hinweis** Zum Installieren des Horizon Agent in diesem Szenario MÜSSEN Sie die Installation über die Befehlszeile durchführen; die standardmäßige „Doppelklick-GUI“ steht hier nicht zur Verfügung.

#### Vorgehensweise

1 Fügen Sie die Rolle „Remote-Desktop-Dienste“ hinzu.

   a Wählen Sie **Starten > Verwaltung > Server Manager** aus, um den Server-Manager zu öffnen.

   b Wählen Sie im rechten Bereich **Rollen** und anschließend **Rollen hinzufügen** aus.

   Die Seite „Bevor Sie beginnen“ des Fensters „Assistenten zum Hinzufügen von Rollen“ wird angezeigt.

   c Klicken Sie auf **Weiter**.

   Die Seite „Serverrollen auswählen“ wird angezeigt.

   d Aktivieren Sie das Kontrollkästchen für Remote-Desktop-Dienste und klicken Sie auf **Weiter**.

   Die Seite „Remote-Desktop-Dienste“ wird angezeigt.

   e Klicken Sie auf **Weiter**.

   Die Seite „Rollen-Dienste auswählen“ wird angezeigt.

   f Aktivieren Sie das Kontrollkästchen für die Remote-Desktop-Sitzungshost und klicken Sie auf **Weiter**.

   Die Seite „Deinstallieren und Neuinstallieren von Anwendungen für Kompatibilität“ wird angezeigt.

   g Klicken Sie auf **Weiter**.

   Die Seite „Authentifizierungsmethode für Remote-Desktop-Sitzungshost angeben“ wird angezeigt.

   h Wählen Sie die entsprechende Authentifizierungsstufe aus und klicken Sie auf **Weiter**.

   Die Seite „Lizenzierungsmodus angeben“ wird angezeigt.

i Geben Sie den Lizenzierungsmodus an und klicken Sie auf **Weiter**.

Die Seite „Benutzergruppen, denen der Zugriff auf diesen RD-Sitzungshostserver gestattet ist, auswählen“ wird angezeigt.

j Fügen Sie Ihre Benutzer oder Benutzergruppen hinzu und klicken Sie auf **Weiter**.

Die Seite „Client-Erfahrung konfigurieren“ wird angezeigt.

k Nehmen Sie die gewünschten Einstellungen vor und klicken Sie auf **Weiter**.

Die Seite „Installationsauswahl bestätigen“ wird angezeigt.

l Bestätigen Sie Ihre Auswahl. Wenn etwas nicht korrekt ist, klicken Sie auf **Zurück**, um zu den vorherigen Schritten zurückzugehen und die Einstellungen zu ändern. Klicken Sie auf **Installieren**.

Die Seite „Installationsfortschritt“ wird angezeigt. Die Installation nimmt einige Minuten in Anspruch. Die Seite „Installationsergebnisse“ wird angezeigt und fordert einen Neustart an.

m Klicken Sie auf **Schließen**.

Ein Dialogfeld, das die Bestätigung für den Neustart anfordert, wird angezeigt.

n Klicken Sie auf **Ja**, um den Server neu zu starten.

o Wenn der Server wieder erreichbar ist, melden Sie sich erneut an.

Die Seite „Wiederaufnehmen der Konfiguration“ wird angezeigt. Es dauert einen Moment, bis die Konfiguration wiederaufgenommen wird. Die Seite „Installationsergebnisse“ wird angezeigt.

p Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.

Das Fenster „Server-Manager“ wird angezeigt.

q Klicken Sie auf **Rollen** und bestätigen Sie, dass die Rolle „Remote-Desktop-Dienste“ installiert ist.

2 Laden Sie den aktuellen Horizon Agent von der VMware-Website (https://my.vmware.com) herunter. Beachten Sie, dass für 32-Bit- und 64-Bit-Betriebssysteme unterschiedliche Downloads angeboten werden.

3 Führen Sie den folgenden Befehl in der Befehlszeile als Administratorbenutzer aus: `VMware-view-agent-x86_64-x.y.z-nnnnnnn.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"`

4 Führen Sie eine benutzerdefinierte Installation mit den folgenden Optionen aus:

- Wählen Sie „vRealize Operations Desktop Agent“ aus.

5 Starten Sie die virtuelle Maschine neu, sobald Sie dazu aufgefordert werden.

### Weiter

- Deaktivieren Sie die schwache Verschlüsselung in SSL und TLS, sodass die Sicherheit beim Arbeiten mit dem Horizon Agent erhöht wird. Bearbeiten Sie hierzu das Gruppenrichtlinienobjekt (GPO) des Active Directory-Servers. Weitere Informationen zur Deaktivierung der schwachen Verschlüsselung in SSL/TLS finden Sie in der entsprechenden Dokumentation zum Horizon Agent, beispielsweise im Dokumentationsset zu VMware Horizon 7.
- Installieren des DaaS Agent

## Installieren des DaaS Agent

Sobald Sie den Horizon Agent installiert haben, installieren Sie den DaaS Agent.

**Hinweis** Die für ältere Versionen des DaaS Agent notwendige manuelle Konfiguration ist nicht mehr erforderlich.

### Vorgehensweise

1. Laden Sie das aktuelle Installationsprogramm für den DaaS Agent von der Download-Website Myvmware.com herunter.
2. Führen Sie das Installationsprogramm auf der VM aus, auf der sich die Vorlage befindet.

### Weiter

Installieren des App Volumes-Agenten

## Installieren des App Volumes-Agenten

Sobald Sie den Horizon-Agenten installiert haben, können Sie den App Volumes-Agenten installieren.

### Vorgehensweise

1. Laden Sie das aktuelle Installationsprogramm für den App Volumes Unified-Agenten von der Download-Website Myvmware.com herunter.
2. Führen Sie das Installationsprogramm auf der VM aus, auf der sich die Vorlage befindet.
3. Deaktivieren Sie „localhost“ bei der Installation und geben Sie die IP-Adresse des primären Mandanten sowie den Port 3443 an (beispielsweise 192.168.12.12:3443).
4. Tragen Sie die IP-Adresse der sekundären Mandanten-Appliance in die Registrierung ein, sodass hohe Verfügbarkeit gewährleistet ist:
   a. Führen Sie „regedit“ aus und navigieren Sie zu „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\svservice\Parameters“.
   b. Geben Sie den Zeichenfolgenwert „Manager2“ mit dem Wert <TA2-IP-Adresse>:3443 ein (beispielsweise 192.168.12.12:3443).

# Konfigurieren von intelligenten VMware Horizon-Richtlinien

Eine Horizon Cloud-Umgebung unterstützt die Verwendung von intelligenten VMware Horizon-Richtlinien zur Steuerung der virtuellen Desktops von Endbenutzern. Diese intelligenten Richtlinien ermöglichen eine richtlinienbasierte Steuerung des Verhaltens von Funktionen wie die USB-Umleitung, das virtuelle Drucken, die Zwischenablagenumleitung und die Client-Laufwerksumleitung sowie der Funktionen für das PCoIP-Anzeigeprotokoll auf den virtuellen Desktops. Durch Verwendung intelligenter Richtlinien können Sie Richtlinien festlegen, die nur beim Eintreten bestimmter Bedingungen gelten. So können Sie beispielsweise eine Richtlinie konfigurieren, mit der die Clientlaufwerksumleitung dann deaktiviert wird, wenn ein Benutzer von einem Gerät außerhalb des Unternehmensnetzwerks eine Verbindung mit einem Remote-Desktop herstellt.

Eine ausführliche Beschreibung der intelligenten VMware Horizon-Richtlinien und Anweisungen zu deren Verwendung finden Sie unter Verwenden von intelligenten Richtlinien in der VMware Horizon-Dokumentation. Informationen zu intelligenten VMware Horizon-Richtlinien erhalten Sie auch im VMware Horizon-Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Für diese intelligenten Richtlinien muss die User Environment Manager-Software und das Installationsprogramm für App Volumes Unified Agent zur Installation der erforderlichen Agenten verwendet werden. Die Software steht auf der VMware-Downloads-Seite zum Herunterladen zur Verfügung. Verwenden Sie die Version User Environment Manager 9.1 oder höher. Die Systemanforderungen zu User Environment Manager und die vollständigen Installationsanweisungen finden Sie in der User Environment Manager-Produktdokumentation. Ausführliche Informationen und Best Practices für die Anwendung von User Environment Manager und App Volumes in Ihrer Umgebung erhalten Sie im Dokument VMware App Volumes mit Best Practices und Vorgängen zur Horizon Cloud-Anwendungsbereitstellung unter vmware.com.

Nach dem Abschluss der Installation und Konfiguration von User Environment Manager und seiner Verwaltungskonsole wie in den oben erwähnten Dokumenten beschrieben müssen Sie zur Konfiguration einer intelligenten Richtlinie auf Ihrer virtuellen Master-Maschine die im Folgenden beschriebenen Schritte auf dieser Master-VM durchführen.

- Sofern noch nicht geschehen, führen Sie das Installationsprogramm für App Volumes Unified Agent wie in Installieren des App Volumes-Agenten beschrieben aus. Dabei wird der User Environment Manager-Agent in der VM installiert. Außerdem wird mit dieser Agentenkomponente der User Environment Manager FlexEngine-Client installiert.
- Definieren Sie mithilfe der User Environment Manager-Verwaltungskonsole die intelligente VMware Horizon-Richtlinie.

  Eine Beschreibung der in User Environment Manager zur Verfügung stehenden Einstellungen für die intelligente VMware Horizon-Richtlinie finden Sie unter Einstellungen für intelligente Horizon-Richtlinien in der VMware Horizon 7-Dokumentation.
- Fügen Sie Bedingungen hinzu, die erfüllt sein müssen, damit die Richtlinie angewendet wird, wie unter Hinzufügen von Bedingungen zu intelligenten Horizon-Richtliniendefinitionen in der VMware Horizon-Dokumentation erläutert.

Beispiele zur Anwendung von intelligenten Horizon-Richtlinien finden Sie im Dokument Reviewer's Guide for View in VMware Horizon 7: Smart Policies (Prüfer-Handbuch für View in VMware Horizon 7: Intelligente Richtlinien) unter vmware.com.

Hinzufügen von Bedingungen zu intelligenten Horizon-Richtliniendefinitionen beschreibt die Anwendung von Horizon Client-Eigenschaftsbedingungen in den intelligenten Richtlinien. Die vordefinierten Horizon Client-Eigenschaften entsprechen den `ViewClient_`-Registrierungsschlüsseln. Beachten Sie, dass nicht alle vordefinierten Eigenschaften, die in Horizon 7 verwendet werden, in einer Horizon Cloud-Umgebng angewendet werden können. Dies betrifft folgende Eigenschaften:

- `ViewClient_Broker_Pool_Tags`
- `ViewClient_Broker_Tags`
- `ViewClient_Launch_Matched_Tags`
- `ViewClient_Broker_DNS_Name`

In einer Horizon Cloud-Umgebung, die mithilfe von Unified Access Gateway konfiguriert wurde, legt der Broker standardmäßig die folgenden Gateway-basierten Eigenschaften für diese Werte wie folgt fest:

- Wenn Ihr Unified Access Gateway extern ist, ist die `ViewClient_Broker_GatewayLocation`-Eigenschaft auf `External` und die `ViewClient_Broker_GatewayType`-Eigenschaft auf `AP` festgelegt.
- Wenn Ihr Unified Access Gateway intern ist, wird die `ViewClient_Broker_GatewayLocation`-Eigenschaft auf Basis der Liste „Interne Netzwerke“ und die `ViewClient_Broker_GatewayType`-Eigenschaft auf `AP` festgelegt.

**Hinweis** Die Liste „Interne Netzwerke“ wird durch Ihren Dienstanbieter erstellt und auf der Seite „Allgemeine Einstellungen“ angezeigt.

Ein Unified Access Gateway mit Ihrer Horizon Cloud-Umgebung zu verwenden, ist eine empfohlene Vorgehensweise. Wenn Sie jedoch nicht über ein Unified Access Gateway verfügen, legt der Broker die `ViewClient_Broker_GatewayLocation`-Eigenschaft auf Basis der Liste „Interne Netzwerke“ und die `ViewClient_Broker_GatewayType`-Eigenschaft auf `None` fest.

## Konfigurieren des direkten Zugriffs von Administratoren auf Desktops

Administratoren können jetzt eine Verbindung mit Desktops mithilfe ihrer Domänenkonten herstellen und müssen nicht mehr über einen lokalen Administratorzugriff verfügen.

Voraussetzung dafür ist, dass bei der DaaS Agent-Installation eine neue Gruppe für DaaS Direct Connect-Benutzer erstellt wird. Diese Gruppe verfügt zwar nicht über lokale Administratorrechte. Sie hat aber die Möglichkeit, mit dem Desktop über Helpdesk Console eine Verbindung herzustellen oder eine direkte RDP-Verbindung zu verwenden.

Es gibt zwei Möglichkeiten, um einen Benutzer zur DaaS Direct Connect-Benutzergruppe hinzuzufügen:

- Aktualisierung des Image.

- Verwendung einer GPO-Richtlinie auf der Mandanten-Appliance.

  **Hinweis** Diese Vorgehensweise ist unabhängig von der Konfiguration der Vorlagen-VM und kann jederzeit durchgeführt werden.

Um Mitglieder durch Aktualisierung des Image hinzuzufügen, führen Sie Folgendes durch:

1 Führen Sie einen Beitritt der Image-VM zur Domäne durch und starten Sie diese erneut.

2 Fügen Sie der DaaS Direct Connect-Benutzergruppe Benutzer hinzu.

3 Veröffentlichen Sie das Image und stellen Sie Desktops bereit. Alle erstellten Desktops, die das Image verwenden, verfügen nun über die Details der Gruppenmitglieder.

Um Mitglieder mithilfe einer GPO-Richtlinie auf der Mandanten-Appliance hinzuzufügen, führen Sie Folgendes durch:

1 Erstellen Sie ein neues GPO.

2 Klicken Sie mit der rechten Maustaste auf das GPO und wählen Sie **Bearbeiten** aus.

3 Wechseln Sie im Gruppenrichtlinienverwaltungs-Editor zu **Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Eingeschränkte Gruppen**.

4 Klicken Sie mit der rechten Maustaste auf **Eingeschränkte Gruppen** und wählen Sie **Gruppe hinzufügen** aus.

5 Geben Sie im Dialogfeld „Gruppe hinzufügen“ die DaaS Direct Connect-Benutzer ein und klicken Sie auf **OK**.

6 Geben Sie in das Textfeld „Mitglieder dieser Gruppe“ im Dialogfeld „Eigenschaften“ die Mitglieder ein, klicken Sie auf **Hinzufügen** und dann auf **OK**.

7 Schließen Sie den Gruppenrichtlinienverwaltungs-Editor sowie die Management-Konsole für Gruppenrichtlinien.

8 Verknüpfen Sie das neu erstellte GPO mit der Domäne.

## Optimieren der Anzeige

Mit den nachfolgenden Aufgaben optimieren Sie die Anzeige auf der VM, auf der sich die Vorlage befindet.

### Hinzufügen der Gruppenrichtlinieneinstellungen für PCoIP

Sie können die Gruppenrichtlinieneinstellungen für PCoIP in die lokale Computerrichtlinienumgebung einfügen.

Zum Konfigurieren der Gruppenrichtlinien müssen Sie zunächst die ADM-Vorlagendatei in die lokale Computerrichtlinienkonfiguration auf dieser VM einfügen.

#### Vorgehensweise

1 Klicken Sie auf der VM, auf der sich die Vorlage befindet, auf **Start > Ausführen**.

2 Geben Sie `gpedit.msc` ein und klicken Sie auf **OK**.

   Die Konsole des Editors für lokale Gruppenrichtlinien wird geöffnet.

3 Prüfen Sie, ob Sie von dieser VM aus eine Verbindung zum View-Verbindungsserver herstellen können.

4 Wählen Sie im Navigationsbereich den Befehl **Richtlinie für „Lokaler Computer“ > Computerkonfiguration**.

5 Klicken Sie mit der rechten Maustaste auf **Administrative Vorlagen**.

   **Hinweis** Wählen Sie „Administrative Vorlagen“ unter „Benutzerkonfiguration“ nicht aus.

6 Wählen Sie **Vorlagen hinzufügen/entfernen**.

7 Klicken Sie im Dialogfeld „Vorlagen hinzufügen/entfernen“ auf **Hinzufügen**.

8 Laden Sie die Datei „pcoip_policies.adm“ aus der Horizon DaaS-Bibliothek unter salesforce.com herunter.

9 Klicken Sie auf **Öffnen**.

10 Schließen Sie das Fenster „Vorlagen hinzufügen/entfernen“.

Die Gruppenrichtlinieneinstellungen für PCoIP werden in die lokale Computerrichtlinienumgebung auf dem Desktopsystem eingefügt und können nunmehr konfiguriert werden.

## Hinzufügen der HTML Access (Blast)-Gruppenrichtlinieneinstellungen

Sie können die Gruppenrichtlinieneinstellungen für HTML Access (Blast) in die lokale Computerrichtlinienumgebung einfügen.

### Vorgehensweise

1 Laden Sie die ZIP-Datei für das View-GPO-Paket von der VMware Horizon-Download-Website herunter.

   Die Datei trägt den Dateinamen „VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip“, wobei x.x.x die Version und yyyyyyy die Buildnummer bezeichnet. Die Datei enthält alle ADM- und ADMX-Dateien mit Gruppenrichtlinieneinstellungen für View.

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

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

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

| Option | Beschreibung |
|---|---|
| **Windows 2008 oder 2012** | a Wählen Sie **Start > Verwaltung > Gruppenrichtlinienverwaltung**.<br>b Erweitern Sie die Domäne, klicken Sie mit der rechten Maustaste auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie „Bearbeiten“. |
| **Windows 2003** | a Wählen Sie **Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer**.<br>b Klicken Sie mit der rechten Maustaste auf die OU, die die View-Desktops enthält, und wählen Sie **Eigenschaften**.<br>c Klicken Sie auf der Registerkarte „Gruppenrichtlinie“ auf **Öffnen**. Das Plug-in „Gruppenrichtlinienverwaltung“ wird geöffnet.<br>d Klicken Sie im rechten Fensterbereich auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **Bearbeiten**. |

Das Fenster „Gruppenrichtlinienobjekt-Editor“ wird angezeigt.

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

5 Klicken Sie auf **Hinzufügen**, navigieren Sie zur Datei „Blast-enUS.adm“ und klicken Sie auf **Öffnen**.

6 Klicken Sie auf **Schließen**. Die Richtlinieneinstellungen in der ADM-Vorlagendatei werden auf das GPO angewendet.

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

7 Konfigurieren Sie die Gruppenrichtlinieneinstellungen für HTML Access.

8 Wenden Sie die Richtlinieneinstellungen auf die Remote-Desktops an.

a Führen Sie den Befehl „gpupdate.exe“ auf den Desktops aus.

b Starten Sie die Desktops neu.

## Konfigurieren der Richtlinieneinstellungen für die Anzeige

Sie können Richtlinieneinstellungen konfigurieren, die die Anzeige auf der VM optimieren, auf der sich die Vorlage befindet.

Legen Sie die nachfolgenden Einstellungen in der Gruppe „Überschreibbare Richtlinie“ vor.

### Vorgehensweise

1 Aktivieren Sie das Kontrollkästchen „Funktion ‚Verlustfrei aufbauen‘ deaktivieren“.

2 Aktivieren Sie die Option „Qualitätsstufen für PCoIP-Image konfigurieren“.

- Legen Sie für „Minimale Image-Qualität“ den Wert 30 fest.
- Legen Sie für „Maximale Image-Qualität“ den Wert 70 fest.
- Legen Sie für „Maximale Frame-Rate“ den Wert 16 fest.

## Aktivieren von 3D-Grafiken

Sie können 3D-Grafiken für einzelne Zuweisungen aktivieren.

Die Unterstützung für 3D-Grafiken erfolgt mithilfe von Soft 3D, auch bekannt als vSGA (weitere Informationen dazu finden Sie im VMware-Whitepaper zur Grafikbeschleunigung auf den Seiten 3 und 4). Für die 3D-Grafik-Funktion gelten die folgenden Voraussetzungen:

- Die virtuelle Hardware muss Version 8 (oder höher) aufweisen.
- Der Desktop muss über das Windows Aero-Design verfügen.
- Server benötigen die dazu erforderliche Hardware.

**Hinweis** Beim Konfigurieren von Desktops mit dieser Funktion beachten Sie die aktuellen PCoIP-Empfehlungen.

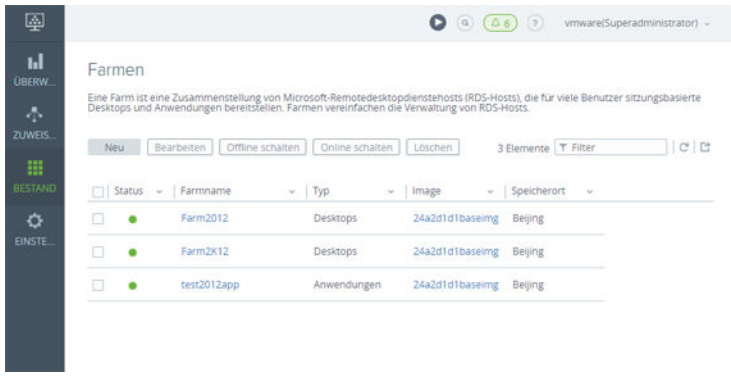
# Farmen in Horizon Cloud

9

Eine Farm ist eine Zusammenstellung von Microsoft Remotedesktopdienstehosts (RDS-Hosts), die für mehrere Benutzer sitzungsbasierte Desktops und Anwendungen bereitstellen. Farmen vereinfachen die Verwaltung der RDS-Hosts. Sie können Farmen für Benutzergruppen erstellen, die unterschiedlich groß sind oder über unterschiedliche Desktop- oder Anwendungsanforderungen verfügen.

Bevor Sie Endbenutzern sitzungsbasierte Desktops oder Remoteanwendungen zuweisen können, müssen Sie die Farmen erstellen, die diese Desktops und Anwendungen bereitstellen. Eine Farm kann entweder sitzungsbasierte Desktops oder Remoteanwendungen bereitstellen.

Verwenden Sie zum Verwalten Ihrer Farmen die Seite „Farmen“ in der Verwaltungskonsole. Zur Seite „Farmen“ gelangen Sie über das Symbol „Bestand“.




Dieses Kapitel behandelt die folgenden Themen:

- Erstellen einer Farm
- Verwalten von Farmen in Horizon Cloud

## Erstellen einer Farm

Sie erstellen Farmen mithilfe der Seite „Farmen“.

**Hinweis** Das RDS-fähige zuweisbare Image wird auch als „RDS-Host“ oder als „RDSH-Image“ (Remote Desktop Services Host, Remotedesktopdienstehost) bezeichnet.

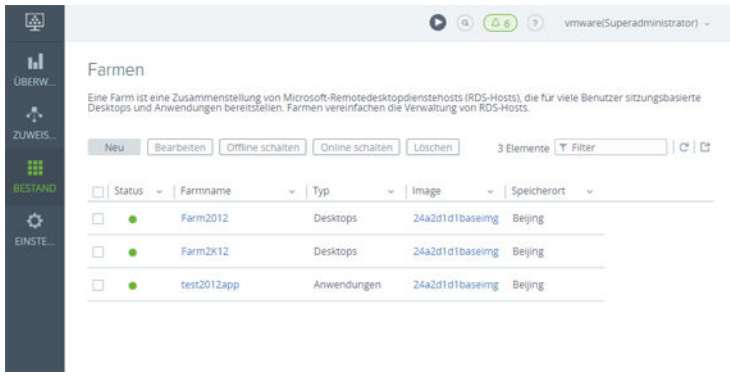
### Voraussetzungen

Stellen Sie sicher, dass mindestens ein zuweisbares Image auf der Seite „Images“ aufgeführt ist, dass dieses Image über ein RDS-fähiges Windows Server-Betriebssystem verfügt und dass es sich in dem Knoten befindet, in dem Sie die Farm erstellen möchten. Sie können in einem Knoten ohne verfügbares zuweisbares Image keine Farm erstellen.

Legen Sie fest, ob diese Farm für sitzungsbasierte Desktops oder für Remoteanwendungen verwendet wird.

### Vorgehensweise

1 Wechseln Sie in der Verwaltungskonsole zu **Bestand > Farmen**.




2 Klicken Sie auf **Neu**.

Der Assistent „Neue Farm“ wird geöffnet.

3 Vervollständigen Sie im Schritt „Definition“ des Assistenten die Felder, treffen Sie Ihr Auswahl nach Bedarf und klicken Sie auf **Weiter**.

**Hinweis** Sie müssen möglicherweise mit der Bildlaufleiste alle erforderlichen Felder einblenden.

| Option | Beschreibung |
|---|---|
| **Name** | Geben Sie einen Namen für diese Farm ein. |
| **Beschreibung** | Geben Sie optional eine Beschreibung ein. |
| **Farmtyp** | Legen Sie den Typ des Objekts fest, das mit dieser Farm für Endbenutzer bereitgestellt wird.<br>■ Wählen Sie **Desktops** aus, wenn Sie mit dieser Farm sitzungsbasierte Desktops bereitstellen möchten.<br>■ Wählen Sie **Anwendungen** aus, wenn Sie mit dieser Farm Remoteanwendungen bereitstellen möchten. Nach der Erstellung einer Anwendungsfarm können Sie mit der Option **Automatisch auf Farm suchen** des Workflows „Neue Anwendung“ Anwendungen von den Servern der Farm in Ihren Anwendungsbestand importieren. |

| Option | Beschreibung |
|---|---|
| **Pod** | Diese Option wird nur angezeigt, wenn Ihr Datencenter mit mehreren Pods konfiguriert ist.<br>Pods enthalten bestimmte zuweisbare Images und Servermodellkapazitäten für Zuweisungen. Sie können Zuweisungen nur anhand von Images im selben Pod erstellen. |
| **Image** | Wählen Sie das zuweisbare RDSH-Image aus. |
| **Bevorzugtes Protokoll** | Wählen Sie ein Standardanzeigeprotokoll für die Endbenutzersitzungen aus.<br>In manchen Umständen ist es erforderlich, ein vom Standardprotokoll abweichendes Protokoll zu verwenden. Wenn z. B. das Clientgerät das Standardprotokoll nicht unterstützt oder der Endbenutzer die Auswahl des Standardprotokolls überschreibt. |
| **Bevorzugter Client-Typ** | Wählen Sie den bevorzugten Client aus, der verwendet werden soll, wenn Endbenutzer ihre sitzungsbasierten Desktops aus dem Portal der Plattform Workspace™ ONE™ starten: Horizon Client oder einen Browser für HTML Access. |
| **Domäne** | Wählen Sie die Active Directory-Domäne aus, die mit Ihrer Umgebung registriert ist. |
| **Domäne beitreten** | Wählen Sie **Ja** aus, damit die Serverinstanzen der Farm automatisch der Domäne beitreten, wenn sie erstellt werden. |
| **Server** | Legen Sie die Anzahl der Server fest, die Sie in dieser Farm verwenden möchten. |
| **Sitzungen pro Server** | Legen Sie die für diese Farm zulässige Anzahl gleichzeitiger Endbenutzersitzungen pro Server fest.<br>**Wichtig** In dieser Version können Sie diese Anzahl nicht mehr aktualisieren, nachdem die Farm erstellt wurde. Folglich müssen Sie den Wert, den Sie hier festlegen, mit Bedacht auswählen. |

Konfigurieren Sie nach Bedarf die erweiterten Eigenschaften.

| Option | Beschreibung |
|---|---|
| **VM-Namen** | Name aller für diese Farm erstellten Server-VMs. Diesen wird eine fortlaufende Zahl angehängt, z. B. win2016-1, win2016-2 etc. Der Name muss mit einem Buchstaben beginnen und darf nur Buchstaben, Bindestriche und Ziffern enthalten. |
| **Computer-OE** | Active Directory-Organisationseinheit, in der sich die Server-VMs befinden sollen. Beispiel: `OU=RootOrgName,DC=DomainComponent,DC=eng` usw. Die Einträge müssen durch Komma getrennt sein und zwischen den Einträgen dürfen keine Leerzeichen stehen.<br>Zur Verwendung von verschachtelten Organisationseinheiten finden Sie Informationen unter Mit verschachtelten Organisationseinheiten arbeiten. |
| **Anmeldeskript ein Mal ausführen** | (Optional) Speicherort der Skripts, die Sie nach Abschluss der Systemvorbereitung ausführen möchten. |

| Option | Beschreibung |
| --- | --- |
| **Intervall für Zeitüberschreitung der Sitzung** | Dies ist die Zeitspanne, während der Sitzungen der Endbenutzer inaktiv sein können, bevor das System eine Abmeldung von den sitzungsbasierten Desktops oder Anwendungen erzwingt, die von dieser Farm bereitgestellt werden. Diese Zeitüberschreitung gilt für die angemeldete Sitzung des zugrunde liegenden Windows-Betriebssystems. Dieses Zeitüberschreitungsintervall ist unabhängig von den Zeitüberschreitungseinstellungen, die die angemeldete Horizon Client- oder HTML Access-Sitzung der Endbenutzer steuern.<br><br>**Vorsicht** Wenn das System die Abmeldung von der zugrunde liegenden Windows-Betriebssystemsitzung erzwingt, gehen alle nicht gespeicherten Daten verloren. Um unerwünschten Datenverlust zu verhindern, legen Sie dieses Intervall hoch genug, um die geschäftlichen Anforderungen Ihrer Endbenutzer zu erfüllen.<br><br>**Hinweis** Wenn bis zum Ablauf des Zeitüberschreitungsintervalls keine Benutzeraktivität stattfindet, erscheint eine Meldung, dass der Benutzer abgemeldet wird, sofern er nicht innerhalb der nächsten 30 Sekunden auf **OK** klickt. Beim Abmelden gehen alle nicht gespeicherten Benutzerdaten, wie z. B. Dokumente oder Dateien, verloren. |
| **Windows-Hotplug aktivieren** | (Optional) Mit der Standardeinstellung **Nein** können Benutzer ihren virtuellen Desktops keine externen Geräte wie z. B. CD-/DVD-Laufwerke, Ethernet-Adapter und ähnliche Gerätetypen dynamisch hinzufügen oder daraus entfernen.<br><br>**Vorsicht** Wenn Sie für diese Umschaltoption **Ja** festlegen, besteht die Möglichkeit, dass Benutzer versehentlich die Verbindung mit den virtuellen Desktops trennen, wenn sie dynamisch die Netzwerkkarten (NICs) oder andere für den Betrieb erforderliche Komponenten unabsichtlich entfernen. Auch wenn Sie diese Einstellung nur in Ausnahmefällen aktivieren, z. B. zur Unterstützung von Thumb-Laufwerken in Ihren virtuellen Desktops, müssen Sie beachten, dass diese Einstellung für alle derartigen Plug&Play-Geräte in den betreffenden Desktops gilt. |

4 Vervollständigen Sie die Felder im Schritt „Management“ des Assistenten, treffen Sie Ihr Auswahl nach Bedarf und klicken Sie auf **Weiter**.

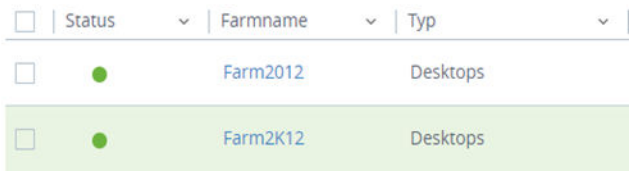
| Option | Beschreibung |
|---|---|
| **Rollierende Wartung** | Wählen Sie den Wartungsmodus aus, entweder auf zeitlicher Basis (**Geplant**) oder basierend auf Benutzersitzungen für die Server dieser Farm (**Sitzung**).<br>Wenn **Geplant** ausgewählt ist, konfigurieren Sie den Wartungszeitraum, entweder täglich oder wöchentlich. Wenn Sie die tägliche Wiederholung auswählen, geben Sie die volle Stunde für den Beginn der Wartung an. Wenn Sie eine wöchentliche Wiederholung auswählen, geben Sie den Wochentag und die volle Stunde an.<br>Wenn **Sitzung** ausgewählt ist, geben Sie die Anzahl der Sitzungen an, ab der die Farm mit der rollierenden Wartung beginnen soll.<br>**Hinweis** Sitzungen, die innerhalb von 15 Minuten abgemeldet werden, werden bei der Berechnung der rollierenden Wartung nicht berücksichtigt, um zu verhindern, dass der Neustart und die Neuerstellung der Server auf einer Anzahl von Sitzungen mit kurzer Laufzeit basiert.<br>Legen Sie im Feld **Parallele Stilllegung von Servern** die Anzahl der Server fest, die gleichzeitig stillgelegt werden können. Wenn sich ein Server im Status der Stilllegung befindet, kann dieser weiterhin für die Benutzersitzungen verwendet werden, die bereits mit dem Server verbunden sind. Es werden dann aber keine neuen Benutzerverbindungen mehr akzeptiert. |
| **Serveraktion** | Wählen Sie die Aktion aus, die auf den Servern während der Wartung durchgeführt werden soll.<br>■ Mit **Neu starten** werden die Server-VMs neu gestartet.<br>■ Mit **Neu erstellen** werden die Server-VMs zuerst gelöscht und danach aus ihrem RDS-Desktop-Image erneut bereitgestellt. |
| **Behandlung der Zeitüberschreitung** | Konfigurieren Sie die Handhabung von bestimmten Benutzersitzungstypen.<br>**Hinweis** Die Benutzersitzungen, die von diesen Einstellungen gesteuert werden, sind die Benutzeranmeldungen bei der Windows-Betriebssystemsitzung des RDS-Sitzungs-Desktop oder der Anwendung. Diese Sitzungen sind nicht die Benutzeranmeldungen in Horizon Client, Horizon HTML Accessoder Workspace ONE.<br>Die Sitzung des Benutzers beginnt, wenn der Benutzer sich beim Windows-Betriebssystem authentifiziert, das dem sitzungsbasierten Desktop oder der Remoteanwendung zugrunde liegt, der bzw. die von den Servern dieser Farm bereitgestellt wird.<br>■ **Zeitüberschreitung für leere Sitzung** – Legen Sie für Anwendungsfarmen fest, wie Benutzersitzungen im Leerlauf gehandhabt werden sollen. Diese können unbegrenzt andauern oder nach einer angegebenen Anzahl von Minuten durch Zeitüberschreitung automatisch beendet werden. Zeitüberschreitungen des Leerlaufs basieren auf der Aktivität des Endpunktgeräts und nicht auf dem sitzungsbasierten Desktop oder der Anwendung. Wenn Sie eine Zeitüberschreitung für eine Sitzung im Leerlauf festlegen, müssen Sie angeben, ob nach dem Zeitablauf die Sitzung getrennt oder der Benutzer abge- |

| Option | Beschreibung |
| --- | --- |
| | meldet wird. Wenn eine Sitzung getrennt wird, wird sie vom Netzwerk getrennt, aber im Arbeitsspeicher beibehalten. Wenn eine Sitzung abgemeldet wird, wird sie nicht im Arbeitsspeicher beibehalten und alle nicht gespeicherten Dokumente gehen verloren.<br>■ **Getrennte Sitzungen abmelden** – Legt fest, dass der Benutzer von einer getrennten Sitzung abgemeldet wird.<br>■ **Maximale Sitzungslebensdauer** – Legt die maximale Anzahl von Minuten fest, die für eine einzelne Benutzersitzung zulässig ist. |

5 Überprüfen Sie im Schritt „Zusammenfassung“ des Assistenten die Einstellungen und klicken Sie auf **Übernehmen**, um mit der Erstellung der Farm zu beginnen.

Das Erstellen der Farm wird gestartet. Sie können den Fortschritt des Vorgangs mithilfe Seite „Aktivität“ überwachen. Wenn als Farmstatus ein grüner Punkt auf der Seite „Farmen“ angezeigt wird:

- Wenn Sie eine Desktop-Farm erstellt haben, können Sie sie verwenden, um eine sitzungsbasierte Desktop-Zuweisung zu erstellen.
- Wenn Sie eine Anwendungsfarm erstellt haben, können Sie diese zum Laden von Anwendungen aus dem den Servern zugrunde liegenden RDS-fähigen Betriebssystem in Ihren Horizon Cloud-Anwendungskatalog verwenden.




### Weiter

Wenn Sie eine Desktop-Farm erstellt haben, müssen Sie im nächsten Schritt eine sitzungsbasierte Desktop-Zuweisung für Ihre Endanwender erstellen. Folgen Sie hierzu den Schritten unter Erstellen einer Zuweisung eines RDSH-Sitzungs-Desktops.

Wenn Sie eine Anwendungsfarm erstellt haben, müssen Sie im nächsten Schritt die Farm durchsuchen, um Anwendungen in Horizon Cloud zu laden und eine Anwendungszuweisung zu erstellen, sodass Ihre Endbenutzer die Remoteanwendungen aus dieser Farm verwenden können.

Weitere Informationen finden Sie unter Kapitel 7 Anwendungen, Importieren neuer Anwendungen aus einer RDSH-Farm mithilfe von „Automatisch auf Farm suchen“ und Manuelles Hinzufügen benutzerdefinierter Anwendungen aus einer RDSH-Farm.

# Verwalten von Farmen in Horizon Cloud

Sie können verschiedene Aktionen mit den Farmen ausführen, die auf der Seite „Farmen“ der Verwaltungskonsole aufgeführt sind.

## Auf der Seite „Farmen“ durchführbare Aktionen

Auf Seitenebene können Sie das Kontrollkästchen neben einer vorhandenen Farm aktivieren und durch Klicken auf eine Schaltfläche die zugehörige Aktion für die Farm ausführen.

**Bearbeiten**

Mit dieser Schaltfläche starten Sie einen Assistenten, in dem Sie bestimmte Einstellungen vornehmen können, z. B. Einstellungen zur Energieverwaltung der Farm, die Mindestanzahl und maximale Anzahl von Servern, über die eine Farm verfügen kann, usw. Der Assistent entspricht dem Assistenten „Neue Farm“ mit schreibgeschützten Feldern für jene Einstellungen, die für eine vorhandene Farm nicht geändert werden können. Eine ausführliche Beschreibung der Felder finden Sie unter Erstellen einer Farm.

Alternativ können Sie auf den Farmnamen klicken und die Einstellungen auf der Übersichtsseite der Farm ändern, anstatt die Schaltfläche **Bearbeiten** zu verwenden.

**Offline schalten**

Mit dieser Schaltfläche öffnen Sie ein Fenster, in dem Sie eine Farm für die Wartung offline schalten können.

**Online schalten**

Mit dieser Schaltfläche öffnen Sie ein Fenster, in dem Sie eine Offline-Farm wieder online schalten können.

**Löschen**

Über diese Schaltfläche können Sie die ausgewählte Farm löschen. Bevor Sie eine Farm mit dieser Schaltfläche löschen können, müssen Sie jedoch alle Zuweisungen löschen, die die Farm verwenden. Sie können die Zuweisungen, die die Farm verwenden, auf der Seite „Zuweisungen“ durch Sortieren der Spalte **Farmen** anzeigen.

**Hinweis** Beim Löschen der Farm werden alle der Farm zugrunde liegenden Server-VMs gelöscht. Wenn eine Farm gelöscht wird, werden alle protokollierten Aktivitäten dieser Farm aus der Seite „Aktivität“ entfernt.

## Auf der Detailseite einer Farm durchführbare Aktionen

Auf der Seite „Farmen“ können Sie durch Klicken auf einen Farmnamen die zugehörige Detailseite anzeigen. Als Erstes wird die Seite „Übersicht“ angezeigt.


**Seite „Übersicht“**

Die Seite „Übersicht“ zeigt die aktuellen Einstellungen der Farm an. Klicken Sie für jeden Seitenabschnitt auf **Bearbeiten**, um diese Einstellungen, die für eine vorhandene Farm aktualisiert werden können, zu ändern. Einige Einstellungen lassen sich für eine erstellte Farm nicht ändern, wie z. B. der zugehörige Knoten.

**Seite „Server“**

Die Seite „Server“ zeigt die in der Farm vorhandenen Serverinstanzen an. Einen ausgewählten Server können sind ein- oder ausschalten (je nach aktuellem Status des Servers) und löschen.


**Seite „Sitzungen“**

Die Seite „Sitzungen“ zeigt die vorhandenen Benutzersitzungen der Farm an. Sie können eine ausgewählte Sitzung trennen oder den Benutzer von dieser Sitzung abmelden. Wenn Sie auf **Trennen** klicken, wird die Sitzung des Benutzers sofort getrennt. Der Benutzer, dessen Sitzung getrennt wird, erhält keine entsprechende Benachrichtigung. Wenn Sie auf **Abmelden** klicken, wird eine Meldung mit einem Kulanzzeitraum angezeigt, in dem der Benutzer noch Dokumente speichern kann, bevor die Sitzung beendet wird.

**Seite „Systemaktivität“**

Die Seite „Systemaktivität“ zeigt die Aktivitäten in der Farm in Bezug auf Systemaktionen an, wie z. B. das Erweitern der Farm,.

**Seite „Benutzeraktivität“**

Die Seite „Benutzeraktivität“ zeigt die Aktivitäten in der Farm in Bezug auf Benutzeraktionen an, wie z. B. das An- und Abmelden von Sitzungen, die von der Farm bereitgestellt werden.

## Verwalten von Servern in einer Farm

Sie können für einzelne Server in einer Farm bestimmte Aktionen ausführen.

### Vorgehensweise

1 Klicken Sie auf **Bestand > Farmen**.

Die Seite „Farmen“ wird angezeigt.

2 Klicken Sie in der Liste auf den Namen einer Farm.

Die Seite mit den Farmdetails wird geöffnet.

3 Klicken Sie oben auf der Seite auf **Server**.

Die Registerkarte „Server“ wird geöffnet und zeigt eine Liste der Server für die Farm an. Mit den Steuerungen oben rechts auf der Seite können Sie die Liste filtern, aktualisieren und exportieren.

Durch Auswahl eines oder mehrerer Server und Klicken auf eine Schaltfläche oben auf der Seite können Sie die nachfolgend aufgeführten Aktionen durchführen.

**Hinweis** Diese Aktionen sind nur dann verfügbar, wenn der Serverstatus grün ist.

| Option | Beschreibung |
|---|---|
| Ausschalten | Fährt die ausgewählten Server herunter.<br>■ Sie können mehrere Server gleichzeitig auswählen.<br>■ Sie können nur VMs herunterfahren, die keine aktiven Benutzersitzungen haben. |
| Einschalten | Startet die ausgewählten ausgeschalteten Server. |
| Löschen | Löscht den ausgewählten Server. |
| Konsole starten | Startet eine Konsole, mit der Sie sich bei der virtuellen Maschine anmelden können. |

# Kapazität

10

Auf der Seite „Kapazität“ werden die aktuelle Desktop-Kapazität und die -Nutzungsdaten angezeigt.

Oben auf der Seite haben Sie folgende Möglichkeiten:

- Filtern der nach Datencenter und Pod angezeigten Informationen mithilfe der Dropdown-Menüs
- Herunterladen eines Berichts im CSV-Format durch Klicken auf den Link **Vollständigen Dienstbericht herunterladen**

Der Hauptbereich der Seite weist zwei Abschnitte auf, die im Folgenden beschrieben werden.

| Abschnitt | Beschreibung |
|---|---|
| Desktop-Modell | Zeigt die gesamte Standardkapazität mit der Anzahl der für jedes Desktop-Modell verwendeten Einheiten und der verfügbaren Einheiten. |
| Speichertypen | Zeigt den Gesamtspeicher mit dem für unterschiedliche Speichertypen verwendeten Anteil und den freien Anteil. Klicken Sie auf das Pfeilsymbol unter „Speicher (GB)“, um den Speicher nach einzelnen Volumes aufgeschlüsselt anzuzeigen. |

# Importierte VMs

11

Importierte VMs sind nicht verwaltete VMs mit unterstützten Betriebssystemen, die in Horizon Cloud importiert werden, um in Images konvertiert oder in dedizierte Desktop-Zuweisungen migriert zu werden.

Mithilfe der Schaltflächen oben auf der Seite können Sie die folgenden Aktionen durchführen.

| Aktion | Beschreibung |
|---|---|
| Umbenennen | Wählen Sie eine VM aus und klicken Sie auf **Umbenennen**. Geben Sie einen neuen Namen in das Feld ein und klicken Sie auf **Speichern**.<br>**Hinweis** Für eine erfolgreiche Durchführung dieser Aktion muss die ausgewählte VM per Agentenpaarbildung mit dem Mandanten gekoppelt werden, und der DaaS-Agent muss den Status „Aktiv“ aufweisen. |
| Herunterfahren | Fährt die VM(s) herunter<br>■ Sie können mehrere VMs gleichzeitig auswählen.<br>■ Der VM-Status muss grün sein.<br>■ Sie können nur VMs herunterfahren, die keine aktiven Benutzersitzungen haben. |
| Neu starten | Führt einen Graceful Restart der VM(s) aus, sodass Sie nicht reagierende VMs ohne Datenverlust wiederherstellen können. Wenn dies nicht funktioniert, ist es unter Umständen erforderlich, die Menüoption „Zurücksetzen“ zu nutzen, um einen Hard Reset der VM mit möglichen Datenverlusten durchzuführen.<br>■ Sie können mehrere VMs gleichzeitig auswählen.<br>■ Der VM-Status muss grün sein. |

Sie können die folgenden Aktionen durchführen, indem Sie auf die Schaltfläche „. . .“ klicken und eine Auswahl aus dem Dropdown-Menü vornehmen.

| Aktion | Beschreibung |
|---|---|
| Anhalten | Hält die ausgewählte VM an |
| Fortsetzen | Setzt den Betrieb der ausgewählten VM fort |
| Einschalten | Schaltet die ausgewählte VM ein |
| Ausschalten | Schaltet die ausgewählte VM aus |
| Zurücksetzen | Setzt die ausgewählte VM zurück |
| Abmelden | Meldet die ausgewählte VM ab |
| Trennen | Trennt die ausgewählte VM |
| In Image konvertieren | Konvertiert die ausgewählte VM in ein Image |

| Aktion | Beschreibung |
|---|---|
| Löschen | Löscht die ausgewählte VM dauerhaft |
| Zu Dienstprogramm-VMs migrieren | Die VM wird zur Seite „Dienstprogramm-VMs“ verschoben. Siehe Verwalten von Dienstprogramm-VMs. |
| Konsole starten | Öffnet eine Konsole für den ausgewählten Desktop. Diese Option ist deaktiviert, wenn die virtuelle Maschine ausgeschaltet oder wenn mehr als eine VM ausgewählt ist. |
| Auf Zuweisung migrieren | Verknüpft die VM(s) mit einer dedizierten Desktop-Zuweisung. Wählen Sie im Dialogfeld „VM(s) migrieren“ im Feld „Zuweisungsname“ eine Zuweisung aus und klicken Sie auf **Migrieren**.<br>■ VMs können nur zu dedizierten Desktop-Zuweisungen mit derselben Desktop Manager-ID migriert werden.<br>■ Die ausgewählte VM muss per Agent-Paarbildung mit dem Mandanten gekoppelt werden, und der DaaS-Agent muss den Status „Aktiv“ aufweisen.<br>■ Der Registrierungseintrag „Use SVI=0“ ist erforderlich. Bei DaaS Agent 17.1.x und View Agent 7.1 ist der Eintrag bereits vorhanden, doch bei älteren Agents muss er manuell hinzugefügt werden. |

# Einstellungen

12

Bearbeiten Sie eine Vielzahl Ihrer Systemeinstellungen.

Wählen Sie das Symbol „Einstellungen“ aus, um auf diese Optionen zuzugreifen.

| Option | Beschreibung |
|---|---|
| Allgemeine Einstellungen | Zeigt Einstellungen für Netzwerke, Domäne usw. an. Sie können auf dieser Seite Einstellungen bearbeiten und Zertifikate hochladen. Siehe Allgemeine Einstellungen bearbeiten. |
| Active Directory | Anzeigen und bearbeiten der Active Directory-Details. Siehe Bearbeiten einer Active Directory-Domäne. |
| Rollen und Berechtigungen | Bearbeiten von Rollen und Berechtigungen. Siehe Bearbeiten von Rollen und Berechtigungen. |
| Infrastruktur | Erstellen Sie Dateifreigaben und führen Sie Aktionen auf vorhandenen Dateifreigaben aus. Siehe Verwalten von Dateifreigaben. |
| Speicherverwaltung | Liste an AppStacks in Ihrer Umgebung anzeigen. Siehe Speicherverwaltung. |
| Erste Schritte | Öffnet den Assistenten für erste Schritte. Siehe Kapitel 3 Assistent für erste Schritte. |
| Dienstprogramm-VMs | Öffnet die Seite „Dienstprogramm-VMs“. Siehe Verwalten von Dienstprogramm-VMs. |
| Zwei-Faktor-Authentifizierung | Konfigurieren der Zwei-Faktor-Authentifizierung für Endbenutzer. Siehe 2-Faktor-Authentifizierung. |

Dieses Kapitel behandelt die folgenden Themen:

- Identitätsverwaltung

# Allgemeine Einstellungen bearbeiten

Auf der Seite „Allgemeine Einstellungen“ können Sie allgemeine Einstellungen bearbeiten und Zertifikate hochladen.

### Vorgehensweise

1 Wählen Sie **Einstellungen > Allgemeine Einstellungen**.

2 Klicken Sie auf **Bearbeiten**.

3 Ändern Sie die folgenden Einstellungen.

| Option | Beschreibung |
|---|---|
| **Netzwerke** | Die Liste „Netzwerke“ zeigt das oder die derzeit genutzten Netzwerke. Diese Liste kann nicht bearbeitet werden. Sollen Netzwerke bearbeitet oder eingefügt werden, werden Sie sich an Ihren Dienstanbieter. |
| **Standarddomäne** | Die Standarddomäne, die Sie bearbeiten. |
| **Zeitüberschreitung der Sitzung** | ■ Client-Taktsignalintervall – steuert das Intervall zwischen Horizon Client-Taktsignalen und dem verbundenen Zustand. In diesen Taktsignalen wird dem Broker die Dauer der Inaktivität gemeldet. Mit Dauer der Inaktivität ist der Zeitraum gemeint, in der keine Interaktion mit dem Endpunktgerät stattfindet (nicht gleichzusetzen mit einer Inaktivität während der Desktopsitzung). In umfangreichen Desktop-Bereitstellungen kann durch das Festlegen der Aktivitätstaktsignale auf längere Intervalle der Netzwerkdatenverkehr reduziert und die Leistung erhöht werden.<br>■ Client-Leerlaufbenutzer – maximale Zeit, die ein Benutzer inaktiv sein kann, ohne dass seine Verbindung zum Mandanten getrennt wird Nach dem Ende dieses Zeitraums wird der Benutzer von allen aktiven Horizon Client-Desktopsitzungen getrennt. Der Benutzer muss sich erneut authentifizieren, um erneut auf den Horizon Client zugreifen zu können.<br>**Hinweis** Legen Sie die Zeitüberschreitung für Client-Leerlaufbenutzer mindestens auf den doppelten Wert des Client-Taktsignalintervalls fest, um unerwartete Trennungen von Desktops zu verhindern.<br>■ Client-Broker-Sitzung – maximale Zeit für die Verbindung einer Horizon Client-Instanz mit dem Mandanten, bevor die Authentifizierung abläuft Das Herunterzählen bis zur Zeitüberschreitung beginnt mit jeder Authentifizierung. Wenn diese Zeitüberschreitung eintritt, können Sie die Arbeit fortsetzen. Wenn Sie eine Aktion ausführen, die zu einer Kommunikation mit dem Broker führt, beispielsweise das Ändern von Einstellungen, müssen Sie sich erneut beim System authentifizieren und sich wieder am Desktop anmelden.<br>**Hinweis** Die Zeitüberschreitung für die Client-Broker-Sitzung muss mindestens gleich der Summe des Client-Taktsignalintervalls und der Zeitüberschreitung für Client-Leerlaufbenutzer sein.<br>■ Zeitüberschreitung des Benutzerportals – gibt an, wie lange Sie sich beim Versuch, eine Verbindung aufzubauen, im Benutzerportal befinden können, bevor Sie sich erneut anmelden müssen. |
| **Benutzerportalkonfiguration** | Diese Funktion ist wird nicht mehr unterstützt. |

| Option | Beschreibung |
|---|---|
| **Überwachen** | Benutzersitzungsinformationen aktivieren – Mit dieser Funktion können vom Cloudüberwachungsdienst (Cloud Monitoring Service, CMS) Benutzer- und Domänendaten für Berichte auf der Seite „Berichte“ verwendet werden. Wenn die Funktion deaktiviert ist, sind die folgenden Elemente nicht verfügbar:<br>■ Die Funktion „Eindeutige Benutzerzusammenfassung“ des Berichts „Auslastung“<br>■ Der Bericht „Sitzungsverlauf“<br>**Hinweis** Die Agenten in den virtuellen Maschinen (RDSH und VDI) benötigen einen ausgehenden Internetzugriff, um Daten an Horizon Cloud senden zu können. |
| **HTML Access** | Anmeldedaten bereinigen, wenn Registerkarte geschlossen ist – Mit dieser Option wird festgelegt, ob die Anmeldedaten für eine Brokersitzung beim Schließen einer HTML Access-Portalregisterkarte gelöscht werden. |
| **Agent-Paarbildung** | Legt eine Richtlinie für den Mandanten fest, die den Zugriff für veraltete Agents (vor 16.6.0) und 16.6.0-Agents regelt. Es gibt folgende Optionen:<br>■ 15.3-Kompatibilitätsmodus – lässt das Koppeln von veralteten Agents und 16.6.0-Agents mit Desktop Manager zu. Dies ist die Standardeinstellung für Upgrade-Einrichtungen.<br>■ 16.6-Upgrade-Modus – schränkt veraltete Agents ein, aber lässt 16.6.0-Agents ohne Bootstrapping auf persistenten Desktops und 16.6.0-Agents mit Bootstrapping zu. Dieser Modus schränkt bereits mit 15.3.x-Agents gekoppelte Desktops nicht ein, es sei denn, der Desktop oder der Agent-Dienst wird neu gestartet.<br>■ 16.6-Modus – lässt nur das Koppeln von 16.6.0-Agents mit Bootstrapping zu. Dieser Modus schränkt Desktops, die bereits mit 15.3.x-Agents gekoppelt sind, sowie 16.6.0-Agents mit Bootstrapping nicht ein, solange der Desktop oder der DaaS-Agent-Dienst nicht neu gestartet wird. Dies ist die Standardeinstellung für neue Installationen.<br>In folgenden Situationen sollten Sie diese Einstellung ändern:<br>■ Vom 15.3-Kompatibilitätsmodus zum 16.6-Upgrade-Modus nur dann wechseln, wenn im System keine Agents vor 16.6 mehr vorhanden sind, dafür aber einige dedizierte Desktops von vor dem Upgrade, deren Agents auf 16.6 aktualisiert wurden<br>■ Vom 15.3-Kompatibilitätsmodus zum 16.6-Modus wechseln, wenn keine Agents vor 16.6 oder 16.6-Agents, die mit veralteten Anmeldeinformationen gekoppelt sind, mehr vorhanden sind Sobald der 16.6-Modus aktiviert ist, funktionieren nur noch VMs, die Bootstrap-Images erstellen und verwenden. |
| **RDSH-Farm** | Definiert Richtlinienparameter für RDSH-Farmen.<br>■ Nachricht zur Erinnerung an die Sitzungslebensdauer – Diese Meldung erinnert Benutzer daran, dass sie nach einer festgelegten Toleranzperiode abgemeldet werden.<br>Die Standardmeldung lautet: „Sehr geehrter Benutzer, Ihre Sitzung hat die maximale Lebensdauer erreicht. Sie werden in \ {0\} Minuten abgemeldet“. \ {0\} steht für den vom Benutzer im Feld „Toleranzperiode“ festgelegten Wert.<br>■ Toleranzperiode – Zeitintervall, nach dem der Benutzer gemäß der Nachricht zur Erinnerung an die Sitzungslebensdauer abgemeldet wird. |
| **Kontaktinformationen** | Kontaktinformationen für Administrator und technischen Support. |

4 Klicken Sie auf **Speichern**.

# Active Directory

Dieser Abschnitt beschreibt die Verfahren zum Registrieren und Konfigurieren von Active Directory-Domänen.

Hinweis:

- Sie müssen die erste Active Directory-Domäne registrieren, bevor Sie mit anderen Services arbeiten können. Bis zum Abschluss dieser Aufgaben sind alle Dienste gesperrt.
- Wenn Sie Benutzer- oder Administratorgruppen definieren, wählen Sie als Gruppentyp für Active Directory immer „Sicherheit“ aus, da Verteilungsgruppen nicht unterstützt werden.

## Registrieren Sie Ihre erste Active Directory-Domäne

Sie müssen die Konfiguration abschließen, indem Sie Active Directory registrieren, den Domänenbeitritt durchführen und den Superadministrator hinzufügen.

**Hinweis** Bevor Sie mit anderen Services arbeiten können, müssen Sie den Active Directory-Registrierungsprozess abschließen. Bis zum Abschluss dieser Aufgaben sind alle Dienste gesperrt.

**Hinweis** Wenn Sie die Domänenregistrierung abgeschlossen haben, sollten Sie keine Gruppen aus einer Organisationseinheit (OU) in eine andere verschieben. Andernfalls kommt es zu Anmeldefehlern für Benutzer.

Wenn Sie vor Abschluss der Registrierung auf **Abbrechen** klicken, können Sie auf der Seite „Erste Schritte“ jederzeit auf **Bearbeiten** klicken, um mit der Registrierung fortzufahren.

### Voraussetzungen

- Die Active Directory-Infrastruktur muss mit einer exakten Zeitquelle synchronisiert werden.
- Wenn Sie externe oder Gesamtstruktur-Vertrauensstellungen verwenden, müssen Stammdomänen registriert werden. Weitere Informationen finden Sie unter Externe und Gesamtstruktur-Vertrauensstellungen.
- Das LDAP-Dienstkonto wird im System als Super-Admin-Benutzer behandelt und darf daher nicht an andere Benutzer weitergegeben werden, die keine Super-Admin-Rechte besitzen. Wenn beispielsweise für ein anderes Produkt ebenfalls ein LDAP-Dienstkonto erforderlich ist, richten Sie hierfür ein eigenes LDAP-Konto ein, damit sich der Benutzer, der dieses neue Konto erhält, nicht als Super-Admin anmelden kann.

### Vorgehensweise

1 Wählen Sie auf der Seite „Erste Schritte“ **Allgemeine Einrichtung**, und klicken Sie dann neben „Active Directory“ auf **Konfigurieren**.

2 Geben Sie im Dialogfeld „Active Directory registrieren“ die angeforderten Registrierungsinformationen an.

| Option | Beschreibung |
|---|---|
| **NETBIOS-Name** | Active Directory-Domänenname |
| **DNS-Domänenname** | Vollständig qualifizierter Active Directory-Domänenname |
| **Protokoll** | Kann nicht bearbeitet werden; LDAP ist die einzige Wahl |
| **Bind-Benutzername** | Domänenadministrator |
| **Bind-Kennwort** | Domänenadministrator-Kennwort |

3 Geben Sie Informationen für das Hilfsdienstkonto-Nr.1 ein.

| Option | Beschreibung |
|---|---|
| **Bind-Benutzername** | Domänenadministrator |
| **Bind-Kennwort** | Domänenadministrator-Kennwort |

**Hinweis** Benutzername und Kennwort müssen im Active Directory vorhanden sein. Andernfalls kann das Konto nicht hinzugefügt werden.

4 Klicken Sie auf **Erweiterte Einstellungen**.

5 Geben Sie Informationen in die Felder „Erweiterte Einstellungen“ ein.

| Option | Beschreibung |
|---|---|
| **Port** | Der Standardwert für dieses Feld ist 389. Sofern Sie keinen Nicht-Standard-Port verwenden, müssen Sie die Einträge in diesem Feld nicht ändern. |
| **Domänencontroller-IP-Adresse** | (Optional) Geben Sie eine einzelne, bevorzugte Domänencontroller-IP-Adresse an, wenn für den AD-Datenverkehr ein spezieller Domänencontroller verwendet werden soll. |
| **Kontext** | Diese Option wird basierend auf den zuvor bereitgestellten Informationen zum DNS-Domänennamen automatisch gefüllt. |

6 Klicken Sie auf **Domänendienst**.

**Hinweis** Wenn eine Fehlermeldung anzeigt, dass die von Ihnen eingegebenen Informationen zum Hilfsdienstkonto ungültig sind, müssen Sie nach dem Abschluss des Domänenbeitritts unten ein gültiges Hilfsdienstkonto durch Bearbeiten der Domänendienstinformationen hinzufügen. Siehe Bearbeiten einer Active Directory-Domäne.

7 Geben Sie die Informationen für den Domänenbeitritt an.

| Option | Beschreibung |
|---|---|
| **Benutzername für den Beitritt** | Domänenadministrator |
| **Kennwort für den Beitritt** | Domänenadministrator-Kennwort |
| **Primäre DNS-Server-IP** | IP-Adresse des primären DNS-Servers |

| Option | Beschreibung |
|---|---|
| **Sekundäre DNS-Server-IP** | (Optional) IP-Adresse des sekundären DNS-Servers |
| **Standard-OE** | Standard-Organisationseinheit |

8 Klicken Sie auf **Speichern**.

9 Verwenden Sie im Dialogfeld „Superadministrator hinzufügen“ die Active Directory-Suchfunktion, um die AD-Administratorgruppe für die Anwendungsadministration auszuwählen.

10 Klicken Sie auf **Speichern**.

11 Wenn der Domänenbeitritts- oder Domänendienstprozess fehlschlägt, müssen Sie den Registrierungsvorgang neu starten.

   a Starten Sie den Browser neu.

   b Melden Sie sich zunächst mit Ihrem My VMware-Konto an.

   c Melden Sie sich mithilfe des Domänendienstkonto-Anmeldenamens und des zugehörigen Kennworts bei dem Active Directory-Konto an.

   d Fahren Sie mit dem Domänenbeitritt fort.

### Weiter

Bei Bedarf können Sie True SSO (Single Sign-on) einrichten. Siehe Konfigurieren von True SSO für eine Active Directory-Domäne.

## Registrieren zusätzlicher Active Directory-Domänen

Optional können Sie zusätzliche Active Directory-Domänen registrieren, damit Sie den Benutzern in diesen Domänen Verwaltungsrollen zuweisen oder Zuweisungen bereitstellen können.

**Hinweis** Wenn Sie die Domänenregistrierung abgeschlossen haben, sollten Sie keine Gruppen aus einer Organisationseinheit (OU) in eine andere verschieben. Andernfalls kommt es zu Anmeldefehlern für Benutzer.

Wenn Sie vor Abschluss der Registrierung auf **Abbrechen** klicken, können Sie auf der Seite „Erste Schritte“ jederzeit auf **Bearbeiten** klicken, um mit der Registrierung fortzufahren.

### Voraussetzungen

- Die Active Directory-Infrastruktur muss mit einer exakten Zeitquelle synchronisiert werden.
- Wenn Sie externe oder Gesamtstruktur-Vertrauensstellungen verwenden, müssen Stammdomänen registriert werden. Weitere Informationen finden Sie unter Externe und Gesamtstruktur-Vertrauensstellungen.

- Das LDAP-Dienstkonto wird im System als Super-Admin-Benutzer behandelt und darf daher nicht an andere Benutzer weitergegeben werden, die keine Super-Admin-Rechte besitzen. Wenn beispielsweise für ein anderes Produkt ebenfalls ein LDAP-Dienstkonto erforderlich ist, richten Sie hierfür ein eigenes LDAP-Konto ein, damit sich der Benutzer, der dieses neue Konto erhält, nicht als Super-Admin anmelden kann.

### Vorgehensweise

1. Wählen Sie in der Verwaltungskonsole **Einstellungen > Active Directory** aus.
2. Klicken Sie auf **Registrieren**.
3. Geben Sie im Dialogfeld „Active Directory registrieren“ die angeforderten Registrierungsinformationen an.

| Option | Beschreibung |
|---|---|
| **NETBIOS-Name** | Active Directory-Domänenname |
| **DNS-Domänenname** | Vollständig qualifizierter Active Directory-Domänenname |
| **Protokoll** | Kann nicht bearbeitet werden; LDAP ist die einzige Wahl |
| **Bind-Benutzername** | Domänenadministrator |
| **Bind-Kennwort** | Domänenadministrator-Kennwort |

4. Geben Sie Informationen für das Hilfsdienstkonto-Nr.1 ein.

| Option | Beschreibung |
|---|---|
| **Bind-Benutzername** | Domänenadministrator |
| **Bind-Kennwort** | Domänenadministrator-Kennwort |

**Hinweis** Benutzername und Kennwort müssen im Active Directory vorhanden sein. Andernfalls kann das Konto nicht hinzugefügt werden.

5. Klicken Sie auf **Erweiterte Einstellungen**.
6. Geben Sie Informationen in die Felder „Erweiterte Einstellungen“ ein.

| Option | Beschreibung |
|---|---|
| **Port** | Der Standardwert für dieses Feld ist 389. Sofern Sie keinen Nicht-Standard-Port verwenden, müssen Sie die Einträge in diesem Feld nicht ändern. |
| **Domänencontroller-IP-Adresse** | (Optional) Geben Sie eine einzelne, bevorzugte Domänencontroller-IP-Adresse an, wenn für den AD-Datenverkehr ein spezieller Domänencontroller verwendet werden soll. |
| **Kontext** | Diese Option wird basierend auf den zuvor bereitgestellten Informationen zum DNS-Domänennamen automatisch gefüllt. |

7 Klicken Sie auf **Domänendienst**.

**Hinweis** Wenn eine Fehlermeldung anzeigt, dass die von Ihnen eingegebenen Informationen zum Hilfsdienstkonto ungültig sind, müssen Sie nach dem Abschluss des Domänenbeitritts unten ein gültiges Hilfsdienstkonto durch Bearbeiten der Domänendienstinformationen hinzufügen. Siehe Bearbeiten einer Active Directory-Domäne.

8 Geben Sie die Informationen für den Domänenbeitritt an.

| Option | Beschreibung |
|---|---|
| **Benutzername für den Beitritt** | Domänenadministrator |
| **Kennwort für den Beitritt** | Domänenadministrator-Kennwort |
| **Primäre DNS-Server-IP** | IP-Adresse des primären DNS-Servers |
| **Sekundäre DNS-Server-IP** | (Optional) IP-Adresse des sekundären DNS-Servers |
| **Standard-OE** | Standard-Organisationseinheit |

9 Klicken Sie auf **Speichern**.

10 Verwenden Sie im Dialogfeld „Superadministrator hinzufügen“ die Active Directory-Suchfunktion, um die AD-Administratorgruppe für die Anwendungsadministration auszuwählen.

11 Klicken Sie auf **Speichern**.

12 Wenn der Domänenbeitritts- oder Domänendienstprozess fehlschlägt, müssen Sie den Registrierungsvorgang neu starten.

a Starten Sie den Browser neu.

b Melden Sie sich zunächst mit Ihrem My VMware-Konto an.

c Melden Sie sich mithilfe des Domänendienstkonto-Anmeldenamens und des zugehörigen Kennworts bei dem Active Directory-Konto an.

d Fahren Sie mit dem Domänenbeitritt fort.

### Weiter

Bei Bedarf können Sie True SSO (Single Sign-on) einrichten. Siehe Konfigurieren von True SSO für eine Active Directory-Domäne.

## Bearbeiten einer Active Directory-Domäne

Sie können eine Active Directory-Domäne nach der anfänglichen Einrichtung bearbeiten.

### Vorgehensweise

1 Wählen Sie **Einstellungen > Active Directory** aus.

Die Seite „Active Directory“ wird angezeigt.

2 Wenn Sie mehrere Active Directorys konfiguriert haben, wählen Sie das Active Directory, das Sie bearbeiten möchten, aus der Liste auf der linken Seite aus.

3 Klicken Sie neben „Domänendienst“ auf **Bearbeiten**, um die Domänendienstinformationen zu bearbeiten.

Das Dialogfeld „Bearbeiten von Active Directory“ wird angezeigt.

4 Bearbeiten Sie die Informationen in den unten beschriebenen Feldern nach Bedarf.

| Option | Beschreibung |
|---|---|
| **NETBIOS-Name** | [Kann nicht bearbeitet werden] Active Directory-Domänenname |
| **DNS-Domänenname** | Vollständig qualifizierter Active Directory-Domänenname |
| **Protokoll** | [Kann nicht bearbeitet werden] LDAP ist die einzige Wahl |
| **Bind-Benutzername** | Domänenadministrator. Nur bearbeiten, wenn zuvor ein neuer Benutzername in Active Directory eingerichtet wurde. |
| **Bind-Kennwort** | Domänenadministrator-Kennwort. Nur bearbeiten, wenn zuvor ein neues Kennwort in Active Directory eingerichtet wurde. |

5 Klicken Sie auf **Erweiterte Einstellungen**.

6 Bearbeiten Sie die Informationen in den folgenden Feldern vom Typ „Erweiterte Eigenschaften“ nach Bedarf.

| Option | Beschreibung |
|---|---|
| **Port** | Der Standardwert für dieses Feld ist 389. Sofern Sie keinen Nicht-Standard-Port verwenden, müssen Sie die Einträge in diesem Feld nicht ändern. |
| **Domänencontroller-IP-Adresse** | (Optional) Geben Sie eine einzelne, bevorzugte Domänencontroller-IP-Adresse an, wenn für den AD-Datenverkehr ein spezieller Domänencontroller verwendet werden soll. |
| **Kontext** | Diese Option wird basierend auf den zuvor bereitgestellten Informationen zum DNS-Domänennamen automatisch gefüllt. |

7 Nehmen Sie Änderungen an Hilfsdienstbindungskonten wie unten beschrieben vor.

- Fügen Sie ein Hilfsdienstbindungskonto hinzu:
  1. Klicken Sie auf den Link **Hilfsdienstbindungskonto hinzufügen**.
  2. Geben Sie Benutzername und Kennwort für das Konto ein.

  **Hinweis** Benutzername und Kennwort müssen im Active Directory vorhanden sein. Andernfalls kann das Konto nicht hinzugefügt werden.

- Ändern Sie das Kennwort für ein Hilfsdienstbindungskonto:
  1. Bestätigen Sie, dass das Kennwort für das Konto bereits in Active Directory geändert wurde.
  2. Klicken Sie auf den Link zum Ändern des Kontokennworts für das entsprechende Konto (z. B. „Kennwort für Konto Nr. 1 ändern“).
  3. Geben Sie das neue Kennwort ein.

  **Hinweis** Sie können den Dienstbenutzernamen für ein Hilfsdienstbindungskonto nicht ändern. Vielmehr müssen Sie das Konto entfernen und mit dem neuen Benutzernamen hinzufügen.

- Sie können ein Hilfsdienstbindungskonto entfernen, indem Sie neben dem Konto auf den Link **Entfernen** klicken.

  **Hinweis** Sie können ein Hilfsdienstbindungskonto nicht entfernen, wenn es sich um das letzte aktive Dienstkonto handelt.

8 Klicken Sie auf **Domänendienst**, um Änderungen zu speichern.

9 Klicken Sie neben „Domänenbeitritt“ auf **Bearbeiten**, um Domänenbeitrittsinformationen zu bearbeiten.

Das Dialogfeld „Domänenbeitritt“ wird angezeigt.

10 Bearbeiten Sie Domänenbeitrittsinformationen nach Bedarf.

| Option | Beschreibung |
|---|---|
| **Benutzername für den Beitritt** | Domänenadministrator. Nur bearbeiten, wenn zuvor ein neuer Benutzername in Active Directory eingerichtet wurde. |
| **Kennwort für den Beitritt** | Domänenadministrator-Kennwort. Nur bearbeiten, wenn zuvor ein neues Kennwort in Active Directory eingerichtet wurde. |
| **Primäre DNS-Server-IP** | IP-Adresse des primären DNS-Servers |
| **Sekundäre DNS-Server-IP** | (Optional) IP-Adresse des sekundären DNS-Servers |
| **Standard-OE** | Standard-Organisationseinheit |

11 Klicken Sie auf **Speichern**.

12 Nehmen Sie im Dialogfeld „Super Administrator hinzufügen“ die gewünschte Änderung vor und klicken Sie auf **Speichern**.

Verwenden Sie die Active Directory-Suchfunktion, um die AD-Administratorgruppe zum Verwalten des Systems auszuwählen.

### Weiter

Bei Bedarf können Sie True SSO (Single Sign-on) einrichten. Siehe Konfigurieren von True SSO für eine Active Directory-Domäne.

## Konfigurieren von True SSO für eine Active Directory-Domäne

Nachdem Sie eine Active Directory-Domäne registriert haben, können Sie True SSO dafür konfigurieren.

### Voraussetzungen

Vor der Konfiguration von True SSO müssen Sie zunächst mindestens einen Identity Manager konfigurieren. Siehe Identitätsverwaltung.

### Vorgehensweise

1 Wählen Sie in der Verwaltungskonsole **Einstellungen > Active Directory** aus.

2 Klicken Sie in der True SSO-Konfiguration auf den Link **Paarbildungs-Token herunterladen**.

   Die Datei pairing_bundle.7z wird in Ihren Downloads-Ordner heruntergeladen.

3 Entpacken Sie die beiden Zertifikatsvorlagendateien aus dem Paket.

   Notieren Sie sich den Speicherort der Dateien. Sie benötigen diesen, wenn Sie den Registrierungsserver in der letzten Phase des Infrastruktur-Setups konfigurieren.

4 Richten Sie die erforderliche Infrastruktur wie unter Einrichten der Infrastruktur für True SSO beschrieben ein.

5 Klicken Sie auf der Seite „Active Directory“ in der Verwaltungskonsole neben „True SSO-Konfiguration“ auf **Hinzufügen**.

   Das Dialogfeld für die True SSO-Konfiguration wird angezeigt.

   **Hinweis** Da Sie das Paarbildungs-Token bereits auf der Seite „Active Directory“ heruntergeladen haben, können Sie den Link **Paarbildungs-Token herunterladen** in diesem Dialogfeld ignorieren.

6 Geben Sie den Namen Ihres Registrierungsservers im Feld „Primärer Registrierungsserver“ ein, und klicken Sie auf die Schaltfläche **Paarbildung testen** neben dem Feld.

   Die anderen Pflichtfelder werden automatisch ausgefüllt.

7 Klicken Sie auf **Speichern**.

8 Um einen sekundären Registrierungsserver für hohe Verfügbarkeit zu konfigurieren, führen Sie die folgenden Schritte aus:

   a Wiederholen Sie die in Einrichten des Registrierungsservers beschriebenen Schritte auf einem zweiten Computer.

   b Bearbeiten Sie die True SSO-Konfiguration und fügen Sie die Adresse des zweiten Registrierungsservers in das Feld „Sekundärer Registrierungsserver“ hinzu, und testen Sie dann die Paarbildung.

   c Speichern Sie die Konfiguration erneut.

Die Konfigurationsinformationen werden jetzt auf der Seite „Active Directory“ unter „True SSO-Konfiguration“ angezeigt.

## Einrichten der Infrastruktur für True SSO

Dieser Abschnitt enthält die Verfahren zum Einrichten der erforderlichen Infrastruktur für die True SSO-Konfiguration.

Führen Sie vor dem Hinzufügen einer True SSO-Konfiguration auf der Seite „Active Directory“ die folgenden Aufgaben aus.

- Installieren und Konfigurieren einer Windows Server-Zertifizierungsstelle (CA)

  **Hinweis** Die Verfahren in diesem Abschnitt gelten für Windows Server 2012 R2. Auf Windows Server 2008 R2 können Sie sehr ähnliche Schritte ausführen.

- Einrichten einer Zertifikatsvorlage für die Zertifizierungsstelle
- Einrichten des Registrierungsservers

Die Zertifizierungsstelle stellt Zertifikate im Namen der Benutzer aus, und diese Zertifikate werden verwendet, um die Benutzer bei ihren zugewiesenen Desktops anzumelden. Die Horizon Cloud-Anwendung fordert den Registrierungsserver zur Ausstellung von Zertifikaten im Namen von Benutzern auf. Der Registrierungsserver generiert das angeforderte Zertifikat im Namen des angeforderten Benutzers über die Zertifizierungsstelle und gibt es an die Horizon Cloud-Anwendung zurück.

### Installieren und Konfigurieren einer Windows Server 2012 R2-Zertifizierungsstelle

Sie können eine Windows Server 2012-Zertifizierungsstelle (CA) mit dem Service Manager-Assistenten einrichten.

Im Folgenden finden Sie die Standardschritte zum Einrichten einer Microsoft-CA. Diese sind hier in einfacher Form aufgeführt, die sich für die Verwendung in einer Testumgebung eignet. Für ein echtes Produktionssystem wird aber empfohlen, dass Sie die Best Practices der Branche zur CA-Konfiguration befolgen.

Wenn Sie weitere Informationen zum Einrichten einer Zertifizierungsstelle benötigen, sehen Sie sich die technischen Standardreferenzen von Microsoft an: Schrittweise Anleitung zu den Windows Server Active Directory-Zertifikatdiensten und Installieren einer Stammzertifizierungsstelle.

**Hinweis** Die Verfahren in diesem Thema gelten für Windows Server 2012 R2. Auf Windows Server 2008 R2 können Sie sehr ähnliche Schritte ausführen.

#### Vorgehensweise

1. Klicken Sie im Server-Manager-Dashboard auf **Rollen und Funktionen hinzufügen**, um den Assistenten zu öffnen. Klicken Sie dann auf **Weiter**.
2. Wählen Sie auf der Seite „Installationstyp auswählen“ die rollenbasierte oder die funktionsbasierte Installation aus, und klicken Sie auf **Weiter**.
3. Behalten Sie auf der Seite zur Serverauswahl die Standardeinstellungen bei, und klicken Sie auf **Weiter**.
4. Auf der Seite „Serverrollen“:
   a. Wählen Sie „Active Directory-Zertifikatdienste“ aus.
   b. Wählen Sie im Dialogfeld „Management-Tool einbeziehen“ aus (sofern zutreffend), und klicken Sie auf **Features hinzufügen**.
   c. Klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite „Features“ auf **Weiter**.
6. Klicken Sie auf der Seite „AD-Zertifikatdienste“ auf **Weiter**.
7. Wählen Sie auf der Seite „Rollendienste“ die Option „Zertifizierungsstelle“ aus, und klicken Sie auf **Weiter**.

8 Wählen Sie auf der Bestätigungsseite „Zielserver bei Bedarf automatisch neu starten“ aus, und klicken Sie auf **Installieren**.

   Der Installationsfortschritt wird angezeigt. Wenn die Installation abgeschlossen ist, wird ein URL-Link angezeigt, über den Sie die neu installierte Zertifizierungsstelle als „Konfigurieren von Active Directory-Zertifikatdiensten“ auf dem Zielserver konfigurieren können.

9 Klicken Sie auf den Konfigurationslink, um den Konfigurationsassistenten zu starten.

10 Geben Sie auf der Seite „Anmeldeinformationen“ Benutzeranmeldeinformationen von der Enterprise-Admin-Gruppe ein, und klicken Sie auf **Weiter**.

11 Wählen Sie auf der Seite „Rollendienste“ die Option „Zertifizierungsstelle“ aus, und klicken Sie auf **Weiter**.

12 Wählen Sie auf der Seite „Installationstyp“ die Option „Unternehmenszertifizierungsstelle“ aus, und klicken Sie auf **Weiter**.

13 Wählen Sie auf der Seite „Zertifizierungsstellentyp“ die Option „Stammzertifizierungsstelle“ oder „Untergeordnete Zertifizierungsstelle“ aus (in diesem Beispiel eine Stammzertifizierungsstelle) und klicken Sie auf **Weiter**.

14 Wählen Sie auf der Seite „Privater Schlüssel“ die Option „Neuen privaten Schlüssel erstellen“ aus, und klicken Sie auf **Weiter**.

15 Geben Sie auf der Seite „Kryptografie“ die folgenden Informationen ein.

| Feld | Beschreibung |
|---|---|
| Kryptografieanbieter | RSA#Microsoft Software Key Storage Provider |
| Schlüssellänge | 4096 (oder nach Bedarf eine andere Länge) |
| Hash-Algorithmus | SHA256 (oder nach Bedarf ein anderer SHA-Algorithmus) |

16 Konfigurieren Sie auf der Seite „Zertifizierungsstellenname“ die gewünschten Einstellungen, oder akzeptieren die Standardeinstellungen, und klicken Sie auf **Weiter**.

17 Konfigurieren Sie auf der Seite „Gültigkeitszeitraum“ die gewünschten Einstellungen, und klicken Sie auf **Weiter**.

18 Klicken Sie auf der Seite „Zertifikatdatenbank“ auf **Weiter**.

19 Überprüfen Sie die Informationen auf der Bestätigungsseite, und klicken Sie auf **Konfigurieren**.

20 Schließen Sie die Konfiguration durch die folgenden Aufgaben ab (führen Sie alle Befehle über die Eingabeaufforderung aus).

a Konfigurieren der Zertifizierungsstelle für die nicht persistente Zertifikatverarbeitung

```
certutil -setreg DBFlags
+DBFLAGS_ENABLEVOLATILEREQUESTS
```

b Konfigurieren der Zertifizierungsstelle, um Offline-CRL-Fehler zu ignorieren

```
certutil -setreg ca\CRLFlags
+CRLF_REVCHECK_IGNORE_OFFLINE
```

c CA-Dienst neu starten

```
net stop certsvc
net start certsvc
```

#### Weiter

Einrichten einer Zertifikatsvorlage für die Zertifizierungsstelle

### Einrichten einer Zertifikatsvorlage für die Zertifizierungsstelle

Sie können die Zertifikatsvorlage in der Zertifizierungsstelle konfigurieren. Die Zertifikatsvorlage ist die Grundlage für die von die Zertifizierungsstelle generierten Zertifikate.

#### Voraussetzungen

Installieren und Konfigurieren einer Windows Server 2012 R2-Zertifizierungsstelle

#### Vorgehensweise

1 Erstellen Sie eine neue universelle Sicherheitsgruppe.

Dadurch können Sie eine einzelne Sicherheitsgruppe verwenden, der Sie die erforderlichen Berechtigungen für die Ausstellung von Zertifikaten im Namen von Benutzern erteilen können. Alle Computer, auf denen VMware-Registrierungsserver installiert sind, können durch Mitgliedschaft in dieser Gruppe diese Berechtigungen erben.

a Klicken Sie auf **Start**, und geben Sie „dsa.msc“ ein.

Das Dialogfeld „Active Directory-Benutzer und -Computer“ wird angezeigt.

b Klicken Sie in der Struktur mit der rechten Maustaste auf den **Benutzerordner** für den Domänencontroller, und wählen Sie **Neu > Gruppe** aus.

Das Dialogfeld „Neues Objekt – Gruppe“ wird angezeigt.

c Geben Sie im Feld „Gruppenname“ einen Namen für die neue Gruppe ein. Beispielsweise TrueSSO-Registrierungsserver.

d Nehmen Sie Einstellungen wie unten beschrieben vor.

| Einstellung | Wert |
|---|---|
| Gruppenbereich | Universal |
| Gruppentyp | Sicherheit |

e Klicken Sie auf **OK**.

Die neue Gruppe wird in der Struktur im Dialogfeld „Active Directory-Benutzer und -Computer“ angezeigt.

f Klicken Sie mit der rechten Maustaste auf die Gruppe, und wählen Sie **Eigenschaften** aus.

g Fügen Sie auf der Registerkarte „Mitglied von“ den Computer hinzu, auf dem der Registrierungsserver installiert wird, und klicken Sie dann auf **OK**.

h Starten Sie die Computer neu, auf denen Registrierungsserver installiert werden

2 Konfigurieren Sie die Zertifikatsvorlage.

a Wählen Sie **Systemsteuerung > Verwaltung > Zertifizierungsstelle**.

b Blenden Sie den lokalen Zertifizierungsstellennamen in der Struktur ein.

c Klicken Sie mit der rechten Maustaste auf den Ordner „Zertifikatvorlagen“, und wählen Sie **Verwalten**.

Die Zertifikatvorlagenkonsole wird angezeigt.

d Klicken Sie mit der rechten Maustaste auf die Vorlage „Smartcard-Anmeldung“, und wählen Sie **Vorlage duplizieren**.

Das Dialogfeld „Eigenschaften der neuen Vorlage“ wird angezeigt.

e Geben Sie die unten beschriebenen Informationen auf den Registerkarten des Dialogfelds ein.

| Registerkarte | Einstellungen |
|---|---|
| Kompatibilität | ■ Aktivieren Sie das Kontrollkästchen „Resultierende Änderungen anzeigen“<br>■ Zertifizierungsstelle – Windows Server 2008 R2<br>■ Zertifikatsempfänger – Windows 7/Server 2008 R2 |
| Allgemein | ■ Vorlagenanzeigename – Namen Ihrer Wahl. Beispiel: True SSO-Vorlage.<br>■ Vorlagenname – Namen Ihrer Wahl. Beispiel: True SSO-Vorlage.<br>■ Gültigkeitsdauer – 1 Stunde<br>■ Erneuerungszeitraum – 0 Wochen |
| Anforderungsverarbeitung | ■ Zweck – Signatur und Smartcard-Anmeldung<br>■ Aktivieren Sie das Kontrollkästchen „Für automatische Erneuerung von Smartcard-zertifikaten ...“ Kontrollkästchen<br>■ Aktivieren Sie das Optionsfeld „Benutzer zur Eingabe während der Registrierung auffordern“ |
| Kryptografie | ■ Anbieterkategorie – Schlüsselspeicheranbieter<br>■ Name des Algorithmus – RSA<br>■ Minimale Schlüsselgröße – 2048<br>■ Aktivieren Sie das Optionsfeld „Verwendung aller auf dem Computer des Antragstellers verfügbaren ...“ Optionsfeld<br>■ Anforderungshash – SHA256 |
| Antragstellername | ■ Wählen Sie das Optionsfeld „Aus diesen Informationen in Active Directory erstellen“<br>■ Format des Antragstellernamen – Vollständiger definierter Name<br>■ Aktivieren Sie das Kontrollkästchen „Benutzerprinzipalname (UPN)“ |
| Server | Aktivieren Sie das Kontrollkästchen „Keine Zertifikate und Anforderungen in der Datenbank der Zertifizierungsstelle speichern“ |
| Ausstellungsvoraussetzungen | ■ Registrierung erfordert Folgendes – Wählen Sie „Diese Anzahl an autorisierten Signaturen“, und geben Sie 1 ein<br>■ Erforderlicher Richtlinientyp für Signatur – Anwendungsrichtlinie<br>■ Anwendungsrichtlinie – Zertifikatsanforderungs-Agent<br>■ Registrierung erfordert Folgendes – Gültiges vorhandenes Zertifikat |
| Sicherheit | Wählen Sie im oberen Bereich der Registerkarte die neue Gruppe aus, die Sie erstellt haben. Wählen Sie dann im unteren Bereich der Registerkarte „Zulassen“ für Lese- und Registrierungsberechtigungen. |

f Klicken Sie auf **OK**.

3 Stellen Sie die Vorlage für True SSO aus.

a Klicken Sie erneut auf den Ordner „Zertifikatvorlagen“, und wählen Sie **Neu > Auszustellende Zertifikatvorlage**.

Das Dialogfeld „Zertifikatvorlagen aktivieren“ wird angezeigt.

b Wählen Sie TrueSsoTemplate, und klicken Sie auf **OK**.

4 Stellen Sie die Registrierungs-Agent-Vorlage aus.

   a Klicken Sie erneut auf den Ordner „Zertifikatvorlagen“, und wählen Sie **Neu > Auszustellende Zertifikatvorlage**.

   Das Dialogfeld „Zertifikatvorlagen aktivieren“ wird angezeigt.

   b Wählen Sie den Registrierungs-Agent-Computer aus, und klicken Sie auf **OK**.

   **Hinweis** Diese Vorlage muss dieselben Sicherheitseinstellungen aufweisen wie die Vorlage, die im vorherigen Schritt ausgestellt wurde.

Die Zertifizierungsstelle ist jetzt eingerichtet und mit einer Zertifikatsvorlage konfiguriert, die sich für True SSO eignet.

#### Weiter

Einrichten des Registrierungsservers

### Einrichten des Registrierungsservers

Der Registrierungsserver ist eine Horizon Cloud-Komponente, die Sie als letzten Schritt bei der Einrichtung der Infrastruktur für True SSO auf einem Windows Server-Computer installieren. Durch Bereitstellung des Registrierungs-Agent-(Computer-)Zertifikats auf dem Server autorisieren Sie diesen Registrierungsserver als Registrierungs-Agent, der Zertifikate im Namen von Benutzern generieren kann.

#### Voraussetzungen

Einrichten einer Zertifikatsvorlage für die Zertifizierungsstelle

#### Vorgehensweise

1 Installieren Sie den Registrierungsserver.

   a Laden Sie die .exe-Datei für den Registrierungsserver von der My VMware-Site herunter. Der Dateiname sollte in etwa „VMware-HorizonCloud-TruessoEnrollmentServer-x86_64-7.3.0-xxxxx.exe“ entsprechen.

   b Bestätigen Sie, dass das System eine Windows Server 2008 R2- oder 2012 R2-Maschine ausführt und mindestens 4 GB Arbeitsspeicher aufweist.

   c Führen Sie das Installationsprogramm aus, und folgen Sie dem Assistenten.

2 Stellen Sie das Registrierungs-Agent-(Computer-)Zertifikat bereit.

   a Öffnen Sie die Microsoft Management Console (MMC).

   b Klicken Sie im Menü „Datei“ auf **Snap-In hinzufügen/entfernen**.

   c Doppelklicken Sie unter „Verfügbare Snap-Ins“ auf **Zertifikate**.

   d Wählen Sie das Computerkonto aus, und klicken Sie auf **Weiter**.

   e Wählen Sie „Lokaler Computer“ aus und klicken Sie auf **Fertigstellen**.

   f Klicken Sie im Dialogfeld „Snap-Ins hinzufügen bzw. entfernen“ auf **OK**.

g Klicken Sie in der MMC auf den Ordner „Persönlich“ unter „Zertifikate“, und wählen Sie **Alle Aufgaben > Neue Zertifikate anfordern**.

h Aktivieren Sie im Dialogfeld „Zertifikatregistrierung“ das Kontrollkästchen für den Registrierungs-Agent (Computer), und klicken Sie auf **Registrieren**.

3 Importieren Sie das Pairing-Paket.

a Klicken Sie in der MMC mit der rechten Maustaste auf den Unterordner „Zertifikate“ im Ordner für vertrauenswürdige Stämme des VMware Horizon Cloud-Registrierungsservers, und wählen Sie **Alle Aufgaben > Importieren**.

b Klicken Sie auf **Weiter**.

c Navigieren Sie zum Speicherort, in dem Sie die Zertifikatdateien aus dem Paket pairing_bundle.7z entpackt haben.

d Importieren die zwei Zertifikatdateien nacheinander.

e Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.

**Weiter**

Führen Sie die verbleibenden Schritte aus, um True SSO in der Verwaltungskonsole zu konfigurieren. Siehe Konfigurieren von True SSO für eine Active Directory-Domäne.

## Externe und Gesamtstruktur-Vertrauensstellungen

Das System unterstützt die Einbeziehung externer (oder Gesamtstruktur-)Vertrauensstellungen zwischen Domänen in verschiedenen Gesamtstrukturen.

Dazu gehören:

- Die Zuweisung/Berechtigung von Benutzern/Gruppen in einer Gesamtstruktur zu bzw. für Ressourcen in einer anderen Gesamtstruktur.
- Support für unidirektionale Vertrauensstellungen.

Damit diese Vertrauensstellungsart problemlos funktioniert, müssen Sie Folgendes tun.

- Registrieren Sie alle Domänen aus allen Gesamtstrukturen, die Konten und Desktops enthalten, die Sie verwenden möchten.
- Registrieren Sie die Stammdomäne der Gesamtstruktur von beiden Seiten einer Gesamtstruktur-Vertrauensstellung. Nur so können Mandanten eine Verbindung zur Stammdomäne der Gesamtstruktur aufbauen und das entsprechende vertrauenswürdige Domänenobjekt (Trusted Domain Object, TDO) entschlüsseln. Diese Voraussetzung gilt auch dann, wenn es keine DaaS-Desktops oder -Benutzer in der Stammdomäne der Gesamtstruktur gibt.
- Aktivieren Sie in jeder Gesamtstruktur für mindestens eine registrierte Domäne den globalen Katalog. Für einen optimalen Arbeitsablauf sollte für alle registrierten Domänen ein globaler Katalog aktiviert sein.

- Um Gruppen aus verschiedenen Gesamtstrukturen Zugriff auf einen Desktop zu gewähren, müssen Sie mindestens eine universelle Gruppe aus jeder Gesamtstruktur registrieren. Die Berechtigung/Zuweisung mittels lokalen Domänengruppen wird nicht unterstützt. Das heißt, dass das System FSPs in 'member'-Attribut-DNs und Token-Gruppen herausfiltert.
- Befolgen Sie bei Domänen von Gesamtstrukturen für den DNS-Namen und den Namenskontext für die Stammdomäne eine hierarchische Struktur. Wenn die übergeordnete Domäne zum Beispiel „example.edu“ heißt, könnte eine untergeordnete Domäne zwar „vpc.example.edu“, aber nicht „vpc.com“ genannt werden.
- Vermeiden Sie Domänen aus externen Gesamtstruktur-Vertrauensstellungen mit sich überschneidenden NETBIOS-Namen, da solche Domänen ausgeschlossen werden. Der registrierte NETBIOS-Name hat stets Vorrang vor dem sich überschneidenden NETBIOS-Namen, der während der Enumeration der Domäne der Gesamtstruktur-Vertrauensstellung gefunden wird.

# Bearbeiten von Rollen und Berechtigungen

Sie können zuvor konfigurierte Rollen bearbeiten.

### Vorgehensweise

1 Wählen Sie **Einstellungen > Rollen und Berechtigungen** aus.

Es wird die Seite „Rollen & Berechtigungen“ angezeigt.

Es sind zwei Standardrollen vorhanden, die im Folgenden gezeigt werden.

| Rolle | Beschreibung |
|---|---|
| Super-Administrator | Benutzer mit dieser Rolle können auf alle Funktionen zugreifen und Änderungen speichern. |
| Demo-Administrator | Benutzer mit dieser Rolle können auf alle Funktionen zugreifen, jedoch keine Änderungen speichern. |

2 Wählen Sie eine Rolle aus der Liste „Rollen“ aus und klicken Sie auf **Bearbeiten**.

3 Verwenden Sie im Bearbeitungsdialogfeld die Active Directory-Suchfunktion, um eine Gruppe für die Rolle auszuwählen, und klicken Sie auf **Speichern**.

**Hinweis** Fügen Sie dieselbe Gruppe nicht sowohl der Rolle „Superadministrator“ als auch der Rolle „Demo-Administrator“ hinzu. Andernfalls besteht die Gefahr, dass Benutzer dieser Gruppe nicht über einen kompletten Zugriff auf alle erwarteten Funktionen verfügen.

# Verwalten von Dateifreigaben

Sie können Dateifreigaben einrichten, mit denen Daten in die Benutzeroberfläche importiert werden.

- Erstellen Sie eine Dateifreigabe auf einer separat verwalteten Maschine außerhalb der Benutzeroberfläche und fügen Sie diese Dateifreigabe dann auf der Seite „Infrastruktur“ ein.

- Sobald die Dateifreigabe in das System aufgenommen wurde, werden die Inhalte automatisch oder manuell importiert (je nach ausgewählter Funktion).
- Zwei Typen von Dateifreigaben unterstützen verschiedene Funktionen:

| Typ | Inhalt |
|---|---|
| Agents | ■ Agentensoftware-Aktualisierung – Die Agentendateien werden automatisch in die Dateifreigabe heruntergeladen, in das System importiert und auf der Seite „Zuweisungen“ bereitgestellt. Siehe Aktualisieren von Agenten für eine Zuweisung. |
| Anwendungen/Images | ■ App Volumes-Integration – Kopieren Sie AppStacks in die Dateifreigabe und importieren Sie sie dann über die Seite „Infrastruktur“. Siehe Importieren von Anwendungen mithilfe von App Volumes. |

## Dateifreigabe erstellen

Sie können eine Dateifreigabe außerhalb der Benutzeroberfläche erstellen.

### Vorgehensweise

1 Legen Sie einen Windows-Ordner wie gewohnt an.

- Bei einer Agenten-Dateifreigabe (also bei einer Dateifreigabe für eine Agentensoftware-Aktualisierung) müssen Sie den Namen „agentFiles“ für den Ordner eingeben. Das System legt dann mehrere Unterordner an, wobei Sie nur zwei Unterordner nutzen. Diese Unterordner werden nachfolgend beschrieben.

| Name des Unterordners | Beschreibung |
|---|---|
| cdsClient | Dieser Ordner enthält Agentendateien, die automatisch vom Aktualisierungsserver heruntergeladen wurden, den Ihr VMware-Vertreter für Sie konfiguriert hat. |
| hotpatch | Dieser Ordner enthält Agentendateien, die Sie manuell dort ablegen. Dies ist nur dann erforderlich, wenn Ihr VMware-Vertreter Sie explizit dazu auffordert. |

- Bei einer Anwendungs-/Image-Dateifreigabe können Sie einen beliebigen Namen eingeben.

2 Legen Sie die folgenden Einstellungen für den Dateifreigabeordner fest:

- Prüfen Sie, ob die Dateifreigabe an die Mandantendomäne angeschlossen ist.
- Aktivieren Sie die Freigabe.
- Tragen Sie einen Domänenbenutzer in die Berechtigungen ein.

3 Notieren Sie die folgenden Informationen, die Sie zum Einfügen des Dateiservers in die Benutzeroberfläche benötigen:

- Benutzername und Kennwort des Domänenbenutzers, den Sie im vorherigen Schritt eingetragen haben
- Quellpfad des Dateifreigabeordners

### Weiter

Fügen Sie die Dateifreigabe in die Benutzeroberfläche ein. Siehe Hinzufügen einer Dateifreigabe auf der Seite „Infrastruktur“.

## Hinzufügen einer Dateifreigabe auf der Seite „Infrastruktur“

Nachdem Sie eine Dateifreigabe außerhalb der Benutzeroberfläche erstellt haben, können Sie sie auf der Seite „Infrastruktur“ hinzufügen.

**Hinweis** Beim Hinzufügen einer Dateifreigabe werden die Inhalte der Dateifreigabe (Agentendateien oder AppStacks) in das System importiert. Wenn Sie später neue Inhalte in der Dateifreigabe ablegen, können Sie diese Inhalte mit der Funktion „Importieren“ importieren.

### Voraussetzungen

Zum Hinzufügen einer Dateifreigabe auf der Seite „Infrastruktur“ müssen Sie sie zunächst außerhalb der Benutzeroberfläche erstellen. Siehe Dateifreigabe erstellen.

### Vorgehensweise

1 Wählen Sie **Einstellungen > Infrastruktur** aus und klicken Sie auf **Dateifreigabe**.

2 Klicken Sie auf **Neu**.

3 Geben Sie die erforderlichen Informationen in das Dialogfeld „Neue Dateifreigabe“ ein.

| Option | Beschreibung |
|---|---|
| **Name** | Name der Dateifreigabe. |
| **Domäne** | Domäne der Dateifreigabe. Nehmen Sie die Auswahl aus der Dropdown-Liste vor. |
| **Benutzername** | Der Admin-Benutzer für die Dateifreigabe. |
| **Kennwort** | Das Admin-Kennwort für die Dateifreigabe. |
| **Typ** | Typ der Dateifreigabe. Wählen Sie „Agenten“ oder „Anwendungen/Images“ in Abhängigkeit davon aus, was die Dateifreigabe enthält.<br>■ Die Agenten-Dateifreigaben dienen lediglich zum Importieren von Agentensoftware-Aktualisierungen.<br>■ Anwendungs-/Images-Dateifreigaben werden zum Importieren von AppStacks verwendet. |
| **Quellpfad** | Netzwerkpfad zur Dateifreigabe |
| **Ziel-Pod** | [nur Anwendungs-/Image-Typ] Dieses Feld wird nur dann angezeigt, wenn der Mandant mehrere Pods umfasst. Wählen Sie den Pod in der Dropdown-Liste aus. |

4 Klicken Sie auf **Speichern**.

## Dateifreigabe bearbeiten

Sie können den Namen, Quellpfad und Ziel-Pod einer Dateifreigabe bearbeiten.

### Vorgehensweise

1 Wählen Sie **Einstellungen > Infrastruktur** aus.

2 Aktivieren Sie das Kontrollkästchen neben der zu bearbeitenden Dateifreigabe.

3 Klicken Sie auf **Bearbeiten**, und nehmen Sie die Änderungen vor.

4 Klicken Sie auf **Speichern**.

## Entfernen einer Dateifreigabe

Sie können eine Dateifreigabe auf der Seite „Infrastruktur“ entfernen.

### Vorgehensweise

1 Wählen Sie auf der Seite „Infrastruktur“ die zu entfernende Dateifreigabe aus.

2 Klicken Sie auf **Entfernen** und bestätigen Sie, dass Sie die Dateifreigabe entfernen möchten.

Die Dateifreigabe wird nicht mehr in der Liste angezeigt.

## Importieren des Inhalts einer Dateifreigabe

Auf der Seite „Infrastruktur“ können Sie den Inhalt einer Dateifreigabe importieren.

### Vorgehensweise

1 Wählen Sie **Einstellungen > Infrastruktur** aus.

2 Wählen Sie die Dateifreigabe auf der Seite „Infrastruktur“ aus.

3 Klicken Sie auf die Schaltfläche „...“ und wählen Sie **Importieren**.

- In den meisten Fällen werden alle Dateien automatisch importiert und auf der entsprechenden Seite in der Benutzeroberfläche bereitgestellt.

| Dateityp | Seite in der Benutzeroberfläche |
|---|---|
| Agents | Seite „Zuweisungen“ (siehe Aktualisieren von Agenten für eine Zuweisung) |
| AppStacks | Seite „Anwendungen“ |

- Wenn eine Agentendatei als Hotpatch bereitgestellt wird, werden Sie aufgefordert, den Hashwert einzugeben, den Ihr VMware-Vertreter Ihnen mitgeteilt hat. Dies ist nur dann erforderlich, wenn Ihr VMware-Vertreter Sie explizit dazu auffordert.

# Speicherverwaltung

Auf der Speicherverwaltungsseite können Sie AppStacks organisieren.

Wählen Sie **Einstellungen > Speicherverwaltung** aus, um die Seite „Speicherverwaltung“ zu öffnen.

## Verwalten von AppStacks

Auf der Registerkarte „AppStacks“ der Seite „Speicherverwaltung“ werden alle AppStacks für den Mandanten aufgeführt.

- Zum Freigeben von Speicherplatz können Sie einen AppStack löschen, indem Sie ihn in der Liste auswählen und auf die Schaltfläche **Löschen** klicken.

  **Hinweis** Es ist nicht möglich, einen AppStack zu löschen, der aktive Benutzersitzungen aufweist.

- Sie können die Liste filtern oder die Seite mithilfe der Steuerelemente in der oberen rechten Ecke der Seite aktualisieren.

# Verwalten von Dienstprogramm-VMs

Dienstprogramm-VMs sind ermittelte VMs mit nicht unterstützten Betriebssystemen, die für Infrastrukturdienste wie DHCP verwendet werden.

Mithilfe der Schaltflächen oben auf der Seite können Sie die folgenden Aktionen durchführen.

| Aktion | Beschreibung |
|---|---|
| Umbenennen | Wählen Sie eine VM aus und klicken Sie auf **Umbenennen**. Geben Sie einen neuen Namen in das Feld ein und klicken Sie auf **Speichern**.<br>**Hinweis** Für eine erfolgreiche Durchführung dieser Aktion muss die ausgewählte VM per Agentenpaarbildung mit dem Mandanten gekoppelt werden, und der DaaS Agent muss den Status „Aktiv“ aufweisen. |
| Herunterfahren | Fährt die VM(s) herunter<br>■ Sie können mehrere VMs gleichzeitig auswählen.<br>■ Der VM-Status muss grün sein.<br>■ Sie können nur VMs herunterfahren, die keine aktiven Benutzersitzungen haben. |
| Neu starten | Führt einen Graceful Restart der VM(s) aus, sodass Sie nicht reagierende VMs ohne Datenverlust wiederherstellen können. Wenn dies nicht funktioniert, ist es unter Umständen erforderlich, die Menüoption „Zurücksetzen“ zu nutzen, um einen Hard Reset der VM mit möglichen Datenverlusten durchzuführen.<br>■ Sie können mehrere VMs gleichzeitig auswählen.<br>■ Der VM-Status muss grün sein. |

Sie können die folgenden Aktionen durchführen, indem Sie auf die Schaltfläche „. . .“ klicken und eine Auswahl aus dem Dropdown-Menü vornehmen.

| Aktion | Beschreibung |
|---|---|
| Anhalten | Hält die ausgewählte VM an |
| Fortsetzen | Setzt den Betrieb der ausgewählten VM fort |
| Einschalten | Schaltet die ausgewählte VM ein |
| Ausschalten | Schaltet die ausgewählte VM aus |
| Zurücksetzen | Setzt die ausgewählte VM zurück |

| Aktion | Beschreibung |
|---|---|
| Abmelden | Meldet die ausgewählte VM ab |
| Trennen | Trennt die ausgewählte VM |
| Zu importierten VMs migrieren | Die VM wird zur Seite „Importierte VMs“ verschoben. Siehe Kapitel 11 Importierte VMs. |

# 2-Faktor-Authentifizierung

Das System unterstützt die RSA SecurID- und Radius-Authentifizierung für interne Benutzer.

Informationen zum Aktivieren der 2-Faktor-Authentifizierung für Benutzer in Ihrem internen Netzwerk finden Sie unter Einrichten der Authentifizierung mit RADIUS und Einrichten der Authentifizierung mit RSA SecurID.

## Einrichten der Authentifizierung mit RADIUS

Mithilfe von RADIUS können Sie die Zwei-Faktor-Authentifizierung für Endbenutzer aktivieren.

**Hinweis** Stellen Sie sicher, dass die IP-Adressen der primären und sekundären Mandanten-Appliance als Clients auf dem RADIUS-Server registriert sind. Beschaffen Sie sich die IP-Adressen für die Mandanten-Appliance von Ihrem VMware-Vertreter.

### Vorgehensweise

1 Wählen Sie **Einstellungen > Zwei-Faktor-Authentifizierung**.

2 Konfigurieren Sie die Authentifizierung.

| Option | Beschreibung |
|---|---|
| **Zwei-Faktor-Authentifizierungsmethode** | Wählen Sie **Radius**. |
| **Benutzernamen beibehalten** | Wählen Sie **Ja** aus, um den Benutzernamen während der Authentifizierung beizubehalten. Der Benutzer, der den Authentifizierungsversuch unternimmt, muss für RSA und die Domänenherausforderung über dieselben Anmeldedaten verfügen. Wenn Sie **Nein** auswählen, wird das Feld für den Benutzernamen nicht gesperrt und der Benutzer hat die Möglichkeit, einen anderen Namen einzugeben. |
| **Nur externe Verbindungen** | Wählen Sie **NEIN** aus, um die Zwei-Faktor-Authentifizierung für interne Benutzer von innerhalb des Systems zu konfigurieren. Verwenden Sie Access Point zum Konfigurieren externer Benutzer. |
| **Anbietername** | (Erforderlich) Name zur Unterscheidung des verwendeten RADIUS-Authentifizierungstyps. |
| **Hostname/IP-Adresse** | (Erforderlich) DNS-Name oder IP-Adresse des Authentifizierungsservers. |
| **Gemeinsamer geheimer Schlüssel** | (Erforderlich) Geheimer Schlüssel für die Kommunikation mit dem Server. Der Wert muss mit dem für den Server konfigurierten Wert übereinstimmen. |
| **Authentifizierungsport** | Der zum Senden und Empfangen von Authentifizierungs-Datenverkehr konfigurierte UDP-Port. Standard ist „1812“. |
| **Kontoführungsport** | Der zum Senden und Empfangen von Kontoführungs-Datenverkehr konfigurierte UDP-Port. Standard ist „1813“. |

| Option | Beschreibung |
|---|---|
| **Vorgang** | Wählen Sie das RADIUS-Authentifizierungsprotokoll aus: PAP, CHAP, MS-CHAPv1 oder MS-CHAPv2. |
| **Zeitüberschreitung des Servers** | Zeitraum in Sekunden, in dem auf eine Antwort vom RADIUS-Server gewartet wird. Die Standardeinstellung ist fünf Sekunden. |
| **Maximale Anzahl an erneuten Versuchen** | Die maximale Anzahl an Wiederholungsversuchen bei fehlgeschlagenen Anforderungen. Die Standardeinstellung ist drei Versuche. |
| **Bereichspräfix** | Der Name und Begrenzer des Bereichs, der dem Benutzernamen während der Authentifizierung vorangestellt wird. |
| **Bereichssuffix** | Der Name und Begrenzer des Bereichs, der dem Benutzernamen während der Authentifizierung angehängt wird. |
| **Hilfsserver** | Die Standardeinstellung ist **NEIN**. Wenn dieser Wert auf **JA** gesetzt ist, geben Sie einen sekundären RADIUS-Server an, der verwendet werden soll, falls der primäre Server nicht antwortet. |

3 Klicken Sie auf **Speichern**.

4 Geben Sie Ihren Benutzernamen und Ihre Kennung in das Dialogfeld „Testauthentifizierung“ ein und klicken Sie dann auf **Test**.

Nach einer erfolgreichen Authentifizierung wird den Benutzern, die eine Authentifizierung bei den Mandanten-Portalen durchführen, ein Dialogfeld angezeigt, in dem sie aufgefordert werden, sich zuerst mit ihren RADIUS-Anmeldedaten und anschließend mit ihren Domänen-Anmeldedaten anzumelden.

5 Wenn die Anmeldedaten der Testauthentifizierung fehlerhaft sind, werden die Einstellungen nicht gespeichert. Korrigieren Sei Ihren Benutzernamen oder Ihre Kennung und versuchen Sie es erneut.

## Einrichten der Authentifizierung mit RSA SecurID

Mithilfe von RSA SecurID können Sie die Zwei-Faktor-Authentifizierung für Endbenutzer aktivieren.

### Vorgehensweise

1 Wählen Sie **Einstellungen > Zwei-Faktor-Authentifizierung**.

2 Konfigurieren Sie die Authentifizierung.

| Option | Beschreibung |
|---|---|
| **Zwei-Faktor-Authentifizierungsmethode** | Wählen Sie **RSA SecurID** |
| **Benutzernamen beibehalten** | Wählen Sie **Ja** aus, um den Benutzernamen während der Authentifizierung beizubehalten. Der Benutzer, der den Authentifizierungsversuch unternimmt, muss für RSA und die Domänenherausforderung über dieselben Anmeldedaten verfügen. Wenn Sie **Nein** auswählen, wird der Benutzername nicht gesperrt und der Benutzer hat die Möglichkeit, einen anderen Namen einzugeben. |

| Option | Beschreibung |
|---|---|
| **Nur externe Verbindungen** | Wenn der Wert „JA“ lautet, ist die Eingabe von RSA-Anmeldedaten für Benutzer innerhalb des Netzwerks nicht erforderlich. Die Unterscheidung zwischen interner und externer Verbindung trifft der Dienstanbieter. Wenn der Wert „NEIN“ lautet, sind alle Benutzer innerhalb und außerhalb des Netzwerks zur Eingabe von RSA-Anmeldedaten verpflichtet. |
| **Konfigurationsdatei hochladen** | Klicken Sie auf **Auswählen** und navigieren Sie zur Datei `sdconf.rec`. Klicken Sie auf **Öffnen**. |

3 Klicken Sie auf **Speichern**.

# Identitätsverwaltung

Auf der Seite „Identitätsverwaltung“ können Sie Identitätsanbieter hinzufügen, bearbeiten und konfigurieren.

Die Seite „Identitätsverwaltung“ zeigt die derzeit konfigurierten Identitätsanbieter und die folgenden Informationen zu den einzelnen Anbietern an:

- Status – Aktueller Status von Identity Manager. Zeigen Sie auf das Symbol, um den Status anzuzeigen.
- Identity Manager-URL – URL des Identity Managers.
- Zeitüberschreitung bei SSO-Token – Zeitüberschreitungswert in Minuten
- Datencenter – Name des Datenzentrums
- Mandantenadresse – Adresse der Mandanten-Appliance

So fügen Sie einen neuen Identity Manager hinzu:

1 Klicken Sie auf **Neu**.

2 Geben Sie die Informationen wie unten beschrieben ein.

| Feld | Beschreibung |
|---|---|
| VMware Identity Manager-URL | URL des Identity Managers. |
| SSO-Token für Zeitüberschreitung | Der Zeitüberschreitungswert in Minuten. |
| Datenzentrum | Name des Datenzentrums. Wählen Sie einen Eintrag in der Dropdown-Liste aus. |
| Mandantenadresse | Adresse der Mandanten-Appliance. |

3 Klicken Sie auf **Speichern**.

So bearbeiten Sie einen vorhandenen Identity Manager:

1 Wählen Sie den Identity Manager in der Liste aus.

2 Klicken Sie auf **Bearbeiten**.

3 Bearbeiten Sie die Informationen wie unten beschrieben.

| Feld | Beschreibung |
|---|---|
| SSO-Token für Zeitüberschreitung | Der Zeitüberschreitungswert in Minuten. |
| Mandantenadresse | Adresse der Mandanten-Appliance. |

4 Klicken Sie auf **Speichern**.

So entfernen Sie einen Identity Manager:

1 Wählen Sie den Identity Manager in der Liste aus.

2 Klicken Sie auf **Entfernen**.

3 Klicken Sie auf **Löschen**, um den Vorgang zu bestätigen.

So konfigurieren Sie die Identitätsverwaltung:

1 Klicken Sie auf **Konfigurieren**.

2 Bearbeiten Sie die Einstellungen wie unten beschrieben.

| Feld | Beschreibung |
|---|---|
| Verwendung von Identity Manager für Remotebenutzer erzwingen | Wählen Sie „JA“, um den Remotebenutzerzugriff nur über IDM zuzulassen. Die Option wird nur angezeigt, wenn der Identity Manager-Status grün ist. |
| Verwendung von Identity Manager für interne Benutzer erzwingen | Wählen Sie „JA“, um internen Benutzerzugriff nur über IDM zuzulassen. Die Option wird nur angezeigt, wenn der Identity Manager-Status grün ist. |

3 Klicken Sie auf **Speichern**.

# Desktop-Verbindungen

13

Dieser Abschnitt enthält Informationen zum Einrichten und Verwalten von Verbindungen für virtuelle Desktop-Maschinen.

Dieses Kapitel behandelt die folgenden Themen:



## Desktop-Protokolle

Es gibt eine Vielzahl von Verbindungsprotokollen für das Herstellen von Verbindungen mit virtuellen Desktop-Maschinen.

VMware Horizon Agent verfügt über einen sehr kleinen Speicherbedarf (90 KB) und unterstützt den vollen Horizon Client-Funktionsumfang: Blast Extreme, Blast mit HTML Access, PCoIP, RDP, HTTPS, SSL, SSO, USB-Umleitung, Druckerunterstützung und Sitzungsverwaltung.

Horizon Agent unterstützt zwei Desktop-Verbindungsarten: native Anwendung (Blast Extreme und PCoIP-Protokolle) und HTML-Zugriff (Blast mit HTML Access-Protokoll).

### Blast Extreme

Blast Extreme ist ein hochleistungsfähiges Anzeigeprotokoll. Das Protokoll enthält WAN-Optimierung und bietet Unterstützung für 3D-Grafiken. Dies führt im Vergleich zu RDP zu einer wesentlich besseren Endbenutzererfahrung.

So verwenden Sie das Blast Extreme-Protokoll

- Auf jedem virtuellen Desktop müssen die neuesten Versionen von Horizon Agent und des DaaS-Agenten installiert sein.
- VMware Horizon Client muss auf dem jeweiligen Endpunktgerät der Endbenutzer installiert sein.
- Blast Extreme ist das standardmäßige Protokoll für native Clients in den Pool-Einstellungen.

### Blast mit HTML Access

Blast mit HTML Access ermöglicht über jeden beliebigen HTML5-konformen Webbrowser den Zugriff auf einen Desktop.

So verwenden Sie Blast mit HTML Access:

- Auf jedem virtuellen Desktop müssen die neuesten Versionen von Horizon Agent und des DaaS-Agenten installiert sein.
- Für den internen Zugriff, der nicht über Access Point erfolgt, muss die SSL-Zertifikatsinstallationsautomatisierung konfiguriert sein. Siehe Automatisieren der Installation des SSL-Zertifikats für VMware Blast.
- Es sind zusätzliche Anforderungen für das Starten von Remoteanwendungen vorhanden, wie dies im Folgenden beschrieben wird.

**Systemanforderungen für das Verwenden von HTML Access (Blast)**

Browser auf Clientsystem:

- Chrome 41, 42 und 43
- Internet Explorer 10 und 11
- Safari 7 und 8 (Mobile Safari wird in dieser Version nicht unterstützt.)
- Firefox 36, 37 und 38

Clientbetriebssysteme:

- Windows 7 SP1 (32 oder 64 Bit)
- Windows 8.x-Desktop (32 oder 64 Bit)
- Windows 10-Desktop (32 oder 64 Bit)
- Mac OS X Mavericks (10.9)
- Mac OS X Yosemite (10.10)
- Chrome OS 28.x oder höher

**HTML Access-Unterstützung (Blast) für RDSH-Anwendungen**

Das Starten von RDSH-Anwendungen wird in HTML Access unterstützt.

Hinweis:

- Das Access Point 2.0-Remotezugriffsgateway muss bereitgestellt werden (erkundigen Sie sich bei Ihrem Dienstanbieter).
- Funktioniert nicht für iOS oder Android.

## Automatisieren der Installation des SSL-Zertifikats für VMware Blast

Der Vorgang in diesem Anhang erleichtert den internen Zugriff, der nicht über Access Point erfolgt. Falls keine Benutzer diese Zugriffsart benötigen, kann dieser Vorgang entfallen.

Hinweis:

- Dieser Vorgang muss für das Image ausgeführt werden, bevor Sie die VM in ein Image konvertieren oder das Image erneut veröffentlichen können.

- Dieser Vorgang muss bei jedem Öffnen und erneuten Veröffentlichen eines Images wiederholt werden.

Sie können das Zertifikat mit einem Post-Sysprep-Skript installieren, sodass keine sysprep-Probleme und Probleme mit Zertifikatsduplikaten auftreten. Außerdem können Sie auch Ihr eigenes standardmäßiges Verfahren ausführen (z. B. Active Directory-GPO und Skripts). Die SSL-Zertifikatsvoraussetzungen finden Sie in der Dokumentation zu den Horizon View-Funktionen.

Konfigurieren Sie die Post-Sysprep-Befehle/-Skripts mit den nachfolgenden Schritten in der Horizon DaaS-Umgebung.

- Importieren Sie das Zertifikat auf dem Testcomputer und notieren Sie den Fingerabdruck des Zertifikats.
- Erstellen Sie ein Post-Sysprep-Skript/eine Post-Sysprep-Batch-Datei auf der VM, auf der sich die Vorlage befindet, und kopieren Sie das Zertifikat.
- Konvertieren Sie die VM, auf der sich die Vorlage befindet, in ein Image oder veröffentlichen Sie das Image erneut.

### Importieren eines Zertifikats und Festhalten des Fingerabdrucks des Zertifikats

Im ersten Schritt für die Automatisierung der Installation des SSL-Zertifikats wird das Zertifikat importiert und der Fingerabdruck festgehalten.

#### Vorgehensweise

1 Binden Sie das Zertifikat-Snap-In mit den nachfolgenden Schritten in MMC ein.

Sie können erst dann Zertifikate in den Windows-Zertifikatspeicher aufnehmen, wenn Sie das Zertifikat-Snap-In in die Microsoft Management Console (MMC) eingebunden haben. Prüfen Sie zunächst, ob die MMC und das Zertifikat-Snap-In auf dem Windows-Gastbetriebssystem vorhanden sind.

a Klicken Sie auf dem Desktop auf **Start** und geben Sie „mmc.exe“ ein.

b Wählen Sie im MMC-Fenster den Befehl **Datei > Snap-In hinzufügen/entfernen**.

c Wählen Sie im Fenster „Snap-In hinzufügen/entfernen“ den Befehl **Zertifikate** und klicken Sie auf **Hinzufügen**.

d Wählen Sie im Fenster „Zertifikat-Snap-In“ den Befehl „Computerkonto“, klicken Sie auf **Weiter**, wählen Sie „Lokaler Computer“ und klicken Sie auf **Fertigstellen**.

e Klicken Sie im Fenster „Snap-In hinzufügen/entfernen“ auf **OK**.

2 Importieren Sie ein Zertifikat für den HTML Access-Agenten mit den nachfolgenden Schritten in den Windows-Zertifikatspeicher.

Soll ein standardmäßiges HTML Access-Agent-Zertifikat durch ein von einer Zertifizierungsstelle signiertes Zertifikat ersetzt werden, importieren Sie das Zertifikat der Zertifizierungsstelle in den Windows-Zertifikatspeicher auf dem lokalen Computer. Prüfen Sie zunächst, ob der HTML Access-Agent installiert ist, ob das von der Zertifizierungsstelle signierte Zertifikat auf den Desktop kopiert wurde und ob das Zertifikat-Snap-In in MMC eingebunden wurde (siehe Schritt 1 oben).

a Erweitern Sie im MMC-Fenster den Knoten „Zertifikate (Lokaler Computer)“ und wählen Sie den persönlichen Ordner aus.

b Wählen Sie im Bereich „Aktionen“ den Befehl **Weitere Aktionen > Alle Aufgaben > Importieren**.

c Klicken Sie im Zertifikatimport-Assistenten auf **Weiter** und navigieren Sie zum Speicherort des Zertifikats.

d Wählen Sie die Zertifikatsdatei aus und klicken Sie auf **Öffnen**.

Zum Ermitteln des Typs der Zertifikatsdatei wählen Sie das Dateiformat der Datei im Dropdown-Menü „Dateiname“.

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

f Aktivieren Sie die Option **Schlüssel als exportierbar markieren**.

g Aktivieren Sie die Option **Alle erweiterten Eigenschaften mit einbeziehen**.

h Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

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

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

1. Doppelklicken Sie im Ordner „Zertifikate (Lokaler Computer) > Persönlich > Zertifikate“ auf das neue Zertifikat.

2. Prüfen Sie, ob die folgende Meldung im Dialogfeld „Zertifikatinformationen“ auf der Registerkarte „Allgemein“ angezeigt wird: „Sie besitzen einen privaten Schlüssel für dieses Zertifikat.“

3 Importieren Sie Stamm- und Zwischenzertifikate für den HTML Access-Agent.

Falls das Stammzertifikat und die Zwischenzertifikate in der Zertifikatskette nicht zusammen mit dem SSL-Zertifikat importiert wurden, das Sie für den HTML Access-Agenten importiert haben, importieren Sie diese Zertifikate in den Windows-Zertifikatspeicher auf dem lokalen Computer.

a Erweitern Sie in der MMC-Konsole den Knoten „Zertifikate (Lokaler Computer)“ und navigieren Sie zum Ordner „Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate“.

- Wenn sich Ihr Stammzertifikat in diesem Ordner befindet und Ihre Zertifikatkette keine Zwischenzertifikate enthält, überspringen Sie diesen Vorgang.
- Falls sich Ihr Stammzertifikat nicht in diesem Ordner befindet, fahren Sie mit Schritt b fort.

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

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

d Wählen Sie die Datei mit dem Stammzertifizierungsstellen-Zertifikat aus und klicken Sie auf **Öffnen**.

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

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

1. Navigieren Sie zum Ordner „Zertifikate (Lokaler Computer) > Zwischenzertifizierungsstellen > Zertifikate“.

2. Wiederholen Sie die Schritte c bis f für jedes zu importierende Zwischenzertifikat.

4 Navigieren Sie im MMC-Fenster mit den Zertifikaten zum Ordner „Zertifikate (Lokaler Computer) > Persönlich > Zertifikate“.

5 Doppelklicken Sie auf das von der Zertifizierungsstelle signierte Zertifikat, das Sie in den Windows-Zertifikatspeicher importiert haben.

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

7 Kopieren Sie den ausgewählten Fingerabdruck in eine Textdatei.

Beispiel:

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

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

### Erstellen eines Post-Sysprep-Skripts/einer Post-Sysprep-Batch-Datei und Kopieren des Zertifikats

Im zweiten Schritt für die Automatisierung der Installation des SSL-Zertifikats wird ein Post-Sysprep-Skript/eine Post-Sysprep-Batch-Datei erstellt und das Zertifikat wird kopiert.

Importieren Sie das SSL-Zertifikat mit dem Post-Build-Konfigurationsskript „SetupComplete.cmd“ und konfigurieren Sie die VMware HTML Access-Registrierung (Windows 7 und höher).

http://technet.microsoft.com/de-de/library/dd744268%28v=ws.10%29.aspx

Beispiel:

- Kopieren Sie die SSL-Zertifikatsdatei auf das Laufwerk C:. In diesem Beispiel ist das die Datei "C:\desktone_ca_cert".
- Erstellen Sie die Datei „SetupComplete.cmd“ im Ordner „%WINDIR%\Setup\Scripts\“. Legen Sie den Ordner „Scripts“ an, sofern er nicht bereits vorhanden ist.
- Tragen Sie die nachfolgenden Befehle in die Datei „SetupComplete.cmd“ ein. Der Fingerabdruckwert entspricht dem oben kopierten Wert.
- Falls die Zertifikatskette ein Stammzertifikat und Zwischenzertifikate enthält, müssen Sie die entsprechenden CertUtil-Befehle in die Batch-Datei eintragen.

```
CertUtil  –importPFX –f  –p "<password>" "C:\desktone_ca_cert.pfx"
        reg add "HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config" /f /v "SslHash" /t REG_SZ /d "31
2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e"
del /F /Q "C:\desktone_ca_cert.pfx"
del /F /Q "%systemroot%\setup\scripts\SetupComplete.cmd"
```

- Speichern Sie die Datei „SetupComplete.cmd“. Sie können die Datei „SetupComplete.cmd“ auf dem Testcomputer testen.

### Konvertieren der VM, auf der sich die Vorlage befindet, in ein Image oder Neuveröffentlichen des Images

Im dritten Schritt für die Automatisierung der Installation des SSL-Zertifikats wird die VM, auf der sich die Vorlage befindet, in ein Image konvertiert oder das Image wird neu veröffentlicht.

#### Vorgehensweise

1. Konvertieren Sie die VM, auf der sich die Vorlage befindet, in ein Image oder veröffentlichen Sie das Image erneut und erstellen Sie eine Zuweisung.
2. Prüfen Sie die HTML Access-Verbindung für das Zertifikat oder prüfen Sie die Zertifikate und die HTML Access-Registrierung auf den Desktops.

**Hinweis** Wenn der HTML Access (Blast)-Dienst selbst dann ein selbstsigniertes Zertifikat erzeugt, wenn Sie das gültige CA-Zertifikat gemäß den obigen Anweisungen festgelegt haben, prüfen Sie zur Fehlerbehebung das Protokoll „%ProgramData%\VMWare\Vmware Blast\Blast-worker.txt“.

### PCoIP

PCoIP ist ein altes, hochleistungsfähiges Anzeigeprotokoll.

Das PCoIP-Protokoll enthält WAN-Optimierung und bietet Unterstützung für 3D-Grafiken. Dies führt im Vergleich zu RDP zu einer wesentlich besseren Endbenutzererfahrung.

So verwenden Sie das PCoIP-Protokoll

- Auf jedem virtuellen Desktop müssen die neuesten Versionen von Horizon Agent und des DaaS-Agenten installiert sein.
- VMware Horizon Client muss auf dem jeweiligen Endpunktgerät der Endbenutzer installiert sein.

## Verwenden von VMware Horizon Client

In diesem Abschnitt werden einige grundlegende Horizon Client-Funktionen und die für die DaaS-Integration spezifischen Umgebungsmerkmale beschrieben. Vollständige Informationen zum Verwenden von Horizon Client finden Sie in der Horizon Client-Dokumentation auf VMware.com.

### Horizon Client-Downloadlink im Desktop-Portal

Horizon Client kann bei Bedarf über das Desktop-Portal heruntergeladen werden.

Wenn ein Benutzer das DaaS-Benutzerportal startet und dann versucht, mithilfe des Blast Extreme- oder PCoIP-Protokolls eine Verbindung zu einem Desktop herzustellen, wird Horizon Client gestartet und der Benutzer wird nahtlos angemeldet. Beim ersten Start einer PCoIP-Verbindung über das Desktop-Portal durch einen Benutzer wird ein Dialogfeld angezeigt, das einen Link zum Herunterladen von Horizon Client enthält.

Wenn Sie das DaaS-Benutzerportal starten und dann versuchen, mithilfe des HTML Access-Protokolls (Blast) eine Verbindung zu einem Desktop herzustellen, werden Sie darüber informiert, dass Sie Horizon Client durch Klicken auf den Link im Informationsdialogfeld herunterladen müssen. Aktivieren Sie zunächst Pop-ups in Ihrem Browser und initiieren Sie dann eine HTML Access-Verbindung.

### Zugreifen auf Desktops und Anwendungen

Beachten Sie beim Starten von Desktops und Remote-Anwendungen Folgendes.

- Wenn Sie sich bei einer Horizon Client-Instanz anmelden und über eine aktive Anwendungssitzung verfügen, werden Sie möglicherweise in Abhängigkeit der Horizon Client-Einstellungen aufgefordert, sich erneut zu verbinden. Horizon Client fordert Sie nur einmal auf, eine erneute Verbindung zu einer Anwendungssitzung herzustellen. Sie werden nicht erneut aufgefordert, bis Sie sich abmelden und erneut anmelden. Wenn das Herstellen der Verbindung der Sitzung fehlerhaft ist, sollten Benutzer versuchen, die Anwendungen normal zu starten.
- Es ist nicht möglich, gleichzeitig über eine aktive RDS-Desktop- und eine aktive Remoteanwendungssitzung zu verfügen.

- Zeitüberschreitungen des Leerlaufs basieren auf der Aktivität des Endpunktgeräts und nicht auf dem Desktop oder der Anwendung.
- RDP ist kein kompatibles Protokoll, wenn Sie auf einem anderen Gerät über PCoIP angemeldet sind. Bevor Sie versuchen, eine Verbindung per RDP herzustellen, müssen Sie sich von der PCoIP-Sitzung abmelden.
- Horizon Client zeigt RDS-Desktops und Remoteanwendungen als startbare Elemente an. Wenn keine Option für das Herstellen der Verbindung zu Ihrem RDS-Pool als ein Desktop angezeigt wird, müssen Sie sicherstellen, dass der RDSH-Dienst für den vollständigen Desktop-Zugriff aktiviert ist und dass Sie über Horizon Client 3.0 oder höher verfügen.
- Der angezeigte Name der Remoteanwendung ist der im Pool zugewiesene Name. Es ist daher wichtig, sinnvolle Namen zu vergeben, um zwischen Anwendungen unterscheiden zu können, wenn ihnen mehrere Pools zugewiesen sind.
- Mit der Funktion „Anwendung zurücksetzen“ werden Sie von allen Anwendungssitzungen abgemeldet, und zwar unabhängig vom Sitzungshost, den Sie verwenden.
- Die USB-Umleitung wird für RDS-basierte Server nicht unterstützt.
- Das Starten von RDSH-Anwendungen wird in HTML Access unterstützt. Siehe Blast mit HTML Access.

## Zugreifen auf lokale Dateien mit Remoteanwendungen und mithilfe der Dateiumleitung

Mit der Funktion der Dateiumleitung können Benutzer lokale Dateien in berechtigten Remoteanwendungen öffnen, die einen bestimmten Dateityp unterstützen.

Diese Funktion wird in Horizon Client mit der Option „Lokale Dateien in gehosteten Anwendungen öffnen“ aktiviert.

Mit dieser Funktionalität können Benutzer Folgendes durchführen:

- Öffnen einer lokalen Datei in einer Remoteanwendung durch Doppelklicken auf die Datei im Clientcomputer oder durch Klicken mit der rechten Maustaste und Auswählen von der Option „Öffnen mit“ und der Remoteanwendung im Menü.
- Navigieren in der Remoteanwendung zu dem Ordner, in dem sich die Datei befindet.
- Speichern der mithilfe der Remoteanwendung vorgenommenen Änderungen auf der lokalen Clientfestplatte.
- Registrieren einer berechtigten Anwendung als Dateihandler für die Dateitypen, die von dieser Anwendung geöffnet werden können, oder festlegen, dass die Datei jedes Mal mit der Remoteanwendung geöffnet wird.

  Wenn eine Anwendung als Standardhandler festgelegt wurde, gilt Folgendes:

  - Das Vorschausymbol der Datei wird als Symbol der berechtigten Anwendung auf der Startseite der Anwendung angezeigt.

- Die Beschreibung des Dateityps wird von der Remoteanwendung überschrieben, wenn vorhanden.
- Durch Doppelklicken auf eine Datei dieses Typs wird View Client gestartet.

## Zeitüberschreitung der Sitzung

Die Sitzung beginnt mit der Authentifizierung des Benutzers. Diese Zeitüberschreitung kann in der Verwaltungskonsole geändert werden.

- Taktintervall für Benutzeraktivität

  Dieser Wert steuert das Taktintervall von Horizon Client. In diesem Takt wird dem Mieter die Dauer der Inaktivität gemeldet. Mit Dauer der Inaktivität ist der Zeitraum gemeint, in der keine Interaktion mit dem Endpunktgerät stattfindet (nicht gleichzusetzen mit einer Inaktivität während der Desktop-Sitzung). Bei großen Desktop-Bereitstellungen kann der Netzwerkdatenverkehr durch einen langsameren Aktivitätstakt reduziert und die Leistung verbessert werden.

- Zeitüberschreitung des Benutzerleerlaufs

  Dieser Wert legt die maximale Zeit fest, die ein Benutzer inaktiv sein kann, ohne dass seine Verbindung zum Mandanten getrennt wird. Nach dem Ende dieses Zeitraums wird der Benutzer von allen aktiven Horizon Client-Desktop-Sitzungen getrennt. Bei seiner Rückkehr zu Horizon Client muss sich der Benutzer wieder authentifizieren.

  **Hinweis** Zur Vermeidung unerwarteter Desktop-Trennungen sollte die Zeitüberschreitung für die Benutzerinaktivität auf jeden Fall größer als das Taktintervall für die Benutzeraktivität sein (am besten mindestens doppelt so groß).

- Zeitüberschreitung für Broker-Sitzung

  Dieser Wert legt die maximale Zeit fest, die Horizon Client mit dem Mandanten verbunden sein kann, bevor seine Authentifizierung abläuft (das Herunterzählen bis zur Zeitüberschreitung beginnt bei jeder Authentifizierung von Neuem). Bei Eintreten einer solchen Zeitüberschreitung werden Sie nicht automatisch vom Desktop getrennt, Sie können also weiterarbeiten. Führen Sie danach jedoch eine Aktion aus, die eine Kommunikation mit dem Broker erfordert (z. B. eine Einstellungsänderung), so müssen Sie sich erneut authentifizieren und wieder beim Desktop anmelden.

  **Hinweis** Die Zeitüberschreitung für die Broker-Sitzung sollte auf jeden Fall größer als die Zeitüberschreitung für die Benutzerinaktivität sein (am besten mindestens die Summe aus dem Taktintervall für die Benutzeraktivität und der Zeitüberschreitung für die Benutzerinaktivität).

**Hinweis** Bei auf Android OS ausgeführten Horizon Client-Instanzen ist bekannt, dass sie diese Richtlinieneinstellung außer Kraft setzen, was eine Sitzungszeitüberschreitung von ca. 10 Minuten bedeutet.

## Zurücksetzen des Benutzerkennworts

Beim Anmelden bei Horizon Client wird der Benutzer möglicherweise aufgefordert, sein Kennwort zu ändern.

- Nach dem Eingeben des neuen Kennworts zeigt Horizon Client eine Meldung über die erfolgreiche Kennwortzurücksetzung an. Das Kennwort wird jedoch tatsächlich nicht aktualisiert, bis die Verbindung zu Horizon Agent erfolgt ist. Wenn bei der Sitzung eine Zeitüberschreitung auftritt, bevor die Verbindung erfolgt, oder wenn der Benutzer nie eine Desktop-Sitzung startet, wird das Kennwort nicht aktualisiert.
- Wenn das neue Kennwort nicht Ad-konform ist, ist die Anmeldung fehlerhaft. Der Benutzer muss dann Horizon Client beenden und versuchen, das Kennwort erneut zurückzusetzen. Die folgenden Zeichenkombinationen sind in Horizon Client-Kennwörtern unzulässig:

  <

  >

  <!—

  &

## Desktop-Optionen

Nach dem Anmelden bei einem Desktop können Benutzer auf „Optionen“ klicken, um das Menü „Optionen“ zu öffnen.

In der folgenden Tabelle werden die im Menü „Optionen“ verfügbaren Funktionen beschrieben.

| | |
|---|---|
| Wechseln zwischen Desktops | Ermöglicht dem Benutzer, auf den Desktop-Auswahlbildschirm zuzugreifen oder zwischen geöffneten Desktop-Sitzungen umzuschalten. Steuerungen und Informationen finden Sie im Abschnitt über den Desktop-Auswahlbildschirm. Dies funktioniert nicht, wenn bei Ihrer Sitzung eine Zeitüberschreitung aufgetreten ist. |
| Verbindung mit diesem Desktop automatisch herstellen | Bei PC und Thin Clients wird dadurch der angegebene Desktop zum standardmäßigen Desktop des Benutzers, wenn der Desktop Bestandteil eines dynamischen Pools ist. Beim nächsten Anmelden wird der Desktop sofort angezeigt, sofern Folgendes erfüllt ist:<br>■ Dem Benutzer ist nur ein Desktop zugeordnet.<br>■ Es gibt kein Problem mit den Anmeldeinformationen oder dem Desktop-Status.<br>Wenn ein Benutzer „Automatische Verbindung“ auswählt und sich dann mit mehreren Desktops anmeldet, wird die Einstellung „Verbindung mit diesem Desktop automatisch herstellen“ auf „aus/falsch“ festgelegt. Wenn bei der Sitzung eine Zeitüberschreitung auftritt, wird die Einstellung „Automatische Verbindung“ nicht gespeichert und der Benutzer kann bei der nächste Anmeldung keine automatische Verbindung herstellen. |

| | |
|---|---|
| Desktop zurücksetzen | Löst einen Desktop-Neustart aus. Dies funktioniert nicht, wenn bei der Sitzung eine Zeitüberschreitung aufgetreten ist. |
| Trennen | Trennt den aktuellen Benutzer von seiner aktiven Sitzung. |
| Trennen und abmelden | Trennt den Benutzer von seiner aktiven Sitzung und meldet ihn ab. |

## Auslösen einer Desktop-Abmeldung

Das Abmelden initiiert einen Aufruf beim DaaS-Agent, der bis zu 30 Sekunden andauern kann.

Wenn ein Benutzer versucht, sich wieder anzumelden, bevor die 30 Sekunden vergangen sind, wird demnach das Abmeldedialogfeld möglicherweise weiterhin angezeigt.

## VRAM-Einstellungen während der Zuweisungsbereitstellung

Zum Vermeiden eines schwarzen Bildschirms stellt die Plattform Zuweisungen dieser Desktops mit einer auf 128 festgelegten Video-RAM-Größe (VRAM) bereit. Diese Einstellung kann durch Ihren Dienstanbieter geändert werden.

# Fehlerbehebung

14

In diesem Abschnitt werden die häufigsten Probleme beschrieben, für die möglicherweise eine Fehlerbehebung erforderlich ist.

Informationen zu anderen Problemen, die möglicherweise bei der Verwendung der VMware-Software auftreten, finden Sie in der VMware-Knowledgebase.

Dieses Kapitel behandelt die folgenden Themen:



## Fehlerbehebung bei Horizon Client-Verbindungen

Es gibt verschiedene Konfigurations-/Einrichtungsprobleme, die dazu führen können, dass Horizon Client nicht richtig verwendet werden kann.

| Problem | Lösung |
|---|---|
| Anmeldungsprobleme | Wenn Sie sich nicht bei Horizon Client anmelden können, sollten Sie prüfen, ob die Version der von Ihnen verwendeten VMware Horizon Client-Instanz mit VMware View 5.1 oder höher kompatibel ist. |
| Desktop wird nicht gestartet. | Wenn der Desktop nicht gestartet wird, müssen Sie sicherstellen, dass keine andere Software in der Umgebung Port 443 verwendet. |
| Verbindung zum Desktop kann nicht hergestellt werden. | Wenn die Fehlermeldung „Verbindung zum Desktop kann nicht hergestellt werden“ angezeigt wird, wird View Agent demnach nicht ausgeführt. Überprüfen Sie in den Programmen der Windows-Systemsteuerung, ob Horizon Agent und View Agent Direct Connect in der Liste der installierten Programme angezeigt werden. Ist dies nicht der Fall, wurde die Installation nicht ordnungsgemäß abgeschlossen und Sie müssen eine Neuinstallation vornehmen. Wenn die View Agent-Software installiert ist, müssen Sie sicherstellen, dass der View Agent-Dienst ausgeführt wird. |

| Problem | Lösung |
|---|---|
| Desktop trennt die Verbindung. | Wenn eine Horizon Client-Sitzung im Leerlauf zu schnell beendet wird, sind demnach die Einstellungen für die Zeitüberschreitung der Sitzung von Horizon Client so konfiguriert, dass der Leerlauf nur für einen sehr kurzen Zeitraum zulässig ist. Sie können die Einstellungen für die Zeitüberschreitung der Sitzung von Horizon Client in der Verwaltungskonsole konfigurieren. |
| Schwarzer Bildschirm | Siehe Schwarzer Bildschirm. |

# Fehlerbehebung bei HTML Access-Verbindungen (Blast)

Es gibt verschiedene Konfigurations-/Einrichtungsprobleme, die dazu führen können, dass eine HTML Access-Verbindung (Blast) nicht richtig gestartet wird.

| Problem | Lösung |
|---|---|
| Browser ist nicht HTML5-konform. | Prüfen Sie, ob die Browserversion mit der in den Anforderungen übereinstimmt. |
| Pop-up-Blocker ist aktiviert. | Der Pop-up-Blocker des Browsers könnte verhindern, dass das neue Fenster für eine HTML Access-Verbindung geöffnet wird. Stellen Sie sicher, dass der Benutzer den Pop-up-Blocker für das Desktop-Portal deaktiviert. |
| Windows-Firewall ist deaktiviert. | Stellen Sie sicher, dass die Windows-Firewall installiert und auf dem Desktop des Benutzers ausgeführt wird. Bei einer deaktivierten Windows-Firewall werden in den HTML Access-Protokollen Fehler gemeldet. |

# Schwarzer Bildschirm

Benutzern wird aus verschiedenen Gründen ein schwarzer Bildschirm angezeigt.

- Beim Aktualisieren von VMware Tools kann es bei der Aktualisierung in einigen Fällen dazu kommen, dass der falsche Videotreiber installiert wird, was zu einem schwarzen Bildschirm führt. Die Problemumgehung besteht darin, sich mithilfe von RDP bei der Sitzung anzumelden und den richtigen Treiber zu installieren.
- Wenn der Systemadministrator einen Desktop aus einem PCoIP-fremden in einen PCoIP-Pool verschiebt und Benutzern ein schwarzer Bildschirm angezeigt wird, wenn sie versuchen, eine Verbindung zum Desktop herzustellen, finden sich hierzu Lösungen in der VMware-Knowledgebase.
  - Lesen Sie beim Anmelden beim virtuellen Desktop für VMware View mithilfe von PCoIP die im Artikel „Schwarzer Bildschirm“ in der VMware-Knowledgebase beschriebenen Schritte.
  - Überprüfen Sie, ob die Video-RAM-Einstellungen (VRAM) in der .vmx-Datei (Einstellungen für die virtuelle Maschine) für den Zugriff über mehrere Monitore beim Verwenden des PCoIP-Protokolls richtig konfiguriert sind. Lesen Sie den VMware-Knowledgebase-Artikel „Determining display and screen resolution settings for PCoIP“ (Ermitteln von Anzeige- und Bildschirmauflösungseinstellungen für PCoIP).

- Überprüfen Sie, ob der Videotreiber für VMware View Agent und das Betriebssystem richtig ist. Lesen Sie den VMware-Knowledgebase-Artikel „The PCoIP server log reports the error: Error attaching to SVGADevTap, error 4000: EscapeFailed“ (Im PCoIP-Serverprotokoll wird der Fehler gemeldet: Fehler beim Anhängen an SVGADevTap, Fehler 4000: EscapeFailed).

# Überschreiben von ADM PCoIP-Standardeinstellungen

ADM kann auf dem Domänencontroller oder auf dem zum Erstellen eines Golden Image verwendeten Master-Desktop-Image konfiguriert werden.

Der Systemadministrator kann die ADM-Standardeinstellungen im Master-Desktop-Image überschreiben; der Administrator führt hierzu „running gpedit.msc“ auf dem Desktop aus und navigiert zum Ordner **Administrative Vorlagen > Klassische adminstrative Vorlagen (ADM) > PCoIP**.

# Fehlermeldungen

In diesem Abschnitt werden Fehlermeldungen beschrieben, auf die Benutzer bei hergestellten Desktop-Verbindungen treffen können.

- Fehler 500

  Wenn einem Benutzer der Fehler 500 in Horizon Client angezeigt wird, sollten Sie sich im Mandantenprotokoll die Ausnahme ansehen, bevor Sie sich an den Support wenden. In der Ausnahme, nach der gesucht werden soll, wird das ViewClientServlet erwähnt.

- Häufige Fehlermeldungen

  In der folgenden Tabelle werden die häufigsten Fehlermeldungen, die Benutzern angezeigt werden können, sowie ihre Ursachen aufgeführt, wenn Horizon Client zum Herstellen der Verbindung zum jeweiligen Desktop verwendet wird. Der Teil „Fehlerdetails“ der Meldung enthält Informationen, die der Kunde benötigt, um das Verbindungsproblem zu beheben.

| | |
|---|---|
| Fehler bei der View Agent-Anmeldung Fehlerdetails: <Meldung vom Agenten> | Fehler beim Senden der View Agent-Anmeldeanforderung |
| Sitzung ist abgelaufen, Horizon Client zum Verbinden neu starten | Es ist eine Desktop-Portal-Sitzungszeitüberschreitung aufgetreten. Die Desktop-Portal-Zeitüberschreitung basiert auf einer beim Dienstanbieter festgelegten Richtlinie (userportal.session.timeout), die durch eine Einstellung in der Verwaltungskonsole außer Kraft gesetzt werden kann. |
| Desktop kann nicht zugeteilt werden – es wird eine Poolaktualisierung durchgeführt. | Warten Sie ein paar Minuten und versuchen Sie es erneut. Es wird eine dynamische Poolaktualisierung durchgeführt. Desktops werden demnach vernichtet und anhand eines neuen oder geänderten Golden Images neu erstellt. Nach Abschluss der Aktualisierung können sich Benutzer an ihrem Desktop anmelden. |

| | |
|---|---|
| Fehler beim Kommunizieren mit dem Desktop Wenden Sie sich an Ihren Administrator. Fehlerdetails: Desktop Agent-Kommunikationsfehler | Fehler beim Analysieren der Authentifizierungsfehlerantwort aufgrund einer unterbrochenen Kommunikation zwischen Horizont Client, Mandant und View Agent Connect In der mit ViewClientServlet verknüpften Datei „desktone.log“ ist möglicherweise eine Warnung oder ein Fehler vorhanden. |
| XML kann nicht analysiert werden. | Data Horizon Client oder Agent gibt eine XML-Datei zurück, die durch die DaaS-Plattform nicht gelesen werden kann. |
| Desktop ist für das Herstellen von Verbindungen nicht bereit (DaaS Agent wird möglicherweise gestartet). Warten Sie ein paar Minuten oder versuchen Sie es erneut. Wenden Sie sich an Ihren Administrator, wenn das Problem weiterhin besteht. | DaaS Agent wird als offline gemeldet. Starten Sie den Desktop neu, wenn das Problem weiterhin besteht und der Konsolenzugriff zu lange dauert. DaaS Agent sollte beim Anzeigen des Desktops angezeigt werden (binnen wenigen Minuten). |
| Desktop ist für das Herstellen von Verbindungen nicht bereit (wird möglicherweise heruntergefahren oder neu gestartet). Warten Sie ein paar Minuten oder versuchen Sie es erneut. Wenden Sie sich an Ihren Administrator, wenn das Problem weiterhin besteht. | Betriebssystemstatus wird nicht ausgeführt. Warten Sie, bis er ausgeführt wird, oder nehmen Sie über das Desktop-Portal oder die Verwaltungskonsole einen Neustart vor. |
| Desktop ist für das Herstellen von Verbindungen nicht bereit (zurzeit im Wartungsmodus). Warten Sie ein paar Minuten oder versuchen Sie es erneut. Wenden Sie sich an Ihren Administrator, wenn das Problem weiterhin besteht. | Wartung für erneuten Beitritt zur Domäne erfolgt für einen dynamischen Desktop. Dies kann auch während der dynamischen Poolaktualisierung auftreten. |
| Verbindung zum Desktop kann nicht hergestellt werden. Wenden Sie sich an Ihren Administrator. Fehlerdetails: View Agent wird nicht ausgeführt. | DaaS Agent hat gemeldet, dass der View Agent-Dienst auf den erforderlichen Ports weder ausgeführt wird noch diese abhört. Stellen Sie sicher, dass View Agent installiert ist und dass die Firewall-Ports geöffnet sind (4172, 32111, 443). Starten Sie die Maschine neu oder prüfen Sie den Dienst „View Agent Connect“ nach Möglichkeit über RDP (Benutzerportal). |
| Verbindung zum Desktop kann nicht hergestellt werden. Wenden Sie sich an Ihren Administrator. Fehlerdetails: VMware Tools wird nicht ausgeführt. | VMware Tools ist offline. Siehe die Fehlerbehebung/Lösung zu VMware Tools. |
| Verbindung zum Desktop kann nicht hergestellt werden. Wenden Sie sich an Ihren Administrator. Fehlerdetails: VMware Tools ist nicht installiert. | VMware Tools sind nicht installiert. Siehe die Fehlerbehebung/Lösung zu VMware Tools. |
| Verbindung zum Desktop kann nicht hergestellt werden. Warten Sie ein paar Minuten und versuchen Sie es erneut. Wenden Sie sich an Ihren Administrator, wenn das Problem weiterhin besteht. | Desktop ist nicht verfügbar. Dies ist eine generische Meldung vom Zuteilungsdienst. Versuchen Sie, den Status der Maschine und des Mandantensystems zu prüfen, um zu sehen, ob andere Probleme vorliegen. |
| Verbindung zum Desktop kann nicht hergestellt werden. Desktop wurde einem anderen Benutzer zugeteilt. Wenden Sie sich an Ihren Administrator. Fehlerdetails: Desktop ist bereits in einem zugeteilten Zustand. | Ein anderer Benutzer wurde diesem Desktop zugeteilt. Es ist eine Sitzung mit einer GUID vorhanden, die sich von der des aktuellen Benutzers unterscheidet. |
| Anmeldefehler. Wenden Sie sich an Ihren Administrator. Fehlerdetails: Suche nach Benutzer-GUID mithilfe der Anmeldeinformationen nicht möglich | Während einer GUID-Suche wurde durch die Horizon DaaS-Software eine Ausnahme erhoben. Mögliche Ursachen: Domänencontroller ist offline, der Fabric-Knoten ist fehlerhaft, allgemeine Mandantenprobleme. |
| Verbindung zum Desktop kann nicht hergestellt werden. Warten Sie ein paar Minuten und versuchen Sie es erneut. Wenden Sie sich an Ihren Administrator, wenn das Problem weiterhin besteht. Fehlerdetails: Unbekannte IP-Adresse | Die IP-Adresse ist null oder ungültig. Die IP-Adresse kann null sein, wenn sich DaaS Agent in der Anmeldung befindet oder die VM gestartet wird. |

| | |
|---|---|
| Verbindung zum Desktop kann nicht hergestellt werden. Wenden Sie sich an Ihren Administrator. Fehlerdetails: Ungültige IP-Adresse <IP_address> | Die IP-Adresse wird nur aufgeführt, wenn sie bekannt ist. |
| Verbindung zum Desktop kann nicht hergestellt werden. Wenden Sie sich an Ihren Administrator. Fehlerdetails: Abrufen der Mandantendomäneninformationen nicht möglich | Es sind keine Domäneninformationen in der Datenbank protokolliert. Die DaaS-Plattform kann den Mandanten mit keiner Domäne verknüpfen. |
| Anmeldefehler: Unbekannter Benutzername oder fehlerhaftes Kennwort Bitte versuchen Sie es erneut. | Benutzername oder Kennwort ist für die angegebene Domäne ungültig. |
| Desktop kann nicht zugeteilt werden, keine Desktops verfügbar. Alle Desktops im Pool werden derzeit verwendet. | Dynamischer Pool verfügt nicht über Desktops, die für den Benutzer zur Verfügung stehen. |
| Verbindung zum Desktop kann nicht hergestellt werden (aktuell verbundenes Protokoll inkompatibel). Melden Sie die vorherige Sitzung ab und versuchen Sie es erneut. | Der Zuteilungsdienst gibt an, dass die aktuelle Sitzung ein nicht kompatibles Protokoll verwendet. |
| Abmeldung nicht möglich. Wenden Sie sich an Ihren Administrator, wenn das Problem weiterhin besteht. Fehlerdetails: Ungültige Sitzungs-ID | Dieser Fehler tritt auf, wenn die DaaS-Plattform die XML nicht analysieren kann, der in der XML zurückgegebene session-id-Schlüssel null ist oder der Schlüssel eine falsche Formatierung aufweist. |
| Abmeldung nicht möglich. Wenden Sie sich an Ihren Administrator, wenn das Problem weiterhin besteht. Fehlerdetails: Verknüpfen der Sitzungs-ID mit aktiven Sitzungen nicht möglich | Es sind keine aktiven Sitzungen für den aktuellen Benutzer vorhanden. |
| Abmeldung nicht möglich. Wenden Sie sich an Ihren Administrator, wenn das Problem weiterhin besteht. Fehlerdetails: Fehler beim Kommunizieren mit Desktop-Manager | Dieser Fehler tritt auf, wenn die DaaS-Plattform eine Ausnahme ausgibt. |
| Der Desktop <x>,<n> ist in der Liste der berechtigten Desktops nicht vorhanden. | In dieser Meldung entspricht <x> dem Namen der Anwendung, die Sie versuchen zu starten, und <n> ist eine Zahl.<br>Diese Meldung gibt an, dass Sie möglicherweise eine inkompatible Horizon Client-Instanz verwenden und die Versionshinweise des Clients lesen sollten, um sicherzustellen, dass er die Remoteanwendungsfunktion unterstützt. |

- Mit Kennwortänderungen in Verbindung stehende Fehlermeldungen

  In der folgenden Tabelle werden die Fehlermeldungen, die einem Benutzer angezeigt werden können, sowie die Ursachen aufgeführt, wenn sie versuchen, ihr Kennwort in Horizon Client zu ändern.

| | |
|---|---|
| Geben Sie das alte und das neue Kennwort ein. | Einige oder alle Kennwortfelder sind leer. |
| Das angegebene alte Kennwort ist ungültig. Versuchen Sie es erneut. | Wenn sich das Kennwort, mit dem Sie sich angemeldet haben, vom „alten Kennwort“ unterscheidet |
| Angegebene neue Kennwörter stimmen nicht überein. Versuchen Sie es erneut. | Der Benutzer hat das Kennwort falsch eingegeben. |

| | |
|---|---|
| Geben Sie ein neues Kennwort ein, das sich vom alten Kennwort unterscheidet. | Das vom Benutzer eingegebene neue Kennwort entspricht seinem alten Kennwort. |
| Kennwort kann nicht geändert werden. Starten Sie Horizon Client neu und versuchen Sie es erneut. Fehlerdetails <Meldung von View Agent> | Nach der Auswahl des Desktops durch den Benutzer, dem Abschließen des Kennwortänderungsbildschirms und dem Klicken auf die Verbindung konnte View Agent das Domänenkennwort nicht ändern.<br>**Hinweis** In einem Benutzerbestätigungsdialogfeld wird nach dem Kennwortänderungsbildschirm fälschlicherweise „Sie haben Ihr Kennwort geändert und sollten es künftig verwenden“ angegeben. |

- Die folgenden Zeichenkombinationen sind in Horizon Client-Kennwörtern unzulässig:

  <

  >

  <!—

  &
- Beispielsweise wird keines der folgenden Kennwörter unterstützt:

  Desktone

  < Desktone>

  Desktone <!—

  Desktone&

## Direkte Notfall-Desktop-Verbindung ohne Mandanten

Wenn in einer Notfallsituation, bei der ein Mandant ausgefallen ist oder nicht mehr erreicht werden kann, das Netzwerk weiter zugänglich ist, können Sie global alle DaaS-Agenten anweisen, einen temporären nativen RDP-Zugriff zuzulassen, damit Endbenutzer eine Verbindung ohne funktionierenden Broker herstellen können.

Um diese temporäre Funktionalität zu aktivieren, fügen Sie die im Folgenden beschriebenen Registrierungsschlüssel den Desktop-VMs entweder direkt oder über eine GPO-Richtlinie hinzu. Fügen Sie die Schlüssel an einem der folgenden Speicherorte hinzu, je nachdem, ob der DaaS Agent auf einem Windows-System mit 32 Bit oder 64 Bit installiert ist:

- HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware DaaS-Agent (32 Bit)
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware DaaS-Agent (64 Bit)

| Schlüssel | Typ | Wert |
|---|---|---|
| AllowDirectConnections | DWORD | 0 = keine direkten Verbindungen zulassen<br>1 = direkte Verbindungen zulassen. |
| DirectConnectionExpiryInUTC | REG_SZ | Zeitpunkt (Datum/Uhrzeit), bis zu dem direkte Verbindungen zulässig sind, wenn der Zugriff auf direkte Verbindungen aktiviert ist (AllowDirectConnections = 1).<br>Datums-/Uhrzeit-Format: JJJJ-MM-TT HH:MM:SS |

Für diese Funktion sind die folgenden Voraussetzungen erforderlich:

- DaaS Agent 17.2 wird verwendet.
- Der RDP-Zugriff wird nicht über View oder andere GPOs blockiert.
- Der Benutzer gehört zu einer Gruppe, der eine Desktop-Zuweisung zugeordnet ist. Der DaaS-Agent konfiguriert die gleichen Benutzer/Gruppen für den RDP-Zugriff auf dem Desktop (lokale RDP-Gruppe).

**Hinweis** Das standardmäßige Aktualisierungsintervall für die Gruppenrichtlinie beträgt 90 Minuten. Wenn die Aktualisierung früher erfolgen soll, müssen Sie zusätzliche Schritte ausführen. Weitere Informationen finden Sie in der entsprechenden Microsoft-Dokumentation.

# Menüoption „Wir freuen uns auf Ihr Feedback“ funktioniert nicht

Wenn Sie in der Verwaltungskonsole auf die Option **Wir freuen uns auf Ihr Feedback** klicken, geschieht nichts oder eine Browserfehlermeldung wird angezeigt.

### Problem

Das Menü „Hilfe“ der Verwaltungskonsole ( ) enthält die Option **Wir freuen uns auf Ihr Feedback**. Wenn Sie darauf klicken, wird abhängig von Ihren Einstellungen für den Browser oder für die E-Mail-Anwendung Ihres lokalen Systems Folgendes angezeigt:

- Es wird nichts angezeigt.
- Eine Browserfehlermeldung wird angezeigt.

### Ursache

Diese Menüauswahl ist so konzipiert, dass damit die neue E-Mail-Aktion der Standard-E-Mail-Anwendung Ihres lokalen Systems mithilfe von `mailto:feedback.horizonair@vmware.com` ausgeführt wird. Dieser Fehler tritt auf, wenn der Browser die `mailto`-Aktion nicht ausführen kann, z. B. wenn diese Bedingungen zutreffen:

- Ihr Browser blockiert Popup-Fenster.
- In der Anwendungsliste Ihres Browsers ist keine Standardaktion für den Inhaltstyp `mailto` konfiguriert oder für den `mailto`-Inhaltstyp ist die Aktion **Immer bestätigen** konfiguriert.

- In Ihrem lokalen System ist keine lokale Standard-E-Mail-Anwendung konfiguriert.

**Lösung**

1. Wenn Ihr Browser Popup-Fenster blockiert, fügen Sie die URL der Verwaltungskonsole zur Ausnahmeliste hinzu.
2. Konfigurieren Sie die Aktion für den `mailto`-Inhaltstyp Ihres Browsers mit einer E-Mail-Anwendung, sodass beim Klicken auf die Option **Wir freuen uns auf Ihr Feedback** ein neues E-Mail-Formular geöffnet wird.
3. Wenn Sie Ihre Browsereinstellungen nicht ändern möchten, können Sie Ihr Feedback manuell übermitteln, indem Sie eine E-Mail an `feedback.horizonair@vmware.com` senden.

# Technische Hinweise

15

Im Folgenden finden Sie technische Hinweise hinsichtlich verschiedener Systemfunktionen.

- Benutzerdefiniertes Branding

  Wenn Sie über ein benutzerdefiniertes Branding-Schema für das Desktop-Portal verfügen, müssen Sie prüfen, ob nach dem Upgrade eines Mandanten alles ordnungsgemäß aussieht. Es gibt einige Bereiche, die Sie aufgrund von VMware-Branding-Änderungen besonders beachten sollten.

  - Anmeldungsseite:

    CSS selector: #productNameInner

    Sie müssen möglicherweise die Eigenschaft „margin-left“ anpassen bzw. die Schriftgröße verringern, beispielsweise:

    font-size: 14px;

  - Andere Seiten:

    Sie müssen möglicherweise dieselben Änderungen wie für die Anmeldeseite vornehmen. Zusätzlich müssen Sie möglicherweise die Hintergrundposition der #banner-Auswahl anpassen:

    background-position: 0px 0px;

- Aktivieren von Post-Sysprep-Befehlen
  - Führen Sie zum Aktivieren von Post-Sysprep-Befehlen die folgenden Schritte auf einem Desktop durch, bevor Sie ihn in ein Image umwandeln.

    1. Erstellen Sie unter dem Treiber C:\ einen Ordner mit dem Namen „sysprep“.

    2. Erstellen Sie im Ordner „sysprep“ eine Batch-Datei mit dem Namen „postprep-extra.bat“.

    3. Tragen Sie die erforderlichen Befehle in die Batch-Datei ein und speichern Sie die Datei.

    4. Wandeln Sie den Desktop in ein Image um. Dateipfad: c:\sysprep\postprep-extra.bat. Sysprep startet diese Batch-Datei während der Ausführung der specialize-Phase (bevor der Agent sich beteiligt und der Domäne beitritt).

  - So legen Sie die Batch-Datei für post sysprep in der Vorlage vor dem Konvertieren zu einem Golden Image (wird vor dem Domänenbeitritt ausgeführt) fest.

    1. Erstellen Sie die Batch-Datei „C:\sysprep\postprep-extra.bat“.

2. Erstellen Sie die Ordnerstruktur „C:\Sysprep\...“ (für Windows 7: „C:\Sysprep\ postprep-extra.bat“).

3. Speichern Sie sie mit Ihren Befehlen. Sysprep führt diese Batch-Datei nach der Ausführung aus.

# Helpdesk Console (Beta-Funktion) 16

Helpdesk Console ist eine Benutzeroberfläche, die Sie für den Zugriff auf VMs, zum Durchführen von Integritätsprüfungen, zum Abrufen von Remoteunterstützung und zum Durchführen anderer Aufgaben verwenden können.

Hinweis zu Beta-Funktionen und Support

HELPDESK CONSOLE WIRD „WIE BESEHEN“ BEREITGESTELLT, UND ZWAR OHNE SERVICE-LEVEL-VEREINBARUNG ODER GEWÄHRLEISTUNG JEGLICHER ART, AUSDRÜCKLICH ODER IMPLIZIT, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE GEWÄHRLEISTUNGEN DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND NICHTVERLETZUNG. DIE AUTOREN ODER COPYRIGHTINHABER SIND UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE ANSPRÜCHE, SCHÄDEN ODER ANDERE HAFTBARKEITEN, OB VERTRAGS-, ZIVILRECHTLICH ODER ANDERWEITIG, DIE AUS ODER IN VERBINDUNG MIT DER SOFTWARE ODER DEREN VERWENDUNG ODER ANDEREN GESCHÄFTSTRANSAKTIONEN MIT DER SOFTWARE ENTSTEHEN.

Bei Fragen oder Problemen hinsichtlich der Verwendung von Helpdesk Console können Sie Ihr Anliegen an deployment@vmware.com senden. VMware ist nicht verpflichtet, Änderungen der Funktionen oder die Behebung von Problemen an Helpdesk Console vorzunehmen.

Dieses Kapitel behandelt die folgenden Themen:



## Zugriff auf Helpdesk Console

Sie können über Ihren Webbrowser auf Helpdesk Console zugreifen.

Hinweis:

- Verwenden Sie HTTPS und nicht HTTP. Bei Verwendung von HTTP wird die Konsole nicht gestartet.
- Chrome ist der einzige unterstützte Browser für den Console-Zugriff. Die folgenden Browser werden nicht unterstützt: Microsoft Internet Explorer, Firefox, Safari und Opera.
- Wenn beim Start für den Konsolenzugriff Fehler auftreten, müssen Sie möglicherweise die folgende URL öffnen und das Zertifikat akzeptieren: https://<tenant_appliance_tenant_network_ip>:18001/
- In einer vCloud Director-basierten Umgebung müssen Sie sicherstellen, dass Ihr Browser das vCloud Director-Serverzertifikat akzeptiert.
- Der Zugriff auf Helpdesk Console ist beschränkt auf:
  - Mandantenadministratoren (Benutzer mit Administratorzugriff auf die Verwaltungskonsole)
  - Mitglieder der AD-Gruppe Horizon_Air_Helpdesk Diese Gruppe kann für die Bereitstellung des Zugriffs verwendet werden, um Mitarbeiter zu unterstützen, die nicht als Mandantenadministratoren fungieren.

### Vorgehensweise

1. Navigieren Sie in einem Chrome-Webbrowser zu „https://<*TenantApplianceNodeAddress*>/haca“, wobei <*TenantApplianceNodeAddress*> die IP-Adresse des Mandanten ist.

   Die Anmeldeseite wird angezeigt.

2. Geben Sie Ihren Administratorbenutzernamen und Ihr Kennwort ein. Bestätigen Sie die Auswahl der richtigen Domäne und klicken Sie auf **Anmelden**.

   Die Registerkarte „Virtuelle Maschine“ wird angezeigt, die eine Liste sämtlicher VMs in allen Pools enthält.

## Starten einer Konsole für eine virtuelle Maschine

Klicken Sie zum Starten einer Konsole für eine virtuelle Maschine in Helpdesk Console auf den VM-Namen in der Liste „Virtuelle Maschinen“.

Es wird eine Konsole geöffnet, die den Anmeldebildschirm für die VM zeigt. Strg+Alt+Entf- und Energievorgänge werden durch die Schaltflächen in der oberen rechten Ecke des Konsolenfensters unterstützt.

## Einrichten einer Integritätsprüfung

Mit dem Tool „Integritätsprüfung“ können Sie die Anwendung von VM-Änderungen überwachen, die möglicherweise den Portzugriff, die Leistung oder den Gesamtzugriff durch Endbenutzer auf den Desktop kompromittieren.

### Vorgehensweise

1 Installieren Sie Horizon DaaS Health Agent auf allen VMs, die überwacht werden. Klicken Sie oben rechts auf der Registerkarte „VM-Integritätsprüfung“ auf den Link **Horizon DaaS Health Agent installieren**, um weitere Informationen zu erhalten.

**Hinweis** Standardmäßig hört Health Agent TCP-Port 10762 ab.

2 Filtern Sie die Liste mithilfe des Felds „Prüffilter“ bzw. der Dropdown-Liste „Pool auswählen“ nach Bedarf.

3 Initiieren Sie die Prüfung, indem Sie eine der folgenden Aktionen durchführen:

- Klicken Sie auf **Einmalige Prüfung**, um sofort eine einzelne Prüfung durchzuführen.
- Geben Sie die Anzahl der Minuten ein und klicken Sie auf **Prüfung planen**, um wiederholte Prüfungen zu einem ausgewählten Zeitraum zu planen.

Informationen für die geprüften VMs werden in den Spalten wie unten beschrieben angezeigt.

| Spalte | Beschreibung |
|---|---|
| VM | Name der virtuellen Maschine |
| Pool | Pool (Zuweisung), zu dem die VM gehört |
| IP | IP-Adresse der VM |
| Ergebnis | Gesamtergebnis der Prüfung Mögliche Ergebnisse:<br>■ Ausschalten – Die VM wird ausgeschaltet.<br>■ Agentenfehler – Health Agent ist auf der VM weder installiert noch erreichbar.<br>■ VM-Problem(e) – Diese Probleme liegen vor, wenn ein „X“ und eine Zahl angezeigt werden. VM hat mindestens ein Problem, das in anderen Spalten ausführlicher aufgezeigt wird. |
| Ports | Überprüft, ob die erforderlichen Ports geöffnet sind |
| Firewall | Gibt an, ob die Firewall der VM aktiviert ist |
| Ruhezustandsrichtlinie | Gibt an, ob eine Richtlinie für die VM festgelegt ist, damit sie in einen Ruhezustandsstatus versetzt werden kann |
| Dienste | Überprüft, ob die folgenden Dienste ausgeführt werden:<br>■ Desktop Windows Manager Session Manager<br>■ VMware HTML Access (Blast)<br>■ VMware Horizon Agent<br>■ VMware DaaS Agent<br>■ VMware Tools |
| RDP-fähig | Überprüft, ob RDP aktiviert und für das Zulassen von Verbindungen von Computern festgelegt ist, auf denen eine RDP-Version ausgeführt wird |
| Fehlerhafte IP | Überprüft, ob der Desktop über keine 169.x.x.x-IP-Adresse verfügt und somit wahrscheinlicher DHCP abruft |

| Spalte | Beschreibung |
|---|---|
| DHCP | Überprüft, ob der Desktop für DHCP festgelegt ist, nicht STATIC |
| Domänenvertrauensstellung | Bestätigt die Domänenvertrauensstellung zwischen Desktop und Domänencontroller |
| Remote-Unterstützung | Überprüft, ob „Remote-Unterstützung“ auf dem Desktop aktiviert ist |

4 Wenn die Prüfung vollständig ist, können Sie die folgenden Aktionen ausführen:

- Bewegen Sie den Mauszeiger über die Fehler in der Tabelle mit den Prüfergebnissen, um zusätzliche Informationen anzuzeigen.
- Klicken Sie oben links in der Liste auf die Schaltfläche **Bericht** (die Schaltfläche heißt **Bericht: <Tag Datum Uhrzeit>**), um den Verlauf der zuletzt durchgeführten Prüfungen anzuzeigen. In dieser Tabelle öffnen Sie durch Doppelklicken an einer beliebigen Stelle in einer Zeile die Ergebnisse für diese Prüfung.
- Aktivieren Sie das Kontrollkästchen **Nur VMs mit Fehler anzeigen**, um die fehlerfreien VMs auszublenden.
- Geben Sie einen Namen oder partiellen Namen im Feld „Suche“ ein und drücken Sie die **Eingabetaste**, um VMs nach Namen zu durchsuchen.
- Wählen Sie im Dropdown-Menü „Anzeigen“ einen Wert aus, um die Anzahl der VMs anzupassen, die pro Seite angezeigt werden.
- Klicken Sie auf **Exportieren** und wählen Sie eine der folgenden Optionen aus:
  - **Kopieren**: Kopiert Informationen in die Zwischenablage
  - **CSV**: Exportiert die Ergebnisse im CSV-Format
  - **PDF**: Exportiert Ergebnisse im PDF-Format
  - **Drucken**: Generiert eine Webdruckversion der Ergebnisse

# Erhalten von Remote-Unterstützung

Das Tool „Remote-Unterstützung“ bietet Helpdesk-Benutzern oder Administratoren die Möglichkeit, eine aktive Benutzersitzung zu spiegeln.

Klicken Sie auf der Registerkarte „Remote-Unterstützung“ auf den Link **Handbuch für Remote-Unterstützung**, um weitere Informationen zu dieser Funktion zu erhalten.

# Anzeigen des Nutzungsberichts

Die Registerkarte „Nutzungsbericht“ zeigt Nutzungstrends an und ermöglicht Ihnen, die Benutzeraktivitäts-Sitzungsberichte anzuzeigen.

„Nutzungsbericht“ kann nach Datum, Pool und Datumstyp gefiltert werden. Zu den unter „Nutzungsbericht“ angezeigten Daten zählen:

- Nutzungstrends – Maximale gleichzeitige Benutzer – Maximale gleichzeitige Sitzungen – Eindeutige Benutzer pro Tag – Gesamtkapazität
- Benutzerinformationen – Clientzugriffsdemografie – Interner vs. Externer Benutzerzugriff
- Sitzungsinformationen – Protokoll, Diensttyp, Sitzungsdauer

Pool-basierte Nutzungsinformationen wie die maximalen gleichzeitigen Benutzer und die eindeutigen Benutzer, die auf einen spezifischen Pool zugreifen, können beim Bestimmen der Gesamtnutzung und der Lizenzierungsanforderungen Ihrer Anwendungen für die RDSH-Pools nützlich sein.

Wählen Sie **Benutzeraktivität** aus dem Dropdown-Menü „Nutzungsbericht“ aus, um die „Benutzeraktivitätsübersicht“ anzuzeigen.

Klicken Sie in der Liste „Benutzeraktivitätsübersicht“ auf einen Benutzernamen, um „Benutzeraktivitätsdetails“ anzuzeigen.

# Image-Upload

Mit der Funktion „Image-Upload“ können Sie Betriebssystem-Images hochladen und für die Zuweisungserstellung verwenden.

Dafür gibt es zwei Möglichkeiten:

- Wenn Sie bereits eine VM vorbereitet haben, können Sie das Image vom aktuellen Speicherort aus hochladen.
- Sie können mithilfe des Tools „hvexport“ eine Horizon View-Desktop-Pool-Vorlage exportieren und dann die vorbereitete Vorlage mit „Image-Upload“ importieren.

## Hochladen eines Images

Der Prozess des Hochladens eines vorhandenen Images besteht aus Folgendem.

- Vorbereiten des Images für den Upload
- Durchführen von Upload-Schritten.
- Fehlerbehebung beim Upload (sofern erforderlich)

### Vorbereiten des Images für den Upload

Der Image-Upload-Dienst kann mit generischen VM-Vorlagen im OVF-Format verwendet werden. Die virtuelle Maschine muss vor dem Import ordnungsgemäß vorbereitet werden.

#### Vorgehensweise

1. Klicken Sie auf den Link „Hilfe“, um Anforderungen für die Desktop-Software bzw. den Desktop-Dienst anzuzeigen.

2 Klicken Sie auf den Link „Agenten herunterladen“ zum Herunterladen der erforderlichen Software (Agent) und des SSL-Zertifikats. Die Dateien werden gemäß Ihrer Mandanten-Appliance-Version durch Ihren Dienstanbieter vorbereitet.

3 Die folgenden Anforderungen müssen erfüllt werden.

- Software

  Sie können erforderliche Software über den Link „Agenten herunterladen“ auf der Seite „Image-Upload-Dienst“ herunterladen. Die folgende Software muss installiert werden:

  - Horizon DaaS Agent
  - Horizon Agent
  - Horizon DaaS Health Agent

- SSL-Zertifikat

  Die Horizon DaaS-Mandantenzertifikatsdatei muss in DaaS Agent konfiguriert werden. Sie können sie über den Link „Agenten herunterladen“ auf der Seite „Image-Upload-Dienst“ herunterladen. Bei einer standardmäßigen DaaS Agent-Installation auf einem x64-System muss die Zertifikatsdatei an den folgenden Speicherort kopiert werden:

  C:\Program Files (x86)\VMware\VMware DaaS Agent\cert\cacert.pem

- Dienste

  Die folgenden Dienste müssen so konfiguriert werden, dass sie automatisch gestartet werden:

  - VMware DaaS Agent (DaaS Agent)
  - VMware Horizon View Agent (WSNM)
  - Windows-Firewall (MpsSvc)
  - Desktop Window Manager Session Manager (UxSms)
  - VMware Blast (VMBlast)

4 Aktualisieren Sie die IP-Adressen der Desktop-Manager in der DaaS-Agentenkonfigurationsdatei, wenn Sie über mehrere Desktop-Manager verfügen. Bei der standardmäßigen DaaS Agent-Installation auf einem x64-System ist die Konfigurationsdatei:

C:\Program Files (x86)\VMware\VMware DaaS Agent\service\MonitorAgent.ini

- Wechseln Sie zu folgender Zeile:

  ;standby_address=<heben Sie die Auskommentierung auf und fügen Sie eine kommagetrennte Standby-Adressenliste hinzu>

- Heben Sie die Auskommentierung der Zeile auf, indem Sie das Semikolon am Anfang entfernen, und fügen Sie durch Kommas getrennte Desktop-Manager-Adressen hinzu. Beispiel:

  standby_address=192.168.11.3,192.168.11.4,192.168.11.5,192.168.11.6

5 Stellen Sie vor dem Ausführen des Exports Folgendes sicher:

- Der Netzwerkadaptertyp lautet VMXNET3. E1000 funktioniert nicht.
- Es ist keine ISO mit der VM verbunden. Sie können jedes virtuelle CD-ROM-Laufwerk sicher entfernen.
- Der Ziel-Hypervisor unterstützt die Version Ihrer virtuellen Maschine. Aufgrund der kombinierten Infrastruktur wird die neueste virtuelle Maschine nicht immer unterstützt. Halten Sie nach Möglichkeit die Version Ihrer virtuellen Maschine gering. Beispielsweise Version 8. Sie können sich hinsichtlich unterstützter VM-Versionen an Ihren Dienstanbieter wenden oder versuchen, das Tool zu verwenden, da es einen Fehler meldet, wenn die VM-Version nicht kompatibel ist.
- Auf der VM ist keine 3D-Grafikkartenfunktion aktiviert.
- Die virtuelle Maschine wird als OVF exportiert, da OVA derzeit durch die Image-Upload-Funktion nicht unterstützt wird.

## Hochladen des Images

Nach dem Vorbereiten des Images können Sie es hochladen.

### Vorgehensweise

1 Klicken Sie auf der Registerkarte „Image-Upload“ auf die Schaltfläche **Dateien auswählen**, um die VM-Dateien auszuwählen.

Dies umfasst für gewöhnlich die folgenden Dateien:

- eine .ovf-Datei
- mindestens eine .vmdk-Datei
- optional eine .mf-Datei

Hinweis:

- Wählen Sie keine .iso-Datei aus. Wenn Sie eine .iso-Datei sehen, sollten Sie Ihre virtuelle Maschine bearbeiten, alle CD-ROM-Treiber entfernen und den Export wiederholen.
- Die OVA-Datei wird derzeit nicht unterstützt. Benennen Sie zum Umwandeln der OVA-Datei in das OVF-Format die OVA-Dateierweiterung „.ova“ in „.zip“ um. Verwenden Sie dann ein zip-Tool zum Extrahieren des Archivs. Die extrahierten Dateien liegen im OVF-Format vor.

Die hochgeladene VM-Vorlage wird in ein Desktop-Image umgewandelt.

2 Klicken Sie nach Auswahl der ovf-Dateien auf den Link **Konfiguration** zum Anzeigen der Konfigurationsseite und nehmen Sie die Eingabe für die richtige Konfiguration vor.

3 Klicken Sie auf die Schaltfläche **Import starten**, um den Importvorgang zu starten.

Der Fortschritt wird mit einer Detailmeldung angezeigt.

**Hinweis** Sie können die hochgeladene VM in ein anderes Datencenter oder einen anderen Desktop-Manager ohne erneuten Upload bereitstellen. Wählen Sie das Optionsfeld **Zuvor hochgeladen** im Abschnitt „Image-Dateien“ aus, um die hochgeladenen Dateien wiederzuverwenden.

### Fehlerbehebung beim Upload

Bei Fehlschlagen des Vorgangs werden die Fehlerdetails im unteren Abschnitt der Registerkarte „Image-Upload“ angezeigt.

- Wenn die virtuelle Maschine noch nicht bereitgestellt wurde, müssen Sie in Abhängigkeit der Fehlerursache möglicherweise eine neue erneut hochladen oder versuchen, eine Neubereitstellung vorzunehmen.
- Wenn die VM bereitgestellt wurde, bei der Konvertierung des Golden Images jedoch Fehler aufgetreten sind, könnte die VM im Pool „Importierter Desktop“ oder in der Musterverwaltung in „Reservierter Desktop“ angezeigt werden. Suchen Sie dort nach der VM und bereiten Sie das Image manuell mithilfe des Konsolenzugriffs in der Helpdesk Console und der Verwaltungskonsole vor. Dadurch können Sie das erneute Hochladen/Bereitstellen überspringen, was sonst bei großen VM-Images lange Zeit in Anspruch nehmen könnte.

## Verwenden einer Vorlage aus Horizon View

So verwenden Sie eine Vorlage aus Horizon View:

- Exportieren der Vorlage aus Horizon View und Vorbereiten des Images
- Hochladen der Datei in die Helpdesk Console

### Exportieren der Vorlage aus Horizon View und Vorbereiten des Images

Das Tool „hvexport“ wird verwendet, um Desktop-Pool-Vorlagen aus Horizon View zu exportieren.

Das Tool hilft auch beim Vorbereiten des Images. Dies umfasst das Prüfen der Konfiguration, das Herunterladen der richtigen Software sowie das automatische Installieren und Herunterladen des DaaS-Zertifikats und das Kopieren in den DaaS-Agenten-Ordner.

#### Vorgehensweise

1. Klicken Sie auf den Link **Hilfe** auf der Seite „Image-Upload“.
2. Klicken Sie auf die Links zum Herunterladen des Tools und der Plattformkonfiguration.

   Die Plattformkonfiguration wird dynamisch generiert und durch das Tool verwendet.
3. Extrahieren Sie das heruntergeladene Archiv.

   Das Tool „hvexport“ umfasst drei Ordner („export“, „repos“ und „software“) und fünf Dateien:

   - hvexport.bat
   - hvexport.jar
   - hvexport.sh
   - ImgUploadSvc.conf
   - readme.txt

Dateien sind wie folgt organisiert:

- Die Datei „ImgUploadSvc.conf“ wird in den Ordner „tool“ heruntergeladen.
- Erforderliche Software wird automatisch in das Verzeichnis „software“ heruntergeladen (z. B. DaaS-Agent, View-Agent).
- Das Verzeichnis „export“ ist das Standardverzeichnis, in das die Horizon View-Desktop-Pool-Vorlage exportiert wird.

**Hinweis** Das Tool ist eine Java-Anwendung und benötigt für die Ausführung JRE.

4 Starten Sie die Anwendung mit hvexport.bat oder .sh. Befolgen Sie die Anleitung des Tools zum Exportieren der VM und bereiten Sie das Betriebssystem-Image vor.

Das Tool ist interaktiv und erstellt schließlich einen verknüpften Klon der VM-Zielvorlage auf vCenter und lädt automatisch die erforderliche Software auf das Gastbetriebssystem hoch. Die folgenden Elemente werden automatisch heruntergeladen:

- Horizon DaaS Agent
- Horizon View Agent
- Horizon DaaS Health Agent

Zusätzlich ist das Mandantenzertifikat (cacert.pem) für die Vorbereitung des Golden Image erforderlich. Das Tool bereitet zudem das Zertifikat vor, das in der zuvor heruntergeladenen Plattformkonfigurationsdatei (ImgUploadSvc.conf) enthalten ist.

Die hochgeladenen Dateien sollten automatisch installiert werden. Sollte die Image-Vorbereitung fehlerhaft sein, können Sie sie manuell auf dem Zieldesktop ausführen.

Das Tool „hvexport“ führt eine Überprüfung der Umgebung nach der Softwareinstallation durch.

Das Tool übernimmt auch den Status in eine Datei, sodass sie neu gestartet werden kann. Felder, in denen zuvor etwas eingegeben wurde, haben einen Standardwert. Beispielsweise die Verbindungsserveradresse.

5 Drücken Sie direkt die EINGABETASTE, um den Standardwert zu verwenden.

## Hochladen der Datei

Nach dem Exportieren der Vorlage und Vorbereiten der Image-Datei können Sie sie in der Helpdesk Console hochladen.

Nach dem Exportieren der Vorlage wird sie standardmäßig im Exportverzeichnis des Tools „hvexport“ angezeigt.

### Vorgehensweise

1. Klicken Sie auf der Registerkarte „Image-Upload“ auf **Datei auswählen** und wählen Sie mit Ausnahme der ggf. vorhandenen .iso-Datei alle Dateien im Exportordner aus. Es sollten eine .ovf-Datei, eine pool.conf-Datei und mindestens eine .vmdk-Datei vorhanden sein. Laden Sie keine ISO-Datei hoch.

   Wenn die pool.conf-Datei ein durch das Tool „hvexport“ exportierter Pool ist, wird die Konfiguration automatisch angezeigt, wobei einige Felder ausgefüllt sind.
2. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.
3. Klicken Sie auf die Schaltfläche „Import starten“.

   Der Importvorgang wird abgeschlossen, wobei der Fortschritt auf dem Bildschirm angezeigt wird.

## Anzeigen des Verlaufs

Die Registerkarte „History“ (Verlauf) stellt das Zugriffsprotokoll für Überwachungszwecke bereit.

Mit den Steuerungen oben auf der Seite können Sie Daten suchen oder nach Pool (Zuweisung) filtern.