

Verwaltung der Horizon Console

DEZ 2019

VMware Horizon 7 7.11



vmware®

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

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2018–2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

1	Verwaltung der VMware Horizon Console	9
2	Verwenden der VMware Horizon Console	10
	Unterstützte Horizon 7-Funktionen	10
	Vorteile der Verwendung von Horizon Console	12
	Installieren und Konfigurieren von Horizon Console	12
	Anmelden bei Horizon Console	12
3	Konfigurieren von Horizon-Verbindungsserver in Horizon Console	15
	Konfigurieren von vCenter Server und Horizon Composer in Horizon Console	15
	Erstellen eines Benutzerkontos für Horizon Composer-AD-Vorgänge	15
	Installation des Produktlizenzschlüssels in Horizon Console	17
	Hinzufügen von vCenter Server-Instanzen zu Horizon 7 in Horizon Console	17
	Konfigurieren von Horizon Composer-Einstellungen	20
	Konfigurieren von Horizon Composer-Domänen	21
	Hinzufügen eines Instant-Clone-Domänenadministrators in Horizon Console	22
	Zulassen, dass vSphere Speicherplatz auf virtuellen Linked-Clone-Maschinen freigibt	23
	Konfigurieren von Horizon Storage Accelerator für vCenter Server	25
	Grenzwerte für parallele Vorgänge für vCenter Server und Horizon Composer	27
	Einstellen der Anzahl paralleler Vorgänge zum Ändern des Betriebszustands, um Remote-Desktop-Anmeldungsüberlastungen zu unterstützen	28
	Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats	29
	Entfernen einer vCenter Server-Instanz aus Horizon 7	31
	Entfernen von Horizon Composer aus Horizon 7	31
	Konflikte bei eindeutigen IDs für vCenter Server	32
	Sichern von Horizon-Verbindungsserver in Horizon Console	33
	Konfigurieren von Einstellungen für Client-Sitzungen in Horizon Console	33
	Globale Einstellungen für Clientsitzungen Horizon Console	33
	Globale Sicherheitseinstellungen für Client-Sitzungen und -Verbindungen in Horizon Console	37
	Globale Client-Einschränkungseinstellungen für Clientsitzungen in Horizon Console	38
	Deaktivieren oder Aktivieren von Horizon-Verbindungsserver in Horizon Console	40
	Bearbeiten der externen URLs für Horizon-Verbindungsserver-Instanzen	40
	Registrieren von Gateways in Horizon Console	42
4	Einrichten der Smartcard-Authentifizierung	43
	Anmelden über eine Smartcard	44
	Konfigurieren der Smart Card-Authentifizierung auf dem Horizon-Verbindungsserver	45
	Anfordern der Zertifizierungsstellenzertifikate	45

Anfordern des CA-Zertifikats von Windows	46
Hinzufügen des CA-Zertifikats zu einer Server-Vertrauensspeicherdatei	47
Ändern von Horizon-Verbindungsserver-Konfigurationseigenschaften	48
Konfigurieren der Smartcard-Einstellungen in Horizon Console	49
Konfigurieren der Smartcard-Authentifizierung auf Drittanbieterlösungen	52
Vorbereiten von Active Directory für die Smartcard-Authentifizierung	52
Hinzufügen von UPNs für Smartcard-Benutzer	53
Hinzufügen des Stammzertifikats zum Enterprise NTAAuth-Speicher	54
Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen	54
Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen	55
Überprüfen der Smartcard-Authentifizierungskonfiguration in Horizon Console	56
Verwenden der Smartcard-Zertifikatsperrüberprüfung	58
Anmelden bei Verwendung der Überprüfung von Zertifikatsperrlisten	59
Anmelden bei Verwendung der OCSP-Zertifikatsperrüberprüfung	59
Konfigurieren der Überprüfung von Zertifikatsperrlisten	60
Konfigurieren der OCSP-Zertifikatsperrüberprüfung	61
Eigenschaften der Smartcard-Zertifikatsperrüberprüfung	62
5 Einrichten anderer Typen der Benutzerauthentifizierung	63
Verwenden der zweistufigen Authentifizierung	63
Anmeldung unter Verwendung der zweistufigen Authentifizierung	64
Aktivieren der Zwei-Faktor-Authentifizierung in Horizon Console	65
Fehlerbehebung bei verweigertem RSA SecureID-Zugriff	68
Fehlerbehebung bei Verweigerung des Zugriffs auf RADIUS	69
Verwenden der SAML-Authentifizierung	69
Verwenden der SAML-Authentifizierung zur VMware Identity Manager-Integration	70
Konfigurieren eines SAML-Authentifikators in Horizon Console	70
Konfigurieren der Proxy-Unterstützung für VMware Identity Manager	73
Ändern des Ablaufzeitraums der Metadaten von Diensteanbietern auf dem Verbindungsserver	73
Generieren von SAML-Metadaten für die Verwendung des Verbindungservers als Dienstanbieter	74
Aspekte der Antwortzeit für mehrere dynamische SAML-Authentifikatoren	75
Konfigurieren von Workspace ONE-Zugriffsrichtlinien in Horizon Console	75
Konfigurieren der biometrischen Authentifizierung	76
6 Authentifizieren von Benutzern und Gruppen	78
Beschränken des Remote-Desktop-Zugriffs außerhalb des Netzwerks	78
Konfigurieren von Remotezugriff	79
Konfigurieren des nicht authentifizierten Zugriffs	79
Erstellen von Benutzern für einen nicht authentifizierten Zugriff	80
Aktivieren des nicht authentifizierten Zugriffs für Benutzer in Horizon Console	81

Erteilen von Berechtigungen für Benutzer für einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen	81
Löschen eines Benutzers für einen nicht authentifizierten Zugriff	82
Nicht authentifizierter Zugriff von Horizon Client aus	83
Konfigurieren von Benutzern für die Hybrid-Anmeldung in Horizon Console	83
Verwenden der Funktion „Als aktueller Benutzer anmelden“, die mit Windows-basierten Horizon Client-Instanzen verfügbar ist	85

7 Konfigurieren der rollenbasierten Verwaltungsdelegierung in Horizon Console 88

Grundlegendes zu Rollen und Berechtigungen	88
Verwenden von Zugriffsgruppen zur Delegierung der Verwaltung von Pools und Farmen in Horizon Console	89
Unterschiedliche Administratoren für unterschiedliche Zugriffsgruppen	90
Unterschiedliche Administratoren für dieselbe Zugriffsgruppe	91
Grundlegendes zu Berechtigungen	91
Verwalten von Administratoren	92
Erstellen eines Administrators in Horizon Console	93
Entfernen eines Administrators in Horizon Console	94
Verwalten und Überprüfen von Berechtigungen	94
Hinzufügen einer Berechtigung in Horizon Console	95
Löschen einer Berechtigung in Horizon Console	96
Überprüfen von Berechtigungen in Horizon Console	97
Verwalten und Prüfen von Zugriffsgruppen	98
Hinzufügen einer Zugriffsgruppe in Horizon Console	98
Verschieben eines Desktop-Pools oder einer Farm in eine andere Zugriffsgruppe in Horizon Console	99
Entfernen einer Zugriffsgruppe in Horizon Console	99
Überprüfen der Objekte in einer Zugriffsgruppe	99
Überprüfen der vCenter-VMs in einer Zugriffsgruppe	100
Verwalten von benutzerdefinierten Rollen	100
Hinzufügen einer benutzerdefinierten Rolle in Horizon Console	101
Ändern der Berechtigungen in einer benutzerdefinierten Rolle in Horizon Console	101
Entfernen einer benutzerdefinierten Rolle in Horizon Console	101
Vordefinierte Rollen und Berechtigungen	102
Vordefinierte Administratorrollen	103
Globale Berechtigungen	106
Objektspezifische Berechtigungen	108
Interne Berechtigungen	109
Erforderliche Berechtigungen für häufige Aufgaben	109
Berechtigungen für die Pool-Verwaltung	109
Berechtigungen für die Verwaltung von Maschinen	110
Berechtigungen für die Verwaltung persistenter Festplatten	111
Berechtigungen für die Verwaltung von Benutzern und Administratoren	111

	Berechtigungen für Horizon Help Desk Tool-Aufgaben	112
	Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle	113
	Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen	114
8	Festlegen von Richtlinien in Horizon Console	115
	Konfigurieren von globalen Richtlinien	115
9	Warten von Horizon 7-Komponenten	117
	Sichern und Wiederherstellen von Horizon 7-Konfigurationsdaten	117
	Sichern von Horizon-Verbindungsserver- und Horizon Composer-Daten	118
	Planen von Horizon 7-Konfigurationssicherungen	119
	Sicherungseinstellungen zur Horizon 7-Konfiguration	119
	Exportieren von Konfigurationsdaten aus Horizon-Verbindungsserver	120
	Wiederherstellen von Horizon-Verbindungsserver- und Horizon Composer-Konfigurationsdaten	122
	Importieren von Konfigurationsdaten in Horizon-Verbindungsserver	122
	Wiederherstellen einer Horizon Composer-Datenbank	124
	Ergebniscodes für das Wiederherstellen der Horizon Console-Datenbank	125
	Exportieren von Daten in Horizon Composer-Datenbank	126
	Ergebniscodes für den Export der Horizon Composer-Datenbank	127
	Überwachen von Horizon 7-Komponenten	127
	Überwachen des Auslastungsstatus des Horizon-Verbindungservers	129
	Überwachen von Diensten auf dem Horizon-Verbindungsserver	130
	Grundlegendes zu Horizon 7-Diensten	131
	Beenden und Starten der Horizon 7-Dienste	131
	Dienste auf einem Verbindungsserver-Host	131
	Dienste auf einem Sicherheitsserver	132
	Ändern des Produktlizenzschlüssels oder der Lizenzmodi in Horizon Console	133
	Überwachen der Lizenznutzung	134
	Zurücksetzen der Daten zur Lizenznutzung	135
	Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit	136
	Integration des Horizon-Verbindungservers mit Skyline Collector-Appliance	136
10	Erste Schritte mit JMP Integrated Workflow	138
	Informationen zu JMP Integrated Workflow	138
	Erste Schritte mit dem integrierten JMP-Arbeitsablauf	139
11	Verwalten von JMP-Einstellungen	141
	Erstmaliges Konfigurieren der JMP-Einstellungen	141
	Verwalten von JMP-Einstellungen	144
	Bearbeiten der JMP Server-Einstellungen	144
	Bearbeiten der Anmeldedaten für Horizon 7	145

Bearbeiten der Horizon-Verbindungsserver-URL	145
Hinzufügen von Active Directory-Domänen	146
Bearbeiten der Informationen zur Active Directory-Domäne	147
Löschen der Informationen der Active Directory-Domäne	147
Hinzufügen von Informationen zu App Volumes	148
Bearbeiten der Informationen zur App Volumes-Instanz	149
Löschen der Informationen zur App Volumes-Instanz	149
Hinzufügen von Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe	150
Bearbeiten der Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe	150
Löschen der Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe	151

12 Verwalten von JMP-Zuweisungen 152

Erstellen einer JMP-Zuweisung	153
Bearbeiten einer JMP-Zuweisung	155
Duplizieren einer JMP-Zuweisung	156
Löschen einer JMP-Zuweisung	157

13 Konfigurieren der Ereignisberichterstattung in Horizon Console 159

Hinzufügen einer Datenbank und eines Datenbankbenutzers für Horizon 7-Ereignisse in Horizon Console	159
Vorbereiten einer SQL Server-Datenbank für die Ereignisberichterstellung in Horizon Console	160
Konfigurieren der Ereignisdatenbank in Horizon Console	161
Konfigurieren der Ereignisprotokollierung in Datei oder Syslog-Server in Horizon Console	163
Überwachen von Ereignissen in Horizon 7	165
Horizon 7-Ereignismeldungen	166

14 Verwenden des Horizon Help Desk Tool in Horizon Console 167

Starten des Horizon Help Desk Tool an der Horizon Console	168
Fehlerbehebung bei Benutzern in Horizon Help Desk Tool	168
Sitzungsdetails für das Horizon Help Desk Tool	172
Sitzungsprozesse für das Horizon Help Desk Tool	178
Anwendungsstatus für Horizon Help Desk Tool	179
Fehlerbehebung bei Desktop- oder Anwendungssitzungen in Horizon Help Desk Tool	180

15 Verwenden des Befehls „vdmadmin“ 182

Verwendung des Befehls „vdmadmin“	184
Authentifizierung für den Befehl „vdmadmin“	185
Ausgabeformat des Befehls „vdmadmin“	185
Optionen des Befehls „vdmadmin“	186
Konfigurieren der Protokollierung in Horizon Agent mithilfe der Option „-A“	187
Außerkraftsetzen von IP-Adressen mithilfe der Option „-A“	190
Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F“	191

Auflisten und Anzeigen von Systemüberwachungen mithilfe der Option „-H“	192
Auflisten und Anzeigen von Berichten zum Horizon 7-Betrieb unter Verwendung der Option „-I“	194
Generieren von Horizon 7-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-I“	195
Zuweisen von dedizierten Computern unter Verwendung der Option „-L“	197
Anzeigen von Informationen zu Maschinen mithilfe der Option „-M“	199
Rückgewinnung von Datenträgerplatz auf virtuellen Maschinen mithilfe der Option „-M“	200
Konfigurieren von Domänenfiltern mithilfe der Option „-N“	201
Konfigurieren von Domänenfiltern	204
Beispiel für die Filterung zum Einschließen von Domänen	206
Beispiel für die Filterung zum Ausschließen von Domänen	207
Anzeigen der Maschinen und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“	209
Konfigurieren von Clients im Kiosk-Modus mithilfe der Option „-Q“	211
Anzeigen des ersten Benutzers einer Maschine mithilfe der Option „-R“	217
Entfernen des Eintrags für eine Verbindungsserver-Instanz oder einen Sicherheitsserver mithilfe der Option „-S“	217
Bereitstellen sekundärer Anmeldeinformationen für Administratoren mithilfe der Option „-T“	219
Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U“	221
Entsperren oder Sperren von virtuellen Maschinen mithilfe der Option „-V“	222
Ermitteln und Lösen von Konflikten bei LDAP-Einträgen und LDAP-Schemas mithilfe der Option „-X“	223

Verwaltung der VMware Horizon Console

1

Verwaltung der VMware Horizon Console beschreibt, wie VMware Horizon[®] 7 konfiguriert und verwaltet wird und wie Administratoren erstellt, Benutzerauthentifizierungen eingerichtet, Richtlinien konfiguriert und Verwaltungsaufgaben in Horizon Console ausgeführt werden. In diesem Dokument wird außerdem die Wartung und Fehlerbehebung für Horizon 7-Komponenten beschrieben.

Informationen zur Verwendung von Horizon Console zum Konfigurieren und Verwalten einer Cloud-Pod-Architektur-Umgebung finden Sie im Dokument *Verwalten der Cloud-Pod-Architektur in Horizon 7*.

Zielgruppe

Diese Informationen richten sich an Benutzer, die VMware Horizon 7 konfigurieren und verwalten möchten. Diese Informationen sind für erfahrene Windows- oder Linux-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und Vorgängen in Rechenzentren vertraut sind.

Verwenden der VMware Horizon Console

2

VMware Horizon Console ist die neueste Version der Weboberfläche, auf der Sie virtuelle Desktops und veröffentlichte Desktops und Anwendungen erstellen und verwalten können. Horizon Console integriert auch die VMware Horizon Just-in-Time Management Platform (JMP) Integrated Workflow-Funktionen für die Verwaltung von Arbeitsumgebungen.

Horizon Console ist nach der Installation und Konfiguration des Horizon-Verbindungsservers verfügbar.

Weitere Informationen zu den Funktionen für den integrierten JMP-Workflow finden Sie unter [Kapitel 10 Erste Schritte mit JMP Integrated Workflow](#).

Dieses Kapitel enthält die folgenden Themen:

- [Unterstützte Horizon 7-Funktionen](#)
- [Vorteile der Verwendung von Horizon Console](#)
- [Installieren und Konfigurieren von Horizon Console](#)
- [Anmelden bei Horizon Console](#)

Unterstützte Horizon 7-Funktionen

Horizon Console basiert auf der HTML5-Technologie und ermöglicht Ihnen, Ihre vollständige Horizon 7-Bereitstellung zu verwalten. Horizon Console ersetzt den Flash-basierten Horizon Administrator.

Weitere Informationen zu Horizon 7-Funktionen, die in Horizon Administrator unterstützt werden, finden Sie im Dokument *Horizon 7-Verwaltung*.

Die folgenden Funktionen werden unterstützt:

- Server
 - Horizon-Verbindungsserver-Konfiguration
 - Ereignisdatenbank
- Berechtigungen
 - Benutzer- und Gruppenberechtigungen
 - Desktop-Berechtigungen

- Anwendungsberechtigungen
- Globale Berechtigungen
- Globale Richtlinien
- Authentifizierung
 - Remotezugriff-Authentifizierung
 - Nicht authentifizierter Zugriff auf veröffentlichte Anwendungen
 - Smartcard-Authentifizierung
 - Rollenbasierte Verwaltungsdelegation
- Virtuelle Desktops
 - Automatisierte, dedizierte Zuweisungspools mit vollständigen virtuellen Maschinen
 - Automatisiert, Instant Clone, dedizierte Zuweisung und dynamische Zuweisung, Pools
 - Automatisierte Desktop-Pools mit Linked Clones
 - Automatisierte, dynamische Zuweisungspools mit vollständigen virtuellen Maschinen
 - Manuelle Desktop-Pools
 - Persistente Festplatten
- Veröffentlichte Desktops
 - Manuelle Farmen
 - Automatisierte Instant-Clone-Farm
 - Automatisierte Linked-Clone-Farmen
 - RDS-Desktop-Pools
- Veröffentlichte Anwendungen
 - Manuelle Anwendungspools
 - Anwendungspools von bestehenden Anwendungen
- Virtuelle Maschinen
 - In vCenter Server verfügbare virtuelle Maschinen
 - Registrierte Maschinen, die nicht in vCenter Server verfügbar sind
- Cloud-Pod-Architektur

Die folgenden Funktionen werden nicht unterstützt:

- ThinApp-Anwendungen
- Sicherheitsserver
- Mirage-Server

Vorteile der Verwendung von Horizon Console

Die Verwendung von Horizon Console hat den Vorteil einer leichteren Desktop- und Anwendungsbereitstellung, einer rechtzeitigen Desktopbereitstellung und einer höheren Sicherheit der Webschnittstelle zur Ausschaltung von Sicherheitsrisiken.

Die Horizon Console-Webschnittstelle wird aktualisiert mit benutzerfreundlichen Arbeitsabläufen zur Bereitstellung und Fehlerbehebung von Desktops und Anwendungen.

Horizon Console enthält auch die JMP Integrated Workflow-Funktionen, die Instant Clone, VMware App Volumes und VMware Dynamic Environment Manager-Technologien in einen integrierten Arbeitsablauf integrieren, um Desktops nach Bedarf und schnell bereitzustellen und zu skalieren. Weitere Informationen finden Sie unter [Informationen zu JMP Integrated Workflow](#).

Horizon Console bietet eine HTML5-basierte Webschnittstelle, die sicherer ist und aktualisiert wurde, um viele Sicherheitsrisiken und Schwachstellen auszuschalten.

Installieren und Konfigurieren von Horizon Console

Die Horizon Console-URL ist auf der Horizon Administrator-Weboberfläche verfügbar, nachdem Sie den Verbindungsserver mit dem Horizon-Verbindungsserver-Installationsprogramm installiert und konfiguriert haben. Der JMP Integrated Workflow ist in Horizon Console verfügbar, nachdem Sie mithilfe des JMP-Server-Installationsprogramms den JMP-Server installiert und konfiguriert haben.

Weitere Informationen zur Installation des Verbindungsservers finden Sie im Dokument *Horizon 7-Installation*.

Informationen zum Installieren und Konfigurieren des JMP-Servers finden Sie im Dokument *VMware Horizon JMP Server Installations- und Einrichtungshandbuch*.

Anmelden bei Horizon Console

Sie müssen sich bei Horizon Console anmelden, um Desktop- oder Anwendungspool-Aufgaben und Fehlerbehebungsaufgaben durchführen sowie JMP-Arbeitsabläufe verwalten zu können. Sie können unter Verwendung einer sicheren Verbindung (TLS) auf Horizon Console zugreifen.

Voraussetzungen

- Stellen Sie sicher, dass der Horizon-Verbindungsserver auf einem dedizierten Computer installiert ist.
- Einem Benutzer muss eine vordefinierte Rolle oder eine Kombination aus vordefinierten Rollen zugewiesen werden, um sich bei Horizon Console anmelden zu können. Sie können sich nicht bei Horizon Console anmelden, wenn dem Benutzer eine benutzerdefinierte Rolle oder eine Kombination aus vordefinierten und benutzerdefinierten Rollen zugewiesen ist. Weitere Informationen zum Konfigurieren des rollenbasierten Zugriffs finden Sie unter [Konfigurieren der rollenbasierten Verwaltungsdelegation](#).
- Vergewissern Sie sich, dass Sie einen von Horizon Console unterstützten Webbrowser verwenden. Weitere Informationen zu unterstützten Webbrowsern finden Sie im Dokument *Horizon 7-Installation*.

Verfahren

- 1 Öffnen Sie Ihren Webbrowser und geben Sie die folgende URL ein. Hierbei steht *Server* für den Hostnamen der Verbindungsserver-Instanz.

https://*Server*/admin

Hinweis Um auf eine Verbindungsserver-Instanz zuzugreifen, deren Hostname nicht aufgelöst werden kann, können Sie die IP-Adresse verwenden. Der Host, den Sie kontaktieren, passt jedoch nicht zum TLS-Zertifikat, das für die Verbindungsserver-Instanz konfiguriert ist. Dies führt dazu, dass der Zugriff blockiert wird oder weniger sicher ist.

Ihr Zugriff auf Horizon Console hängt von der Art des Zertifikats ab, das auf dem Verbindungsserver-Computer konfiguriert ist.

Wenn Sie den Webbrowser auf dem Verbindungsserver-Host öffnen, verwenden Sie für die Verbindung **https://127.0.0.1** anstelle von **https://localhost**. Diese Methode ist sicherer, da mögliche DNS-Angriffe bei der localhost-Auflösung vermieden werden.

Option	Beschreibung
Sie haben ein Zertifikat konfiguriert, das von einer Zertifizierungsstelle für Verbindungsserver signiert ist.	Wenn Sie zum ersten Mal eine Verbindung herstellen, zeigt Ihr Webbrowser die Seite Willkommen bei VMware Horizon 7 an.
Das standardmäßige selbstsignierte Zertifikat, das mit dem Verbindungsserver bereitgestellt wird, ist konfiguriert.	Bei der ersten Verbindungsherstellung zeigt Ihr Webbrowser möglicherweise eine Warnung an, nach der das mit der Adresse verknüpfte Sicherheitszertifikat nicht durch eine vertrauenswürdige Zertifizierungsstelle ausgegeben wurde. Klicken Sie auf Ignorieren , um unter Verwendung des aktuellen TLS-Zertifikats fortzufahren.

- 2 Um immer die Horizon Console-Anmeldeseite zu verwenden, klicken Sie auf **Immer diese Option verwenden**.

Hinweis Wenn Sie auf **Immer diese Option verwenden** und auf **Start** klicken, wird ab dem nächsten Mal immer die Horizon Console-Anmeldeseite angezeigt, sobald Sie eine Registerkarte im Webbrowser öffnen und **https://server/admin** eingeben. Um erneut auf die Seite **Willkommen bei VMware Horizon 7** zuzugreifen, wechseln Sie zu **https://server/admin/#home**.

- 3 Klicken Sie unter Horizon Console auf **Start**, um die Horizon Console-Anmeldeseite zu öffnen.
- 4 Melden Sie sich als Benutzer mit Anmeldedaten an, um auf das Administratorkonto zuzugreifen.

Sie führen zum ersten Mal eine Zuweisung zur Administratorrolle durch, wenn Sie eine eigenständige Verbindungsserver-Instanz oder die erste Verbindungsserver-Instanz in einer replizierten Gruppe installieren. Standardmäßig wird das Konto ausgewählt, das Sie zum Installieren des Verbindungsservers verwenden. Sie können dieses Konto jedoch zur lokalen Gruppe der Administratoren oder zu einer globalen Domänengruppe ändern.

Wenn Sie die lokale Gruppe der Administratoren wählen, können Sie jeden Domänenbenutzer verwenden, der direkt oder über eine globale Gruppenmitgliedschaft zu dieser Gruppe hinzugefügt wurde. Sie können keine zu dieser Gruppe hinzugefügten lokalen Benutzer verwenden.

Nächste Schritte

Um den CPA-Pod oder den Clusternamen des Verbindungsservers zu identifizieren, mit dem Sie arbeiten, können Sie den Namen in der Horizon Console-Kopfzeile und auf der Webbrowser-Registerkarte anzeigen.

Konfigurieren von Horizon-Verbindungsserver in Horizon Console

3

Nachdem Sie Horizon-Verbindungsserver installiert und die Erstkonfiguration durchgeführt haben, können Sie vCenter Server-Instanzen und Horizon Composer-Dienste zu Ihrer Horizon 7-Bereitstellung hinzufügen, Rollen erstellen, um Administratorverantwortlichkeiten zu delegieren, sowie Sicherungen Ihrer Konfigurationsdaten planen.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren von vCenter Server und Horizon Composer in Horizon Console](#)
- [Sichern von Horizon-Verbindungsserver in Horizon Console](#)
- [Konfigurieren von Einstellungen für Client-Sitzungen in Horizon Console](#)
- [Deaktivieren oder Aktivieren von Horizon-Verbindungsserver in Horizon Console](#)
- [Bearbeiten der externen URLs für Horizon-Verbindungsserver-Instanzen](#)
- [Registrieren von Gateways in Horizon Console](#)

Konfigurieren von vCenter Server und Horizon Composer in Horizon Console

Um virtuelle Maschinen als Remote-Desktops zu verwenden, müssen Sie Horizon 7 für die Kommunikation mit vCenter Server konfigurieren. Zum Erstellen und Verwalten von Linked-Clone-Desktop-Pools müssen Sie Horizon Console-Einstellungen in Horizon Composer konfigurieren.

Sie können auch Speichereinstellungen für Horizon 7 konfigurieren. Sie können ESXi-Hosts erlauben, Datenträgerplatz auf virtuellen Linked-Clone-Maschinen zurückzugewinnen. Um es ESXi-Hosts zu gestatten, Daten von virtuellen Maschinen im Cache zu speichern, müssen Sie Horizon Storage Accelerator für vCenter Server aktivieren.

Erstellen eines Benutzerkontos für Horizon Composer-AD-Vorgänge

Wenn Sie Horizon Composer verwenden, müssen Sie ein Benutzerkonto in Active Directory erstellen, damit Horizon Composer bestimmte Vorgänge in Active Directory ausführen kann. Horizon Composer benötigt dieses Konto, um virtuelle Linked-Clone-Maschinen zur Active Directory-Domäne hinzuzufügen.

Erstellen Sie ein separates Benutzerkonto zur Verwendung mit Horizon Composer zur Gewährleistung der Sicherheit. Durch das Erstellen eines separaten Kontos können Sie sicherstellen, dass keine zusätzlichen Berechtigungen für andere Zwecke gewährt werden. Sie können diesem Konto die Mindestberechtigungen erteilen, die zum Erstellen und Entfernen von Computerobjekten in einem festgelegten Active Directory-Container erforderlich sind. Beispielsweise sind die Berechtigungen eines Domänenadministrators nicht für das Horizon Composer-Konto erforderlich.

Verfahren

- 1 Erstellen Sie in Active Directory ein Benutzerkonto, das sich in derselben Domäne wie Ihr Verbindungsserver-Host oder in einer vertrauenswürdigen Domäne befindet.
- 2 Fügen Sie die Berechtigungen **Computerobjekte erstellen**, **Computerobjekte löschen** und **Alle Eigenschaften schreiben** für das Konto in dem Active Directory-Container hinzu, in dem die Linked-Clone-Computerkonten erstellt werden bzw. in den die Linked-Clone-Computerkonten verschoben werden sollen.

Die folgende Liste zeigt alle für das Benutzerkonto erforderlichen Berechtigungen, einschließlich der standardmäßig zugewiesenen Berechtigungen:

- Inhalt auflisten
- Alle Eigenschaften lesen
- Alle Eigenschaften schreiben
- Berechtigungen lesen
- Kennwort zurücksetzen
- Computerobjekte erstellen
- Computerobjekte löschen

Hinweis Weniger Berechtigungen sind erforderlich, wenn Sie die Einstellung **Wiederverwendung bereits bestehender Computerkonten zulassen** für einen Desktop-Pool auswählen. Stellen Sie sicher, dass dem Benutzerkonto die folgenden Berechtigungen zugewiesen sind:

- Inhalt auflisten
 - Alle Eigenschaften lesen
 - Berechtigungen lesen
 - Kennwort zurücksetzen
-

- 3 Stellen Sie sicher, dass die Berechtigungen für das Benutzerkonto für den Active Directory-Container und alle untergeordneten Objekte des Containers gelten.

Nächste Schritte

Geben Sie das Konto in Horizon Console an, wenn Sie Horizon Composer-Domänen im Assistenten **vCenter Server hinzufügen** konfigurieren und Linked-Clone-Desktop-Pools konfigurieren sowie bereitstellen.

Installation des Produktlizenzschlüssels in Horizon Console

Bevor Sie den Verbindungsserver verwenden können, müssen Sie einen Produktlizenzschlüssel eingeben.

Hinweis Der Lizenzschlüssel des Produkts ist nicht erforderlich, wenn Sie eine Horizon 7-Abonnementlizenz besitzen. Weitere Informationen zu Abonnementlizenzen finden Sie unter „Aktivieren von Horizon 7 für Abonnementlizenzen“ im Dokument *Horizon 7-Installation*.

Bei der ersten Anmeldung zeigt Horizon Console die Seite „Lizenzierung und Verwendung“ an.

Sie müssen keinen Lizenzschlüssel konfigurieren, wenn Sie eine replizierte Verbindungsserver-Instanz oder einen Sicherheitsserver installieren. Replizierte Instanzen und Sicherheitsserver verwenden den allgemeinen Lizenzschlüssel, der in der View LDAP-Konfiguration gespeichert ist.

Hinweis Verbindungsserver erfordern einen gültigen Lizenzschlüssel. Der Lizenzschlüssel des Produkts ist 25 Zeichen lang.

Verfahren

- 1 Wählen Sie in Horizon Console die Optionen **Einstellungen > Produktlizenzierung und -verwendung**.
- 2 Klicken Sie im Bereich **Lizenzierungseinstellungen** auf **Lizenz bearbeiten**.
- 3 Geben Sie die Seriennummer der Lizenz ein und klicken Sie auf **OK**.
- 4 Überprüfen Sie das Ablaufdatum der Lizenz.
- 5 Überprüfen Sie, ob die Lizenzen für Desktops, die Remote-Ausführung von Anwendungen sowie View Composer aktiviert oder deaktiviert sind, je nach der VMware Horizon 7-Edition, zu deren Verwendung Ihre Produktlizenz Sie berechtigt.

Nicht alle Funktionen von VMware Horizon 7 sind in allen Editionen verfügbar. Einen Funktionsvergleich der einzelnen Editionen finden Sie unter <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

Hinzufügen von vCenter Server-Instanzen zu Horizon 7 in Horizon Console

Sie müssen Horizon 7 für die Herstellung einer Verbindung mit vCenter Server-Instanzen in Ihrer Horizon 7-Bereitstellung konfigurieren. vCenter Server erstellt und verwaltet die virtuellen Maschinen, die von Horizon 7 in Desktop-Pools verwendet werden.

Wenn Sie vCenter Server-Instanzen in einer Gruppe im verknüpften Modus ausführen, muss jede vCenter Server-Instanz Horizon 7 separat hinzugefügt werden.

Horizon 7 stellt über eine sichere Verbindung (TLS) eine Verbindung mit der vCenter Server-Instanz her.

Voraussetzungen

- Installieren Sie den Verbindungsserver-Produktlizenzschlüssel.

- Erstellen Sie einen vCenter Server-Benutzer mit der Berechtigung, Vorgänge in vCenter Server auszuführen, die zur Unterstützung von Horizon 7 erforderlich sind. Wenn Sie Horizon Composer verwenden, müssen Sie dem Benutzer zusätzliche Berechtigungen gewähren.

Weitere Informationen zum Konfigurieren eines vCenter Server-Benutzers für Horizon 7 finden Sie im Dokument *Horizon 7-Installation*.

- Stellen Sie sicher, dass auf dem vCenter Server-Host ein TLS-Serverzertifikat installiert ist. Installieren Sie in einer Produktionsumgebung ein gültiges Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) signiert ist.

In einer Testumgebung können Sie das Standardzertifikat verwenden, das zusammen mit vCenter Server installiert wird. Sie müssen jedoch den Zertifikatfingerabdruck akzeptieren, wenn Sie Horizon 7 zu vCenter Server hinzufügen.

- Stellen Sie sicher, dass alle Instanzen des Verbindungsservers in der replizierten Gruppe dem Stamm-CA-Zertifikat für das Serverzertifikat vertrauen, das auf dem vCenter Server-Host installiert ist. Überprüfen Sie, ob sich das Stamm-CA-Zertifikat im Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** in den Zertifikatspeichern der lokalen Windows-Computer auf den Verbindungsserver-Hosts befindet. Ist dies nicht der Fall, importieren Sie das Stamm-CA-Zertifikat in die Zertifikatspeicher der lokalen Windows-Computer.

Siehe „Importieren eines Stammzertifikats und Zwischenzertifikats in den Windows-Zertifikatspeicher“ im Dokument *Horizon 7-Installation*.

- Stellen Sie sicher, dass die vCenter Server-Instanz ESXi-Hosts enthält. Wenn in der vCenter Server-Instanz keine Hosts konfiguriert sind, können Sie die Instanz nicht zu Horizon 7 hinzufügen.
- Wenn Sie ein Upgrade auf vSphere 5.5 oder eine höhere Version durchführen, müssen Sie sicherstellen, dass dem Domänenadministratorkonto, das Sie als Benutzer von vCenter Server verwenden, explizit Berechtigungen zur Anmeldung bei vCenter Server über einen lokalen Benutzer von vCenter Server zugewiesen wurden.
- Wenn Sie Horizon 7 im FIPS-Modus verwenden möchten, müssen Sie über Hosts mit vCenter Server 6.0 oder höher und mit ESXi 6.0 oder höher verfügen.

Weitere Informationen finden Sie unter „Installieren von Horizon 7 im FIPS-Modus“ im Dokument *Horizon 7-Installation*.

- Machen Sie sich mit den Einstellungen vertraut, die die maximalen Grenzwerte für Betriebsvorgänge für vCenter Server und Horizon Composer festlegen.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Server**.
- 2 Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen**.

- 3 Geben Sie im Textfeld **Serveradresse** der vCenter Server-Einstellungen den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) der vCenter Server-Instanz ein.

Der FQDN umfasst den Hostnamen und den Domännennamen. Beispiel: Im FQDN **myserverhost.companydomain.com** ist **myserverhost** der Hostname und **companydomain.com** die Domäne.

Hinweis Wenn Sie einen Server unter Verwendung eines DNS-Namens oder einer URL angeben, führt Horizon 7 kein DNS-Lookup durch, um zu überprüfen, ob ein Administrator Horizon 7 diesen Server zuvor unter Verwendung seiner IP-Adresse hinzugefügt hatte. Es entsteht ein Konflikt, wenn eine vCenter Server-Instanz sowohl mit dem DNS-Namen als auch mit der IP-Adresse angegeben wird.

- 4 Geben Sie den Namen des vCenter Server-Benutzers ein.

Beispiel: **domain\user** oder **user@domain.com**

- 5 Geben Sie das Kennwort für den vCenter Server-Benutzer ein.
- 6 (Optional) Geben Sie eine Beschreibung für diese vCenter Server-Instanz ein.
- 7 Geben Sie die TCP-Portnummer ein.

Der Standardport lautet 443.

- 8 (Optional) Wählen Sie **VMware Cloud on AWS** aus, wenn der vCenter Server auf VMware Cloud on AWS bereitgestellt wird.

Weitere Informationen zur Integration von Horizon 7 mit VMware Cloud on AWS finden Sie im Dokument *Horizon 7-Integration*.

- 9 Stellen Sie unter „Erweiterte Einstellungen“ die Grenzwerte für gleichzeitige Vorgänge für vCenter Server- und Horizon Composer-Vorgänge ein.
- 10 Klicken Sie auf **Weiter** und folgen Sie den Eingabeaufforderungen, um den Assistenten zu beenden.

Nächste Schritte

Konfigurieren Sie die Horizon Composer-Einstellungen.

- Wenn die vCenter Server-Instanz mit einem signierten TLS-Zertifikat konfiguriert ist und der Verbindungsserver dem Stammzertifikat vertraut, zeigt der Assistent „vCenter Server hinzufügen“ die Seite „Horizon Composer-Einstellungen“ an.
- Wenn die vCenter Server-Instanz mit einem Standardzertifikat konfiguriert ist, müssen Sie zunächst festlegen, ob der Fingerabdruck des vorhandenen Zertifikats akzeptiert werden soll. Siehe [Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats](#).

Wenn Horizon 7 mehrere vCenter Server-Instanzen verwendet, wiederholen Sie diese Schritte, um die anderen vCenter Server-Instanzen hinzuzufügen.

Konfigurieren von Horizon Composer-Einstellungen

Um Horizon Composer zu verwenden, müssen Sie Einstellungen konfigurieren, die eine Verbindung zwischen Horizon Composer und dem Horizon 7-Dienst ermöglichen. Horizon Composer kann auf seinem eigenen separaten Host oder auf demselben Host wie vCenter Server installiert werden.

Es muss eine Eins-zu-eins-Zuordnung zwischen jedem Horizon Composer-Dienst und jeder vCenter Server-Instanz geben. Ein Horizon Composer-Dienst kann jeweils nur mit einer vCenter Server-Instanz zusammenarbeiten. Eine vCenter Server-Instanz kann jeweils nur mit einem Horizon Composer-Dienst verknüpft werden.

Nach der ursprünglichen Horizon 7-Bereitstellung können Sie den Horizon Composer-Dienst auf einen neuen Host zur Unterstützung einer wachsenden oder sich ändernden Horizon 7-Bereitstellung migrieren. Sie können die ursprünglichen Horizon Composer-Einstellungen in Horizon Console bearbeiten, müssen jedoch zusätzliche Schritte ausführen, um sicherzustellen, dass die Migration erfolgreich ist.

Voraussetzungen

- Stellen Sie sicher, dass Sie in Active Directory einen Benutzer erstellt haben, der über die Berechtigung zum Hinzufügen und Entfernen virtueller Maschinen zur Active Directory-Domäne bzw. aus der Active Directory-Domäne verfügt, die Ihre Linked Clones enthält. Siehe [Erstellen eines Benutzerkontos für Horizon Composer-AD-Vorgänge](#).
- Vergewissern Sie sich, dass Horizon 7 zur Verbindungsherstellung mit vCenter Server konfiguriert wurde. Dazu müssen Sie die Seite „vCenter Server-Informationen“ im Assistenten „vCenter Server hinzufügen“ ausfüllen. Siehe [Hinzufügen von vCenter Server-Instanzen zu Horizon 7 in Horizon Console](#).
- Stellen Sie sicher, dass dieser Horizon Composer-Dienst nicht bereits konfiguriert wurde, um eine Verbindung zu einer anderen vCenter Server-Instanz herzustellen.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Server**.
- 2 Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen** und geben Sie die vCenter Server-Informationen auf der Seite **vCenter Server-Einstellungen** an. Klicken Sie dann auf **Weiter**.
- 3 Wählen Sie auf der Seite **Horizon Composer-Einstellungen** die Option **Horizon Composer nicht verwenden**, wenn Sie Horizon Composer nicht verwenden.

Wenn Sie **Horizon Composer nicht verwenden** auswählen, werden die anderen Horizon Composer-Einstellungen inaktiv. Wenn Sie auf **Weiter** klicken, zeigt der Assistent „vCenter Server hinzufügen“ die Seite **Speichereinstellungen** an.

- 4 Wenn Sie Horizon Composer verwenden, wählen Sie den Speicherort des Horizon Composer-Hosts aus.

Option	Beschreibung
Horizon Composer wird auf demselben Host installiert wie vCenter Server.	<ul style="list-style-type: none"> a Wählen Sie Horizon Composer wurde zusammen mit vCenter Server installiert. b Vergewissern Sie sich, dass die Portnummer der Portnummer entspricht, die Sie beim Installieren des Horizon Composer-Dienstes in vCenter Server angegeben haben. Die standardmäßige Portnummer lautet 18443.
Horizon Composer wird auf seinem eigenen separaten Host installiert.	<ul style="list-style-type: none"> a Wählen Sie Eigenständiger Horizon Composer-Server. b Geben Sie im Textfeld für die Horizon Composer-Serveradresse den vollqualifizierten Domänennamen (FQDN) des Horizon Composer-Hosts ein. c Geben Sie den Namen des Horizon Composer-Benutzers ein. Beispiel: domain.com\user oder user@domain.com d Geben Sie das Kennwort des Horizon Composer-Benutzers ein. e Vergewissern Sie sich, dass die Portnummer der Portnummer entspricht, die Sie beim Installieren des Horizon Composer-Dienstes angegeben haben. Die standardmäßige Portnummer lautet 18443.

- 5 Klicken Sie auf **Weiter**, um die Seite **Horizon Composer-Domänen** anzuzeigen.

Nächste Schritte

Konfigurieren Sie die Horizon Composer-Domänen.

- Wenn die Horizon Composer-Instanz mit einem signierten TLS-Zertifikat konfiguriert ist und der Verbindungsserver dem Stammzertifikat vertraut, zeigt der Assistent „vCenter Server hinzufügen“ die Seite „Horizon Composer-Domänen“ an.
- Wenn die Horizon Composer-Instanz mit einem Standardzertifikat konfiguriert ist, müssen Sie zunächst festlegen, ob der Fingerabdruck des vorhandenen Zertifikats akzeptiert werden soll.

Konfigurieren von Horizon Composer-Domänen

Sie müssen eine Active Directory-Domäne konfigurieren, in der Horizon Composer Linked-Clone-Desktops bereitstellt. Sie können mehrere Domänen für Horizon Composer konfigurieren. Nachdem Sie Horizon 7 zunächst vCenter Server- und Horizon Composer-Einstellungen hinzugefügt haben, können Sie weitere Horizon Composer-Domänen hinzufügen, indem Sie die vCenter Server-Instanz in Horizon Console bearbeiten.

Voraussetzungen

- Ihr Active Directory-Administrator muss einen Horizon Composer-Benutzer für AD-Vorgänge erstellen. Dieser Domänenbenutzer benötigt die Berechtigung zum Hinzufügen und Entfernen virtueller Maschinen in der Active Directory-Domäne, die Ihre Linked Clones enthält. Weitere Informationen zu den erforderlichen Berechtigungen für diesen Benutzer finden Sie unter [Erstellen eines Benutzerkontos für Horizon Composer-AD-Vorgänge](#).

- Stellen Sie in Horizon Console sicher, dass Sie die Seiten **vCenter Server-Einstellungen** und **Horizon Composer-Einstellungen** im Assistenten **vCenter Server hinzufügen** abgeschlossen haben.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Server**.
- 2 Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen** und geben Sie die vCenter Server-Informationen auf der Seite **vCenter Server-Einstellungen** an. Klicken Sie dann auf **Weiter**.
- 3 Wenn Sie Horizon Composer verwenden, wählen Sie auf der Seite **Horizon Composer-Einstellungen** den Speicherort des Horizon Composer-Hosts aus und klicken Sie auf **Weiter**.
Weitere Informationen zu Horizon Composer finden Sie unter [Konfigurieren von Horizon Composer-Einstellungen](#).
- 4 Klicken Sie auf der Seite **Horizon Composer-Domänen** auf **Hinzufügen**, um den Horizon Composer-Benutzer für die Kontoinformationen der AD-Vorgänge hinzuzufügen.
- 5 Geben Sie den Domänennamen der Active Directory-Domäne ein.
Beispiel: **domain.com**
- 6 Geben Sie den Domänenbenutzernamen (einschließlich des Domänennamens) des Horizon Composer-Benutzers ein.
Beispiel: **domain.com\admin**
- 7 Geben Sie das Kontokennwort ein.
- 8 Klicken Sie auf **OK**.
- 9 Um Domänenbenutzerkonten mit Berechtigungen in weiteren Active Directory-Domänen hinzuzufügen, in denen Sie Linked-Clone-Pools bereitgestellt haben, wiederholen Sie die vorangehenden Schritte.
- 10 Klicken Sie auf **Weiter**, um die Seite **Speichereinstellungen** anzuzeigen.

Nächste Schritte

Aktivieren Sie die Rückgewinnung von Festplattenspeicherplatz für virtuelle Maschinen und konfigurieren Sie Horizon Storage Accelerator für Horizon 7.

Hinzufügen eines Instant-Clone-Domänenadministrators in Horizon Console

Vor dem Erstellen eines Instant-Clone-Desktop-Pools müssen Sie Horizon 7 einen Instant-Clone-Domänenadministrator hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass der Instant-Clone-Domänenadministrator über die erforderlichen Active Directory-Domänenberechtigungen verfügt. Weitere Informationen finden Sie unter „Erstellen eines Benutzerkontos für Instant-Clone-Vorgänge“ im Dokument *Horizon 7-Installation*.

Verfahren

- 1 Wählen Sie in Horizon Console die Optionen **Einstellungen > Domänenkonten für Instant Clone** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie die Domäne für den Instant-Clone-Domänenadministrator aus.
- 4 Geben Sie den Benutzernamen und das Kennwort ein.

Nächste Schritte

In Horizon Console können Sie einen Instant-Clone-Domänenadministrator hinzufügen oder entfernen oder die Liste der Instant-Clone-Administratoren in Microsoft Excel exportieren. Navigieren Sie zu **Einstellungen > Domänenkonten für Instant Clone** und wählen Sie einen Instant-Clone-Domänenadministrator aus. Klicken Sie auf **Bearbeiten**, um die Domänen- und Anmeldeinformationen für den Administrator zu bearbeiten. Klicken Sie auf **Entfernen**, um einen Administrator zu entfernen. Klicken Sie auf das Exportsymbol, um die Liste der Instant-Clone-Administratoren in eine Microsoft Excel-Datei zu exportieren.

Zulassen, dass vSphere Speicherplatz auf virtuellen Linked-Clone-Maschinen freigibt

In vSphere Version 5.1 oder höher können Sie die Funktion zur Rückgewinnung von Festplattenspeicherplatz für Horizon 7 aktivieren. Horizon 7 erstellt virtuelle Linked-Clone-Maschinen in einem effizienten Festplattenformat, mit dem ESXi-Hosts nicht genutzten Festplattenspeicherplatz in den Linked Clones zurückgewinnen können. Dadurch kann der insgesamt erforderliche Speicherplatz für Linked Clones reduziert werden.

Wenn Benutzer mit Linked-Clone-Desktops interagieren, nimmt die Größe der Betriebssystemfestplatte der Klone zu und kann schließlich fast so viel Festplattenspeicherplatz belegen wie Full-Clone-Desktops. Durch die Zurückgewinnung von Festplattenspeicher verringert sich die Größe der Betriebssystemfestplatten, ohne dass Sie dazu die Linked Clones aktualisieren oder neu zusammenstellen müssen. Der Datenträgerplatz kann zurückgewonnen werden, während die virtuellen Maschinen eingeschaltet sind und Benutzer mit ihren Remote-Desktops interagieren.

Die Rückgewinnung von Datenträgerplatz eignet sich insbesondere für Bereitstellungen, die keine speicherplatzsparenden Strategien wie Aktualisierung oder Abmeldung nutzen können. Büroanwender beispielsweise, die Anwenderprogramme auf dedizierten Remote-Desktops installieren, könnten ihre persönlichen Anwendungen verlieren, wenn Remote-Desktops aktualisiert oder neu zusammengestellt würden. Mit der Rückgewinnung von Datenträgerplatz kann Horizon 7 Linked Clones ungefähr in der gleichen verringerten Größe erhalten, die sie bei der ersten Bereitstellung hatten.

Diese Funktion besteht aus zwei Komponenten: speicherplatzsparendes Festplattenformat und Vorgänge zur Rückgewinnung von Speicherplatz.

In vSphere Version 5.1 oder höher erstellt Horizon 7 Linked Clones mit platzsparenden Betriebssystemfestplatten, wenn eine übergeordnete virtuelle Maschine die virtuelle Hardwareversion 9 oder höher aufweist, unabhängig davon, ob Vorgänge zur Rückgewinnung von Datenträgerplatz aktiviert sind oder nicht.

Zum Aktivieren der Vorgänge zur Rückgewinnung von Festplattenspeicherplatz müssen Sie Horizon Console verwenden, um die Rückgewinnung von Festplattenspeicherplatz für vCenter Server zu aktivieren und VM-Festplattenspeicher für einzelne Desktop-Pools zurückzugewinnen. Die Einstellung für die Rückgewinnung von Datenträgerplatz für vCenter Server ermöglicht es Ihnen, diese Funktion auf allen Desktop-Pools zu deaktivieren, die von der vCenter Server-Instanz verwaltet werden. Wenn Sie die Funktion für vCenter Server deaktivieren, wird die Einstellung auf Desktop-Pool-Ebene übergangen.

Für die Funktion zur Rückgewinnung von Datenträgerplatz gelten folgende Richtlinien:

- Sie funktioniert nur auf platzsparenden Betriebssystemfestplatten in Linked Clones.
- Sie wirkt sich nicht auf persistente Horizon Composer-Festplatten aus.
- Sie funktioniert nur mit vSphere Version 5.1 oder höher auf virtuellen Maschinen, die die virtuelle Hardwareversion 9 oder höher aufweisen.
- Sie funktioniert nicht auf Full-Clone-Desktops.
- Sie funktioniert auf virtuellen Maschinen mit SCSI-Controllern. IDE-Controller werden nicht unterstützt.

Die systemeigene NFS-Snapshot-Technologie (VAAI) wird nicht in Pools unterstützt, die virtuelle Maschinen mit platzsparenden Festplatten enthalten.

Voraussetzungen

- Stellen Sie sicher, dass Ihr vCenter Server und die ESXi-Hosts, einschließlich aller ESXi-Hosts in einem Cluster, in der Version 5.1 mit ESXi 5.1-Download-Patch ESXi510-201212001 oder höher vorliegen.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Server**.
- 2 Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen** und füllen Sie die Assistentenseiten **vCenter Server hinzufügen** aus, auf die die Seite **Speichereinstellungen** folgt.
- 3 Wählen Sie auf der Seite **Speichereinstellungen** die Option **VM-Festplattenspeicher zurückgewinnen** aus.

Diese Option ist standardmäßig ausgewählt, wenn Sie eine Neuinstallation von Horizon 7 durchführen. Sie müssen **VM-Festplattenspeicher zurückgewinnen** auswählen, wenn Sie ein Upgrade auf eine höhere Version von Horizon 7 durchführen.

Nächste Schritte

Konfigurieren Sie Horizon Storage Accelerator auf der Seite **Speichereinstellungen**.

Um die Konfiguration der Rückgewinnung von Datenträgerplatz in Horizon 7 abzuschließen, richten Sie die Rückgewinnung von Datenträgerplatz für Desktop-Pools ein.

Konfigurieren von Horizon Storage Accelerator für vCenter Server

In vSphere können Sie ESXi-Hosts so konfigurieren, dass Festplattendaten von virtuellen Maschinen zwischengespeichert werden. Diese Funktion, Horizon Storage Accelerator genannt, verwendet die CBRC-Funktion (Content Based Read Cache) in ESXi-Hosts. Horizon Storage Accelerator verbessert die Leistung von Horizon 7 bei E/A-Überlastungen, die auftreten können, wenn viele virtuelle Maschinen gleichzeitig starten oder Antivirenschans ausführen. Die Funktion ist außerdem nützlich, wenn Administratoren oder Benutzer häufig Anwendungen oder Daten laden. Statt das gesamte Betriebssystem oder die gesamte Anwendung wieder und wieder aus dem Speichersystem zu lesen, kann ein Host gemeinsame Datenblöcke aus dem Cache lesen.

Durch Verringern der E/A-Vorgänge pro Sekunde bei sogenannten „Boot Storms“ senkt Horizon Storage Accelerator die Last des Speicher-Arrays. Dadurch wird weniger Speicher-E/A-Bandbreite belegt, sodass die Horizon 7-Bereitstellung unterstützt wird.

Um das Caching auf Ihren ESXi-Hosts zu aktivieren, wählen Sie die Horizon Storage Accelerator-Einstellung im Assistenten **vCenter Server hinzufügen** in Horizon Console wie in dieser Vorgehensweise beschrieben aus.

Stellen Sie sicher, dass Horizon Storage Accelerator auch für einzelne Desktop-Pools konfiguriert ist. Damit Horizon Storage Accelerator für einen Desktop-Pool genutzt werden kann, muss die Funktion sowohl für vCenter Server als auch für den jeweiligen Desktop-Pool aktiviert werden.

Horizon Storage Accelerator ist für Desktop-Pools standardmäßig aktiviert. Die Funktion kann beim Erstellen oder Bearbeiten eines Pools deaktiviert oder aktiviert werden. Es empfiehlt sich, diese Funktion zu aktivieren, wenn Sie erstmalig einen Desktop-Pool erstellen. Wenn Sie die Funktion aktivieren, indem Sie einen vorhandenen Pool bearbeiten, müssen Sie sicherstellen, dass ein neues Replikat und seine Digest-Festplatten erstellt werden, bevor Linked Clones bereitgestellt werden. Sie können ein neues Replikat erstellen, indem Sie den Pool zu einem neuen Snapshot neu zusammenstellen oder den Pool in einem neuen Datenspeicher neu verteilen. Digest-Dateien können für die virtuellen Maschinen in einem Desktop-Pool nur konfiguriert werden, wenn sie ausgeschaltet sind.

Sie können Horizon Storage Accelerator für Desktop-Pools aktivieren, die Linked Clones enthalten, und auch für Pools, die vollständige virtuelle Maschinen enthalten.

Die systemeigene NFS-Snapshot-Technologie (VAAI) wird nicht in Pools unterstützt, die für Horizon Storage Accelerator aktiviert sind.

Horizon Storage Accelerator kann nun in Konfigurationen eingesetzt werden, in denen eine mehrstufige Speicherung von Horizon 7-Replikaten verwendet wird und Replikate in einem anderen Datenspeicher gespeichert werden als Linked Clones. Wenngleich bei der Verwendung von Horizon Storage Accelerator mit der mehrstufigen Speicherung von Horizon 7-Replikaten keine erheblichen Leistungsvorteile erzielt werden, sind bestimmte Vorteile im Hinblick auf die Kapazität möglich, wenn die Replikate in einem separaten Datenspeicher gespeichert werden. Aus diesem Grund wird diese Kombination getestet und unterstützt.

Wichtig Wenn Sie diese Funktion mit mehreren Horizon 7-Pods verwenden möchten, die gemeinsam einige ESXi-Hosts nutzen, müssen Sie die Horizon Storage Accelerator-Funktion für alle Pools auf den gemeinsam genutzten ESXi-Hosts aktivieren. Sind die Einstellungen für mehrere Pods nicht einheitlich, kann dies zur Instabilität der virtuellen Maschinen auf den gemeinsam genutzten ESXi-Hosts führen.

Voraussetzungen

- Stellen Sie sicher, dass Ihr vCenter Server und Ihre ESXi-Hosts in der Version 5.1 oder höher vorliegen.
Überprüfen Sie in einem ESXi-Cluster, ob alle Hosts mindestens in der Version 5.1 ausgeführt werden.
- Stellen Sie sicher, dass dem vCenter Server-Benutzer die Berechtigung **Host > Konfiguration > Erweiterte Einstellungen** in vCenter Server zugewiesen wurde.
Lesen Sie dazu die Themen im Dokument *Horizon 7-Installation*, in denen die Horizon 7- und Horizon Composer-Rechte beschrieben werden, die der vCenter Server-Benutzer benötigt.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Server**.
- 2 Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen** und füllen Sie die Assistentenseiten **vCenter Server hinzufügen** aus, auf die die Seite **Speichereinstellungen** folgt.
- 3 Wählen Sie auf der Seite **Speichereinstellungen** die Option **Horizon-Speicherbeschleunigung aktivieren** aus.
Diese Option ist standardmäßig ausgewählt.
- 4 Geben Sie eine standardmäßige Größe für den Host-Cache an.
Diese Größe gilt für alle ESXi-Hosts, die von dieser vCenter Server-Instanz verwaltet werden.
Der Standardwert ist 1.024 MB. Die Cachegröße muss zwischen 100 MB und 2.048 MB betragen.
- 5 Um für einen einzelnen ESXi-Host eine andere Cachegröße anzugeben, wählen Sie einen ESXi-Host aus, und klicken Sie auf **Cachegröße bearbeiten**.
 - a Aktivieren Sie im Dialogfeld „Host-Cache“ das Kontrollkästchen **Standard-Hostzwischen Speichergöße außer Kraft setzen**.
 - b Geben Sie unter **Größe des Host-Caches** einen Wert zwischen 100 MB und 2.048 MB an, und klicken Sie auf **OK**.

- 6 Klicken Sie auf der Seite mit den Speichereinstellungen auf **Weiter**.
- 7 Klicken Sie nach der Überprüfung der Einstellungen auf der Seite **Bereit zum Abschließen** auf **Senden**.

Nächste Schritte

Konfigurieren Sie die Einstellungen für Clientsitzungen und -verbindungen. Weitere Informationen finden Sie unter „Konfigurieren von Einstellungen für Clientsitzungen“ im Dokument *Horizon 7-Verwaltung*.

Um die Horizon Storage Accelerator-Einstellungen in Horizon 7 abzuschließen, konfigurieren Sie Horizon Storage Accelerator für Desktop-Pools. Weitere Informationen finden Sie unter „Konfigurieren der Horizon-Speicherbeschleunigung für Desktop-Pools“ im Dokument *Einrichten von virtuellen Desktops in Horizon Console*.

Grenzwerte für parallele Vorgänge für vCenter Server und Horizon Composer

Wenn Sie vCenter Server zu Horizon 7 hinzufügen oder die vCenter Server-Einstellungen bearbeiten, können Sie mehrere Optionen konfigurieren, die die maximale Anzahl an parallelen Vorgängen festlegen, die von vCenter Server und Horizon Composer ausgeführt werden.

Sie konfigurieren diese Optionen im Bereich „Erweiterte Einstellungen“ auf der Seite **vCenter Server-Einstellungen** im Assistenten **vCenter Server hinzufügen**.

Tabelle 3-1. Grenzwerte für parallele Vorgänge für vCenter Server und Horizon Composer

Einstellung	Beschreibung
Maximale Anzahl paralleler vCenter-Bereitstellungsvorgänge	<p>Legt die maximale Anzahl paralleler Anforderungen fest, die ein Verbindungsserver zum Bereitstellen und Löschen vollständiger virtueller Maschinen in dieser vCenter Server-Instanz senden kann.</p> <p>Der Standardwert lautet 20.</p> <p>Diese Einstellung gilt nur für vollständige virtuelle Maschinen.</p>
Maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands	<p>Legt die maximale Anzahl an parallelen Betriebsvorgängen fest (Starten, Herunterfahren, Anhalten usw.), die auf virtuellen Maschinen ausgeführt werden können, die in dieser vCenter Server-Instanz von einem Verbindungsserver verwaltet werden.</p> <p>Der Standardwert ist 50.</p> <p>Richtlinien zum Berechnen eines Wertes für diese Einstellung finden Sie unter Einstellen der Anzahl paralleler Vorgänge zum Ändern des Betriebszustands, um Remote-Desktop-Anmeldungsüberlastungen zu unterstützen</p> <p>Diese Einstellung gilt für vollständige virtuelle Maschinen und Linked Clones.</p>

Tabelle 3-1. Grenzwerte für parallele Vorgänge für vCenter Server und Horizon Composer (Fortsetzung)

Einstellung	Beschreibung
Maximal mögliche gleichzeitige Horizon Composer-Wartungsvorgänge	<p>Legt die maximale Anzahl an parallelen Horizon Composer-Vorgängen zur Aktualisierung, Neuzusammenstellung und Neuverteilung fest, die auf den Linked Clones ausgeführt werden können, die von dieser Horizon Composer-Instanz verwaltet werden.</p> <p>Der Standardwert ist 12.</p> <p>Remote-Desktops mit aktiven Sitzungen müssen abgemeldet werden, bevor ein Wartungsvorgang ausgeführt werden kann. Wenn Sie Benutzer zur Abmeldung zwingen, sobald ein Wartungsvorgang beginnt, entspricht die maximale Anzahl paralleler Vorgänge auf Remote-Desktops, die eine Abmeldung erfordern, der Hälfte des konfigurierten Wertes. Wenn Sie für diese Einstellung beispielsweise den Wert 24 konfigurieren und Benutzer zur Abmeldung zwingen, sind maximal 12 parallele Vorgänge auf Remote-Desktops möglich, die Abmeldungen erfordern.</p> <p>Diese Einstellung gilt nur für Linked Clones.</p>
Maximal mögliche gleichzeitige Horizon Composer-Bereitstellungsvorgänge	<p>Legt die maximale Anzahl an parallelen Erstellungs- und Löschvorgängen fest, die auf Linked Clones ausgeführt werden können, die von dieser Horizon Composer-Instanz verwaltet werden.</p> <p>Der Standardwert ist 8.</p> <p>Diese Einstellung gilt nur für Linked Clones.</p>
Maximal mögliche gleichzeitige Vorgänge für Instant Clone-Engines	<p>Legt die maximale Anzahl an parallelen Erstellungs- und Löschvorgängen fest, die auf Instant Clones ausgeführt werden können, die von dieser vCenter Server-Instanz verwaltet werden.</p> <p>Diese Einstellung gilt nur für Instant Clones.</p>

Einstellen der Anzahl paralleler Vorgänge zum Ändern des Betriebszustands, um Remote-Desktop-Anmeldungsüberlastungen zu unterstützen

Die Einstellung **Maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands** legt die maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands fest, die auf virtuellen Remote-Desktop-Maschinen in einer vCenter Server-Instanz stattfinden können. Diese Obergrenze ist standardmäßig auf 50 festgelegt. Sie können diesen Wert ändern, um Einschaltzeiten zu Spitzenzeiten zu unterstützen, während derer sich viele Benutzer gleichzeitig bei ihren Desktops anmelden.

Die empfohlene Vorgehensweise besteht darin, während einer Pilotphase den korrekten Wert für diese Einstellung zu ermitteln. Als Planungshilfe lesen Sie „Architekturentwurfselemente und Planungsanleitungen“ im Dokument *Planung der Horizon 7-Architektur*.

Die erforderliche Anzahl paralleler Vorgänge zum Ändern des Betriebszustands basiert auf der Spitzenrate, mit der Desktops eingeschaltet werden, sowie der Zeit, die für das Einschalten, Booten und Verfügbarwerden für eine Verbindung benötigt wird. Im Allgemeinen entspricht der empfohlene Maximalwert für Betriebsvorgänge der Gesamtzeit, die der Desktop zum Starten benötigt, multipliziert mit der Spitzenrate für Einschaltvorgänge.

Der durchschnittliche Desktop benötigt beispielsweise zwei bis drei Minuten zum Starten. Daher sollte die maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands dreimal so hoch wie die Spitzenrate für Einschaltvorgänge sein. Bei einer Standardeinstellung von 50 wird erwartet, dass eine Einschalttrate von 16 Desktops pro Minute während Spitzenzeiten unterstützt wird.

Das System wartet maximal fünf Minuten auf den Start eines Desktops. Wenn die Startzeit länger ist, können andere Fehler auftreten. Wenn Sie vorsichtig sein möchten, legen Sie eine maximale Anzahl paralleler Vorgänge zum Ändern des Betriebszustands fest, die fünf Mal höher als die Einschalttrate während Spitzenzeiten ist. Bei einer vorsichtigen Herangehensweise unterstützt die Standardeinstellung 50 eine Einschalttrate während Spitzenzeiten von 10 Desktops pro Minute.

Anmeldungen und daher Desktop-Einschaltvorgänge finden üblicherweise auf normal verteilte Weise während eines bestimmten Zeitfensters statt. Sie können die Einschalttrate während Spitzenzeiten in etwa ermitteln, indem Sie annehmen, dass diese in der Mitte des Zeitfensters auftritt, während der ungefähr 40 Prozent der Einschaltvorgänge in einem Sechstel des Zeitfensters erfolgen. Wenn sich Benutzer beispielsweise zwischen 8:00 und 9:00 Uhr morgens anmelden, beträgt das Zeitfenster eine Stunde, und 40 Prozent dieser Anmeldungen erfolgen in den zehn Minuten zwischen 8:25 und 8:35 Uhr. Wenn es 2.000 Benutzer gibt, von denen 20 Prozent ihre Desktops ausgeschaltet haben, dann erfolgen 40 Prozent der 400 Desktop-Einschaltvorgänge während dieser zehn Minuten. Die Einschalttrate während Spitzenzeiten beträgt 16 Desktops pro Minute.

Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats

Wenn Sie vCenter Server- und Horizon Composer-Instanzen zu Horizon 7 hinzufügen, müssen Sie sicherstellen, dass die TLS-Zertifikate, die für vCenter Server- und Horizon Composer-Instanzen verwendet werden, gültig sind und vom Verbindungsserver als vertrauenswürdig anerkannt werden. Wenn die mit vCenter Server und Horizon Composer installierten Standardzertifikate immer noch an Ort und Stelle sind, müssen Sie festlegen, ob Sie die Fingerabdrücke dieser Zertifikate akzeptieren wollen.

Wenn eine vCenter Server- oder Horizon Composer-Instanz mit einem Zertifikat konfiguriert ist, das von einer Zertifizierungsstelle (CA) signiert ist, und das Stammzertifikat vom Verbindungsserver als vertrauenswürdig anerkannt wird, müssen Sie den Fingerabdruck des Zertifikats nicht akzeptieren. Es sind keine Schritte erforderlich.

Wenn Sie ein Standardzertifikat durch ein von einer Zertifizierungsstelle signiertes Zertifikat ersetzen, der Verbindungsserver das Stammzertifikat jedoch nicht als vertrauenswürdig einstuft, müssen Sie festlegen, ob der Zertifikatfingerabdruck akzeptiert wird. Bei einem Fingerabdruck handelt es sich um einen kryptografischen Hash-Wert eines Zertifikats. Anhand des Fingerabdrucks wird rasch ermittelt, ob ein Zertifikat mit einem anderen Zertifikat übereinstimmt (z. B. mit dem zuvor akzeptierten Zertifikat).

Hinweis Wenn Sie vCenter Server und Horizon Composer auf demselben Windows Server-Host installieren, können sie dasselbe TLS-Zertifikat verwenden, aber Sie müssen das Zertifikat separat für jede Komponente konfigurieren.

Einzelheiten zur Konfiguration von TLS-Zertifikaten finden Sie unter „Konfigurieren von TLS-Zertifikaten für Horizon 7-Server“ im Dokument *Horizon 7-Installation*.

Sie fügen zunächst vCenter Server und Horizon Composer in Horizon Console mithilfe des Assistenten **vCenter Server hinzufügen** hinzu. Wenn ein Zertifikat nicht als vertrauenswürdig eingestuft wird und Sie den Fingerabdruck nicht akzeptieren, können Sie vCenter Server und vCenter Server nicht hinzufügen.

Nachdem diese Server hinzugefügt wurden, können Sie sie im Dialogfeld **vCenter Server bearbeiten** neu konfigurieren.

Hinweis Ein Zertifikatfingerabdruck muss außerdem akzeptiert werden, wenn Sie eine Aktualisierung von einer früheren Version durchführen und ein vCenter Server- oder Horizon Composer-Zertifikat als nicht vertrauenswürdig eingestuft wird. Gleiches gilt, wenn Sie ein vertrauenswürdiges Zertifikat durch ein nicht vertrauenswürdiges Zertifikat ersetzen.

Verfahren

- 1 Klicken Sie auf **Zertifikat anzeigen**, wenn Horizon Console das Dialogfeld „Ungültiges Zertifikat ermittelt“ anzeigt.
- 2 Überprüfen Sie den Zertifikatfingerabdruck im Fenster mit den Zertifikatsinformationen.
- 3 Untersuchen Sie den Fingerabdruck des Zertifikats, das für die vCenter Server- oder Horizon Composer-Instanz konfiguriert wurde.
 - a Starten Sie auf dem vCenter Server- oder Horizon Composer-Host das MMC-Snap-In und öffnen Sie den Windows-Zertifikatspeicher.
 - b Navigieren Sie zum vCenter Server- oder Horizon Composer-Zertifikat.
 - c Klicken Sie auf die Registerkarte mit den Zertifikatsdetails, um den Zertifikatfingerabdruck anzuzeigen.

Untersuchen Sie den Zertifikatfingerabdruck gleichermaßen auf einen SAML-Authentifikator. Führen Sie die vorstehenden Schritte gegebenenfalls auf dem SAML-Authentifikatorhost aus.

- 4 Überprüfen Sie, ob der Fingerabdruck im Fenster der Zertifikatsinformationen mit dem Fingerabdruck für die vCenter Server- oder die Horizon Composer-Instanz übereinstimmt.

Überprüfen Sie ebenfalls, ob die Fingerabdrücke für einen SAML-Authentifikator übereinstimmen.
- 5 Geben Sie an, ob der Zertifikatfingerabdruck akzeptiert wird.

Option	Beschreibung
Die Fingerabdrücke stimmen überein.	Klicken Sie auf Akzeptieren , um das Standardzertifikat zu verwenden.
Die Fingerabdrücke stimmen nicht überein.	Klicken Sie auf Ablehnen . Behandeln Sie das Problem der nicht übereinstimmenden Zertifikate. Möglicherweise haben Sie z. B. eine falsche IP-Adresse für vCenter Server oder Horizon Composer angegeben.

Entfernen einer vCenter Server-Instanz aus Horizon 7

Sie können die Verbindung zwischen Horizon 7 und einer vCenter Server-Instanz entfernen. Dann werden in Horizon 7 die virtuellen Maschinen, die in dieser vCenter Server-Instanz erstellt wurden, nicht mehr verwaltet.

Voraussetzungen

Löschen Sie alle virtuellen Maschinen, die mit der vCenter Server-Instanz verknüpft sind. Weitere Informationen zum Löschen virtueller Maschinen finden Sie unter „Löschen eines Desktop-Pools“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Server**.
- 2 Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz aus.
- 3 Klicken Sie auf **Entfernen**.

Sie werden über ein Dialogfeld gewarnt, dass Horizon 7 über keinen Zugriff auf die virtuellen Maschinen mehr verfügt, die von dieser vCenter Server-Instanz verwaltet werden.

- 4 Klicken Sie auf **OK**.

Horizon 7 kann nicht länger auf die virtuellen Maschinen zugreifen, die in der vCenter Server-Instanz erstellt wurden.

Entfernen von Horizon Composer aus Horizon 7

Sie können die Verbindung zwischen Horizon 7 und dem Horizon Composer-Dienst, der mit einer vCenter Server-Instanz verknüpft ist, entfernen.

Bevor Sie die Verbindung mit Horizon Composer deaktivieren, müssen Sie alle von Horizon Composer erstellten virtuellen Linked-Clone-Maschinen aus Horizon 7 entfernen. Horizon 7 verhindert, dass Sie Horizon Composer entfernen, wenn noch Linked Clones vorhanden sind. Nachdem die Verbindung zu Horizon Composer deaktiviert wurde, kann Horizon 7 neue Linked Clones weder bereitstellen noch verwalten.

Verfahren

- 1 Entfernen Sie die von Horizon Composer erstellten Linked-Clone-Desktop-Pools.
 - a Wählen Sie in Horizon Console die Optionen **Bestandsliste > Desktops** aus.
 - b Wählen Sie einen Desktop-Pool mit Linked Clones aus und klicken Sie auf **Löschen**.

Sie werden über ein Dialogfeld gewarnt, dass Sie den Desktop-Pool mit Linked Clones endgültig aus Horizon 7 löschen. Wenn die virtuellen Linked-Clone-Maschinen mit persistenten Festplatten konfiguriert sind, können Sie die persistenten Festplatten trennen oder löschen.

- c Klicken Sie auf **OK**.

Die virtuellen Maschinen werden aus vCenter Server gelöscht. Darüber hinaus werden die zugehörigen Horizon Composer-Datenbankeinträge und die von Horizon Composer erstellten Replikate entfernt.

- d Wiederholen Sie diese Schritte für jeden von Horizon Composer erstellten Linked-Clone-Desktop-Pool.

- 2 Navigieren Sie zu **Einstellungen > Server**.

- 3 Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz, mit der Horizon Composer verknüpft ist, aus.

- 4 Klicken Sie auf **Bearbeiten**.

- 5 Wählen Sie auf der Registerkarte **Horizon Composer** unter „Horizon Composer Server-Einstellungen“ die Option **Horizon Composer nicht verwenden** aus und klicken Sie auf **OK**.

In dieser vCenter Server-Instanz können Sie keine Desktop-Pools mit Linked Clones mehr erstellen, es ist jedoch weiterhin möglich, in der vCenter Server-Instanz vollständige VM-Desktop-Pools zu erstellen und zu verwalten.

Nächste Schritte

Falls Sie vorhaben, Horizon Composer auf einem anderen Host zu installieren und Horizon 7 neu zu konfigurieren, um eine Verbindung zum neuen Horizon Composer-Dienst herzustellen, müssen Sie bestimmte zusätzliche Schritte durchführen. Weitere Informationen zum Migrieren von Horizon Composer ohne virtuelle Linked-Clone-Maschinen finden Sie im Dokument *Horizon 7-Verwaltung*.

Konflikte bei eindeutigen IDs für vCenter Server

Wenn Sie mehrere vCenter Server-Instanzen in Ihrer Umgebung konfiguriert haben, kann das Hinzufügen einer neuen Instanz aufgrund von Konflikten bei eindeutigen IDs fehlschlagen.

Problem

Sie versuchen eine vCenter Server-Instanz zu Horizon 7 hinzuzufügen, die eindeutige ID der neuen vCenter Server-Instanz erzeugt jedoch einen Konflikt mit einer vorhandenen Instanz.

Ursache

Zwei vCenter Server-Instanzen können nicht dieselbe eindeutige ID verwenden. Standardmäßig wird die eindeutige vCenter Server-ID zufällig generiert, Sie können die ID jedoch bearbeiten.

Lösung

- 1 Klicken Sie in vSphere Client auf **Verwaltung > vCenter Server-Einstellungen > Laufzeiteinstellungen**.

- 2 Geben Sie eine neue eindeutige ID ein und klicken Sie auf **OK**.

Details zum Bearbeiten von eindeutigen vCenter Server-IDs finden Sie in der Dokumentation zu vSphere.

Sichern von Horizon-Verbindungsserver in Horizon Console

Nachdem Sie die anfängliche Konfiguration des Horizon-Verbindungservers abgeschlossen haben, sollten Sie regelmäßige Sicherungen Ihrer Horizon 7- und Horizon Composer-Konfigurationsdaten planen.

Informationen zum Sichern und Wiederherstellen Ihrer Horizon 7-Konfiguration finden Sie unter [Sichern von Horizon-Verbindungsserver- und Horizon Composer-Daten](#).

Konfigurieren von Einstellungen für Client-Sitzungen in Horizon Console

Sie können globale Einstellungen für die Clientsitzungen und -verbindungen konfigurieren, die von einer Verbindungsserver-Instanz oder replizierten Gruppe verwaltet werden. Sie können die Dauer bis zur Zeitüberschreitung von Sitzungen festlegen, Meldungen vor der Anmeldung und Warnmeldungen anzeigen sowie sicherheitsbezogene Clientverbindungsoptionen festlegen.

Globale Einstellungen für Clientsitzungen Horizon Console

Allgemeine globale Einstellungen bestimmen die Dauer bis zur Zeitüberschreitung von Sitzungen, SSO-Aktivierung und Zeitüberschreitungslimits sowie Statusaktualisierungen in Horizon Console. Sie bestimmen außerdem, ob Meldungen vor der Anmeldung und Warnmeldungen angezeigt werden und ob Windows Server von Horizon Console als unterstütztes Betriebssystem für Remote-Desktops behandelt wird, sowie weitere Einstellungen.

In Horizon Console können Sie globale Einstellungen konfigurieren, indem Sie zu **Einstellungen > Globale Einstellungen > Allgemeine Einstellungen** navigieren.

Änderungen an sämtlichen Einstellungen in der folgenden Tabelle werden sofort wirksam. Der Horizon 7-Verbindungsserver oder Horizon Client müssen nicht neu gestartet werden.

Tabelle 3-2. Allgemeine globale Einstellungen für Clientsitzungen

Einstellung	Beschreibung
Zeitüberschreitung für View Administrator-Sitzung	<p>Bestimmt, wie lange eine Horizon Console-Sitzung im Leerlauf bleibt, bevor die Sitzung abläuft.</p> <hr/> <p>Wichtig Wenn Sie den Zeitüberschreitungszeitpunkt für die Horizon Console-Sitzung auf eine hohe Minutenzahl einstellen, steigt das Risiko, dass Horizon Console unautorisiert genutzt wird. Seien Sie vorsichtig, wenn Sie zulassen, dass eine Sitzung lange Zeit im Leerlauf bleibt.</p> <hr/> <p>Standardmäßig beträgt die Zeitüberschreitung für die Horizon Console-Sitzung 30 Minuten. Sie können als Zeitüberschreitung für eine Sitzung 10 bis 4.320 Minuten (72 Stunden) festlegen.</p> <p>Vor der Zeitüberschreitung einer Sitzung wird eine Warnmeldung mit einem Countdown von 60 Sekunden angezeigt. Wenn Sie vor dem Ende des Countdowns in der Sitzung klicken, wird diese fortgesetzt. Nach 60 Sekunden wird eine Fehlermeldung angezeigt, die Sie darüber informiert, dass die Sitzung abgelaufen ist und Sie sich erneut anmelden müssen.</p>
Trennung der Benutzer erzwingen	<p>Trennt nach Ablauf der angegebenen Anzahl von Minuten seit der Anmeldung des Benutzers bei Horizon 7 alle Desktops und Anwendungen. Alle Desktops und Anwendungen werden gleichzeitig getrennt, unabhängig davon, wann der Benutzer sie geöffnet hat.</p> <p>Für Clients, die die Remote-Ausführung von Anwendungen nicht unterstützen, gilt für das maximale Zeitlimit ein Wert von 1200 Minuten, wenn der Wert dieser Einstellung auf Nie gesetzt wurde oder 1200 Minuten übersteigt.</p> <p>Die Standardeinstellung ist Nach 600 Minuten.</p>
Einmalige Anmeldung (Single Sign-On, SSO)	<p>Bei aktivierter SSO werden die Anmeldeinformationen eines Benutzers von Horizon 7 zwischengespeichert, sodass der Benutzer Remote-Desktops oder -anwendungen starten kann, ohne Anmeldedaten für eine Anmeldung bei der Remote-Windows-Sitzung angeben zu müssen. Der Standard ist Aktiviert.</p> <p>Wenn Sie die True SSO-Funktion verwenden möchten, die mit Horizon 7 oder späteren Versionen eingeführt wurde, muss „SSO“ aktiviert sein. True SSO verfährt wie folgt: Wenn sich ein Benutzer mit einer anderen Authentifizierungsmethode als mit den Active Directory-Anmeldeinformationen anmeldet, generiert die True SSO-Funktion kurzfristige Zertifikate, die anstelle der zwischengespeicherten Anmeldeinformationen verwendet werden, nachdem sich der Benutzer bei VMware Identity Manager angemeldet hat.</p> <hr/> <p>Hinweis Wenn ein Desktop über Horizon Client gestartet wird und dieser Desktop gesperrt ist, sei es durch den Benutzer oder durch Windows auf der Grundlage einer Sicherheitsrichtlinie, und wenn auf diesem Desktop Horizon 7 Agent 6.0 oder höher oder Horizon Agent 7.0 oder höher ausgeführt wird, werden die SSO-Anmeldedaten des Benutzers vom Horizon 7-Verbindungsserver verworfen. Der Benutzer muss seine Anmeldedaten angeben, um einen neuen Desktop oder eine neue Anwendung zu starten, oder sich erneut mit getrennten Desktops oder Anwendungen verbinden. Um SSO erneut zu aktivieren, muss der Benutzer zunächst die Verbindung zum Horizon 7-Verbindungsserver trennen oder Horizon Client beenden und eine erneute Verbindung zum Horizon 7-Verbindungsserver herstellen. Wenn der Desktop jedoch aus Workspace ONE oder VMware Identity Manager gestartet wurde und gesperrt ist, werden die SSO-Anmeldeinformationen nicht verworfen.</p>

Tabelle 3-2. Allgemeine globale Einstellungen für Clientsitzungen (Fortsetzung)

Einstellung	Beschreibung
Automatische Status-Updates aktivieren	<p>Legt fest, ob Statusaktualisierungen in der globalen Statusanzeige im oberen linken Bereich von Horizon Console mit einem Intervall von wenigen Minuten aktualisiert werden. Die Dashboard-Seite von Horizon Console wird ebenfalls mit einem Intervall von wenigen Minuten aktualisiert.</p> <p>Diese Einstellung ist standardmäßig nicht aktiviert.</p>
Für Clients, die Anwendungen unterstützen. Verbindungen zu Anwendungen trennen und SSO-Anmeldeinformationen verwerfen, sobald der Benutzer nicht mehr mit Tastatur und Maus arbeitet:	<p>Schützt Anwendungssitzungen, wenn auf dem Client-Gerät keine Tastatur- oder Mausaktivitäten stattfinden. Bei Festlegung auf Nach ... Minuten trennt Horizon 7 nach Ablauf der angegebenen Anzahl von Minuten ohne Benutzeraktivität sämtliche Anwendungssitzungen und verwirft die SSO-Anmeldeinformationen. Desktop-Sitzungen werden nicht getrennt. Benutzer müssen sich erneut anmelden, um eine Verbindung zu den getrennten Anwendungen wiederherzustellen, oder einen neuen Desktop bzw. eine neue Anwendung starten.</p> <p>Diese Einstellung wird auch für die True SSO-Funktion verwendet. Nachdem die SSO-Anmeldeinformationen verworfen wurden, werden die Benutzer zur Eingabe der Active Directory-Anmeldeinformationen aufgefordert. Wenn sich Benutzer bei VMware Identity Manager ohne AD-Anmeldeinformationen angemeldet haben und nicht wissen, welche AD-Anmeldeinformationen eingegeben werden müssen, können sich die Benutzer bei VMware Identity Manager ab- und wieder anmelden und verfügen dann wieder Zugriff auf ihre Remote-Desktops und -anwendungen.</p> <p>Wichtig Benutzer müssen berücksichtigen, dass ihre Desktops verbunden bleiben, wenn sie sowohl Anwendungen als auch Desktops geöffnet haben und ihre Anwendungen aufgrund dieser Zeitüberschreitung getrennt werden. Sie können sich nicht darauf verlassen, dass diese Zeitüberschreitung ihre Desktops schützt.</p> <p>Bei der Einstellung Nie trennt Horizon 7 in keinem Fall Anwendungen oder verwirft SSO-Anmeldeinformationen aufgrund von Benutzerinaktivität.</p> <p>Die Standardeinstellung ist Nie.</p>
Andere Clients. SSO-Anmeldeinformationen verwerfen:	<p>Verwirft SSO-Anmeldedaten nach Ablauf der angegebenen Anzahl von Minuten. Diese Einstellung gilt für Clients, die die Remote-Ausführung von Anwendungen nicht unterstützen. Bei Festlegung von Nach ... Minuten müssen sich die Benutzer nach Ablauf der angegebenen Anzahl von Minuten nach der Anmeldung bei Horizon 7 erneut anmelden, um eine Verbindung zu einem Desktop herzustellen, unabhängig von den Benutzeraktivitäten auf dem Client-Gerät.</p> <p>Wenn dieser Wert auf Nie gesetzt ist, speichert Horizon 7 die SSO-Anmeldedaten, bis der Benutzer Horizon Client schließt oder bis das für Trennung der Benutzer erzwingen angegebene Zeitlimit erreicht ist, je nachdem, welcher Fall zuerst eintritt.</p> <p>Die Standardeinstellung ist Nach 15 Minuten.</p>
Vor der Anmeldung gezeigte Meldung anzeigen	<p>Zeigt Horizon Client-Benutzern bei der Anmeldung einen Haftungsausschluss oder eine andere Meldung an.</p> <p>Geben Sie Ihre Informationen oder Anweisungen in das Textfeld im Dialogfeld „Globale Einstellungen“ ein.</p> <p>Wenn keine Meldung angezeigt werden soll, lassen Sie das Kontrollkästchen deaktiviert.</p>

Tabelle 3-2. Allgemeine globale Einstellungen für Clientsitzungen (Fortsetzung)

Einstellung	Beschreibung
Vor erzwungener Abmeldung eine Warnung anzeigen	<p>Zeigt eine Warnmeldung an, wenn eine Benutzerabmeldung aufgrund einer geplanten oder sofortigen Aktualisierung erzwungen wird, z.B. beim Start einer Desktop-Aktualisierung. Mit dieser Einstellung wird auch festgelegt, wie lange nach dem Anzeigen der Meldung gewartet wird, bis der Benutzer abgemeldet wird.</p> <p>Aktivieren Sie das Kontrollkästchen, um eine Warnmeldung anzuzeigen.</p> <p>Geben Sie die Anzahl der Minuten ein, die nach der Anzeige der Meldung und vor dem Abmelden des Benutzers abgewartet werden sollen. Der Standardwert lautet 5 Minuten.</p> <p>Geben Sie Ihre Warnmeldung ein. Sie können die Standardmeldung verwenden:</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Für Ihren Computer liegt ein wichtiges Update vor – er wird in 5 Minuten heruntergefahren. Speichern Sie jetzt alle noch nicht gespeicherten Arbeiten.</p> </div>
Windows Server-Desktops aktivieren	<p>Legt fest, ob verfügbare Windows Server 2008 R2- und Windows Server 2012 R2-Computer zur Verwendung als Desktops ausgewählt werden können. Wenn diese Einstellung aktiviert ist, werden in Horizon Console alle verfügbaren Windows Server-Computer angezeigt, einschließlich der Computer, auf denen Horizon 7-Serverkomponenten installiert sind.</p> <hr/> <p>Hinweis Die Horizon Agent-Software darf nicht auf derselben virtuellen Maschine oder demselben physischen Computer wie eine andere Horizon 7-Server-Softwarekomponente installiert sein, Sicherheitsserver, Horizon 7-Verbindungsserver oder Horizon 7 Composer eingeschlossen.</p>
Anmeldedaten bereinigen, wenn Registerkarte für HTML Access geschlossen wird	<p>Löscht die Anmeldedaten aus dem Cache, wenn der Benutzer eine Registerkarte schließt, die eine Verbindung zu einem Remote-Desktop oder einer Remoteanwendung herstellt, oder wenn er eine Registerkarte schließt, die eine Verbindung zur Seite für die Auswahl von Desktop und Anwendung im HTML Access-Client herstellt.</p> <p>Wenn diese Einstellung aktiviert ist, entfernt Horizon 7 auch in den folgenden HTML Access-Client-Szenarios die Anmeldedaten aus dem Cache:</p> <ul style="list-style-type: none"> ■ Ein Benutzer aktualisiert die Seite für die Auswahl von Desktop und Anwendung oder die Seite für die Remote-Sitzung. ■ Der Server präsentiert ein selbstsigniertes Zertifikat, ein Benutzer startet einen Remote-Desktop oder eine Remoteanwendung und der Benutzer akzeptiert das Zertifikat, wenn die Sicherheitswarnung erscheint. ■ Ein Benutzer führt einen URI-Befehl auf der Registerkarte aus, die die Remote-Sitzung enthält. <p>Wenn diese Einstellung deaktiviert ist, bleiben die Anmeldedaten im Cache. Diese Funktion ist standardmäßig deaktiviert.</p> <hr/> <p>Hinweis Diese Funktion ist in Horizon 7 Version 7.0.2 und höher verfügbar.</p>
Serverinformationen in der Kunden-Benutzeroberfläche ausblenden	<p>Aktivieren Sie diese Sicherheitseinstellung, um die Server-URL-Informationen in Horizon Client 4.4 oder höher auszublenden.</p>

Tabelle 3-2. Allgemeine globale Einstellungen für Clientsitzungen (Fortsetzung)

Einstellung	Beschreibung
Domänenliste in der Kunden-Benutzeroberfläche ausblenden	<p>Aktivieren Sie diese Sicherheitseinstellung, um das Dropdown-Menü „Domäne“ in Horizon Client 4.4 oder höher auszublenden.</p> <p>Wenn sich Benutzer bei einer Verbindungsserver-Instanz anmelden, für die die globale Einstellung Domänenliste in der Kunden-Benutzeroberfläche ausblenden aktiviert wurde, ist das Dropdown-Menü „Domäne“ in Horizon Client ausgeblendet. Benutzer müssen dann die Domäneninformationen im Textfeld Benutzername von Horizon Client bereitstellen. So müssen Benutzer z. B. ihren Benutzernamen im Format <code>domain\username</code> oder <code>username@domain</code> eingeben.</p> <hr/> <p>Wichtig Wenn Sie die Einstellung Domänenliste in der Kunden-Benutzeroberfläche ausblenden aktivieren und die zweistufige Authentifizierung (RSA SecureID oder RADIUS) für die Verbindungsserver-Instanz auswählen, dürfen Sie nicht die Windows-Benutzernamenübereinstimmung erzwingen. Wenn Sie die Windows-Benutzernamenübereinstimmung erzwingen, werden Benutzer daran gehindert, Domäneninformationen im Textfeld „Benutzername“ einzugeben, und die Anmeldung schlägt immer fehl. Dies gilt nicht für Horizon Client Version 5.0 und höher, wenn eine einzelne Benutzerdomäne vorhanden ist.</p> <hr/> <p>Wichtig Weitere Informationen zu den Auswirkungen dieser Einstellung auf die Sicherheit und Benutzerfreundlichkeit finden Sie im Dokument <i>Horizon 7-Sicherheit</i>.</p>
Domänenliste senden	<p>Aktivieren Sie das Kontrollkästchen, damit der Verbindungsserver die Liste der Domännennamen an den Client sendet, bevor der Benutzer authentifiziert wird.</p> <hr/> <p>Wichtig Weitere Informationen zu den Auswirkungen dieser Einstellung auf die Sicherheit und Benutzerfreundlichkeit finden Sie im Dokument <i>Horizon 7-Sicherheit</i>.</p>

Globale Sicherheitseinstellungen für Client-Sitzungen und -Verbindungen in Horizon Console

Globale Sicherheitseinstellungen bestimmen, ob Clients nach Unterbrechungen erneut authentifiziert werden, der Sicherheitsmodus für Nachrichten aktiviert und der Sicherheitsstatus erweitert ist.

In Horizon Console können Sie globale Sicherheitseinstellungen konfigurieren, indem Sie zu **Einstellungen > Globale Einstellungen > Sicherheitseinstellungen** navigieren.

Für alle Horizon Client-Verbindungen und Horizon Console-Verbindungen mit Horizon 7 ist TLS erforderlich. Wenn Ihre Horizon 7-Bereitstellung Lastausgleichsmodule oder andere Zwischenserver mit Client-Verbindung verwendet, können Sie TLS darauf verlagern und dann Nicht-TLS-Verbindungen auf einzelnen Verbindungsserver-Instanzen und Sicherheitsservern konfigurieren.

Tabelle 3-3. Globale Sicherheitseinstellungen für Clientsitzungen und -verbindungen

Einstellung	Beschreibung
Sichere Tunnelverbindungen nach Netzwerkunterbrechung neu authentifizieren	<p>Legt fest, ob die Anmeldedaten nach einer Netzwerkunterbrechung neu authentifiziert werden müssen, wenn Horizon-Clients sichere Tunnelverbindungen zu Remote-Desktops verwenden.</p> <p>Wenn Sie diese Einstellungen auswählen, fordert Horizon Client im Fall einer Unterbrechung einer sicheren Tunnelverbindung vom Benutzer eine Neuauthentifizierung zur erneuten Verbindung an.</p> <p>Diese Einstellung bietet erhöhte Sicherheit. Wenn beispielsweise ein Laptop gestohlen und in ein anderes Netzwerk bewegt wurde, kann der Benutzer nicht automatisch Zugang zum Remote-Desktop erlangen, ohne Anmeldeinformationen einzugeben.</p> <p>Ist diese Einstellung nicht ausgewählt, stellt der Client die Verbindung mit dem Remote-Desktop wieder her, ohne den Benutzer zur erneuten Authentifizierung aufzufordern.</p> <p>Diese Einstellung hat keine Auswirkung, wenn der sichere Tunnel nicht verwendet wird.</p>
Sicherheitsmodus für Nachrichten	<p>Bestimmt den Sicherheitsmechanismus, der zum Senden von JMS-Nachrichten zwischen Komponenten verwendet wird.</p> <ul style="list-style-type: none"> ■ Wenn für den Modus Aktiviert eingestellt ist, werden zwischen Horizon 7-Komponenten übertragene JMS-Nachrichten signiert und überprüft. ■ Wenn der Modus auf Erweitert festgelegt ist, wird die Sicherheit durch gegenseitig authentifizierte TLS gewährleistet. JMS-Verbindungen und Zugriffssteuerung zu JMS-Themen <p>Für Neuinstallationen wird der Sicherheitsmodus für Nachrichten standardmäßig auf Erweitert festgelegt. Bei einem Upgrade von einer vorherigen Version wird die in der vorherigen Version verwendete Einstellung beibehalten.</p>
Erweiterter Sicherheitsstatus (schreibgeschützt)	<p>Schreibgeschütztes Feld, das angezeigt wird, wenn Sicherheitsmodus für Meldungen von Aktiviert in Erweitert geändert wird. Da die Änderung phasenweise erfolgt, wird in diesem Feld der Fortschritt für die verschiedenen Phasen angezeigt:</p> <ul style="list-style-type: none"> ■ Warten auf Nachrichtenbus-Neustart ist die erste Phase. Dieser Zustand wird angezeigt, bis Sie entweder alle Verbindungsserver-Instanzen im Pod oder den VMware Horizon Message Bus-Komponenten-Dienst auf allen Verbindungsserver-Hosts im Pod manuell neu starten. ■ Erweiterter Modus wird aktiviert ist der nächste Status. Nachdem alle Horizon Message Bus-Komponenten-Dienste neu gestartet wurden, beginnt das System damit, den Sicherheitsmodus für Nachrichten für alle Desktops und Sicherheitsserver in Erweitert zu ändern. ■ Erweitert ist der endgültige Status und gibt an, dass alle Komponenten nun Erweitert als Sicherheitsmodus für Nachrichten verwenden.

Globale Client-Einschränkungseinstellungen für Clientsitzungen in Horizon Console

Globale Client-Einschränkungseinstellungen können das Starten von virtuellen Desktops, veröffentlichten Desktops und veröffentlichten Anwendungen auf bestimmte Clients und Versionen einschränken.

In Horizon Console können Sie globale Client-Einschränkungseinstellungen konfigurieren, indem Sie zu **Einstellungen > Globale Einstellungen > Client-Einschränkungseinstellungen** navigieren und die Version für Horizon Clients eingeben.

Horizon Clients müssen die Version 4.5.0 oder höher aufweisen, mit Ausnahme von Horizon Clients für Chrome, für die Version 4.8.0 oder höher erforderlich ist. Frühere Versionen von Horizon Client werden daran gehindert, eine Verbindung mit Remote-Desktops und veröffentlichten Anwendungen herzustellen, wenn diese Funktion konfiguriert ist.

Hinweis Client-Einschränkungseinstellungen verhindern nur, dass Endbenutzer Remote-Desktops und veröffentlichte Anwendungen starten. Diese Funktion verhindert nicht, dass sich Endbenutzer bei Horizon 7 anmelden.

Tabelle 3-4. Globale Client-Einschränkungseinstellungen für Clientsitzungen

Einstellung	Beschreibung
Horizon Client für Windows	Geben Sie eine Horizon Client-Versionsnummer ab 4.5.0 ein.
Horizon Client für Linux	Geben Sie eine Horizon Client-Versionsnummer ab 4.5.0 ein.
Horizon Client für Mac	Geben Sie eine Horizon Client-Versionsnummer ab 4.5.0 ein.
Horizon Client für iOS	Geben Sie eine Horizon Client-Versionsnummer ab 4.5.0 ein.
Horizon Client für Android	Geben Sie eine Horizon Client-Versionsnummer ab 4.5.0 ein.
Horizon Client für UWP	Geben Sie eine Horizon Client-Versionsnummer ab 4.5.0 ein.
Horizon Client für Chrome	Geben Sie eine Horizon Client-Versionsnummer ab 4.8.0 ein.
Horizon Client für HTML Access	Geben Sie eine Horizon Client-Versionsnummer ab 4.5.0 ein.
Zusätzliche Clients blockieren	<p>Wenn Sie diese Option auswählen, werden alle anderen Clienttypen mit Ausnahme der Horizon Clients in der Whitelist daran gehindert, Desktops oder veröffentlichte Anwendungen zu starten.</p> <p>Wenn Sie jedoch möchten, dass Ihre Endbenutzer andere Clienttypen zum Starten von Desktops und veröffentlichten Anwendungen verwenden, müssen Sie den Clienttyp dem LDAP-Attribut <code>pae-AdditionalClientTypes</code> hinzufügen, um die Blockierungseinstellungen für diesen Clienttyp zu umgehen.</p> <p>Sie können das Dienstprogramm „ADSI-Editor“ zum Bearbeiten von LDAP-Attributen auf dem Verbindungsserver verwenden. Im Dienstprogramm „ADSI-Editor“ ist das LDAP-Attribut <code>pae-AdditionalClientTypes</code> unter <code>CN=Common, OU=Global, OU=Properties, DC=vdi, DC=vmware, DC=int</code> verfügbar.</p>
Meldung	Geben Sie die Meldung ein, die angezeigt werden soll, wenn ein Benutzer versucht, einen Desktop oder eine veröffentlichte Anwendung über einen Clienttyp oder eine Client-Version zu starten, die nicht in der Whitelist enthalten ist.

Deaktivieren oder Aktivieren von Horizon-Verbindungsserver in Horizon Console

Sie können eine Verbindungsserver-Instanz deaktivieren, um die Anmeldung von Benutzern an ihren virtuellen oder veröffentlichten Desktops und Anwendungen zu verhindern. Wenn Sie eine Instanz deaktivieren, können Sie sie wieder aktivieren.

Benutzer, die derzeit bei ihren Desktops und Anwendungen angemeldet sind, sind von der Deaktivierung einer Verbindungsserver-Instanz nicht betroffen.

Mit Ihrer Horizon 7-Bereitstellung wird bestimmt, inwiefern Benutzer durch das Deaktivieren einer Instanz betroffen sind.

- Wenn es sich um eine einzelne, eigenständige Verbindungsserver-Instanz handelt, können sich Benutzer bei ihren Desktops oder Anwendungen nicht anmelden. Sie können keine Verbindung mit Verbindungsserver herstellen.
- Wenn es sich um eine replizierte Verbindungsserver-Instanz handelt, wird mit Ihrer Netzwerktopologie bestimmt, ob Benutzer zu einer anderen replizierten Instanz weitergeleitet werden. Falls Benutzer auf eine andere Instanz zugreifen können, können sie sich bei ihren Desktops und Anwendungen anmelden.

Verfahren

- 1 Wählen Sie in Horizon Console **Einstellungen > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die Verbindungsserver-Instanz aus.
- 3 Klicken Sie auf **Deaktivieren**.

Sie können die Instanz erneut aktivieren, indem Sie auf **Aktivieren** klicken.

Bearbeiten der externen URLs für Horizon-Verbindungsserver-Instanzen

Sie können Horizon Console verwenden, um externe URLs für Verbindungsserver-Instanzen zu bearbeiten.

Ein Verbindungsserver-Host kann standardmäßig nur über Tunnelclients kontaktiert werden, die sich im selben Netzwerk befinden. Tunnelclients, die außerhalb Ihres Netzwerks ausgeführt werden, müssen eine durch den Client auflösbare URL zur Verbindungsherstellung mit einem Verbindungsserver-Host verwenden.

Wenn Benutzer mit dem PCoIP-Anzeigeprotokoll eine Verbindung mit Remote-Desktops herstellen, kann Horizon Client eine weitere Verbindung mit dem PCoIP Secure Gateway auf dem Verbindungsserver-Host aufbauen. Zur Verwendung des PCoIP Secure Gateway muss ein Clientsystem auf eine IP-Adresse zugreifen können, die dem Client eine Verbindungsherstellung mit dem Verbindungsserver-Host ermöglicht. Sie geben diese IP-Adresse in der externen PCoIP-URL an.

Eine dritte URL kann von Benutzern verwendet werden, um mit dem Blast Secure Gateway sichere Verbindungen herzustellen.

Bei den externen URLs für den sicheren Tunnel, für PCoIP und für Blast muss es sich um die Adressen handeln, mit denen Clientsysteme diesen Host erreichen.

Verfahren

- 1 Wählen Sie in Horizon Console **Einstellungen > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.

- 3 Geben Sie im Textfeld **Externe URL** die externe URL des sicheren Tunnels ein.

Die URL muss das Protokoll, den durch Clients auflösbaren Hostnamen und die Portnummer enthalten.

Beispiel: `https://horizon.beispiel.com:443`

Hinweis Um auf eine Verbindungsserver-Instanz zuzugreifen, deren Hostname nicht aufgelöst werden kann, können Sie die IP-Adresse verwenden. Der Host, den Sie kontaktieren, passt jedoch nicht zu dem TLS-Zertifikat, das für die Verbindungsserver-Instanz konfiguriert ist. Dies führt dazu, dass der Zugriff blockiert wird oder weniger sicher ist.

- 4 Geben Sie im Textfeld **PCoIP – Externe URL** die externe URL des PCoIP Secure Gateway ein.

Geben Sie die externe PCoIP-URL als IP-Adresse mit der Portnummer 4172 ein. Schließen Sie keinen Protokollnamen ein.

Beispiel: `10.20.30.40:4172`

Die URL muss die IP-Adresse und Portnummer enthalten, die ein Clientsystem zur Verbindungsherstellung mit dieser Verbindungsserver-Instanz benötigt.

- 5 Geben Sie im Textfeld **Externe Blast-URL** die externe URL des Blast Secure Gateway ein.

Die URL muss das HTTPS-Protokoll, den durch den Client auflösbaren Hostnamen sowie die Portnummer enthalten.

Beispiel: `https://myserver.example.com:8443`

Standardmäßig schließt die URL den FQDN der externen URL für den sicheren Tunnel sowie die standardmäßige Portnummer 8443 ein. Die URL muss den FQDN und die Portnummer enthalten, die ein Clientsystem zur Verbindungsherstellung mit diesem Host benötigt.

- 6 Stellen Sie sicher, dass Clientsysteme mit allen Adressen in diesem Dialogfeld eine Verbindung mit diesem Host herstellen können.

- 7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Die externen URLs werden sofort aktualisiert. Es ist kein Neustart des Verbindungsservers erforderlich, damit die Änderungen wirksam werden.

Registrieren von Gateways in Horizon Console

Horizon Clients verbinden sich über ein Gateway oder eine Unified Access Gateway-Appliance, die Sie in Horizon Console registrieren.

Sie können Gateways in Horizon Console registrieren oder ihre Registrierung aufheben. Um die Registrierung des Gateways aufzuheben, wählen Sie das Gateway oder die Unified Access Gateway-Appliance aus und klicken Sie auf **Registrierung aufheben**.

Verfahren

- 1 Wählen Sie in Horizon Console **Einstellungen > Server** aus.
- 2 Klicken Sie auf der Registerkarte **Gateways** auf **Registrieren**.
- 3 Geben Sie den FQDN des Gateways oder der Unified Access Gateway-Appliance ein.
- 4 Klicken Sie auf **OK**.

Einrichten der Smartcard-Authentifizierung

4

Zur Erhöhung der Sicherheit können Sie eine Verbindungsserver-Instanz oder einen Sicherheitsserver so konfigurieren, dass sich Benutzer und Administratoren unter Verwendung von Smartcards authentifizieren können.

Eine Smartcard ist eine kleine Kunststoffkarte, auf der sich ein Computerchip befindet. Der Chip, der mit einem Mini-Computer vergleichbar ist, bietet eine sichere Datenspeicherung und umfasst u.a. private Schlüssel und Zertifikate für öffentliche Schlüssel. Ein vom US-Verteidigungsministerium verwendeter Smartcard-Typ wird als Common Access Card (CAC) bezeichnet.

Bei der Smartcard-Authentifizierung führt ein Benutzer oder ein Administrator eine Smartcard in einen Smartcard-Leser ein, der mit dem Clientcomputer verbunden ist, und gibt anschließend eine PIN ein. Die Smartcard-Authentifizierung bietet eine zweistufige Authentifizierung, indem einerseits überprüft wird, ob die Person im Besitz der Smartcard ist, und andererseits, ob die Person die erforderliche PIN kennt.

Weitere Informationen zu den Hardware- und Softwareanforderungen für die Implementierung der Smartcard-Authentifizierung finden Sie im Dokument *Horizon 7-Installation*. Die Microsoft TechNet-Website enthält ausführliche Informationen zu Planung und Implementierung der Smartcard-Authentifizierung für Windows-Systeme.

Für den Einsatz von Smartcards müssen Clientcomputer über Smartcard-Middleware und einen Smartcard-Leser verfügen. Um Zertifikate auf Smartcards zu installieren, müssen Sie einen Computer einrichten, der als Registrierungsstelle fungiert. Informationen dazu, ob ein bestimmter Horizon Client-Typ Smartcards unterstützt, finden Sie in der Horizon Client-Dokumentation unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

Dieses Kapitel enthält die folgenden Themen:

- [Anmelden über eine Smartcard](#)
- [Konfigurieren der Smart Card-Authentifizierung auf dem Horizon-Verbindungsserver](#)
- [Konfigurieren der Smartcard-Authentifizierung auf Drittanbieterlösungen](#)
- [Vorbereiten von Active Directory für die Smartcard-Authentifizierung](#)
- [Überprüfen der Smartcard-Authentifizierungskonfiguration in Horizon Console](#)
- [Verwenden der Smartcard-Zertifikatsperrüberprüfung](#)

Anmelden über eine Smartcard

Wenn ein Benutzer oder Administrator eine Smartcard in einen Smartcard-Leser einführt, werden die Benutzerzertifikate auf der Smartcard in den lokalen Zertifikatspeicher auf dem Clientsystem kopiert, sofern es sich bei dem Client-Betriebssystem um Windows handelt. Die Zertifikate im lokalen Zertifikatspeicher sind für alle auf dem Clientcomputer ausgeführten Anwendungen verfügbar, einschließlich der Horizon Client-Anwendung.

Wenn ein Benutzer oder Administrator eine Verbindung zu einer Verbindungsserver-Instanz oder einem Sicherheitsserver herstellt, die bzw. der für die Smartcard-Authentifizierung konfiguriert ist, sendet die Verbindungsserver-Instanz oder der Sicherheitsserver eine Liste vertrauenswürdiger Zertifizierungsstellen an das Clientsystem. Das Clientsystem gleicht die Liste vertrauenswürdiger Zertifizierungsstellen mit den verfügbaren Benutzerzertifikaten ab, wählt ein geeignetes Zertifikat aus und fordert den Benutzer oder Administrator zur Eingabe einer Smartcard-PIN auf. Wenn mehrere gültige Benutzerzertifikate vorhanden sind, fordert das Clientsystem den Benutzer oder Administrator zur Auswahl eines Zertifikats auf.

Das Clientsystem sendet das Benutzerzertifikat an die Verbindungsserver-Instanz oder den Sicherheitsserver, die bzw. der das Zertifikat basierend auf der Zertifikatvertrauensstellung und der Gültigkeitsdauer überprüft. Benutzer und Administratoren können sich normalerweise erfolgreich authentifizieren, wenn ihr Benutzerzertifikat signiert und gültig ist. Wenn eine Zertifikatssperrüberprüfung konfiguriert ist, können sich Benutzer oder Administratoren mit gesperrten Benutzerzertifikaten nicht authentifizieren.

In einigen Umgebungen kann das Smartcard-Zertifikat eines Benutzers mehreren Active Directory-Domänenbenutzerkonten zugeordnet sein. Ein Benutzer besitzt möglicherweise mehrere Konten mit Administratorrechten und muss daher angeben, welches Konto bei der Smartcard-Anmeldung im Feld für den Benutzernamenhinweis verwendet werden soll. Damit das Feld für den Benutzernamenhinweis im Anmeldungsdialogfeld von Horizon Client angezeigt wird, muss der Administrator die Funktion für Hinweise zu Smartcard-Benutzernamen für die Verbindungsserverinstanz in Horizon Console aktivieren. Der Smartcard-Benutzer kann dann bei der Smartcard-Anmeldung im Feld für den Benutzernamenhinweis einen Benutzernamen oder UPN eingeben.

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

Der Wechsel des Anzeigeprotokolls wird mit der Smartcard-Authentifizierung in Horizon Client nicht unterstützt. Zur Änderung des Anzeigeprotokolls nach der Authentifizierung per Smartcard in Horizon Client muss sich der Benutzer abmelden und wieder anmelden.

Konfigurieren der Smart Card-Authentifizierung auf dem Horizon-Verbindungsserver

Um die Smartcard-Authentifizierung zu konfigurieren, müssen Sie ein Stammzertifikat anfordern und es zu einer Server-Vertrauensspeicherdatei hinzufügen, die Verbindungsserver-Konfigurationseigenschaften ändern und die Smartcard-Authentifizierungseinstellungen festlegen. Abhängig von Ihrer Umgebung müssen möglicherweise weitere Schritte ausgeführt werden.

Verfahren

1 [Anfordern der Zertifizierungsstellenzertifikate](#)

Sie müssen alle anwendbaren Zertifizierungsstellenzertifikate (CA-Zertifikate) für alle vertrauenswürdigen Benutzerzertifikate auf den Smartcards anfordern, die von Ihren Benutzern und Administratoren verwendet werden. Diese Zertifikate beinhalten Stammzertifikate und gegebenenfalls Zwischenzertifikate, wenn das Smartcard-Zertifikat des Benutzers von einer Zwischenzertifizierungsstelle ausgestellt wurde.

2 [Anfordern des CA-Zertifikats von Windows](#)

Wenn Sie über ein von einer Zertifizierungsstelle signiertes Benutzerzertifikat oder eine Smartcard mit Zertifikat verfügen und Windows dem Stammzertifikat vertraut, können Sie das Stammzertifikat aus Windows exportieren. Handelt es sich beim Aussteller des Benutzerzertifikats um eine Zwischenzertifizierungsstelle, können Sie dieses Zertifikat exportieren.

3 [Hinzufügen des CA-Zertifikats zu einer Server-Vertrauensspeicherdatei](#)

Sie müssen für alle vertrauenswürdigen Benutzer und Administratoren Stammzertifikate oder Zwischenzertifikate oder beide zu einer Server-Vertrauensspeicherdatei hinzufügen. Verbindungsserver-Instanzen und Sicherheitsserver verwenden diese Informationen zur Authentifizierung von Smartcard-Benutzern und Administratoren.

4 [Ändern von Horizon-Verbindungsserver-Konfigurationseigenschaften](#)

Zur Aktivierung der Smartcard-Authentifizierung müssen auf Ihrem Verbindungsserver Verbindungsserver-Konfigurationseigenschaften geändert werden.

5 [Konfigurieren der Smartcard-Einstellungen in Horizon Console](#)

In Horizon Console können Einstellungen für verschiedene Smartcard-Authentifizierungsszenarien festgelegt werden.

Anfordern der Zertifizierungsstellenzertifikate

Sie müssen alle anwendbaren Zertifizierungsstellenzertifikate (CA-Zertifikate) für alle vertrauenswürdigen Benutzerzertifikate auf den Smartcards anfordern, die von Ihren Benutzern und Administratoren verwendet werden. Diese Zertifikate beinhalten Stammzertifikate und gegebenenfalls Zwischenzertifikate, wenn das Smartcard-Zertifikat des Benutzers von einer Zwischenzertifizierungsstelle ausgestellt wurde.

Wenn Sie nicht über das Stamm- oder Zwischenzertifikat der Zertifizierungsstelle verfügen, welche die Zertifikate auf den von Ihren Benutzern und Administratoren verwendeten Smartcards signiert hat, können Sie die Zertifikate auch aus einem von einer Zertifizierungsstelle signierten Benutzerzertifikat oder aus einer Smartcard mit Zertifikat exportieren. Siehe [Anfordern des CA-Zertifikats von Windows](#).

Verfahren

- ◆ Fordern Sie die CA-Zertifikate aus einer der nachfolgend aufgeführten Quellen an.
 - Microsoft IIS-Server, auf dem die Microsoft-Zertifikatdienste ausgeführt werden. Informationen zum Installieren von Microsoft IIS, Ausstellen von Zertifikaten und Verteilen von Zertifikaten in Ihrer Organisation finden Sie auf der Microsoft TechNet-Website.
 - Öffentliches Stammzertifikat einer vertrauenswürdigen Zertifizierungsstelle. Dies ist die gängigste Quelle eines Stammzertifikats in Umgebungen, die bereits über eine Smartcard-Infrastruktur und einen standardisierten Ansatz für die Smartcard-Verteilung und -Authentifizierung verfügen.

Anfordern des CA-Zertifikats von Windows

Wenn Sie über ein von einer Zertifizierungsstelle signiertes Benutzerzertifikat oder eine Smartcard mit Zertifikat verfügen und Windows dem Stammzertifikat vertraut, können Sie das Stammzertifikat aus Windows exportieren. Handelt es sich beim Aussteller des Benutzerzertifikats um eine Zwischenzertifizierungsstelle, können Sie dieses Zertifikat exportieren.

Verfahren

- 1 Wenn das Benutzerzertifikat auf einer Smartcard vorhanden ist, führen Sie die Smartcard in den Leser ein, um das Benutzerzertifikat zu Ihrem persönlichen Speicher hinzuzufügen.

Wenn das Benutzerzertifikat nicht im persönlichen Speicher angezeigt wird, exportieren Sie das Benutzerzertifikat über die Lesersoftware in eine Datei. Diese Datei wird in Schritt 4 dieser Vorgehensweise verwendet.

- 2 Wählen Sie in Internet Explorer **Tools > Internetoptionen** aus.
- 3 Klicken Sie auf der Registerkarte **Inhalte** auf **Zertifikate**.
- 4 Wählen Sie auf der Registerkarte **Eigene Zertifikate** das gewünschte Zertifikat aus und klicken Sie auf **Anzeigen**.

Wenn das Benutzerzertifikat nicht in der Liste enthalten ist, klicken Sie auf **Importieren**, um das Zertifikat manuell aus einer Datei zu importieren. Nach dem Import können Sie das Zertifikat aus der Liste auswählen.

- 5 Wählen Sie auf der Registerkarte **Zertifizierungspfad** das oberste Zertifikat in der Struktur und klicken Sie auf **Zertifikat anzeigen**.

Ein Benutzerzertifikat kann als Bestandteil einer Vertrauenshierarchie signiert werden – das Signaturzertifikat selbst kann durch ein anderes Zertifikat höherer Ebene signiert sein. Wählen Sie das übergeordnete Zertifikat (das Zertifikat, das zum Signieren des Benutzerzertifikats verwendet wurde) als Stammzertifikat aus. In einigen Fällen kann es sich beim Aussteller um eine Zwischenzertifizierungsstelle handeln.

- 6 Klicken Sie auf der Registerkarte **Details** auf **In Datei kopieren**.

Der **Zertifikatexport-Assistent** wird geöffnet.

- 7 Klicken Sie auf **Weiter > Weiter** und geben Sie einen Namen sowie einen Speicherort für die Exportdatei an.
- 8 Klicken Sie auf **Weiter**, um die Datei am angegebenen Speicherort als Stammzertifikat zu speichern.

Hinzufügen des CA-Zertifikats zu einer Server-Vertrauensspeicherdatei

Sie müssen für alle vertrauenswürdigen Benutzer und Administratoren Stammzertifikate oder Zwischenzertifikate oder beide zu einer Server-Vertrauensspeicherdatei hinzufügen. Verbindungsserver-Instanzen und Sicherheitsserver verwenden diese Informationen zur Authentifizierung von Smartcard-Benutzern und Administratoren.

Voraussetzungen

- Fordern Sie die Stammzertifikate oder Zwischenzertifikate an, die zur Signierung der Zertifikate auf den von Ihren Benutzern oder Administratoren verwendeten Smartcards verwendet wurden. Siehe [Anfordern der Zertifizierungsstellenzertifikate](#) und [Anfordern des CA-Zertifikats von Windows](#).

Wichtig Diese Zertifikate können Zwischenzertifikate beinhalten, wenn das Smartcard-Zertifikat des Benutzers von einer Zwischenzertifizierungsstelle ausgestellt wurde.

- Stellen Sie sicher, dass das Dienstprogramm `keytool` dem Systempfad auf Ihrem Verbindungsserver- oder Sicherheitsserver-Host hinzugefügt wurde. Weitere Informationen finden Sie im Dokument *Horizon 7-Installation*.

Verfahren

- 1 Verwenden Sie das Dienstprogramm `keytool` auf Ihrem Verbindungsserver- oder Sicherheitsserver-Host, um das Stammzertifikat oder das Zwischenzertifikat oder beide in die Server-Vertrauensspeicherdatei zu importieren.

Beispiel:

```
keytool -import -alias Alias -file Stammzertifikat -keystore truststorefile.key
```

In diesem Befehl steht *Alias* für einen eindeutigen Namen eines neuen Eintrags in der Vertrauensspeicherdatei (Groß-/Kleinschreibung wird beachtet), *Stammzertifikat* gibt das Stammzertifikat oder das Zwischenzertifikat an, das Sie angefordert oder exportiert haben, und *truststorefile.key* ist der Name der Vertrauensspeicherdatei, der Sie das Stammzertifikat hinzufügen. Wenn die Datei nicht vorhanden ist, wird sie im aktuellen Verzeichnis erstellt.

Hinweis Über das Dienstprogramm `keytool` werden Sie möglicherweise zum Erstellen eines Kennworts für die Vertrauensspeicherdatei aufgefordert. Sie werden nach dem Kennwort gefragt, wenn Sie zu einem späteren Zeitpunkt zusätzliche Zertifikate zur Vertrauensspeicherdatei hinzufügen müssen.

- 2 Kopieren Sie die Vertrauensspeicherdatei in den SSL-Gatewaykonfigurationsordner auf dem Verbindungsserver- oder Sicherheitsserver-Host.

Beispiel: `install_directory\VMware\VMware View\Server\sslgateway\conf\truststorefile.key`

Nächste Schritte

Ändern Sie die Verbindungsserver-Konfigurationseigenschaften, um die Smartcard-Authentifizierung zu aktivieren.

Ändern von Horizon-Verbindungsserver-Konfigurationseigenschaften

Zur Aktivierung der Smartcard-Authentifizierung müssen auf Ihrem Verbindungsserver Verbindungsserver-Konfigurationseigenschaften geändert werden.

Voraussetzungen

Fügen Sie die Zertifikate der Zertifizierungsstelle für alle vertrauenswürdigen Benutzerzertifikate einer Server-Vertrauensspeicherdatei hinzu. Diese Zertifikate beinhalten Stammzertifikate und gegebenenfalls Zwischenzertifikate, wenn das Smartcard-Zertifikat des Benutzers von einer Zwischenzertifizierungsstelle ausgestellt wurde.

Verfahren

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im TLS/SSL-Gatewaykonfigurationsordner auf dem Verbindungsserver-Host.
Beispiel: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 2 Fügen Sie die Eigenschaften `trustKeyfile`, `trustStoretype` und `useCertAuth` zur Datei `locked.properties` hinzu.
 - a Setzen Sie `trustKeyfile` auf den Namen Ihrer Vertrauensspeicherdatei.
 - b Setzen Sie `trustStoretype` auf **jks**.
 - c Setzen Sie `useCertAuth` auf **true**, um die Zertifikatauthentifizierung zu aktivieren.
- 3 Starten Sie den Verbindungsserver-Dienst neu, damit die Änderungen wirksam werden.

Beispiel: `locked.properties`-Datei

Mit der gezeigten Datei wird angegeben, dass sich das Stammzertifikat für alle vertrauenswürdigen Benutzer in der Datei `lonqa.key` befindet. Zudem wird der Vertrauensspeichertyp auf `jks` gesetzt und die Zertifikatauthentifizierung wird aktiviert.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
```


Nächste Schritte

Wenn Sie die Smartcard-Authentifizierung für eine Verbindungsserver-Instanz konfiguriert haben, konfigurieren Sie die Smartcard-Authentifizierungseinstellungen in Horizon Console.

Konfigurieren der Smartcard-Einstellungen in Horizon Console

In Horizon Console können Einstellungen für verschiedene Smartcard-Authentifizierungsszenarien festgelegt werden.

Voraussetzungen

- Ändern Sie Verbindungsserver-Konfigurationseigenschaften auf Ihrem Verbindungsserver-Host.
- Überprüfen Sie, ob Horizon-Clients HTTPS-Verbindungen direkt mit Ihrem Verbindungsserver oder Sicherheitsserverhost herstellen. Die Authentifizierung per Smartcard wird nicht unterstützt, wenn Sie TLS auf ein Zwischengerät auslagern.

Verfahren

- 1 Wählen Sie in Horizon Console **Einstellungen > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.

- 3 Um die Smartcard-Authentifizierung für Remote-Desktop- und Anwendungsbenutzer zu konfigurieren, führen Sie folgende Schritte durch.

- a Wählen Sie auf der Registerkarte **Authentifizierung** aus dem Dropdown-Menü **Smartcard-Authentifizierung für Benutzer** im Abschnitt „Horizon-Authentifizierung“ eine Konfigurationsoption aus.

Option	Aktion
Nicht zulässig	Die Smartcard-Authentifizierung ist auf der Verbindungsserver-Instanz deaktiviert.
Optional	Benutzer können für die Verbindung mit der Verbindungsserver-Instanz die Smartcard-Authentifizierung oder die Kennwortauthentifizierung verwenden. Wenn die Smartcard-Authentifizierung fehlschlägt, muss der Benutzer ein Kennwort angeben.
Erforderlich	Benutzer müssen für die Verbindung mit der Verbindungsserver-Instanz die Smartcard-Authentifizierung verwenden. Wenn die Smartcard-Authentifizierung erforderlich ist, schlägt die Authentifizierung von Benutzern fehl, die das Kontrollkästchen Als aktueller Benutzer anmelden zur Herstellung einer Verbindung mit der Verbindungsserver-Instanz aktivieren. Diese Benutzer müssen sich bei der Anmeldung beim Verbindungsserver erneut mit ihrer Smartcard und ihrer PIN authentifizieren. Hinweis Die Smartcard-Authentifizierung ersetzt nur die Windows-Kennwortauthentifizierung. Wenn SecurID aktiviert ist, müssen sich die Benutzer sowohl über SecurID als auch per Smartcard authentifizieren.

- b Konfigurieren Sie die Richtlinie zum Entfernen von Smartcards.

Die Richtlinie zum Entfernen von Smartcards kann nicht konfiguriert werden, wenn für die Smartcard-Authentifizierung **Nicht zulässig** festgelegt ist.

Option	Aktion
Trennen der Benutzer von der Verbindungsserver-Instanz beim Entfernen der Smartcards.	Aktivieren Sie das Kontrollkästchen Benutzersitzungen nach Entfernung der Smartcard trennen .
Benutzer bleiben beim Entfernen der Smartcards weiterhin mit dem Verbindungsserver verbunden und können neue Desktop- oder Anwendungssitzungen ohne erneute Authentifizierung starten.	Deaktivieren Sie das Kontrollkästchen Benutzersitzungen nach Entfernung der Smartcard trennen .

Die Richtlinie zum Entfernen von Smartcards gilt nicht für Benutzer, die mit der Verbindungsserver-Instanz verbunden sind, für die das Kontrollkästchen **Als aktueller Benutzer anmelden** aktiviert ist, selbst wenn sie sich an ihrem Clientsystem mit einer Smartcard anmelden.

- c Konfigurieren der Hinweisfunktion für den Smartcard-Benutzernamen.

Die Hinweisfunktion für den Smartcard-Benutzernamen kann nicht konfiguriert werden, wenn für die Smartcard-Authentifizierung **Nicht zulässig** festgelegt ist.

Option	Aktion
Benutzern die Verwendung eines einzigen Smartcard-Zertifikats zur Authentifizierung bei mehreren Benutzerkonten erlauben.	Aktivieren Sie das Kontrollkästchen Hinweise für Smartcard-Benutzernamen zulassen .
Benutzern keine Verwendung eines einzigen Smartcard-Zertifikats zur Authentifizierung bei mehreren Benutzerkonten erlauben.	Deaktivieren Sie das Kontrollkästchen Hinweise für Smartcard-Benutzernamen zulassen .

- 4 Um die Smartcard-Authentifizierung für Administratoren zu konfigurieren, die sich bei Horizon Console anmelden, wählen Sie im Abschnitt **Horizon Administrator-Authentifizierung** eine Konfigurationsoption aus dem Dropdown-Menü **Smartcard-Authentifizierung für Administratoren** aus.

Option	Aktion
Nicht zulässig	Die Smartcard-Authentifizierung ist auf der Verbindungsserver-Instanz deaktiviert.
Optional	Administratoren können die Authentifizierung per Smartcard oder Kennwort verwenden, um sich bei Horizon Console anzumelden. Wenn die Smartcard-Authentifizierung fehlschlägt, muss der Administrator ein Kennwort angeben.
Erforderlich	Administratoren müssen die Smartcard-Authentifizierung verwenden, wenn sie sich bei Horizon Console anmelden.

- 5 Klicken Sie auf **OK**.

- 6 Starten Sie den Verbindungsserver-Dienst neu.

Mit einer Ausnahme müssen Sie den Verbindungsserver-Dienst neu starten, damit die Änderungen an den Smartcard-Einstellungen in Kraft treten. Sie können die Smartcard-Authentifizierungseinstellungen zwischen **Optional** und **Erforderlich** ändern, ohne den Verbindungsserver-Dienst neu starten zu müssen.

Aktuell angemeldete Benutzer und Administratoren sind von Änderungen an Smartcard-Einstellungen nicht betroffen.

Nächste Schritte

Bereiten Sie Active Directory bei Bedarf für die Smartcard-Authentifizierung vor. Siehe [Vorbereiten von Active Directory für die Smartcard-Authentifizierung](#).

Überprüfen Sie die Konfiguration der Smartcard-Authentifizierung. Siehe [Überprüfen der Smartcard-Authentifizierungskonfiguration in Horizon Console](#).

Konfigurieren der Smartcard-Authentifizierung auf Drittanbieterlösungen

Drittanbieterlösungen wie Lastenausgleichsdienste oder Gateways können die Smart Card-Authentifizierung durch Absolvieren einer SAML-Zusicherung durchführen, die das X.590-Zertifikat und die verschlüsselte PIN der Smartcard enthält.

In diesem Abschnitt werden die Aufgaben dargestellt, die zur Einrichtung von Drittanbieterlösungen für die Bereitstellung des relevanten X.590-Zertifikats für den Verbindungsserver notwendig sind, nachdem das Zertifikat durch den Partnerdienst bestätigt wurde. Da diese Funktion die SAML-Authentifizierung verwendet, muss dabei in Horizon Console ein SAML-Authentifikator erstellt werden.

Informationen zur Konfiguration der Smartcard-Authentifizierung auf Unified Access Gateway finden Sie in der Unified Access Gateway-Dokumentation.

Verfahren

- 1 Erstellen Sie einen SAML-Authentifikator für das Gateway oder den Lastenausgleichsdienst eines Drittanbieters.

Siehe [Konfigurieren eines SAML-Authentifikators in Horizon Console](#).
- 2 Erweitern Sie den Ablaufzeitraum der Metadaten des Verbindungservers, sodass Remotesitzungen nicht nach nur 24 Stunden beendet werden.

Siehe [Ändern des Ablaufzeitraums der Metadaten von Dienst Anbietern auf dem Verbindungsserver](#).
- 3 Bei Bedarf konfigurieren Sie das Drittanbietergerät für die Anwendung der Dienstanbietermetadaten des Verbindungservers.

Weitere Informationen dazu erhalten Sie in der Produktdokumentation des Drittanbietergeräts.
- 4 Konfigurieren Sie die Smartcard-Einstellungen auf dem Drittanbietergerät.

Weitere Informationen dazu erhalten Sie in der Produktdokumentation des Drittanbietergeräts.

Vorbereiten von Active Directory für die Smartcard-Authentifizierung

Sie müssen in Active Directory möglicherweise bestimmte Aufgaben ausführen, wenn Sie die Smartcard-Authentifizierung implementieren.

■ [Hinzufügen von UPNs für Smartcard-Benutzer](#)

Da sich die Smartcard-Anmeldung auf Benutzerprinzipalnamen (User Principal Names, UPNs) stützt, müssen die Active Directory-Konten von Benutzern und Administratoren, die sich in Horizon 7 per Smartcard authentifizieren, über einen gültigen UPN verfügen.

■ **Hinzufügen des Stammzertifikats zum Enterprise NTAAuth-Speicher**

Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat dem Enterprise NTAAuth-Speicher in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

■ **Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen**

Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat zur Gruppenrichtlinie „Vertrauenswürdige Stammzertifizierungsstellen“ in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

■ **Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen**

Wenn Sie eine Zwischenzertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Zwischenzertifikat zur Gruppenrichtlinie „Zwischenzertifizierungsstellen“ in Active Directory hinzufügen.

Hinzufügen von UPNs für Smartcard-Benutzer

Da sich die Smartcard-Anmeldung auf Benutzerprinzipalnamen (User Principal Names, UPNs) stützt, müssen die Active Directory-Konten von Benutzern und Administratoren, die sich in Horizon 7 per Smartcard authentifizieren, über einen gültigen UPN verfügen.

Wenn sich der Smartcard-Benutzer in einer anderen Domäne befindet als derjenigen, von der Ihr Stammzertifikat ausgegeben wurde, müssen Sie den Benutzer-UPN auf den alternativen Antragstellernamen (Subject Alternative Name, SAN) festlegen, der im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle angegeben ist. Wenn Ihr Stammzertifikat von einem anderen Server in der aktuellen Domäne des Smartcard-Benutzers ausgegeben wurde, ist eine Änderung des Benutzer-UPNs nicht erforderlich.

Hinweis Sie müssen möglicherweise den UPN für integrierte Active Directory-Konten angeben, selbst wenn das Zertifikat von derselben Domäne ausgegeben wurde. Für integrierte Konten, einschließlich des Administratorkontos, ist standardmäßig kein UPN festgelegt.

Voraussetzungen

- Sie können den alternativen Antragstellernamen (SAN) abrufen, indem Sie im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle die Zertifikateigenschaften anzeigen.
- Wenn das Dienstprogramm „ADSI Edit“ nicht auf Ihrem Active Directory-Server zur Verfügung steht, laden Sie die entsprechenden Windows-Supporttools von der Microsoft-Website herunter und installieren Sie sie.

Verfahren

- 1 Starten Sie auf Ihrem Active Directory-Server das Dienstprogramm ADSI-Editor.
- 2 Erweitern Sie im linken Fensterbereich die Domäne, in der sich der Benutzer befindet, und doppelklicken Sie auf CN=Users.

- 3 Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf den Benutzer und anschließend auf **Eigenschaften**.
- 4 Doppelklicken Sie auf das Attribut `userPrincipalName` und geben Sie den SAN-Wert für das Zertifikat der vertrauenswürdigen Zertifizierungsstelle ein.
- 5 Klicken Sie auf **OK**, um die Attributeinstellung zu speichern.

Hinzufügen des Stammzertifikats zum Enterprise NTAAuth-Speicher

Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat dem Enterprise NTAAuth-Speicher in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

Verfahren

- ◆ Verwenden Sie auf dem Active Directory-Server den Befehl `certutil`, um das Zertifikat im Enterprise NTAAuth-Speicher zu veröffentlichen.

Beispiel:

```
certutil -dspublish -f Pfad_zum_Zertifikat_der_Stammzertifizierungsstelle  
NTAuthCA
```

Die Zertifizierungsstelle wird jetzt als vertrauenswürdig eingestuft und kann Zertifikate dieses Typs ausstellen.

Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen

Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat zur Gruppenrichtlinie „Vertrauenswürdige Stammzertifizierungsstellen“ in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

Verfahren

- 1 Navigieren Sie auf dem Active Directory-Server zum Plug-In „Gruppenrichtlinienmanagement“.

AD-Version	Navigationspfad
Windows 2003	<ol style="list-style-type: none"> a Wählen Sie Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer. b Klicken Sie mit der rechten Maustaste auf Ihre Domäne und wählen Sie Eigenschaften aus. c Klicken Sie auf der Registerkarte Gruppenrichtlinie auf Öffnen, um das Plug-In Gruppenrichtlinienverwaltung zu öffnen. d Klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.
Windows 2008	<ol style="list-style-type: none"> a Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.
Windows 2012 R2	<ol style="list-style-type: none"> a Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.
Windows 2016	<ol style="list-style-type: none"> a Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.

- 2 Erweitern Sie den Abschnitt **Computerkonfiguration** und öffnen Sie **Windows-Einstellungen \Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel**.
- 3 Klicken Sie mit der rechten Maustaste auf **Vertrauenswürdige Stammzertifizierungsstellen** und wählen Sie **Importieren**.
- 4 Folgen Sie den Anweisungen des Assistenten, um das Stammzertifikat (z.B. rootCA.cer) zu importieren. Klicken Sie anschließend auf **OK**.
- 5 Schließen Sie das Fenster „Gruppenrichtlinie“.

Alle Systeme in der Domäne verfügen nun über eine Kopie des Stammzertifikats in ihrem vertrauenswürdigen Stammspeicher.

Nächste Schritte

Wenn Sie eine Zwischenzertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Zwischenzertifikat zur Gruppenrichtlinie „Zwischenzertifizierungsstellen“ in Active Directory hinzufügen. Siehe [Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen](#).

Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen

Wenn Sie eine Zwischenzertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Zwischenzertifikat zur Gruppenrichtlinie „Zwischenzertifizierungsstellen“ in Active Directory hinzufügen.

Verfahren

- 1 Navigieren Sie auf dem Active Directory-Server zum Plug-In „Gruppenrichtlinienmanagement“.

AD-Version	Navigationspfad
Windows 2003	<ol style="list-style-type: none"> a Wählen Sie Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer. b Klicken Sie mit der rechten Maustaste auf Ihre Domäne und wählen Sie Eigenschaften aus. c Klicken Sie auf der Registerkarte Gruppenrichtlinie auf Öffnen, um das Plug-In Gruppenrichtlinienverwaltung zu öffnen. d Klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.
Windows 2008	<ol style="list-style-type: none"> a Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.
Windows 2012 R2	<ol style="list-style-type: none"> a Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.
Windows 2016	<ol style="list-style-type: none"> a Wählen Sie Start > Administrative Tools > Gruppenrichtlinienverwaltung. b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf Standard-Domänenrichtlinie und klicken Sie anschließend auf Bearbeiten.

- 2 Erweitern Sie den Abschnitt **Computerkonfiguration** und öffnen Sie die Richtlinie für **Windows-Einstellungen\Sicherheitseinstellungen\Öffentlicher Schlüssel**.
- 3 Klicken Sie mit der rechten Maustaste auf **Zwischenzertifizierungsstellen** und wählen Sie **Importieren**.
- 4 Folgen Sie den Anweisungen des Assistenten, um das Zwischenzertifikat (z.B. intermediateCA.cer) zu importieren. Klicken Sie anschließend auf **OK**.
- 5 Schließen Sie das Fenster „Gruppenrichtlinie“.

Alle Systeme in der Domäne verfügen nun über eine Kopie des Zwischenzertifikats in ihrem Zwischenzertifizierungsstellen-Speicher.

Überprüfen der Smartcard-Authentifizierungskonfiguration in Horizon Console

Nach der erstmaligen Einrichtung der Smartcard-Authentifizierung oder bei nicht ordnungsgemäßer Funktionsweise der Smartcard-Authentifizierung sollten Sie die Konfiguration der Smartcard-Authentifizierung überprüfen.

Verfahren

- ◆ Stellen Sie sicher, dass jedes Clientsystem über Smartcard-Middleware, eine Smartcard mit gültigem Zertifikat sowie einen Smartcard-Leser verfügt. Stellen Sie für Endbenutzer sicher, dass sie über Horizon Client verfügen.

In der Dokumentation Ihres Smartcard-Anbieters finden Sie Informationen zur Konfiguration der Smartcard-Software und -Hardware.

- ◆ Wählen Sie auf jedem Client-System **Start > Einstellungen > Systemsteuerung > Internetoptionen > Inhalt > Zertifikate > Persönlich** aus, um sicherzustellen, dass die Zertifikate für die Smartcard-Authentifizierung verfügbar sind.

Wenn ein Benutzer oder ein Administrator eine Smartcard in den Smartcard-Leser einlegt, kopiert Windows Zertifikate von der Smartcard auf den Computer des Benutzers. Anwendungen auf dem Clientsystem, einschließlich Horizon Client, können diese Zertifikate verwenden.

- ◆ Überprüfen Sie in der Datei `locked.properties` auf dem Verbindungsserver- oder Sicherheitsserver-Host, dass die Eigenschaft `useCertAuth` auf **true** gesetzt und richtig geschrieben ist.

Die Datei `locked.properties` befindet sich im Verzeichnis `Installationsverzeichnis\VMware\VMware View\Server\sslgateway\conf`. Die Eigenschaft `useCertAuth` wird durch den Tippfehler `userCertAuth` häufig falsch angegeben.

- ◆ Wenn Sie die Smartcard-Authentifizierung auf einer Verbindungsserver-Instanz konfiguriert haben, überprüfen Sie die Smartcard-Authentifizierungseinstellung in Horizon Console.

- a Wählen Sie **Einstellungen > Server** aus.
- b Wählen Sie auf der Registerkarte **Verbindungsserver** die Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- c Wenn Sie die Smartcard-Authentifizierung für Benutzer konfiguriert haben, stellen Sie auf der Registerkarte **Authentifizierung** sicher, dass **Smartcard-Authentifizierung für Benutzer** auf **Optional** oder **Erforderlich** festgelegt ist.
- d Wenn Sie die Smartcard-Authentifizierung für Administratoren konfiguriert haben, stellen Sie auf der Registerkarte **Authentifizierung** sicher, dass **Smartcard-Authentifizierung für Administratoren** auf **Optional** oder **Erforderlich** festgelegt ist.

Sie müssen den Verbindungsserver-Dienst neu starten, damit die Änderungen an den Smartcard-Einstellungen in Kraft treten.

- ◆ Wenn sich der Smartcard-Benutzer in einer anderen Domäne befindet als derjenigen, von der Ihr Stammzertifikat ausgegeben wurde, stellen Sie sicher, dass der Benutzer-UPN auf den alternativen Antragstellernamen (SAN) festgelegt ist, der im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle angegeben ist.
 - a Sie können den alternativen Antragstellernamen (SAN) ermitteln, indem Sie im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle die Zertifikateigenschaften anzeigen.
 - b Wählen Sie auf Ihrem Active Directory-Server **Start > Verwaltung > Active Directory-Benutzer und -Computer** aus.
 - c Klicken Sie im Ordner **Benutzer** mit der rechten Maustaste auf den Benutzer und wählen Sie **Eigenschaften**.

Der Benutzerprinzipalname wird auf der Registerkarte **Konto** in den Textfeldern **Benutzeranmeldename** angezeigt.

- ◆ Wenn Smartcard-Benutzer das PCoIP-Anzeigeprotokoll oder das VMware Blast-Anzeigeprotokoll zur Herstellung einer Verbindung mit Einzelsitzungs-Desktops verwenden, müssen Sie sicherstellen, dass die Horizon Agent-Komponente „Smartcard-Umleitung“ auf Computern für Einzelbenutzer installiert ist. Mit der Smartcard-Funktion können sich Benutzer bei Einzelsitzungs-Desktops mit Smartcards anmelden. RDS-Hosts, für die die Remote-Desktop-Dienste-Rolle installiert ist, unterstützen die Smartcard-Funktion automatisch und Sie müssen diese Funktion nicht installieren.
- ◆ Überprüfen Sie auf dem Verbindungsserver- oder Sicherheitsserver-Host die Protokolldateien unter *Laufwerk:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs* auf Meldungen, die die Aktivierung der Smartcard-Authentifizierung angeben.

Verwenden der Smartcard-Zertifikatssperrüberprüfung

Sie können verhindern, dass sich Benutzer mit gesperrten Benutzerzertifikaten mit Smartcards authentifizieren, indem Sie die Zertifikatssperrüberprüfung konfigurieren. Wenn Benutzer eine Organisation verlassen, eine Smartcard verlieren oder die Abteilung wechseln, werden Zertifikate häufig gesperrt.

Horizon 7 unterstützt die Zertifikatssperrüberprüfung mit Zertifikatssperrlisten und dem Online Certificate Status Protocol (OCSP). Eine Zertifikatssperrliste ist eine Liste mit gesperrten Zertifikaten, die von der Zertifizierungsstelle veröffentlicht wird, die das Zertifikat ausgestellt hat. OCSP ist ein Zertifikatüberprüfungsprotokoll, das zum Abrufen des Sperrstatus eines X.509-Zertifikats verwendet wird.

Die Zertifikatssperrüberprüfung kann auf einer Verbindungsserver-Instanz oder auf einem Sicherheitsserver konfiguriert werden. Wenn eine Verbindungsserver-Instanz mit einem Sicherheitsserver kombiniert wird, konfigurieren Sie die Zertifikatssperrüberprüfung auf dem Sicherheitsserver. Der Zugriff auf die Zertifizierungsstelle muss über den Verbindungsserver- oder Sicherheitsserver-Host möglich sein.

Auf einer Verbindungsserver-Instanz oder einem Sicherheitsserver können sowohl Zertifikatsperrlisten als auch OCSPs verwendet werden. Wenn Sie die Überprüfung mit beiden Zertifikatsperrüberprüfungen konfigurieren, versucht Horizon 7 zunächst, OCSP zu verwenden. Wenn dies nicht möglich ist, wird die Zertifikatsperrliste verwendet. Wenn über die Zertifikatsperrliste keine Überprüfung möglich ist, greift Horizon 7 nicht auf OCSP zurück.

- **Anmelden bei Verwendung der Überprüfung von Zertifikatsperrlisten**

Wenn Sie die Überprüfung von Zertifikatsperrlisten konfigurieren, erstellt und liest Horizon 7 eine Zertifikatsperrliste, um den Sperrstatus eines Benutzerzertifikats zu ermitteln.

- **Anmelden bei Verwendung der OCSP-Zertifikatsperrüberprüfung**

Wenn Sie die OCSP-Zertifikatsperrüberprüfung konfigurieren, sendet Horizon 7 eine Anforderung an einen OCSP-Antwortdienst, um den Sperrstatus eines bestimmten Benutzerzertifikats zu ermitteln. Horizon 7 verwendet ein OCSP-Signaturzertifikat, um die Gültigkeit der vom OCSP-Antwortdienst erhaltenen Antworten zu überprüfen.

- **Konfigurieren der Überprüfung von Zertifikatsperrlisten**

Wenn Sie die Überprüfung von Zertifikatsperrlisten konfigurieren, liest Horizon 7 eine Zertifikatsperrliste, um den Sperrstatus eines Smartcard-Benutzerzertifikats zu ermitteln.

- **Konfigurieren der OCSP-Zertifikatsperrüberprüfung**

Wenn Sie die OCSP-Zertifikatsperrüberprüfung konfigurieren, sendet Horizon 7 eine Überprüfungsanforderung an einen OCSP-Antwortdienst, um den Sperrstatus eines Smartcard-Benutzerzertifikats zu ermitteln.

- **Eigenschaften der Smartcard-Zertifikatsperrüberprüfung**

In der Datei `locked.properties` können Werte zum Aktivieren und Konfigurieren der Smartcard-Zertifikatsperrüberprüfung gesetzt werden.

Anmelden bei Verwendung der Überprüfung von Zertifikatsperrlisten

Wenn Sie die Überprüfung von Zertifikatsperrlisten konfigurieren, erstellt und liest Horizon 7 eine Zertifikatsperrliste, um den Sperrstatus eines Benutzerzertifikats zu ermitteln.

Wenn ein Benutzerzertifikat gesperrt wurde und die Smartcard-Authentifizierung optional ist, wird der Benutzer über das Dialogfeld **Geben Sie Ihren Benutzernamen und das Kennwort ein** zur Angabe eines Kennworts für die Authentifizierung aufgefordert. Wenn die Smartcard-Authentifizierung erforderlich ist, wird eine Fehlermeldung angezeigt und der Benutzer kann nicht authentifiziert werden. Dasselbe geschieht, wenn Horizon 7 die Zertifikatsperrliste nicht lesen kann.

Anmelden bei Verwendung der OCSP-Zertifikatsperrüberprüfung

Wenn Sie die OCSP-Zertifikatsperrüberprüfung konfigurieren, sendet Horizon 7 eine Anforderung an einen OCSP-Antwortdienst, um den Sperrstatus eines bestimmten Benutzerzertifikats zu ermitteln. Horizon 7 verwendet ein OCSP-Signaturzertifikat, um die Gültigkeit der vom OCSP-Antwortdienst erhaltenen Antworten zu überprüfen.

Wenn das Benutzerzertifikat gesperrt wurde und die Smartcard-Authentifizierung optional ist, wird der Benutzer über das Dialogfeld **Geben Sie Ihren Benutzernamen und das Kennwort ein** zur Angabe eines Kennworts für die Authentifizierung aufgefordert. Wenn die Smartcard-Authentifizierung erforderlich ist, wird eine Fehlermeldung angezeigt, und der Benutzer kann nicht authentifiziert werden.

Wenn Horizon 7 keine oder eine ungültige Antwort vom OCSP-Antwortdienst erhält, wird die Überprüfung von Zertifikatssperrlisten verwendet.

Konfigurieren der Überprüfung von Zertifikatssperrlisten

Wenn Sie die Überprüfung von Zertifikatssperrlisten konfigurieren, liest Horizon 7 eine Zertifikatssperrliste, um den Sperrstatus eines Smartcard-Benutzerzertifikats zu ermitteln.

Voraussetzungen

Machen Sie sich mit den Eigenschaften der Datei `locked.properties` für die Überprüfung von Zertifikatssperrlisten vertraut. Siehe [Eigenschaften der Smartcard-Zertifikatssperrüberprüfung](#).

Verfahren

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im TLS/SSL-Gatewaykonfigurationsordner auf dem Verbindungsserver- oder Sicherheitsserver-Host.
Beispiel: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 2 Fügen Sie die Eigenschaften `enableRevocationChecking` und `crlLocation` zur Datei `locked.properties` hinzu.
 - a Setzen Sie `enableRevocationChecking` auf **true**, um die Smartcard-Zertifikatssperrüberprüfung zu aktivieren.
 - b Setzen Sie `crlLocation` auf den Speicherort der Zertifikatssperrliste. Als Wert kann eine URL oder ein Dateipfad angegeben werden.
- 3 Starten Sie den Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Beispiel: `locked.properties`-Datei

Mit der gezeigten Datei wird die Smartcard-Authentifizierung und die Smartcard-Zertifikatssperrüberprüfung aktiviert, die Überprüfung von Zertifikatssperrlisten konfiguriert und eine URL als Speicherort der Zertifikatssperrliste angegeben.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

Konfigurieren der OCSP-Zertifikatsperrüberprüfung

Wenn Sie die OCSP-Zertifikatsperrüberprüfung konfigurieren, sendet Horizon 7 eine Überprüfungsanforderung an einen OCSP-Antwortdienst, um den Sperrstatus eines Smartcard-Benutzerzertifikats zu ermitteln.

Voraussetzungen

Machen Sie sich mit den Eigenschaften der Datei `locked.properties` für die OCSP-Zertifikatssperrüberprüfung vertraut. Siehe [Eigenschaften der Smartcard-Zertifikatssperrüberprüfung](#).

Verfahren

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im TLS/SSL-Gatewaykonfigurationsordner auf dem Verbindungsserver- oder Sicherheitsserver-Host.

Beispiel: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 2 Fügen Sie die Eigenschaften `enableRevocationChecking`, `enableOCSP`, `ocspURL` und `ocspSigningCert` zur Datei `locked.properties` hinzu.
 - a Setzen Sie `enableRevocationChecking` auf **true**, um die Smartcard-Zertifikatssperrüberprüfung zu aktivieren.
 - b Setzen Sie `enableOCSP` auf **true**, um die OCSP-Zertifikatssperrüberprüfung zu aktivieren.
 - c Setzen Sie `ocspURL` auf die URL des OCSP-Antwortdiensts.
 - d Setzen Sie `ocspSigningCert` auf den Speicherort der Datei, die das Signaturzertifikat des OCSP-Antwortdiensts enthält.
- 3 Starten Sie den Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Beispiel: `locked.properties`-Datei

Mit der gezeigten Datei wird die Smartcard-Authentifizierung und die Smartcard-Zertifikatssperrüberprüfung aktiviert, die Überprüfung von Zertifikatssperrlisten und die OCSP-Zertifikatssperrüberprüfung konfiguriert sowie der Speicherort des OCSP-Antwortdiensts und die Datei mit dem OCSP-Signaturzertifikat angegeben.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

Eigenschaften der Smartcard-Zertifikatsperrüberprüfung

In der Datei `locked.properties` können Werte zum Aktivieren und Konfigurieren der Smartcard-Zertifikatsperrüberprüfung gesetzt werden.

[Tabelle 4-1. Eigenschaften für die Smartcard-Zertifikatsperrüberprüfung](#) listet die Eigenschaften der Datei `locked.properties` für die Zertifikatsperrüberprüfung auf.

Tabelle 4-1. Eigenschaften für die Smartcard-Zertifikatsperrüberprüfung

Eigenschaft	Beschreibung
<code>enableRevocationChecking</code>	<p>Setzen Sie diese Eigenschaft auf true, um die Zertifikatsperrüberprüfung zu aktivieren.</p> <p>Wenn diese Eigenschaft auf false gesetzt ist, ist die Zertifikatsperrüberprüfung deaktiviert und alle anderen Eigenschaften für die Zertifikatsperrüberprüfung werden ignoriert.</p> <p>Der Standardwert lautet false.</p>
<code>crlLocation</code>	<p>Gibt den Speicherort der Zertifikatsperrliste als URL oder Dateipfad an.</p> <p>Wenn Sie keine URL angeben oder die angegebene URL nicht gültig ist, verwendet Horizon 7 die Liste der Zertifikatsperrlisten des Benutzerzertifikats, wenn <code>allowCertCRLs</code> auf true gesetzt ist oder nicht angegeben wurde.</p> <p>Wenn Horizon 7 nicht auf eine Zertifikatsperrliste zugreifen kann, schlägt die Überprüfung von Zertifikatsperrlisten fehl.</p>
<code>allowCertCRLs</code>	<p>Wenn diese Eigenschaft auf true gesetzt ist, extrahiert Horizon 7 eine Liste mit Zertifikatsperrlisten aus dem Benutzerzertifikat.</p> <p>Der Standardwert lautet true.</p>
<code>enableOCSP</code>	<p>Setzen Sie diese Eigenschaft auf true, um die OCSP-Zertifikatsperrüberprüfung zu aktivieren.</p> <p>Der Standardwert lautet false.</p>
<code>ocspURL</code>	Gibt die URL eines OCSP-Antwortdiensts an.
<code>ocspResponderCert</code>	Gibt die Datei mit dem Signaturzertifikat des OCSP-Antwortdiensts an. Horizon 7 stellt anhand dieses Zertifikats sicher, dass die Antworten des OCSP-Antwortdiensts gültig sind.
<code>ocspSendNonce</code>	<p>Wenn diese Eigenschaft auf true gesetzt ist, wird mit OCSP-Anforderungen eine Nonce gesendet, um wiederholte Antworten zu verhindern.</p> <p>Der Standardwert lautet false.</p>
<code>ocspCRLFailover</code>	<p>Wenn diese Eigenschaft auf true gesetzt ist, verwendet Horizon 7 beim Fehlschlagen der OCSP-Zertifikatsperrüberprüfung die Überprüfung von Zertifikatsperrlisten.</p> <p>Der Standardwert lautet true.</p>

Einrichten anderer Typen der Benutzerauthentifizierung

5

Horizon 7 nutzt die vorhandene Active Directory-Infrastruktur für die Benutzer- und Administratorauthentifizierung und -verwaltung. Sie können Horizon 7 auch mit anderen Arten der Authentifizierung neben Smartcards integrieren, um Benutzer von Remote-Desktops und Remoteanwendungen zu authentifizieren, z. B. mit Lösungen zur biometrischen Authentifizierung oder mit Zwei-Faktor-Authentifizierungen wie RSA SecurID und RADIUS.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden der zweistufigen Authentifizierung](#)
- [Verwenden der SAML-Authentifizierung](#)
- [Konfigurieren der biometrischen Authentifizierung](#)

Verwenden der zweistufigen Authentifizierung

Sie können eine Horizon-Verbindungsserver-Instanz konfigurieren, sodass Benutzer eine RSA SecurID-Authentifizierung oder RADIUS (Remote Authentication Dial-In User Service)-Authentifizierung verwenden müssen.

- RADIUS unterstützt ein breites Spektrum an alternativen tokenbasierten Zwei-Faktor-Authentifizierungsmöglichkeiten.
- Horizon 7 bietet auch eine offene Standarderweiterungsschnittstelle, die es Drittanbietern ermöglicht, fortschrittliche Authentifizierungserweiterungen in Horizon 7 zu integrieren.

Da Zwei-Faktor-Authentifizierungslösungen wie RSA SecurID und RADIUS mit Authentifizierungsmanagern arbeiten, die auf separaten Servern installiert sind, müssen Sie diese Server für den Verbindungsserver-Host konfigurieren und zugänglich machen. Wenn Sie beispielsweise RSA SecurID verwenden, wäre RSA Authentication Manager der Authentifizierungsmanager. Wenn Sie RADIUS verwenden, wäre der Authentifizierungsmanager ein RADIUS-Server.

Für die Verwendung der Zwei-Faktor-Authentifizierung muss jeder Benutzer über einen Token wie einen RSA SecurID-Token verfügen, der bei seinem Authentifizierungsmanager registriert ist. Bei einem Zwei-Faktor-Authentifizierungstoken handelt es sich um Hardware oder Software, über die in festgelegten Intervallen ein Authentifizierungscode generiert wird. Oft erfordert die Authentifizierung Kenntnis einer PIN und eines Authentifizierungscode.

Wenn es mehrere Verbindungsserver-Instanzen gibt, können Sie die Zwei-Faktor-Authentifizierung für einige Instanzen konfigurieren und für andere eine andere Benutzerauthentifizierungsmethode einrichten. Sie können beispielsweise die Zwei-Faktor-Authentifizierung nur für Benutzer konfigurieren, die von außerhalb des Firmennetzwerks über das Internet auf Remote-Desktops und -Anwendungen zugreifen.

Horizon 7 ist gemäß dem RSA SecurID Ready-Programm zertifiziert und unterstützt die vollständige Palette von SecurID-Funktionen, einschließlich New PIN Mode, Next Token Code Mode, RSA Authentication Manager und Lastenausgleich.

- **Anmeldung unter Verwendung der zweistufigen Authentifizierung**

Wenn sich ein Benutzer bei einer Verbindungsserver-Instanz anmeldet, für welche die RSA SecurID- oder RADIUS-Authentifizierung aktiviert wurde, wird in Horizon Client ein eigenes Anmeldedialogfeld angezeigt.

- **Aktivieren der Zwei-Faktor-Authentifizierung in Horizon Console**

Sie können eine Verbindungsserver-Instanz für die RSA SecurID- oder RADIUS-Authentifizierung aktivieren, indem Sie die Verbindungsserver-Einstellungen in Horizon Console bearbeiten.

- **Fehlerbehebung bei verweigertem RSA SecureID-Zugriff**

Bei der Verbindung von Horizon Client mit RSA SecurID-Authentifizierung wird der Zugriff verweigert.

- **Fehlerbehebung bei Verweigerung des Zugriffs auf RADIUS**

Bei der Verbindung von Horizon Client mit der zweistufigen RADIUS-Authentifizierung wird der Zugriff verweigert.

Anmeldung unter Verwendung der zweistufigen Authentifizierung

Wenn sich ein Benutzer bei einer Verbindungsserver-Instanz anmeldet, für welche die RSA SecurID- oder RADIUS-Authentifizierung aktiviert wurde, wird in Horizon Client ein eigenes Anmeldedialogfeld angezeigt.

Der Benutzer gibt seinen RSA SecurID- oder RADIUS-Authentifizierungsbenutzernamen und -Passcode in das eigene Anmeldedialogfeld ein. Ein Zwei-Faktor-Authentifizierungs-Passcode umfasst typischerweise eine PIN, auf die ein Token-Code folgt.

- Wenn in RSA Authentication Manager festgelegt ist, dass Benutzer nach der Eingabe von RSA SecurID-Benutzernamen und -Passcode eine neue RSA SecurID-PIN eingeben müssen, wird ein entsprechendes Dialogfeld angezeigt. Nach dem Festlegen einer neuen PIN werden die Benutzer aufgefordert, vor der Anmeldung auf den nächsten Token-Code zu warten. Wenn RSA Authentication Manager für die Verwendung von PINs konfiguriert ist, die vom System generiert werden, wird ein Dialogfeld zur Bestätigung der PIN angezeigt.
- Die RADIUS-Authentifizierung beim Anmelden bei Horizon 7 erfolgt auf ähnliche Weise wie die RSA SecurID-Authentifizierung. Wenn der RADIUS-Server eine Zugriffsaufforderung ausgibt, wird in Horizon Client ein Dialogfeld angezeigt, das der RSA SecurID-Eingabeaufforderung für den nächsten

Token-Code ähnelt. Die Unterstützung für RADIUS-Aufforderungen ist derzeit auf die Eingabeaufforderung für Texteingaben begrenzt. Vom RADIUS-Server gesendeter Aufforderungstext wird nicht angezeigt. Komplexere Aufforderungsformen wie Multiple Choice und Bildauswahl werden derzeit nicht unterstützt.

Nach Eingabe der Anmeldedaten in Horizon Client durch den Benutzer kann der RADIUS-Server eine SMS-Textnachricht, eine E-Mail oder über einen anderen Out-of-Band-Mechanismus einen Text mit einem Code an das Mobiltelefon des Benutzers senden. Der Benutzer kann dann den betreffenden Text und Code in Horizon Client eingeben, um die Authentifizierung abzuschließen.

- Da einige RADIUS-Anbieter die Möglichkeit bieten, Benutzer aus Active Directory zu importieren, werden Endbenutzer möglicherweise zunächst aufgefordert, Active Directory-Anmeldeinformationen anzugeben, bevor sie zur Eingabe des RADIUS-Authentifizierungsbenutzernamens und -Passcodes aufgefordert werden.

Aktivieren der Zwei-Faktor-Authentifizierung in Horizon Console

Sie können eine Verbindungsserver-Instanz für die RSA SecurID- oder RADIUS-Authentifizierung aktivieren, indem Sie die Verbindungsserver-Einstellungen in Horizon Console bearbeiten.

Voraussetzungen

Installieren und konfigurieren Sie die Software für Zwei-Faktor-Authentifizierung, z. B. RSA SecurID oder RADIUS auf einem Authentifizierungsmanager-Server.

- Exportieren Sie im Fall der RSA SecurID-Authentifizierung die Datei `sdconf.rec` für die Verbindungsserver-Instanz aus RSA Authentication Manager. Weitere Informationen finden Sie in der RSA Authentication Manager-Dokumentation.
- Befolgen Sie für die RADIUS-Authentifizierung die Anweisungen in der Konfigurationsdokumentation des Anbieters. Notieren Sie sich den Hostnamen oder die IP-Adresse des RADIUS-Servers, die Portnummer, unter der die RADIUS-Authentifizierung überwacht wird (in der Regel 1812), den Authentifizierungstyp (PAP, CHAP, MS-CHAPv1 oder MS-CHAPv2) und den gemeinsamen geheimen Schlüssel. Sie können diese Werte in Horizon Console eingeben. Sie können Werte für einen primären und einen sekundären RADIUS-Authentifikator eingeben.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Server**.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie auf der Registerkarte **Authentifizierung** im Bereich **Erweiterte Authentifizierung** aus dem Dropdown-Menü **2-Faktor-Authentifizierung** die Option **RSA SecureID** oder **RADIUS** aus.

- 4 Um die Übereinstimmung von RSA SecurID- oder RADIUS-Benutzernamen und Benutzernamen in Active Directory zu erzwingen, wählen Sie **Abstimmung von SecurID- und Windows-Benutzernamen erzwingen** oder **Abstimmung von 2-Faktor- und Windows-Benutzernamen erzwingen**.

Bei Auswahl dieser Option müssen die Benutzer den RSA SecurID- bzw. RADIUS-Benutzernamen auch für die Active Directory-Authentifizierung verwenden. Wenn Sie diese Option nicht auswählen, können unterschiedliche Namen gewählt werden.

- 5 Klicken Sie für RSA SecurID auf **Datei hochladen** und geben Sie den Speicherort der Datei `sdconf.rec` ein oder klicken Sie auf **Durchsuchen**, um nach der Datei zu suchen.

6 Füllen Sie für die RADIUS-Authentifizierung die übrigen Felder aus:

- a Wählen Sie **Den gleichen Benutzernamen und das gleiche Kennwort für die RADIUS- und Windows-Authentifizierung verwenden**, wenn die ursprüngliche RADIUS-Authentifizierung eine Windows-Authentifizierung verwendet, die eine Out-of-Band-Übertragung eines Token-Codes auslöst, der wiederum als Teil einer RADIUS-Aufforderung verwendet wird.

Wenn Sie dieses Kontrollkästchen aktivieren, werden die Benutzer nach der RADIUS-Authentifizierung nicht zur Eingabe der Windows-Anmeldedaten aufgefordert, wenn die RADIUS-Authentifizierung den Windows-Benutzernamen und das Windows-Kennwort verwendet. Die Benutzer müssen den Windows-Benutzernamen und das Windows-Kennwort nach der RADIUS-Authentifizierung nicht erneut eingeben.

- b Wählen Sie im Dropdown-Menü **Authentifikator** die Option **Neuen Authentifikator erstellen** und füllen Sie die Seite aus.
- Damit benutzerdefinierte Benutzernamen- und Kennungsbezeichnungen im RADIUS-Authentifizierungsdialogfeld für Endbenutzer angezeigt werden, geben Sie benutzerdefinierte Bezeichnungen in die Felder **Benutzernamenbezeichnung** und **Kennungsbezeichnung** ein.
 - Legen Sie für **Kontoführungsport** den Wert **0** fest, es sei denn, Sie möchten die RADIUS-Kontoführung aktivieren. Legen Sie für diesen Port nur dann eine Portnummer fest, die nicht null ist, wenn Ihr RADIUS-Server das Erfassen von Kontoführungsdaten unterstützt. Wenn der RADIUS-Server Kontoführungsnachrichten nicht unterstützt und Sie für diesen Port eine Portnummer ungleich null festlegen, werden die Nachrichten gesendet, ignoriert und daraufhin mehrere Male erneut gesendet, was zu einer Verzögerung bei der Authentifizierung führt.

Kontoführungsdaten können verwendet werden, um basierend auf den Nutzungszeiten und -daten Rechnungen für die Benutzer auszustellen. Darüber hinaus können Kontoführungsdaten für statistische Zwecke sowie zur allgemeinen Netzwerküberwachung verwendet werden.

- Wenn Sie eine Bereichspräfixzeichenfolge angeben, wird diese Zeichenfolge an den Anfang des Benutzernamens gestellt, wenn dieser an den RADIUS-Server gesendet wird. Wenn der in Horizon Client eingegebene Benutzername beispielsweise **JDoe** lautet und als Bereichspräfix **DOMÄNE-A** angegeben wird, wird **DOMÄNE-A\JDoe** als Benutzername an den RADIUS-Server gesendet. Wenn Sie die Bereichssuffix- oder Postfixzeichenfolge **@mycorp.com** verwenden, wird entsprechend **JDoe@mycorp.com** als Benutzername an den RADIUS-Server gesendet.

7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Der Verbindungsserver-Dienst muss nicht neu gestartet werden. Die erforderlichen Konfigurationsdateien werden automatisch verteilt und die Konfigurationseinstellungen werden umgehend angewendet.

Wenn Benutzer Horizon Client öffnen und sich beim Verbindungsserver authentifizieren, werden Sie zur Zwei-Faktor-Authentifizierung aufgefordert. Bei der RADIUS-Authentifizierung werden im Anmelde-Dialogfeld Aufforderungen in Textform angezeigt, die die angegebene Tokenbezeichnung enthalten.

Änderungen bei den RADIUS-Authentifizierungseinstellungen betreffen Remote-Desktop- und Anwendungssitzungen, die nach dem Ändern der Konfiguration gestartet werden. Aktuelle Sitzungen sind von Änderungen an den RADIUS-Authentifizierungseinstellungen nicht betroffen.

Nächste Schritte

Wenn Sie über eine replizierte Gruppe von Verbindungsserver-Instanzen verfügen und auf diesen Instanzen außerdem eine RADIUS-Authentifizierung einrichten möchten, können Sie eine bestehende RADIUS-Authentifikatorkonfiguration verwenden.

Fehlerbehebung bei verweigertem RSA SecureID-Zugriff

Bei der Verbindung von Horizon Client mit RSA SecurID-Authentifizierung wird der Zugriff verweigert.

Problem

Bei einer Horizon Client-Verbindung mit RSA SecurID wird die Meldung **Zugriff verweigert** angezeigt und die RSA Authentication Manager-Protokollüberwachung zeigt den Fehler **Knotenverifizierung fehlgeschlagen** an.

Ursache

Das RSA-Agentenhost-Knotenkennwort muss zurückgesetzt werden.

Lösung

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Server**.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie auf der Registerkarte **Authentifizierung** im Bereich **Erweiterte Authentifizierung** aus dem Dropdown-Menü **2-Faktor-Authentifizierung** die Option **RSA SecureID** aus.
- 4 Wählen Sie **Geheimen Schlüssel des Knotens löschen** aus und klicken Sie auf **OK**.
- 5 Wählen Sie auf dem Computer, auf dem RSA Authentication Manager ausgeführt wird, das Verzeichnis **Start > Programme > RSA Security > RSA Authentication Manager Host Mode**.
- 6 Wählen Sie **Agentenhost > Agentenhost bearbeiten**.
- 7 Wählen Sie den Verbindungsserver aus der Liste aus und deaktivieren Sie das Kontrollkästchen **Knotenkennwort erstellt**.
Die Option **Knotenkennwort erstellt** wird bei jeder Bearbeitung standardmäßig ausgewählt.
- 8 Klicken Sie auf **OK**.

Fehlerbehebung bei Verweigerung des Zugriffs auf RADIUS

Bei der Verbindung von Horizon Client mit der zweistufigen RADIUS-Authentifizierung wird der Zugriff verweigert.

Problem

Eine Horizon Client-Verbindung unter Verwendung der zweistufigen RADIUS-Authentifizierung zeigt Zugriff verweigert an.

Ursache

RADIUS erhält keine Antwort vom RADIUS-Server, wodurch eine Zeitüberschreitung von Horizon 7 auftritt.

Lösung

Die folgenden allgemeinen Konfigurationsfehler führen am häufigsten zu dieser Situation:

- Der RADIUS-Server wurde nicht so konfiguriert, dass die Verbindungsserver-Instanz als RADIUS-Client akzeptiert wird. Jede Verbindungsserver-Instanz mit RADIUS muss auf dem RADIUS-Server als Client festgelegt werden. Weitere Informationen finden Sie in der Dokumentation für das Produkt der zweistufigen RADIUS-Authentifizierung.
- Die gemeinsamen geheimen Werte auf der Verbindungsserver-Instanz und dem RADIUS-Server stimmen nicht überein.

Verwenden der SAML-Authentifizierung

Die Security Assertion Markup Language (SAML) ist ein XML-basierter Standard, der zur Beschreibung und zum Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen unterschiedlichen Sicherheitsdomänen verwendet wird. SAML überträgt Informationen zu Benutzern zwischen Identitätsanbietern und Diensteanbietern in XML-Dokumenten namens SAML-Zusicherungen.

Sie können die SAML-Authentifizierung für die Integration von Horizon 7 mit VMware Workspace ONE, VMware Identity Manager oder mit einem qualifizierten Lastausgleichsdienst oder Gateway von Drittanbietern verwenden. Wenn Sie SAML für ein Gerät von Drittanbietern konfigurieren, finden Sie in der Dokumentation des Anbieters Informationen zur Konfiguration von Horizon 7 für die Verwendung damit. Wenn SSO aktiviert ist, haben Benutzer, die sich bei VMware Identity Manager oder dem Gerät eines Drittanbieters anmelden, die Möglichkeit, Remote-Desktops und -anwendungen zu starten, ohne einen zweiten Anmeldevorgang durchführen zu müssen. Mit der SAML-Authentifizierung haben Sie auch die Möglichkeit, die Smartcard-Authentifizierung für VMware Access Point oder für Drittanbietergeräte zu implementieren.

Zur Delegierung der Verantwortlichkeit für die Authentifizierung bei Workspace ONE, VMware Identity Manager oder dem Gerät eines Drittanbieters müssen Sie einen SAML-Authentifikator in Horizon 7 erstellen. Ein SAML-Authentifikator enthält den Vertrauensstellungs- und Metadaten austausch zwischen Horizon 7 und Workspace ONE, VMware Identity Manager oder dem Gerät des Drittanbieters. Sie verknüpfen einen SAML-Authentifikator mit einer Verbindungsserver-Instanz.

Verwenden der SAML-Authentifizierung zur VMware Identity Manager-Integration

Die Integration zwischen Horizon 7 und VMware Identity Manager (früher als Workspace ONE bezeichnet) verwendet den SAML 2.0-Standard zum Aufbau von gegenseitigem Vertrauen, das für die SSO-Funktion (Single Sign-On) äußerst wichtig ist. Wenn SSO aktiviert ist, können Benutzer, die sich bei VMware Identity Manager oder Workspace ONE mit Active Directory-Anmeldedaten anmelden, Remote-Desktops und -Anwendungen starten, ohne einen zweiten Anmeldevorgang zu durchlaufen.

Wenn VMware Identity Manager und Horizon 7 integriert sind, erzeugt VMware Identity Manager ein eindeutiges SAML-Artefakt, sobald sich ein Benutzer bei VMware Identity Manager anmeldet und auf ein Desktop- oder Anwendungssymbol klickt. VMware Identity Manager verwendet dieses SAML-Artefakt zum Erstellen eines URI (Uniform Resource Identifier). Der URI enthält Informationen zur Verbindungsserver-Instanz, in der sich der Desktop- oder Anwendungspool befindet, die Angabe, welcher Desktop oder welche Anwendung gestartet werden soll, und das SAML-Artefakt.

VMware Identity Manager sendet das SAML-Artefakt an Horizon Client, der seinerseits das Artefakt an die Verbindungsserver-Instanz sendet. Die Verbindungsserver-Instanz verwendet das SAML-Artefakt, um die SAML-Zusicherung von VMware Identity Manager abzurufen.

Nachdem eine Verbindungsserver-Instanz eine SAML-Zusicherung erhalten hat, validiert sie die Zusicherung, entschlüsselt das Kennwort des Benutzers und verwendet das entschlüsselte Kennwort, um den Desktop oder die Anwendung zu starten.

Die Einrichtung von VMware Identity Manager und die Horizon 7-Integration erfordert auch die Konfiguration von VMware Identity Manager mit Horizon 7-Informationen und die Konfiguration von Horizon 7 zur Delegierung der Verantwortlichkeit zur Authentifizierung an VMware Identity Manager.

Zur Delegierung der Verantwortlichkeit für die Authentifizierung an VMware Identity Manager müssen Sie einen SAML-Authentifikator in Horizon 7 erstellen. Ein SAML-Authentifikator enthält den Vertrauens- und Metadaten austausch zwischen Horizon 7 und VMware Identity Manager. Sie verknüpfen einen SAML-Authentifikator mit einer Verbindungsserver-Instanz.

Hinweis Wenn Sie den Zugriff auf Ihre Desktops und Anwendungen über VMware Identity Manager ermöglichen möchten, müssen Sie die Desktop- und Anwendungspools als Benutzer mit Administratorrolle für die Stammzugriffsgruppe in Horizon Console erstellen. Wenn Sie dem Benutzer die Administratorrolle für eine andere Zugriffsgruppe als die Stammzugriffsgruppe gewähren, erkennt VMware Identity Manager den in Horizon 7 konfigurierten SAML-Authentifikator nicht und Sie können den Pool nicht in VMware Identity Manager konfigurieren.

Konfigurieren eines SAML-Authentifikators in Horizon Console

Um Remote-Desktops und -anwendungen aus VMware Identity Manager zu starten oder um mit Remote-Desktops und -anwendungen mithilfe eines Lastausgleichsdienstes oder eines Gateways von Drittanbietern eine Verbindung herzustellen, müssen Sie in Horizon Console einen SAML-Authentifikator erstellen. Ein SAML-Authentifikator enthält den Vertrauensstellungs- und Metadaten austausch zwischen Horizon 7 und dem Gerät, mit dem Clients eine Verbindung herstellen.

Sie verknüpfen einen SAML-Authentifikator mit einer Verbindungsserver-Instanz. Wenn Ihre Bereitstellung mehr als eine Verbindungsserver-Instanz beinhaltet, müssen Sie den SAML-Authentifikator mit jeder Instanz verknüpfen.

Sie können festlegen, dass ein statischer Authentifikator und mehrere dynamische Authentifikatoren zur gleichen Zeit aktiv sein können. Sie haben die Möglichkeit, (dynamische) vIDM- und (statische) Unified Access Gateway-Authentifikatoren zu konfigurieren und sie im aktiven Zustand zu belassen. Verbindungen können über beide Arten von Authentifikatoren hergestellt werden.

Sie können mehrere SAML-Authentifikatoren für einen Verbindungsserver konfigurieren, und alle Authentifikatoren können gleichzeitig aktiv sein. Allerdings müssen die auf dem Verbindungsserver konfigurierten SAML-Authentifikatoren jeweils über eine eigene Entitäts-ID verfügen.

Im Dashboard wird der Status des SAML-Authentifikators immer grün angezeigt, da es sich um vordefinierte Metadaten handelt, die von Haus aus statisch sind. Der Wechsel von rot zu grün betrifft nur dynamische Authentifikatoren.

Informationen zur Konfiguration eines SAML-Authentifikators für VMware Unified Access Gateway-Appliances finden Sie in der Unified Access Gateway-Dokumentation.

Voraussetzungen

- Stellen Sie sicher, dass Workspace ONE, VMware Identity Manager oder ein Gateway bzw. ein Lastausgleichsdienst eines Drittanbieters installiert und konfiguriert ist. Weitere Informationen finden Sie in der Installationsdokumentation des betreffenden Produkts.
- Stellen Sie sicher, dass das Stammzertifikat der signierenden Zertifizierungsstelle für das SAML-Serverzertifikat auf dem Verbindungsserver-Host installiert ist. VMware empfiehlt nicht, SAML-Authentifikatoren zur Verwendung selbstsignierter Zertifikate zu konfigurieren. Informationen zur Zertifikatauthentifizierung finden Sie im Dokument *Horizon 7-Installation*.
- Notieren Sie sich den FQDN oder die IP-Adresse des Workspace ONE-Servers, des VMware Identity Manager-Servers oder des externen Lastausgleichsdiensts.
- Wenn Sie Workspace ONE oder VMware Identity Manager verwenden, notieren Sie sich die URL der Connector-Web-Schnittstelle.
- Wenn Sie einen Authentifikator für eine Unified Access Gateway-Appliance oder eine Drittanbieter-Appliance erstellen, für die Sie SAML-Metadaten generieren und einen statischen Authentifikator erstellen müssen, führen Sie den Vorgang zur Generierung der SAML-Metadaten auf dem Gerät aus und kopieren Sie dann die Metadaten.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Server**.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** eine Serverinstanz aus, die mit dem SAML-Authentifikator verknüpft werden soll, und klicken Sie auf **Bearbeiten**.

- 3 Wählen Sie auf der Registerkarte **Authentifizierung** eine Einstellung aus dem Dropdown-Menü **Delegierung von Authentifizierung an VMware Horizon (SAML 2.0-Authentifikator)** aus, um den SAML-Authentifikator zu aktivieren oder zu deaktivieren.

Option	Beschreibung
Deaktiviert	Die SAML-Authentifizierung ist deaktiviert. Sie können Remote-Desktops und -anwendungen nur aus Horizon Client heraus starten.
Zulässig	Die SAML-Authentifizierung ist aktiviert. Sie können Remote-Desktops und -anwendungen sowohl von Horizon Client und VMware Identity Manager als auch vom Gerät eines Drittanbieters aus starten.
Erforderlich	Die SAML-Authentifizierung ist aktiviert. Sie können Remote-Desktops und -anwendungen nur von VMware Identity Manager oder vom Gerät eines Drittanbieters aus starten. Sie können Desktops oder Anwendungen nicht manuell aus Horizon Client heraus starten.

Sie können die einzelnen Verbindungsserver-Instanzen in Ihrer Bereitstellung so konfigurieren, dass sie abhängig von Ihren Anforderungen über unterschiedliche SAML-Authentifizierungseinstellungen verfügen.

- 4 Klicken Sie auf **SAML-Authentifikatoren verwalten** und dann auf **Hinzufügen**.
- 5 Konfigurieren Sie den SAML-Authentifikator im Dialogfeld zum Hinzufügen von SAML 2.0-Authentifikatoren.

Option	Beschreibung
Typ	Wählen Sie für eine Unified Access Gateway-Appliance oder ein Drittanbietergerät Statisch aus. Wählen Sie für VMware Identity Manager die Option Dynamisch aus. Für dynamische Authentifikatoren können Sie eine Metadaten-URL und eine Verwaltungs-URL angeben. Bei statischen Authentifikatoren müssen Sie zunächst die Metadaten auf der Unified Access Gateway-Appliance oder dem Drittanbietergerät generieren, die Metadaten kopieren und diese dann in das Textfeld SAML-Metadaten einfügen.
Bezeichnung	Eindeutiger Name, der den SAML-Authentifikator identifiziert.
Beschreibung	Kurzbeschreibung des SAML-Authentifikators. Dieser Wert ist optional.
Metadaten-URL	(Für dynamische Authentifikatoren) URL zum Abrufen aller Informationen, die für den Austausch von SAML-Informationen zwischen dem SAML-Identitätsanbieter und der Verbindungsserver-Instanz erforderlich sind. Klicken Sie in der URL <code>https://<IHR HORIZON SERVER-NAME>/SAAS/API/1.0/GET/metadata/idp.xml</code> auf <IHR HORIZON SERVER-NAME> und ersetzen Sie diese Zeichenfolge mit dem FQDN oder der IP-Adresse des VMware Identity Manager-Servers oder des externen Lastausgleichsdiensts (Drittanbietergerät).
Verwaltungs-URL	(Für dynamische Authentifikatoren) URL für den Zugriff auf die Verwaltungskonsole des SAML-Identitätsanbieters. Für VMware Identity Manager sollte diese URL auf die VMware Identity Manager Connector-Webschnittstelle verweisen. Dieser Wert ist optional.

Option	Beschreibung
SAML-Metadaten	(Für statische Authentifikatoren) Metadaten text, den Sie generiert und von der Unified Access Gateway-Appliance oder einem Drittanbietergerät kopiert haben.
Aktiviert für den Verbindungsserver	Aktivieren Sie dieses Kontrollkästchen, um den Authentifikator zu aktivieren. Sie können mehrere Authentifikatoren aktivieren. Nur aktivierte Authentifikatoren werden in der Liste angezeigt.

- 6 Klicken Sie auf **OK**, um die SAML-Authentifikatorkonfiguration zu speichern.

Sofern Sie gültige Informationen angegeben haben, müssen Sie entweder das selbstsignierte Zertifikat akzeptieren (nicht empfohlen) oder ein vertrauenswürdigen Zertifikat für Horizon 7 und VMware Identity Manager oder ein Drittanbietergerät verwenden.

Der neu erstellte Authentifikator wird im Dialogfeld „SAML-Authentifikatoren verwalten“ angezeigt.

Nächste Schritte

Erweitern Sie den Ablaufzeitraum der Metadaten des Verbindungsservers, sodass Remotesitzungen nicht nach nur 24 Stunden beendet werden. Siehe [Ändern des Ablaufzeitraums der Metadaten von Diensteanbietern auf dem Verbindungsserver](#).

Konfigurieren der Proxy-Unterstützung für VMware Identity Manager

Horizon 7 bietet eine Proxy-Unterstützung für den VMware Identity Manager (vIDM)-Server. Die Proxy-Details wie z. B. der Hostname und die Portnummer können in der ADAM-Datenbank konfiguriert werden, und die HTTP-Anforderungen lassen sich über den Proxy-Server weiterleiten.

Diese Funktion unterstützt eine hybride Bereitstellung, bei der die lokale Horizon 7-Bereitstellung mit einem vIDM-Server kommunizieren kann, der in der Cloud gehostet wird.

Voraussetzungen

Verfahren

- 1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem Verbindungsserver-Host.
- 2 Erweitern Sie die ADAM ADSI-Baumstruktur im Objektpfad:
`cd=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common Attributes`.
- 3 Wählen Sie **Aktion > Eigenschaften** aus und fügen Sie die Werte für die Einträge `pae-SAMLProxyName` und `pae-SAMLProxyPort` hinzu.

Ändern des Ablaufzeitraums der Metadaten von Diensteanbietern auf dem Verbindungsserver

Wenn Sie den Ablaufzeitraum nicht ändern, akzeptiert der Verbindungsserver nach 24 Stunden keine SAML-Zusicherungen des SAML-Authentifikators mehr, wie eine Unified Access Gateway-Appliance oder einen externen Identitätsanbieter, und der Metadaten austausch muss wiederholt werden.

Mithilfe dieses Verfahrens können Sie die Anzahl der Tage angeben, nach denen der Verbindungsserver keine SAML-Zusicherungen mehr vom Identitätsanbieter akzeptiert. Diese Anzahl wird nach dem Ende des aktuellen Ablaufzeitraums angewendet. Beträgt der aktuelle Ablaufzeitraum beispielsweise einen Tag und Sie haben 90 Tage angegeben, generiert der Verbindungsserver nach einem Tag Metadaten mit einem Ablaufzeitraum von 90 Tagen.

Voraussetzungen

Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogramms ADSI-Editor mit Ihrer Windows-Betriebssystemversion.

Verfahren

- 1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem Verbindungsserver-Host.
- 2 Wählen Sie im Konsolenbaum **Verbinden mit**.
- 3 Geben Sie im Textfeld **Definierten Namen oder Namenskontext auswählen bzw. eintippen** den definierten Namen **DC=vdi**, **DC=vmware**, **DC=int** ein.
- 4 Wählen Sie im Bereich „Computer“ **localhost:389** aus oder geben Sie diesen Wert oder einen vollqualifizierten Domännennamen (FQDN) des Verbindungsserver-Hosts, gefolgt von Port 389, ein.
Beispiel: **localhost:389** oder **meincomputer.example.com:389**
- 5 Erweitern Sie den ADSI-Editor-Strukturbaum, erweitern Sie **OU=Properties**, wählen Sie **OU=Global** aus, und doppelklicken Sie auf **CN=Common** im rechten Bereich.
- 6 Im Dialogfeld „Eigenschaften“ bearbeiten Sie das Attribut **pae-NameValuePair**, um die folgenden Werte hinzuzufügen:

```
cs-samlencryptionkeyvaliditydays=Anzahl von Tagen
cs-samlsigningkeyvaliditydays=Anzahl von Tagen
```

In diesem Beispiel steht *Anzahl von Tagen* für die Anzahl der Tage, nach denen ein Remote-Verbindungsserver keine SAML-Zusicherungen mehr akzeptiert. Nach diesem Zeitraum muss der Austausch von SAML-Metadaten wiederholt werden.

Generieren von SAML-Metadaten für die Verwendung des Verbindungsservers als Dienstanbieter

Nachdem Sie einen SAML-Authentifikator für den gewünschten Identitätsanbieter erstellt und aktiviert haben, müssen Sie eventuell auch die Metadaten des Verbindungsservers generieren. Mit diesen Metadaten können Sie einen Dienstanbieter in der Unified Access Gateway-Appliance oder einen Lastausgleichsdienst von Drittanbietern als Identitätsanbieter erstellen.

Voraussetzungen

Stellen Sie sicher, dass ein SAML-Authentifikator für den Identitätsanbieter erstellt wurde: Unified Access Gateway oder ein Lastausgleichsdienst von Drittanbietern oder ein Gateway.

Verfahren

- 1 Öffnen Sie eine neue Browserregisterkarte und geben Sie die URL für das Abrufen der Verbindungsserver-SAML-Metadaten ein.

`https://connection-server.example.com/SAML/metadata/sp.xml`

In diesem Beispiel stellt *connection-server.example.com* den vollqualifizierten Domännennamen (FQDN) des Verbindungsserver-Hosts dar.

Diese Seite zeigt die SAML-Metadaten des Verbindungsservers an.

- 2 Speichern Sie mit der Option **Speichern unter** die Webseite in einer XML-Datei.

So können Sie die Seite z. B. in einer Datei mit dem Namen `connection-server-metadata.xml` speichern. Der Inhalt dieser Datei beginnt mit dem folgenden Text:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

Nächste Schritte

Mit der entsprechenden Vorgehensweise für den Identitätsanbieter kopieren Sie die SAML-Metadaten für den Verbindungsserver. Nähere Informationen finden Sie in der Dokumentation zu Unified Access Gateway oder zu einem Lastausgleichsdienst von Drittanbietern oder zum Gateway.

Aspekte der Antwortzeit für mehrere dynamische SAML-Authentifikatoren

Angenommen, Sie haben eine SAML 2.0-Authentifizierung auf einer Verbindungsserver-Instanz als optional oder erforderlich konfiguriert und mehrere dynamische SAML-Authentifikatoren mit der Verbindungsserver-Instanz verknüpft. Dann erhöht sich, wenn kein dynamischer SAML-Authentifikator erreichbar ist, die Antwortzeit beim Starten von Remote-Desktops aus anderen dynamischen SAML-Authentifikatoren.

Sie können die Antwortzeit beim Starten von Remote-Desktops auf anderen dynamischen SAML-Authentifikatoren reduzieren, indem Sie die nicht erreichbaren dynamischen SAML-Authentifikatoren mithilfe von Horizon Console deaktivieren. Erläuterungen zum Deaktivieren eines SAML-Authentifikators finden Sie unter [Konfigurieren eines SAML-Authentifikators in Horizon Console](#).

Konfigurieren von Workspace ONE-Zugriffsrichtlinien in Horizon Console

Workspace ONE- oder VMware Identity Manager (vIDM)-Administratoren können durch Konfiguration von Zugriffsrichtlinien den Zugriff auf berechtigte Desktops und Anwendungen in Horizon 7 beschränken. Um die in vIDM erstellten Richtlinien zu erzwingen, aktivieren Sie für Horizon Client den Workspace ONE-Modus, damit Horizon Client den Benutzer zum Workspace ONE-Client übertragen kann, um Berechtigungen zu starten. Wenn Sie sich bei Horizon Client anmelden, werden Sie von der Zugriffsrichtlinie zur Anmeldung über Workspace ONE weitergeleitet, um auf Ihre veröffentlichten Desktops und Anwendungen zugreifen zu können.

Voraussetzungen

- Konfigurieren Sie die Zugriffsrichtlinien für Anwendungen in Workspace ONE. Weitere Informationen zum Einrichten von Zugriffsrichtlinien finden Sie im Dokument *Administratorhandbuch für VMware Identity Manager*.
- Erteilen Sie Benutzern in Horizon Console Berechtigungen für veröffentlichte Desktops und Anwendungen.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Server**.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** eine Serverinstanz aus, die mit einem SAML-Authentifikator verknüpft ist, und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie auf der Registerkarte **Authentifizierung** für die Option **Delegierung von Authentifizierung an VMware Horizon (SAML 2.0-Authentifikator)** die Einstellung **Erforderlich** aus.

Diese Option aktiviert die SAML-Authentifizierung. Der Endbenutzer kann eine Verbindung mit Horizon Server nur mit einem von vIDM oder von einem externen Identitätsanbieter bereitgestellten SAML-Token herstellen. Sie können Desktops oder Anwendungen nicht manuell aus Horizon Client heraus starten.

- 4 Wählen Sie **Workspace ONE-Modus aktivieren** aus.
- 5 Geben Sie in das Textfeld **Serverhostname von Workspace ONE** den FQDN-Wert des Workspace ONE-Hostnamens ein.
- 6 (Optional) Wählen Sie **Verbindungen von Clients, die den Workspace ONE-Modus nicht unterstützen, blockieren** aus, um den Zugriff von Horizon Clients, die den Workspace ONE-Modus unterstützen, auf Anwendungen einzuschränken.

Horizon Clients vor Version 4.5 unterstützen den Workspace ONE-Modus nicht. Wenn Sie diese Option auswählen, haben Horizon Clients vor Version 4.5 keinen Zugriff auf Anwendungen in Workspace ONE. Die Funktion des Workspace ONE-Modus ist für Versionen höher als Horizon 7 Version 7.2 nicht aktiviert, wenn die Workspace ONE-Version älter als Version 2.9.1 ist.

Konfigurieren der biometrischen Authentifizierung

Sie können die biometrische Authentifizierung durch Bearbeitung des `pae-ClientConfig`-Attributs in der LDAP-Datenbank konfigurieren.

Voraussetzungen

Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogrammes ADSI-Editor auf Ihrem Windows Server.

Verfahren

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

- 2 Wählen Sie im Dialogfeld „Verbindungseinstellungen“ **DC=vdi,DC=vmware,DC=int** aus oder verbinden Sie sich damit.
- 3 Wählen Sie im Bereich „Computer“ **localhost:389** aus oder geben Sie diesen Wert oder einen vollqualifizierten Domännennamen (FQDN) des Verbindungsserver-Hosts, gefolgt von Port 389, ein.

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

- 4 Für das Objekt **CN=Common, OU=Global, OU=Properties** bearbeiten Sie das Attribut **pae-ClientConfig** und fügen Sie den Wert **BioMetricsTimeout=<integer>** hinzu.

Die folgenden BioMetricsTimeout-Werte sind gültig:

Wert für BioMetricsTimeout	Beschreibung
0	Die biometrische Authentifizierung wird nicht unterstützt. Hierbei handelt es sich um die Standardeinstellung.
-1	Die biometrische Authentifizierung wird ohne zeitliche Beschränkung unterstützt.
Eine beliebige positive Ganzzahl	Die biometrische Authentifizierung wird unterstützt und kann für die angegebene Anzahl an Minuten verwendet werden.

Die neuen Einstellungen werden sofort wirksam. Der Verbindungsserver-Dienst oder das Clientgerät müssen nicht neu gestartet werden.

Authentifizieren von Benutzern und Gruppen

6

Nach der Anmeldung bei Horizon Console können Sie die Authentifizierung für Benutzer und Gruppen einrichten und so den Zugriff auf Anwendungen und Desktops steuern.

Sie haben die Möglichkeit, den Remotezugriff zu konfigurieren, um den Zugriff auf Desktops von außerhalb des Netzwerks für Benutzer und Gruppen zu beschränken. Sie können die Konfiguration für Benutzer für einen nicht authentifizierten Zugriff auf deren veröffentlichte Anwendungen von Horizon Client aus ohne erforderliche AD-Anmeldedaten einrichten.

Dieses Kapitel enthält die folgenden Themen:

- [Beschränken des Remote-Desktop-Zugriffs außerhalb des Netzwerks](#)
- [Konfigurieren des nicht authentifizierten Zugriffs](#)
- [Konfigurieren von Benutzern für die Hybrid-Anmeldung in Horizon Console](#)
- [Verwenden der Funktion „Als aktueller Benutzer anmelden“, die mit Windows-basierten Horizon Client-Instanzen verfügbar ist](#)

Beschränken des Remote-Desktop-Zugriffs außerhalb des Netzwerks

Sie können den Zugriff aus einem externen Netzwerk für bestimmte berechtigte Benutzer und Gruppen zulassen, während Sie den Zugriff für andere berechtigte Benutzer und Gruppen beschränken. Alle berechtigten Benutzer haben aus dem internen Netzwerk Zugriff auf Desktops und Anwendungen. Wenn Sie den Zugriff aus dem externen Netzwerk nicht auf bestimmte Benutzer beschränken, können alle berechtigten Benutzer aus dem externen Netzwerk zugreifen.

Aus Sicherheitsgründen müssen Administratoren gegebenenfalls den Zugriff von Benutzern und Gruppen von außerhalb des Netzwerks auf Remote-Desktops und Remoteanwendungen innerhalb des Netzwerks beschränken. Wenn ein Benutzer mit beschränkten Berechtigungen aus einem externen Netzwerk auf das System zugreift, wird eine Meldung angezeigt, die ihm mitteilt, dass er nicht berechtigt ist, das System zu verwenden. Der Benutzer muss sich im internen Netzwerk befinden, um auf Desktop- und Anwendungspool-Berechtigungen zugreifen zu können.

Konfigurieren von Remotezugriff

Sie können den Zugriff auf die Verbindungsserver-Instanz von außerhalb des Netzwerks bestimmten Benutzern und Gruppen erlauben und für andere Benutzer und Gruppen beschränken.

Voraussetzungen

- Eine Unified Access Gateway-Appliance, ein Sicherheitsserver oder ein Lastausgleichsdienst müssen außerhalb des Netzwerks als Gateway zur Verbindungsserver-Instanz, für die der Benutzer über eine Berechtigung verfügt, bereitgestellt werden. Weitere Informationen zur Bereitstellung einer Unified Access Gateway-Appliance finden Sie im Dokument *Bereitstellen und Konfigurieren von Unified Access Gateway*.
- Benutzer, die Remotezugriff erhalten, müssen über Berechtigungen für Desktop- oder Anwendungspools verfügen.

Verfahren

- 1 Wählen Sie in Horizon Console die Option **Benutzer und Gruppen** aus.
- 2 Klicken Sie auf die Registerkarte **Remotezugriff**.
- 3 Klicken Sie auf **Hinzufügen**, wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf **Suchen**, um basierend auf den angegebenen Suchkriterien nach Benutzern oder Gruppen zu suchen.

Hinweis Benutzer mit nicht authentifiziertem Zugriff werden nicht in den Suchergebnissen angezeigt.

- 4 Wählen Sie zum Bereitstellen des Remote-Zugriffs für einen Benutzer oder eine Benutzergruppe mit nicht authentifiziertem Zugriff einen Benutzer oder eine Gruppe aus und klicken Sie auf **OK**.
- 5 Um einem Benutzer oder einer Gruppe den Remotezugriff zu entziehen, wählen Sie den Benutzer oder die Gruppe aus und klicken Sie auf **Löschen** und dann auf **OK**.

Konfigurieren des nicht authentifizierten Zugriffs

Administratoren haben die Möglichkeit, die Konfiguration für einen nicht authentifizierten Zugriff durch Benutzer auf deren veröffentlichte Anwendungen von einem Horizon Client aus ohne erforderliche AD-Anmeldedaten einzurichten. Die Einrichtung eines nicht authentifizierten Zugriffs ist immer dann empfehlenswert, wenn Ihre Benutzer einen nahtlosen Zugriff auf eine Anwendung mit eigener Sicherheits- und Benutzerverwaltung benötigen.

Wenn ein Benutzer eine veröffentlichte Anwendung startet, die für einen nicht authentifizierten Zugriff konfiguriert ist, erstellt der RDS-Host auf Anforderung eine lokale Benutzersitzung und teilt diese Sitzung dem Benutzer zu.

Hinweis Der nicht authentifizierte Zugriff wird für Anwendungen, die in einem Desktop-Pool veröffentlicht werden, nicht unterstützt.

Diese Funktion erfordert eine eingerichtete Umgebung von Horizon 7 Version 7.1 und Horizon Client Version 4.4.

Informationen zu den Regeln und Richtlinien für die Konfiguration von Benutzern für einen nicht authentifizierten Zugriff finden Sie im Dokument *Horizon 7-Verwaltung*.

Erstellen von Benutzern für einen nicht authentifizierten Zugriff

Administratoren können Benutzer für einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen erstellen. Wenn ein Administrator einen Benutzer für einen nicht authentifizierten Zugriff konfiguriert hat, kann sich dieser Benutzer bei der Verbindungsserver-Instanz von Horizon Client aus nur mit dem nicht authentifizierten Zugriff anmelden.

Voraussetzungen

- Administratoren können für jedes Active Directory-Konto nur einen Benutzer erstellen.
- Administratoren haben nicht die Möglichkeit, Gruppen nicht authentifizierter Benutzer zu erstellen. Wenn Sie einen Benutzer für einen nicht authentifizierten Zugriff erstellen und für diesen AD-Benutzer aktuell eine Clientsitzung ausgeführt wird, müssen Sie die Clientsitzung neu starten, damit die Änderungen wirksam werden.
- Wenn Sie einen Benutzer mit Desktop-Berechtigungen erstellen und diesem Benutzer nicht authentifizierten Zugriff gewähren, dann hat der Benutzer keinen Zugriff auf die berechtigten Desktops.

Verfahren

- 1 Wählen Sie in Horizon Console die Option **Benutzer und Gruppen** aus.
- 2 Klicken Sie auf der Registerkarte **Nicht authentifizierter Zugriff** auf **Hinzufügen**.
- 3 Wählen Sie im Assistenten **Nicht authentifizierten Benutzer hinzufügen** mindestens ein Suchkriterium aus und klicken Sie auf **Suchen**, um basierend auf den angegebenen Suchkriterien nach Benutzern zu suchen.
- 4 Wählen Sie einen Benutzer aus und klicken Sie auf **Weiter**.
- 5 Geben Sie den Benutzeralias ein.

Der Standardbenutzeralias ist der für das AD-Konto konfigurierte Benutzername. Endbenutzer können sich mit dem Benutzeralias von Horizon Client aus bei der Verbindungsserver-Instanz anmelden.

- 6 (Optional) Überprüfen Sie die Benutzerdetails und fügen Sie Kommentare hinzu.
- 7 Klicken Sie auf **Senden**.

Der Verbindungsserver erstellt den Benutzer für einen nicht authentifizierten Zugriff und zeigt die Benutzerdetails inklusive Benutzeralias, Benutzername, Vor- und Nachname, Domäne, Anwendungsberechtigungen und Sitzungen an.

Nächste Schritte

Wenn Sie Benutzer für einen nicht authentifizierten Zugriff erstellt haben, müssen Sie den nicht authentifizierten Zugriff auf dem Verbindungsserver aktivieren, damit Benutzer eine Verbindung mit veröffentlichten Anwendungen herstellen und auf diese zugreifen können. Weitere Informationen finden Sie unter „Aktivieren des nicht authentifizierten Zugriffs für Benutzer“ im Dokument *Horizon 7-Verwaltung*.

Aktivieren des nicht authentifizierten Zugriffs für Benutzer in Horizon Console

Wenn Sie Benutzer für einen nicht authentifizierten Zugriff erstellt haben, müssen Sie den nicht authentifizierten Zugriff auf dem Verbindungsserver aktivieren, damit Benutzer eine Verbindung mit veröffentlichten Anwendungen herstellen und auf diese zugreifen können.

Verfahren

- 1 Wählen Sie in Horizon Console **Einstellungen > Server** aus.
- 2 Klicken Sie auf die Registerkarte **Verbindungsserver**.
- 3 Wählen Sie die Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 4 Klicken Sie auf die Registerkarte **Authentifizierung**.
- 5 Ändern Sie den Wert von **Nicht authentifizierter Zugriff** auf **Aktiviert**.
- 6 Wählen Sie im Dropdown-Menü **Standardmäßiger Benutzer für nicht authentifizierten Zugriff** einen Benutzer als Standardbenutzer aus.

Der Standardbenutzer muss im lokalen Pod einer Cloud-Pod-Architektur-Umgebung enthalten sein. Wenn Sie einen Standardbenutzer aus einem anderen Pod auswählen, erstellt der Verbindungsserver den Benutzer auf dem lokalen Pod, bevor der Benutzer als Standardbenutzer festgelegt wird.

- 7 (Optional) Geben Sie den standardmäßigen Wert für die Zeitüberschreitung von Sitzungen für den Benutzer ein.

Die Standardeinstellung hierfür beträgt zehn Minuten nach Beginn der Leerlaufzeit.

- 8 Klicken Sie auf **OK**.

Nächste Schritte

Erteilen Sie nicht authentifizierten Benutzern die Berechtigung für veröffentlichte Anwendungen. Siehe [Erteilen von Berechtigungen für Benutzer für einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen](#).

Erteilen von Berechtigungen für Benutzer für einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen

Wenn Sie einen Benutzer für einen nicht authentifizierten Zugriff erstellt haben, müssen Sie dem Benutzer eine Berechtigung für den Zugriff auf veröffentlichte Anwendungen erteilen.

Voraussetzungen

- Erstellen Sie auf der Basis einer Gruppe von RDS-Hosts eine Farm. Weitere Informationen zum Erstellen von Farmen finden Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon Console*.
- Erstellen Sie einen Anwendungspool für veröffentlichte Anwendungen, die auf einer Farm von RDS-Hosts ausgeführt werden. Weitere Informationen zum Erstellen von veröffentlichten Anwendungen finden Sie unter *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon Console*.

Verfahren

- 1 Wählen Sie in Horizon Console die Option **Benutzer und Gruppen** aus.
- 2 Wählen Sie auf der Registerkarte **Berechtigungen** die Option **Anwendungsberechtigung hinzufügen** im Dropdown-Menü **Berechtigungen** aus.
- 3 Klicken Sie auf **Hinzufügen**, wählen Sie mindestens ein Suchkriterium aus, aktivieren Sie das Kontrollkästchen für **Nicht authentifizierte Benutzer** und klicken Sie auf **Suchen**, um Benutzer für einen nicht authentifizierten Zugriff gemäß Ihren Suchkriterien zu ermitteln.
- 4 Wählen Sie die Benutzer aus, denen Sie Berechtigungen für die Anwendungen im Pool erteilen möchten, und klicken Sie auf **OK**.
- 5 Wählen Sie die Anwendungen im Pool aus und klicken Sie auf **Absenden**.

Nächste Schritte

Verwenden Sie zur Anmeldung bei Horizon Client einen Benutzer für einen nicht authentifizierten Zugriff. Siehe [Nicht authentifizierter Zugriff von Horizon Client](#) aus.

Löschen eines Benutzers für einen nicht authentifizierten Zugriff

Wenn Sie einen Benutzer für einen nicht authentifizierten Zugriff löschen, müssen Sie auch die Anwendungspoolberechtigungen für diesen Benutzer entfernen.

Sie können keinen Benutzer für einen nicht authentifizierten Zugriff löschen, der als Standardbenutzer festgelegt ist. Wenn Sie den Standardbenutzer löschen, zeigt Horizon Console sowohl eine interne Fehlermeldung als auch eine Meldung zum erfolgreichen Entfernen des Benutzers an. Der Standardbenutzer wird jedoch nicht aus Horizon Console entfernt.

Hinweis Wenn Sie einen Benutzer für einen nicht authentifizierten Zugriff löschen und für diesen AD-Benutzer aktuell eine Clientsitzung ausgeführt wird, müssen Sie die Clientsitzung neu starten, damit die Änderungen wirksam werden.

Verfahren

- 1 Wählen Sie in Horizon Console die Option **Benutzer und Gruppen** aus.
- 2 Wählen Sie auf der Registerkarte **Nicht authentifizierter Zugriff** den Benutzer aus und klicken Sie auf **Löschen**.
- 3 Klicken Sie auf **OK**.

Nächste Schritte

Entfernen Sie die Anwendungsberechtigungen für den Benutzer.

Nicht authentifizierter Zugriff von Horizon Client aus

Melden Sie sich bei Horizon Client mit einem nicht authentifizierten Zugriff an und starten Sie die veröffentlichte Anwendung.

Zur Erhöhung der Sicherheit verfügt der Benutzer für einen nicht authentifizierten Zugriff über einen Benutzeralias, den Sie für die Anmeldung bei Horizon Client verwenden können. Wenn Sie einen Benutzeralias auswählen, müssen Sie keine AD-Anmeldedaten und keinen UPN angeben. Nach der Anmeldung bei Horizon Client können Sie durch Klicken auf Ihre veröffentlichten Anwendungen diese starten. Weitere Informationen zur Installation und Einrichtung von Horizon Clients finden Sie in der Horizon Client-Dokumentation auf der Webseite [VMware Horizon Clients-Dokumentation](#).

Voraussetzungen

- Stellen Sie sicher, dass der Verbindungsserver von Horizon 7 Version 7.1 für den nicht authentifizierten Zugriff konfiguriert ist.
- Vergewissern Sie sich, dass die Benutzer für einen nicht authentifizierten Zugriff in Horizon Administrator erstellt wurden. Wenn es sich beim Standardbenutzer für einen nicht authentifizierten Zugriff um den einzigen Benutzer für einen nicht authentifizierten Zugriff handelt, stellt Horizon Client die Verbindung mit der Verbindungsserver-Instanz mit dem Standardbenutzer her.

Verfahren

- 1 Starten Sie Horizon Client.
- 2 Wählen Sie in Horizon Client die Option **Anonym mit nicht authentifiziertem Zugriff anmelden** aus.
- 3 Stellen Sie eine Verbindung mit der Verbindungsserver-Instanz her.
- 4 Wählen Sie aus dem Dropdown-Menü einen Benutzeralias aus und klicken Sie auf **Anmelden**.
Der Standardbenutzer erhält das Suffix „Standard“.
- 5 Doppelklicken Sie auf eine veröffentlichte Anwendung, um diese zu starten.

Konfigurieren von Benutzern für die Hybrid-Anmeldung in Horizon Console

Nachdem Sie einen Benutzer mit nicht authentifiziertem Zugriff erstellt haben, können Sie die Hybrid-Anmeldung für den Benutzer aktivieren. Durch die Aktivierung der Hybrid-Anmeldung können Benutzer

mit nicht authentifiziertem Zugriff über die Domäne auf Netzwerkressourcen wie Dateifreigaben oder Netzwerkdrucker zugreifen, ohne Anmeldedaten eingeben zu müssen.

Hinweis Die Funktion der Hybrid-Anmeldung verwendet denselben Domänenbenutzer für alle angemeldeten Benutzer für einen bestimmten Benutzer mit nicht authentifiziertem Zugriff mit Konfiguration für die Hybrid-Anmeldung.

Hinweis Wenn Sie die Registerkarte „Benutzerprofil“ verwenden, um das Stammverzeichnis als einen Netzwerkpfad vom RDS-Hostcomputer festzulegen, entfernt die administrative Benutzeroberfläche auf Windows standardmäßig alle vorhandenen Berechtigungen des Stammverzeichnisordners und fügt Berechtigungen für den Administrator und den lokalen Benutzer mit Vollzugriff hinzu. Verwenden Sie das Administratorkonto, um den lokalen Benutzer aus der Liste der Berechtigungen zu löschen, und fügen Sie dann den Domänenbenutzer mit den Berechtigungen, die Sie für den Benutzer benötigen, hinzu.

Voraussetzungen

- Überprüfen Sie, ob Sie die benutzerdefinierten Optionen für die Hybrid-Anmeldung aktiviert haben, als Sie Horizon Agent auf dem RDS-Host installiert haben. Weitere Informationen zu benutzerdefinierten Horizon Agent-Setup-Optionen für einen RDS-Host finden Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon Console*.
- Überprüfen Sie, ob Sie einen Benutzer mit nicht authentifiziertem Zugriff erstellt haben. Siehe [Erstellen von Benutzern für einen nicht authentifizierten Zugriff](#).
- Überprüfen Sie, ob die Kerberos-DES-Verschlüsselung für das Benutzerkonto in der Domäne deaktiviert ist. Die Kerberos-DES-Verschlüsselung wird für die Funktion der Hybrid-Anmeldung nicht unterstützt.

Verfahren

- 1 Wählen Sie in Horizon Console die Option **Benutzer und Gruppen** aus.
- 2 Klicken Sie auf der Registerkarte **Nicht authentifizierter Zugriff** auf **Hinzufügen**.
- 3 Wählen Sie im Assistenten **Nicht authentifizierten Benutzer hinzufügen** mindestens ein Suchkriterium aus und klicken Sie auf **Suchen**, um basierend auf den angegebenen Suchkriterien nach einem Benutzer mit nicht authentifiziertem Zugriff zu suchen.

Der Benutzer muss über einen gültigen UPN verfügen.
- 4 Wählen Sie einen Benutzer mit nicht authentifiziertem Zugriff und klicken Sie auf **Weiter**.

Wiederholen Sie diesen Schritt, um mehrere Benutzer hinzuzufügen.
- 5 (Optional) Geben Sie den Benutzeralias ein.

Der Standardbenutzeralias ist der für das AD-Konto konfigurierte Benutzername. Endbenutzer können sich mit dem Benutzeralias von Horizon Client aus bei der Verbindungsserver-Instanz anmelden.
- 6 (Optional) Überprüfen Sie die Benutzerdetails und fügen Sie Kommentare hinzu.

7 Wählen Sie **Hybrid-Anmeldung aktivieren** aus.

Die Option **True SSO aktivieren** ist standardmäßig aktiviert. True SSO muss für die Horizon 7-Umgebung aktiviert sein. Benutzer mit nicht authentifiziertem Zugriff, für die die Hybrid-Anmeldung aktiviert ist, verwenden True SSO zur Anmeldung am Verbindungsserver über Horizon Client.

Hinweis Wenn der Verbindungsserver-Pod nicht für True SSO konfiguriert ist, kann der Benutzer eine berechtigte Anwendung mit nicht authentifiziertem Zugriff starten. Allerdings verfügt der Benutzer nicht über Netzwerkzugriff, da True SSO nicht auf dem Pod aktiviert ist.

8 (Optional) Damit der Benutzer sich bei der Verbindungsserver-Instanz von Horizon Client anmelden kann, wählen Sie **Kennwortanmeldung aktivieren** aus und geben Sie das Kennwort des Benutzers ein.

Verwenden Sie diese Einstellung, wenn Sie True SSO nicht für die Horizon 7-Umgebung konfiguriert haben.

In einer CPA-Umgebung funktioniert die Funktion der Hybrid-Anmeldung nur auf dem Verbindungsserver-Pod, auf dem der Hybrid-Anmelde-Benutzer mit der Einstellung **Kennwortanmeldung aktivieren** konfiguriert wurde und zum Zugriff auf veröffentlichte Anwendungen berechtigt ist.

In einer CPA-Umgebung mit Pod A und Pod B, in der der Hybrid-Anmelde-Benutzer mit der Einstellung **Kennwortanmeldung aktivieren** konfiguriert ist, ist dieser zum Zugriff auf eine Anwendung auf Pod A berechtigt. Der Benutzer kann die Anwendung von einem Client aus, der mit Pod A oder Pod B verbunden ist, anzeigen und starten. Wenn derselbe Benutzer allerdings zum Zugriff auf eine weitere Anwendung auf Pod B berechtigt ist, kann der Benutzer die Anwendung nicht von einem Client aus anzeigen und starten, der mit Pod B verbunden ist. Damit die Funktion der Hybrid-Anmeldung auf Pod B funktioniert, müssen Sie einen weiteren Hybrid-Anmelde-Benutzer mit konfigurierter Einstellung **Kennwortanmeldung aktivieren** erstellen und ihn zum Zugriff auf Anwendungen berechtigen. Weitere Informationen zum Einrichten einer CPA-Umgebung finden Sie im Dokument *Verwalten der Cloud-Pod-Architektur in Horizon 7*.

9 Klicken Sie auf **Fertigstellen**.

Nächste Schritte

Erteilen Sie dem Benutzer Berechtigungen zum Zugriff auf veröffentlichte Anwendungen. Siehe [Erteilen von Berechtigungen für Benutzer für einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen](#).

Verwenden der Funktion „Als aktueller Benutzer anmelden“, die mit Windows-basierten Horizon Client-Instanzen verfügbar ist

Wenn Benutzer mit Horizon Client für Windows im Menü **OptionenAls aktueller Benutzer anmelden** aktivieren, werden die Anmeldeinformationen, die sie bei der Anmeldung am Clientsystem angegeben haben, für die Authentifizierung an der Horizon-Verbindungsserver-Instanz und am Remote-Desktop verwendet. Es ist keine weitere Benutzerauthentifizierung erforderlich.

Zur Unterstützung dieser Funktion werden Benutzeranmeldedaten sowohl in der Verbindungsserver-Instanz als auch auf dem Clientsystem gespeichert.

- Auf der Verbindungsserver-Instanz werden Anmeldedaten verschlüsselt und in der Benutzersitzung zusammen mit dem Benutzernamen, der Domäne und dem optionalen UPN gespeichert. Die Anmeldeinformationen werden hinzugefügt, wenn eine Authentifizierung erfolgt, und gelöscht, wenn das Sitzungsobjekt zerstört wird. Das Sitzungsobjekt wird zerstört, wenn sich der Benutzer abmeldet, das Zeitlimit der Sitzung überschritten wird oder die Authentifizierung fehlschlägt. Das Sitzungsobjekt befindet sich im flüchtigen Speicher und wird nicht in Horizon LDAP oder in einer Datei auf der Festplatte gespeichert.
- Aktivieren Sie in der Verbindungsserver-Instanz die Einstellung **Anmeldung als aktueller Benutzer zulassen**, damit die Verbindungsserver-Instanz die Anmeldedaten akzeptieren kann, die übergeben werden, wenn Benutzer **Als aktueller Benutzer anmelden** im Menü **Optionen** in Horizon Client aktiviert haben.

Wichtig Bevor Sie diese Einstellung aktivieren, müssen Sie sich mit den Sicherheitsrisiken vertraut machen. Einzelheiten finden Sie im Beitrag zu den sicherheitsrelevanten Servereinstellungen für die Benutzerauthentifizierung im Dokument *Horizon 7-Sicherheit*.

- Auf dem Clientsystem werden die Anmeldedaten der Benutzer verschlüsselt in einer Tabelle im Authentication Package, einer Komponente von Horizon Client, gespeichert. Die Anmeldeinformationen werden der Tabelle hinzugefügt, wenn sich der Benutzer anmeldet, und aus der Tabelle entfernt, wenn er sich abmeldet. Die Tabelle verbleibt im flüchtigen Speicher.

Mit Horizon Client-Gruppenrichtlinieneinstellungen können Administratoren die Verfügbarkeit der Einstellung **Als aktueller Benutzer anmelden** im Menü **Optionen** steuern und die Standardeinstellung festlegen. Außerdem können Administratoren mithilfe einer Gruppenrichtlinie festlegen, welche Verbindungsserver-Instanzen die Benutzeridentitäts- und Anmeldedaten akzeptieren, die übergeben werden, wenn Benutzer **Als aktueller Benutzer anmelden** in Horizon Client aktivieren.

Die Funktion „Rekursives Entsperrern“ wird aktiviert, sobald sich ein Benutzer beim Verbindungsserver mit der Funktion „Als aktueller Benutzer anmelden“ anmeldet. Die Funktion der rekursiven Entsperrung entsperrt alle Remotesitzungen, wenn der Clientcomputer entsperrt wird. Administratoren können die Funktion „Rekursives Entsperrern“ mit der globalen Richtlinieneinstellung **Remotesitzungen entsperrern, wenn der Clientcomputer entsperrt wird** in Horizon Client steuern. Weitere Informationen zu globalen Richtlinieneinstellungen für Horizon Client finden Sie in der Horizon Client-Dokumentation auf der Webseite [VMware Horizon Clients-Dokumentation](#).

Für die Funktion „Als aktueller Benutzer anmelden“ gelten folgende Einschränkungen und Anforderungen:

- Wenn die Smartcard-Authentifizierung auf einer Verbindungsserver-Instanz erforderlich ist, schlägt die Authentifizierung bei Benutzern fehl, die **Als aktueller Benutzer anmelden** aktivieren, wenn sie eine Verbindung zur Verbindungsserver-Instanz herstellen. Diese Benutzer müssen sich bei der Anmeldung beim Verbindungsserver erneut mit ihrer Smartcard und ihrer PIN authentifizieren.
- Die Uhrzeit auf dem System, an dem sich der Client anmeldet, und die Uhrzeit auf dem Verbindungsserver-Host müssen synchronisiert werden.

- Wenn die standardmäßige Zuweisung des Benutzerrechts **Auf diesen Computer vom Netzwerk aus zugreifen** auf dem Clientsystem geändert wird, muss die Änderung gemäß Beschreibung in VMware Knowledge Base-Artikel 1025691 erfolgen.
- Die Client-Maschine muss in der Lage sein, mit dem Active Directory-Unternehmensserver zu kommunizieren, und darf keine zwischengespeicherten Anmeldedaten für die Authentifizierung verwenden. Wenn sich Benutzer beispielsweise von außerhalb des Unternehmensnetzwerks bei ihren Client-Maschinen anmelden, werden zwischengespeicherte Anmeldedaten für die Authentifizierung verwendet. Wenn der Benutzer dann versucht, eine Verbindung mit einem Sicherheitsserver oder einer Verbindungsserver-Instanz herzustellen, ohne zunächst eine VPN-Verbindung herzustellen, wird der Benutzer aufgefordert, Anmeldedaten anzugeben, und die Funktion „Als aktueller Benutzer anmelden“ funktioniert nicht.

Konfigurieren der rollenbasierten Verwaltungsdelegierung in Horizon Console

7

Eine wichtige Verwaltungsaufgabe in einer Horizon 7-Umgebung besteht darin, festzulegen, wer Horizon Console verwenden kann und zur Ausführung welcher Aufgaben diese Benutzer autorisiert sind. Bei der rollenbasierten Verwaltungsdelegierung können Sie Administratorberechtigungen gezielt zuweisen, indem Sie bestimmten Active Directory-Benutzern und -Gruppen Administratorrollen zuweisen.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zu Rollen und Berechtigungen](#)
- [Verwenden von Zugriffsgruppen zur Delegierung der Verwaltung von Pools und Farmen in Horizon Console](#)
- [Grundlegendes zu Berechtigungen](#)
- [Verwalten von Administratoren](#)
- [Verwalten und Überprüfen von Berechtigungen](#)
- [Verwalten und Prüfen von Zugriffsgruppen](#)
- [Verwalten von benutzerdefinierten Rollen](#)
- [Vordefinierte Rollen und Berechtigungen](#)
- [Erforderliche Berechtigungen für häufige Aufgaben](#)
- [Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen](#)

Grundlegendes zu Rollen und Berechtigungen

Die Möglichkeit, Aufgaben in Horizon Console auszuführen, wird durch ein Zugriffssteuerungssystem bestimmt, das Administratorrollen und -berechtigungen umfasst. Dieses System ist mit dem vCenter Server-Zugriffssteuerungssystem vergleichbar.

Eine Administratorrolle ist eine Sammlung aus Berechtigungen. Berechtigungen befähigen zur Durchführung bestimmter Aktionen, beispielsweise zum Gewähren von Benutzerberechtigungen für einen Desktop-Pool. Berechtigungen steuern außerdem, welche Objekte ein Administrator in Horizon Console anzeigen kann. Wenn ein Administrator beispielsweise keine Berechtigungen zum Anzeigen oder Ändern globaler Richtlinien besitzt, ist die Einstellung **Globale Richtlinien** nicht im Navigationsbereich sichtbar, wenn sich der Administrator bei Horizon Console anmeldet.

Administratorberechtigungen sind entweder global oder objektspezifisch. Globale Berechtigungen steuern systemweite Vorgänge, beispielsweise das Anzeigen und Ändern globaler Einstellungen. Objektspezifische Berechtigungen steuern Vorgänge für bestimmte Arten von Objekten.

Administratorrollen kombinieren typischerweise alle Berechtigungen, die zum Durchführen einer Verwaltungsaufgabe höherer Ebene erforderlich sind. Horizon Console umfasst vordefinierte Rollen, welche die zur Ausführung häufiger Verwaltungsaufgaben erforderlichen Berechtigungen enthalten. Sie können diese vordefinierten Rollen Administratorbenutzern und -gruppen zuweisen oder eigene Rollen erstellen, indem Sie ausgewählte Berechtigungen miteinander kombinieren. Die vordefinierten Rollen können nicht geändert werden.

Sie erstellen Administratoren, indem Sie Benutzer und Gruppen aus Ihren Active Directory-Benutzern und -Gruppen auswählen und diesen Administratorrollen zuweisen. Wenn die Rolle objektspezifische Berechtigungen enthält, müssen Sie möglicherweise die Rolle auf eine Zugriffsgruppe anwenden. Administratoren erhalten Berechtigungen über ihre Rollenzuweisungen. Berechtigungen können Administratoren nicht direkt zugewiesen werden. Ein Administrator mit mehreren Rollenzuweisungen erhält die Summe aller Berechtigungen in diesen Rollen.

Verwenden von Zugriffsgruppen zur Delegation der Verwaltung von Pools und Farmen in Horizon Console

Standardmäßig werden automatisierte Desktop-Pools, manuelle Desktop-Pools und Farmen in der Stammzugriffsgruppe erstellt, die in Horizon Console als / oder Root(/) angezeigt wird. Veröffentlichte Desktop-Pools und Anwendungspools erben die Zugriffsgruppe ihrer Farmen. Sie können Zugriffsgruppen unter der Stammzugriffsgruppe erstellen, um die Verwaltung von spezifischen Pools oder Farmen an unterschiedliche Administratoren zu delegieren.

Hinweis Sie können die Zugriffsgruppe eines veröffentlichten Desktop-Pools oder eines Anwendungspools nicht direkt ändern. Sie müssen die Zugriffsgruppe der Farm ändern, zu der der veröffentlichte Desktop-Pool oder der Anwendungspool gehört.

Eine virtuelle oder physische Maschine erbt die Zugriffsgruppe von ihrem Desktop-Pool. Eine verbundene persistente Festplatte erbt die Zugriffsgruppe ihrer Maschine. Sie können einschließlich der Stammzugriffsgruppe maximal 100 Zugriffsgruppen haben.

Sie konfigurieren den Administratorzugriff auf die Ressourcen in einer Zugriffsgruppe, indem Sie einem Administrator für diese Zugriffsgruppe eine Rolle zuweisen. Administratoren können ausschließlich auf Ressourcen in Zugriffsgruppen zugreifen, für die ihnen Rollen zugewiesen wurden. Die Rolle, die einem Administrator für eine Zugriffsgruppe zugewiesen wurde, bestimmt die Zugriffsebene des Administrators für die Ressourcen in dieser Zugriffsgruppe.

Da Rollen von der Stammzugriffsgruppe geerbt werden, verfügt ein Administrator mit einer Rolle für die Stammzugriffsgruppe für sämtliche Zugriffsgruppen über diese Rolle. Administratoren mit der Administratorenrolle für die Stammzugriffsgruppe sind übergeordnete Administratoren, da sie über Vollzugriff auf alle Objekte innerhalb des Systems verfügen.

Eine Rolle muss mindestens eine objektspezifische Berechtigung enthalten, um auf eine Zugriffsgruppe angewendet werden zu können. Rollen, die ausschließlich globale Berechtigungen enthalten, können nicht auf Zugriffsgruppen angewendet werden.

Sie können mithilfe von Horizon Console Zugriffsgruppen erstellen und vorhandene Desktop-Pools in Zugriffsgruppen verschieben. Wenn Sie einen automatisierten Desktop-Pool, einen manuellen Pool oder eine Farm erstellen, können Sie die standardmäßige Stammzugriffsgruppe annehmen oder eine andere Zugriffsgruppe auswählen.

- **Unterschiedliche Administratoren für unterschiedliche Zugriffsgruppen**

Sie können unterschiedliche Administratoren zur Verwaltung verschiedener Zugriffsgruppen in Ihrer Konfiguration erstellen.

- **Unterschiedliche Administratoren für dieselbe Zugriffsgruppe**

Sie können unterschiedliche Administratoren zur Verwaltung derselben Zugriffsgruppe erstellen.

Unterschiedliche Administratoren für unterschiedliche Zugriffsgruppen

Sie können unterschiedliche Administratoren zur Verwaltung verschiedener Zugriffsgruppen in Ihrer Konfiguration erstellen.

Wenn sich die Desktop-Pools für den Geschäftsbetrieb beispielsweise in einer anderen Zugriffsgruppe befinden als die Desktop-Pools für Softwareentwickler, können Sie unterschiedliche Administratoren zum Verwalten der Ressourcen in jeder dieser Zugriffsgruppen erstellen.

Tabelle 7-1. Unterschiedliche Administratoren für unterschiedliche Zugriffsgruppen zeigt ein Beispiel für diese Art der Konfiguration.

Tabelle 7-1. Unterschiedliche Administratoren für unterschiedliche Zugriffsgruppen

Administrator	Rolle	Zugriffsgruppe
view-domain.com\Admin1	Bestandslistenadministratoren	/CorporateDesktops
view-domain.com\Admin2	Bestandslistenadministratoren	/DeveloperDesktops

In diesem Beispiel wurde dem Administrator „Admin1“ die Rolle „Bestandslistenadministratoren“ für die Zugriffsgruppe CorporateDesktops zugewiesen, und der Administrator „Admin2“ verfügt über die Rolle „Bestandslistenadministratoren“ für die Zugriffsgruppe DeveloperDesktops.

Unterschiedliche Administratoren für dieselbe Zugriffsgruppe

Sie können unterschiedliche Administratoren zur Verwaltung derselben Zugriffsgruppe erstellen.

Wenn sich zum Beispiel Ihre Unternehmens-Desktop-Pools in einer Zugriffsgruppe befinden, können Sie einen Administrator erstellen, der diese Pools anzeigen und modifizieren kann, und einen anderen Administrator, der sie nur anzeigen kann.

Tabelle 7-2. Unterschiedliche Administratoren für dieselbe Zugriffsgruppe zeigt ein Beispiel für diese Art der Konfiguration.

Tabelle 7-2. Unterschiedliche Administratoren für dieselbe Zugriffsgruppe

Administrator	Rolle	Zugriffsgruppe
view-domain.com\Admin1	Bestandslistenadministratoren	/CorporateDesktops
view-domain.com\Admin2	Bestandslistenadministratoren (Nur Lesezugriff)	/CorporateDesktops

In diesem Beispiel hat der Administrator namens Admin1 die Rolle des Bestandslistenadministrators für die Zugriffsgruppe namens CorporateDesktops und der Administrator namens Admin2 die Rolle „Bestandslistenadministratoren (Nur Lesezugriff)“ für dieselbe Zugriffsgruppe inne.

Grundlegendes zu Berechtigungen

Horizon Console stellt die Kombination einer Rolle, eines Administratorbenutzers oder einer Administratorgruppe sowie einer Zugriffsgruppe als Berechtigung dar. Die Rolle definiert die Aktionen, die ausgeführt werden können, der Benutzer oder die Gruppe gibt an, wer die Aktion ausführen kann, und die Zugriffsgruppe enthält die Objekte, die Ziel der Aktion sind.

Berechtigungen werden in Horizon Console unterschiedlich angezeigt, abhängig davon, ob Sie einen Administratorbenutzer oder eine Administratorgruppe, eine Zugriffsgruppe oder eine Rolle auswählen.

Die folgende Tabelle zeigt, wie Berechtigungen in Horizon Console angezeigt werden, wenn Sie einen Administratorbenutzer oder eine Administratorgruppe auswählen. Der Administratorbenutzer heißt „Admin 1“ und verfügt über zwei Berechtigungen.

Tabelle 7-3. Berechtigungen auf der Registerkarte „Administratoren und Gruppen“ für Admin 1

Rolle	Zugriffsgruppe
Bestandslistenadministratoren	MarketingDesktops
Administratoren (Nur Lesezugriff)	/

Die erste Berechtigung zeigt, dass Admin 1 über die Rolle „Bestandslistenadministratoren“ auf der Zugriffsgruppe MarketingDesktops verfügt. Die zweite Berechtigung zeigt, dass Admin 1 über die Rolle „Administratoren (Lesezugriff)“ für die Stammzugriffsgruppe verfügt.

Die folgende Tabelle zeigt, wie dieselben Berechtigungen in Horizon Console angezeigt werden, wenn Sie die Zugriffsgruppe MarketingDesktops auswählen.

Tabelle 7-4. Berechtigungen auf der Registerkarte „Ordner“ für „MarketingDesktops“

Admin	Rolle	Vererbt
horizon-domain.com\Admin1	Bestandslistenadministratoren	
horizon-domain.com\Admin1	Administratoren (Nur Lesezugriff)	Ja

Die erste Berechtigung ist dieselbe wie die erste Berechtigung in [Tabelle 7-3. Berechtigungen auf der Registerkarte „Administratoren und Gruppen“ für Admin 1](#). Die zweite Berechtigung wird von der zweiten Berechtigung geerbt, wie in [Tabelle 7-3. Berechtigungen auf der Registerkarte „Administratoren und Gruppen“ für Admin 1](#) gezeigt. Da Zugriffsgruppen die Berechtigungen von der Stammzugriffsgruppe erben, verfügt Admin1 über die Rolle „Administratoren (Lesezugriff)“ für die Zugriffsgruppe MarketingDesktops. Wenn eine Berechtigung vererbt wurde, erscheint in der Spalte „Vererbt“ der Wert „Ja“.

Die folgende Tabelle zeigt, wie die erste Berechtigung in Horizon Console in [Tabelle 7-3. Berechtigungen auf der Registerkarte „Administratoren und Gruppen“ für Admin 1](#) angezeigt wird, wenn Sie die Rolle „Bestandslistenadministratoren“ auswählen.

Tabelle 7-5. Berechtigungen auf der Registerkarte „Rollenberechtigungen“ für Bestandslistenadministratoren

Administrator	Zugriffsgruppe
horizon-domain.com\Admin1	/MarketingDesktops

Verwalten von Administratoren

Benutzer mit der Administratorrolle können Horizon Console zum Hinzufügen und Entfernen von Administratorbenutzern und -gruppen verwenden.

Die Administratorrolle ist die einflussreichste Rolle in Horizon Console. Zu Beginn wird Mitgliedern des Administratorkontos die Administratorrolle gewährt. Sie geben das Administratorkonto an, wenn Sie Verbindungsserver installieren. Das Administratorkonto kann die lokale Administratorengruppe (BUILTIN\Administrators) auf dem Verbindungsserver-Computer oder ein Domänenbenutzer- oder Gruppenkonto sein.

Hinweis Die Gruppe „Domänen-Admins“ ist standardmäßig Mitglied der lokalen Administratorengruppe. Wenn Sie das Administratorkonto als die lokale Administratorengruppe festgelegt haben und nicht möchten, dass Domänenadministratoren vollen Zugriff auf Bestandslistenobjekte und Horizon 7-Konfigurationseinstellungen haben, müssen Sie die Domänenadministratorengruppe aus der Gruppe der lokalen Administratoren entfernen.

■ Erstellen eines Administrators in Horizon Console

Um einen Administrator zu erstellen, wählen Sie in Horizon Console einen Benutzer oder eine Gruppe aus den Active Directory-Benutzern und -Gruppen aus und weisen Sie dem Benutzer bzw. der Gruppe eine Administratorrolle zu.

■ [Entfernen eines Administrators in Horizon Console](#)

Sie können einen Administratorbenutzer oder eine Administratorgruppe entfernen. Der letzte übergeordnete Administrator innerhalb des Systems kann nicht entfernt werden. Bei einem übergeordneten Administrator handelt es sich um einen Administrator mit der Administratorenrolle für die Stammzugriffsgruppe.

Erstellen eines Administrators in Horizon Console

Um einen Administrator zu erstellen, wählen Sie in Horizon Console einen Benutzer oder eine Gruppe aus den Active Directory-Benutzern und -Gruppen aus und weisen Sie dem Benutzer bzw. der Gruppe eine Administratorrolle zu.

Voraussetzungen

- Machen Sie sich mit den vordefinierten Administratorrollen vertraut. Siehe [Vordefinierte Rollen und Berechtigungen](#).
- Machen Sie sich mit den empfohlenen Vorgehensweisen für das Erstellen von Administratorbenutzern und -gruppen vertraut. Siehe [Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen](#).
- Um dem Administrator eine benutzerdefinierte Rolle zuzuweisen, erstellen Sie die benutzerdefinierte Rolle. Siehe [Hinzufügen einer benutzerdefinierten Rolle in Horizon Console](#).
- Zum Erstellen eines Administrators, der bestimmte Desktop-Pools verwalten darf, erstellen Sie eine Zugriffsgruppe und verschieben Sie die Desktop-Pools in dieser Zugriffsgruppe. Siehe [Verwalten und Prüfen von Zugriffsgruppen](#).

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Administratoren**.
- 2 Klicken Sie auf der Registerkarte **Administratoren und Gruppen** auf **Benutzer oder Gruppe hinzufügen**.
- 3 Klicken Sie auf **Hinzufügen**, wählen Sie mindestens ein Suchkriterium und klicken Sie auf **Suchen**, um basierend auf den angegebenen Suchkriterien nach Active Directory-Benutzern oder -Gruppen zu filtern.
- 4 Wählen Sie den Active Directory-Benutzer bzw. die Active Directory-Gruppe, den/die Sie als Administratorbenutzer oder -gruppe konfigurieren möchten, klicken Sie auf **OK** und anschließend auf **Weiter**.

Mithilfe der Strg- und Umschalt-Taste können Sie mehrere Benutzer und Gruppen auswählen.

- Wählen Sie eine Rolle, die Sie dem Administratorbenutzer oder der Administratorgruppe zuweisen möchten.

Die Spalte **Gilt für eine Zugriffsgruppe** gibt an, ob eine Rolle auf Zugriffsgruppen angewendet werden kann. Nur Rollen, die objektspezifische Berechtigungen enthalten, können auf Zugriffsgruppen angewendet werden. Rollen, die ausschließlich globale Berechtigungen enthalten, werden nicht auf Zugriffsgruppen angewendet.

Option	Aktion
Die ausgewählte Rolle gilt für Zugriffsgruppen	Wählen Sie eine oder mehrere Zugriffsgruppen aus und klicken Sie auf Weiter .
Die Rolle soll für alle Zugriffsgruppen gelten	Wählen Sie die Stammzugriffsgruppe aus und klicken Sie auf Weiter .

- Klicken Sie auf **Fertig stellen**, um den Administratorbenutzer oder die Administratorgruppe zu erstellen.

Der neue Administratorbenutzer bzw. die Administratorgruppe wird im linken Fensterbereich angezeigt. Die ausgewählte Rolle und Zugriffsgruppe werden im rechten Fensterbereich auf der Registerkarte **Administratoren und Gruppen** angezeigt.

Entfernen eines Administrators in Horizon Console

Sie können einen Administratorbenutzer oder eine Administratorgruppe entfernen. Der letzte übergeordnete Administrator innerhalb des Systems kann nicht entfernt werden. Bei einem übergeordneten Administrator handelt es sich um einen Administrator mit der Administratorenrolle für die Stammzugriffsgruppe.

Verfahren

- Navigieren Sie in Horizon Console zu **Einstellungen > Administratoren**.
- Wählen Sie auf der Registerkarte **Administratoren und Gruppen** den Administratorbenutzer oder die Administratorgruppe, klicken Sie auf **Benutzer oder Gruppe entfernen** und anschließend auf **OK**.

Der Administratorbenutzer oder die Administratorgruppe wird nicht länger auf der Registerkarte **Administratoren und Gruppen** angezeigt.

Verwalten und Überprüfen von Berechtigungen

Sie können mit Horizon Console Berechtigungen für spezifische Administratorbenutzer und -gruppen, Rollen und Zugriffsgruppen hinzufügen, löschen und überprüfen.

■ [Hinzufügen einer Berechtigung in Horizon Console](#)

Sie können eine Berechtigung hinzufügen, die einen bestimmten Administratorbenutzer oder eine Administratorgruppe, eine bestimmte Rolle oder eine bestimmte Zugriffsgruppe umfasst.

- [Löschen einer Berechtigung in Horizon Console](#)

Sie können eine Berechtigung löschen, die einen bestimmten Administratorbenutzer oder eine Administratorgruppe, eine bestimmte Rolle oder eine bestimmte Zugriffsgruppe umfasst.

- [Überprüfen von Berechtigungen in Horizon Console](#)

Sie können die Berechtigungen überprüfen, die einen bestimmten Administrator oder eine bestimmte Gruppe, eine bestimmte Rolle oder eine bestimmte Zugriffsgruppe umfassen.

Hinzufügen einer Berechtigung in Horizon Console

Sie können eine Berechtigung hinzufügen, die einen bestimmten Administratorbenutzer oder eine Administratorgruppe, eine bestimmte Rolle oder eine bestimmte Zugriffsgruppe umfasst.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Administratoren**.

2 Erstellen Sie die Berechtigung.

Option	Aktion
Erstellen einer Berechtigung, die einen bestimmten Administratorbenutzer oder eine bestimmte Administratorgruppe umfasst.	<ul style="list-style-type: none"> a Wählen Sie auf der Registerkarte Administratoren und Gruppen den Administrator oder die Administratorgruppe und klicken Sie auf Berechtigung hinzufügen. b Wählen Sie eine Rolle. c Wenn die Rolle nicht auf Zugriffsgruppen angewendet wird, klicken Sie auf Fertig stellen. d Wenn die Rolle auf Zugriffsgruppen angewendet wird, klicken Sie auf Weiter, wählen Sie eine oder mehrere Zugriffsgruppen aus und klicken Sie auf Fertig stellen. Eine Rolle muss mindestens eine objektspezifische Berechtigung enthalten, um auf eine Zugriffsgruppe angewendet werden zu können.
Erstellen einer Berechtigung, die eine bestimmte Rolle umfasst.	<ul style="list-style-type: none"> a Wählen Sie auf der Registerkarte Rollenberechtigungen die gewünschte Rolle, klicken Sie auf Berechtigungen und anschließend auf Berechtigung hinzufügen. b Klicken Sie auf Hinzufügen, wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf Suchen, um basierend auf den angegebenen Suchkriterien nach Administratorbenutzern oder -gruppen zu suchen. c Wählen Sie einen Administratorbenutzer oder eine Administratorgruppe, den bzw. die Sie in die Berechtigung einschließen möchten, und klicken Sie auf OK. Mithilfe der Strg- und Umschalt-Taste können Sie mehrere Benutzer und Gruppen auswählen. d Wenn die Rolle nicht auf Zugriffsgruppen angewendet wird, klicken Sie auf Fertig stellen. e Wenn die Rolle auf Zugriffsgruppen angewendet wird, klicken Sie auf Weiter, wählen Sie eine oder mehrere Zugriffsgruppen aus und klicken Sie auf Fertig stellen. Eine Rolle muss mindestens eine objektspezifische Berechtigung enthalten, um auf eine Zugriffsgruppe angewendet werden zu können.
Erstellen einer Berechtigung, die eine bestimmte Zugriffsgruppe umfasst.	<ul style="list-style-type: none"> a Wählen Sie auf der Registerkarte Zugriffsgruppen die gewünschte Zugriffsgruppe aus und klicken Sie auf Berechtigung hinzufügen. b Klicken Sie auf Hinzufügen, wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf Suchen, um basierend auf den angegebenen Suchkriterien nach Administratorbenutzern oder -gruppen zu suchen. c Wählen Sie einen Administratorbenutzer oder eine Administratorgruppe, den bzw. die Sie in die Berechtigung einschließen möchten, und klicken Sie auf OK. Mithilfe der Strg- und Umschalt-Taste können Sie mehrere Benutzer und Gruppen auswählen. d Klicken Sie auf Weiter, wählen Sie eine Rolle und klicken Sie auf Fertig stellen. Eine Rolle muss mindestens eine objektspezifische Berechtigung enthalten, um auf eine Zugriffsgruppe angewendet werden zu können.

Löschen einer Berechtigung in Horizon Console

Sie können eine Berechtigung löschen, die einen bestimmten Administratorbenutzer oder eine Administratorgruppe, eine bestimmte Rolle oder eine bestimmte Zugriffsgruppe umfasst.

Wenn Sie die letzte Berechtigung für einen Administratorbenutzer oder eine Administratorgruppe entfernen, wird der jeweilige Administratorbenutzer bzw. die Administratorgruppe ebenfalls entfernt. Da mindestens ein Administrator über die Administratorrolle für die Stammzugriffsgruppe verfügen muss, können Sie keine Berechtigung entfernen, die zum Entfernen des Administrators führen würde. Eine vererbte Berechtigung kann nicht gelöscht werden.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Administratoren**.
- 2 Wählen Sie die Berechtigung aus, die gelöscht werden soll.

Option	Aktion
Löschen einer Berechtigung, die für einen bestimmten Administrator oder eine bestimmte Gruppe gilt.	Wählen Sie den Administrator oder die Gruppe auf der Registerkarte Administratoren und Gruppen aus.
Löschen einer Berechtigung, die für eine bestimmte Rolle gilt.	Wählen Sie die Rolle auf der Registerkarte Rollen aus.
Löschen einer Berechtigung, die für eine bestimmte Zugriffsgruppe gilt.	Wählen Sie den Ordner auf der Registerkarte Zugriffsgruppen aus.

- 3 Wählen Sie die Berechtigung und klicken Sie auf **Berechtigung entfernen**.

Überprüfen von Berechtigungen in Horizon Console

Sie können die Berechtigungen überprüfen, die einen bestimmten Administrator oder eine bestimmte Gruppe, eine bestimmte Rolle oder eine bestimmte Zugriffsgruppe umfassen.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Administratoren**.
- 2 Überprüfen Sie die Berechtigungen.

Option	Aktion
Überprüfen der Berechtigungen, die einen bestimmten Administrator oder eine bestimmte Gruppe umfassen.	Wählen Sie den Administrator oder die Gruppe auf der Registerkarte Administratoren und Gruppen aus.
Überprüfen der Berechtigungen, die eine bestimmte Rolle umfassen.	Wählen Sie die Rolle auf der Registerkarte Rollenberechtigungen aus und klicken Sie auf Berechtigungen .
Überprüfen der Berechtigungen, die eine bestimmte Zugriffsgruppe umfassen.	Wählen Sie den Ordner auf der Registerkarte Zugriffsgruppen aus.

Verwalten und Prüfen von Zugriffsgruppen

Sie können mithilfe von Horizon Console Zugriffsgruppen hinzufügen und löschen und die Desktop-Pools und Maschinen in einer bestimmten Zugriffsgruppe überprüfen.

■ Hinzufügen einer Zugriffsgruppe in Horizon Console

Sie können die Verwaltung von spezifischen Maschinen, Desktop-Pools oder Farmen an unterschiedliche Administratoren delegieren, indem Sie Zugriffsgruppen erstellen. Standardmäßig befinden sich Desktop-Pools, Anwendungspools und Farmen in der Stammzugriffsgruppe.

■ Verschieben eines Desktop-Pools oder einer Farm in eine andere Zugriffsgruppe in Horizon Console

Nach dem Erstellen einer Zugriffsgruppe können Sie automatisierte Desktop-Pools, manuelle Pools oder Farmen in die neue Zugriffsgruppe verschieben.

■ Entfernen einer Zugriffsgruppe in Horizon Console

Wenn eine Zugriffsgruppe keine Objekte enthält, kann sie entfernt werden. Die Stammzugriffsgruppe kann nicht entfernt werden.

■ Überprüfen der Objekte in einer Zugriffsgruppe

Sie können Desktop-Pools, Anwendungspools, Farmen oder persistente Festplatten in einer bestimmten Zugriffsgruppe in Horizon Console anzeigen.

■ Überprüfen der vCenter-VMs in einer Zugriffsgruppe

Sie können die vCenter-VMs in einer speziellen Zugriffsgruppe in Horizon Console anzeigen. Eine vCenter-VM erbt die Zugriffsgruppe von ihrem Pool.

Hinzufügen einer Zugriffsgruppe in Horizon Console

Sie können die Verwaltung von spezifischen Maschinen, Desktop-Pools oder Farmen an unterschiedliche Administratoren delegieren, indem Sie Zugriffsgruppen erstellen. Standardmäßig befinden sich Desktop-Pools, Anwendungspools und Farmen in der Stammzugriffsgruppe.

Sie können einschließlich der Stammzugriffsgruppe maximal 100 Zugriffsgruppen haben.

Verfahren

- 1 Wechseln Sie in Horizon Console zum Dialogfeld „Zugriffsgruppe“.

Option	Aktion
An Desktops	<ul style="list-style-type: none"> ■ Wählen Sie Bestandsliste > Desktops aus. ■ Wählen Sie im Dropdown-Menü Zugriffsgruppe die Option Neue Zugriffsgruppe aus.
In Farmen	<ul style="list-style-type: none"> ■ Wählen Sie Bestandsliste > Farmen aus. ■ Wählen Sie im Dropdown-Menü Zugriffsgruppe die Option Neue Zugriffsgruppe aus.

- 2 Geben Sie einen Namen und eine Beschreibung für die Zugriffsgruppe ein und klicken Sie auf **OK**.

Die Beschreibung ist optional.

Nächste Schritte

Verschieben Sie ein oder mehrere Objekte in die Zugriffsgruppe.

Verschieben eines Desktop-Pools oder einer Farm in eine andere Zugriffsgruppe in Horizon Console

Nach dem Erstellen einer Zugriffsgruppe können Sie automatisierte Desktop-Pools, manuelle Pools oder Farmen in die neue Zugriffsgruppe verschieben.

Verfahren

- 1 Wählen Sie in Horizon Console die Optionen **Bestandsliste > Desktops** bzw. **Bestandsliste > Farmen** aus.
- 2 Wählen Sie einen Pool oder eine Farm aus.
- 3 Wählen Sie **Zugriffsgruppe ändern** aus dem Dropdown-Menü **Zugriffsgruppe** aus.
- 4 Wählen Sie die Zugriffsgruppe und klicken Sie auf **OK**.

Horizon Console verschiebt den Pool bzw. die Farm in die Zugriffsgruppe, die Sie ausgewählt haben.

Entfernen einer Zugriffsgruppe in Horizon Console

Wenn eine Zugriffsgruppe keine Objekte enthält, kann sie entfernt werden. Die Stammzugriffsgruppe kann nicht entfernt werden.

Voraussetzungen

Wenn die Zugriffsgruppe Objekte enthält, verschieben Sie die Objekte in eine andere Zugriffsgruppe oder die Stammzugriffsgruppe. Siehe [Verschieben eines Desktop-Pools oder einer Farm in eine andere Zugriffsgruppe in Horizon Console](#).

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Administratoren**.
- 2 Wählen Sie auf der Registerkarte **Zugriffsgruppen** die Zugriffsgruppe aus und klicken Sie auf **Zugriffsgruppe entfernen**.
- 3 Klicken Sie auf **OK**, um die Zugriffsgruppe zu entfernen.

Überprüfen der Objekte in einer Zugriffsgruppe

Sie können Desktop-Pools, Anwendungspools, Farmen oder persistente Festplatten in einer bestimmten Zugriffsgruppe in Horizon Console anzeigen.

Verfahren

- 1 Navigieren Sie in Horizon Console auf die Hauptseite für diese Objekte.

Objekt	Aktion
Desktop-Pools	Wählen Sie Bestandsliste > Desktops aus.
Anwendungspools	Wählen Sie Bestandsliste > Anwendungen aus.
Farmen	Wählen Sie Bestandsliste > Farmen aus.
Persistente Festplatten	Wählen Sie Bestandsliste > Persistente Festplatten aus.

Standardmäßig werden die Objekte in allen Zugriffsgruppen angezeigt.

- 2 Wählen Sie eine Zugriffsgruppe aus dem Dropdown-Menü **Zugriffsgruppe** im Hauptfensterbereich aus.

Die Objekte in der Zugriffsgruppe, die Sie ausgewählt haben, werden angezeigt.

Überprüfen der vCenter-VMs in einer Zugriffsgruppe

Sie können die vCenter-VMs in einer speziellen Zugriffsgruppe in Horizon Console anzeigen. Eine vCenter-VM erbt die Zugriffsgruppe von ihrem Pool.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Bestandsliste > Maschinen**.

- 2 Wählen Sie die Registerkarte **vCenter-VMs** aus.

Standardmäßig werden die vCenter-VMs in allen Zugriffsgruppen angezeigt.

- 3 Wählen Sie eine Zugriffsgruppe aus dem Dropdown-Menü **Zugriffsgruppe** aus.

Die vCenter-VMs in der ausgewählten Zugriffsgruppe werden angezeigt.

Verwalten von benutzerdefinierten Rollen

Sie können mithilfe von Horizon Console benutzerdefinierte Rollen hinzufügen, ändern und löschen.

■ [Hinzufügen einer benutzerdefinierten Rolle in Horizon Console](#)

Wenn die vordefinierten Administratorrollen nicht Ihren Anforderungen entsprechen, können Sie ausgewählte Berechtigungen kombinieren, um eigene Rollen in Horizon Console zu erstellen.

■ [Ändern der Berechtigungen in einer benutzerdefinierten Rolle in Horizon Console](#)

Sie können die Berechtigungen in einer benutzerdefinierten Rolle ändern. Vordefinierte Administratorrollen können nicht geändert werden.

■ [Entfernen einer benutzerdefinierten Rolle in Horizon Console](#)

Wenn eine benutzerdefinierte Rolle nicht in einer Berechtigung enthalten ist, können Sie die Rolle entfernen. Vordefinierte Administratorrollen können nicht entfernt werden.

Hinzufügen einer benutzerdefinierten Rolle in Horizon Console

Wenn die vordefinierten Administratorrollen nicht Ihren Anforderungen entsprechen, können Sie ausgewählte Berechtigungen kombinieren, um eigene Rollen in Horizon Console zu erstellen.

Voraussetzungen

Machen Sie sich mit den Administratorberechtigungen vertraut, die Sie zum Erstellen benutzerdefinierter Rollen verwenden können. Siehe [Vordefinierte Rollen und Berechtigungen](#).

Hinweis Bei der Erstellung einer benutzerdefinierten Administratorrolle sind keine globalen Berechtigungen für den benutzerdefinierten Administratorbenutzer verfügbar. Nur vordefinierte Administratorrollen haben globale Berechtigungen. Diese ermöglichen die Verwaltung von globalen Berechtigungen in einer Cloud-Pod-Architektur-Umgebung.

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Administratoren**.
- 2 Klicken Sie auf der Registerkarte **Rollenrechte** auf **Rolle hinzufügen**.
- 3 Geben Sie einen Namen und eine Beschreibung für die neue Rolle ein, wählen Sie eine oder mehrere Berechtigungen aus und klicken Sie auf **OK**.

Die neue Rolle wird im linken Fensterbereich angezeigt.

Ändern der Berechtigungen in einer benutzerdefinierten Rolle in Horizon Console

Sie können die Berechtigungen in einer benutzerdefinierten Rolle ändern. Vordefinierte Administratorrollen können nicht geändert werden.

Voraussetzungen

Machen Sie sich mit den Administratorberechtigungen vertraut, die Sie zum Erstellen benutzerdefinierter Rollen verwenden können. Siehe [Vordefinierte Rollen und Berechtigungen](#).

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Administratoren**.
- 2 Wählen Sie auf der Registerkarte **Rollenrechte** die gewünschte Rolle aus.
- 3 Zeigen Sie die Rechte der Rolle an und klicken Sie auf **Bearbeiten**.
- 4 Wählen Sie Berechtigungen, oder heben Sie die Auswahl von Berechtigungen auf.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Entfernen einer benutzerdefinierten Rolle in Horizon Console

Wenn eine benutzerdefinierte Rolle nicht in einer Berechtigung enthalten ist, können Sie die Rolle entfernen. Vordefinierte Administratorrollen können nicht entfernt werden.

Voraussetzungen

Wenn die Rolle in einer Berechtigung enthalten ist, löschen Sie die Berechtigung. Siehe [Löschen einer Berechtigung in Horizon Console](#).

Verfahren

- 1 Navigieren Sie in Horizon Console zu **Einstellungen > Administratoren**.
- 2 Wählen Sie auf der Registerkarte **Rollenrechte** die gewünschte Rolle aus und klicken Sie auf **Rolle entfernen**.

Die Schaltfläche **Rolle entfernen** steht für vordefinierte Rollen oder für benutzerdefinierte Rollen, die in einer Berechtigung enthalten sind, nicht zur Verfügung.

- 3 Klicken Sie auf **OK**, um die Rolle zu entfernen.

Vordefinierte Rollen und Berechtigungen

Horizon Console umfasst vordefinierte Rollen, die Sie Ihren Administratorbenutzern und -gruppen zuweisen können. Sie können auch eigene Administratorrollen erstellen, indem Sie ausgewählte Berechtigungen kombinieren.

■ [Vordefinierte Administratorrollen](#)

Die vordefinierten Administratorrollen kombinieren die einzelnen Berechtigungen, die zur Ausführung allgemeiner Verwaltungsaufgaben erforderlich sind. Die vordefinierten Rollen können nicht geändert werden.

■ [Globale Berechtigungen](#)

Globale Berechtigungen steuern systemweite Vorgänge, beispielsweise das Anzeigen und Ändern globaler Einstellungen. Rollen, die ausschließlich globale Berechtigungen enthalten, können nicht auf Zugriffsgruppen angewendet werden.

■ [Objektspezifische Berechtigungen](#)

Objektspezifische Berechtigungen steuern Vorgänge für bestimmte Arten von Bestandslistenobjekten. Rollen, die objektspezifische Berechtigungen enthalten, können auf Zugriffsgruppen angewendet werden.

■ [Interne Berechtigungen](#)

Einige der vordefinierten Administratorrollen können interne Berechtigungen enthalten. Beim Erstellen benutzerdefinierter Rollen können keine internen Berechtigungen ausgewählt werden.

Vordefinierte Administratorrollen

Die vordefinierten Administratorrollen kombinieren die einzelnen Berechtigungen, die zur Ausführung allgemeiner Verwaltungsaufgaben erforderlich sind. Die vordefinierten Rollen können nicht geändert werden.

Hinweis Indem Sie Benutzern eine Kombination aus vordefinierten oder benutzerdefinierten Rollen zuweisen, erhalten Benutzer Zugriff auf Vorgänge, die innerhalb der einzelnen vordefinierten oder benutzerdefinierten Rollen nicht möglich sind.

Die folgende Tabelle beschreibt die vordefinierten Rollen und gibt an, ob eine Rolle auf eine Zugriffsgruppe angewendet werden kann.

Tabelle 7-6. Vordefinierte Rollen in Horizon Console

Rolle	Benutzerfähigkeiten	Gilt für eine Zugriffsgruppe
Administratoren	<p>Durchführen aller Administratöraufgaben wie das Erstellen weiterer Benutzer und Gruppen mit Administratorrechten. In einer Cloud-Pod-Architektur-Umgebung können Administratoren mit dieser Rolle einen Pod-Verbund konfigurieren und verwalten und Remote-Pod-Sitzungen verwalten.</p> <p>Administratoren mit der Administratorenrolle für die Stammzugriffsgruppe sind übergeordnete Benutzer, da sie über Vollzugriff auf alle Bestandslistenobjekte innerhalb des Systems verfügen. Da die Administratorenrolle sämtliche Berechtigungen umfasst, sollte sie einer eingeschränkten Anzahl an Benutzern zugewiesen werden. Anfänglich wird Mitgliedern der lokalen Administratorengruppe auf Ihrem Verbindungsserver-Host diese Rolle für die Stammzugriffsgruppe zugewiesen.</p> <p>Wichtig Ein Administrator muss zur Ausführung der folgenden Aufgaben über die Administratorenrolle für die Stammzugriffsgruppe verfügen:</p> <ul style="list-style-type: none"> ■ Hinzufügen und Löschen von Zugriffsgruppen. ■ Verwalten von ThinApp-Anwendungen und Konfigurationseinstellungen in Horizon Console. ■ Verwenden der Befehle <code>vdmadmin</code>, <code>vdmimport</code> und <code>lvmutil</code>. 	Ja
Administratoren (Nur Lesezugriff)	<ul style="list-style-type: none"> ■ Anzeigen von globalen Einstellungen und Bestandslistenobjekten, jedoch keine Berechtigung zum Ändern dieser Elemente und Einstellungen. ■ Anzeigen, jedoch nicht Modifizieren von ThinApp-Anwendungen und -Einstellungen. ■ Ausführen aller PowerShell-Befehle und Befehlszeilenprogramme einschließlich <code>vdmexport</code>, aber ausschließlich <code>vdmadmin</code>, <code>vdmimport</code> und <code>lvmutil</code>. <p>In einer Cloud-Pod-Architektur-Umgebung können Administratoren mit dieser Rolle Bestandslistenobjekte und Einstellungen der globalen Datenschicht anzeigen.</p> <p>Wenn Administratoren über diese Rolle für eine Zugriffsgruppe verfügen, können sie die Bestandsobjekte in dieser Zugriffsgruppe nur anzeigen.</p>	Ja
Agent-Registrierungsadministratoren	Registrieren nicht verwalteter Maschinen, z. B. physischer Systeme, eigenständiger virtueller Maschinen und RDP-Hosts.	Nein
Administratoren für globale Konfigurationen und Richtlinien	Anzeigen und Ändern globaler Richtlinien und Konfigurationseinstellungen, mit Ausnahme von Administratorrollen und -berechtigungen sowie ThinApp-Anwendungen und -Einstellungen.	Nein
Administratoren für globale Konfigurationen und Richtlinien (Nur Lesezugriff)	Anzeigen, jedoch nicht Ändern globaler Richtlinien und Konfigurationseinstellungen, mit Ausnahme von Administratorrollen und -berechtigungen sowie ThinApp-Anwendungen und -Einstellungen.	Nein

Tabelle 7-6. Vordefinierte Rollen in Horizon Console (Fortsetzung)

Rolle	Benutzerfähigkeiten	Gilt für eine Zugriffsgruppe
Helpdesk-Administratoren	<p>Durchführen von Desktop- und Anwendungsaktionen wie z. B. Herunterfahren, Zurücksetzen oder Neustart und Durchführen von Remoteunterstützungsaktionen wie das Beenden von Prozessen für den Desktop oder die Anwendung eines Benutzers. Ein Administrator benötigt Berechtigungen für die Stammzugriffsgruppe, um auf Horizon Help Desk Tool zuzugreifen.</p> <ul style="list-style-type: none"> ■ Schreibgeschützter Zugriff auf Horizon Help Desk Tool. ■ Verwalten globaler Sitzungen. ■ Kann sich anmelden bei Horizon Console. ■ Ausführen aller computer- und sitzungsbezogenen Befehle. ■ Verwaltung von Remoteprozessen und -anwendungen. ■ Remoteunterstützung für den virtuellen Desktop oder den veröffentlichten Desktop. 	Nein
Helpdesk-Administratoren (schreibgeschützt)	<p>Anzeigen von Benutzer- und Sitzungsinformationen sowie Aufschlüsseln der Sitzungsdetails. Ein Administrator benötigt Berechtigungen für die Stammzugriffsgruppe, um auf Horizon Help Desk Tool zuzugreifen.</p> <ul style="list-style-type: none"> ■ Schreibgeschützter Zugriff auf Horizon Help Desk Tool. ■ Kann sich anmelden bei Horizon Console. 	Nein
Bestandslistenadministratoren	<ul style="list-style-type: none"> ■ Durchführen aller maschinen-, sitzungs- und poolbezogenen Vorgänge. ■ Verwalten persistenter Festplatten. ■ Neusynchronisieren, Aktualisieren und Neuverteilen von Linked-Clone-Pools sowie Ändern des standardmäßigen Pool-Images. ■ Verwalten automatisierter Farmen. <p>Wenn Administratoren über diese Rolle für eine Zugriffsgruppe verfügen, können sie nur diese Vorgänge für die Bestandsobjekte in dieser Zugriffsgruppe durchführen.</p> <p>Administratoren mit dieser Rolle können eine manuelle Farm oder einen nicht verwalteten manuellen Pool nicht erstellen oder RDS-Hosts der Farm oder einem nicht verwalteten manuellen Pool nicht hinzufügen oder daraus entfernen.</p>	Ja
Bestandslistenadministratoren (Nur Lesezugriff)	<p>Anzeigen, aber nicht Ändern von Bestandsobjekten.</p> <p>Wenn Administratoren über diese Rolle für eine Zugriffsgruppe verfügen, können sie die Bestandsobjekte in dieser Zugriffsgruppe nur anzeigen.</p>	Ja

Tabelle 7-6. Vordefinierte Rollen in Horizon Console (Fortsetzung)

Rolle	Benutzerfähigkeiten	Gilt für eine Zugriffsgruppe
Lokale Administratoren	<p>Durchführen aller lokalen Administratöraufgaben, außer dem Erstellen weiterer Benutzer und Gruppen mit Administratorrechten. In einer Cloud-Pod-Architektur-Umgebung können Administratoren mit dieser Rolle keine Vorgänge für die globale Datenschicht durchführen oder Sitzungen auf Remote-Pods verwalten.</p> <hr/> <p>Hinweis Ein Administrator mit der Rolle „Lokale Administratoren“ kann nicht auf Horizon Help Desk Tool zugreifen. Administratoren in einer Nicht-CPA-Umgebung verfügen nicht über das Recht zur Verwaltung globaler Sitzungen, das zum Durchführen von Aufgaben in Horizon Help Desk Tool erforderlich ist.</p>	Ja
Lokale Administratoren (Nur Lesezugriff)	<p>Identisch mit der Rolle „Administratoren (Nur Lesezugriff)“, außer der Anzeige von Bestandslistenobjekten und -einstellungen in der globalen Datenschicht. Administratoren mit dieser Rolle haben Lesezugriff nur auf den lokalen Pod.</p> <hr/> <p>Hinweis Ein Administrator mit der Rolle „Lokale Administratoren (Nur Lesezugriff)“ kann nicht auf Horizon Help Desk Tool zugreifen. Administratoren in einer Nicht-CPA-Umgebung verfügen nicht über das Recht zur Verwaltung globaler Sitzungen, das zum Durchführen von Aufgaben in Horizon Help Desk Tool erforderlich ist.</p>	Ja

Globale Berechtigungen

Globale Berechtigungen steuern systemweite Vorgänge, beispielsweise das Anzeigen und Ändern globaler Einstellungen. Rollen, die ausschließlich globale Berechtigungen enthalten, können nicht auf Zugriffsgruppen angewendet werden.

Die folgende Tabelle zeigt die globalen Berechtigungen sowie die vordefinierten Rollen, die diese Berechtigungen enthalten.

Tabelle 7-7. Globale Berechtigungen

Berechtigung	Benutzerfähigkeiten	Vordefinierte Rollen
Konsoleninteraktion	<p>Melden Sie sich bei Horizon Console an und verwenden Sie es.</p> <hr/> <p>Hinweis Ab Horizon 7 Version 7.10 wird die Berechtigung Konsoleninteraktion neuen Rollen automatisch hinzugefügt und ist nicht Teil der Liste globaler Berechtigungen in Horizon Console.</p>	<p>Administratoren</p> <p>Administratoren (Nur Lesezugriff)</p> <p>Bestandslistenadministratoren</p> <p>Bestandslistenadministratoren (Nur Lesezugriff)</p> <p>Administratoren für globale Konfigurationen und Richtlinien</p> <p>Administratoren für globale Konfigurationen und Richtlinien (Nur Lesezugriff)</p> <p>Helpdesk-Administratoren</p> <p>Helpdesk-Administratoren (nur Lesezugriff)</p> <p>Lokale Administratoren</p> <p>Lokale Administratoren (Nur Lesezugriff)</p>
Direkte Interaktion	<p>Ausführen aller PowerShell-Befehle und Befehlszeilenprogramme mit Ausnahme von vdmadmin und vdmimport.</p> <p>Administratoren müssen über die Administratorrolle für die Stammzugriffsgruppe verfügen, um die Befehle vdmadmin, vdmimport und lmvutil verwenden zu können.</p> <hr/> <p>Hinweis Ab Horizon 7 Version 7.10 wird die Berechtigung Direkte Interaktion neuen Rollen automatisch hinzugefügt und ist nicht Teil der Liste globaler Berechtigungen in Horizon Console.</p>	<p>Administratoren</p> <p>Administratoren (Nur Lesezugriff)</p>
Globale Konfiguration und globale Richtlinien verwalten	Anzeigen und Ändern globaler Richtlinien und Konfigurationseinstellungen, Administratorrollen und -berechtigungen ausgenommen.	<p>Administratoren</p> <p>Administratoren für globale Konfigurationen und Richtlinien</p>
Globale Sitzungen verwalten	Verwalten von globalen Sitzungen in einer Cloud-Pod-Architektur-Umgebung.	Administratoren
Rollen und Berechtigungen verwalten	Erstellen, Ändern und Löschen von Administratorrollen und -berechtigungen.	Administratoren

Tabelle 7-7. Globale Berechtigungen (Fortsetzung)

Berechtigung	Benutzerfähigkeiten	Vordefinierte Rollen
Agent registrieren	Installieren Sie Horizon Agent auf nicht verwalteten Computern, z. B. auf physischen Systemen, eigenständigen virtuellen Maschinen und RDS-Hosts. Während der Horizon Agent-Installation müssen Sie Ihre Administratoranmeldeinformationen angeben, um den nicht verwalteten Computer bei der Verbindungsserver-Instanz zu registrieren.	Administratoren Agent-Registrierungsadministratoren
vCenter-Konfiguration verwalten (schreibgeschützt)	Schreibgeschützter Zugriff auf die vCenter Server-Konfiguration.	Administratoren Administratoren (Nur Lesezugriff) Bestandslistenadministratoren Bestandslistenadministratoren (Nur Lesezugriff) Lokale Administratoren Lokale Administratoren (Nur Lesezugriff)

Objektspezifische Berechtigungen

Objektspezifische Berechtigungen steuern Vorgänge für bestimmte Arten von Bestandslistenobjekten. Rollen, die objektspezifische Berechtigungen enthalten, können auf Zugriffsgruppen angewendet werden.

Die folgende Tabelle beschreibt die objektspezifischen Berechtigungen. Die vordefinierten Rollen Administrators (Administratoren) und Inventory Administrators (Bestandslistenadministratoren) umfassen all diese Berechtigungen.

Tabelle 7-8. Objektspezifische Berechtigungen

Berechtigung	Benutzerfähigkeiten	Objekt
Farmer und Desktop-Pools aktivieren	Aktivieren und Deaktivieren von Desktop-Pools.	Desktop-Pool, Farm
Berechtigung für Desktop- und Anwendungspools verleihen	Hinzufügen und Entfernen von Benutzerberechtigungen.	Desktop-Pool, Anwendungspool
Verwalten von Wartungsvorgängen auf automatisierten Desktops und Farmen	Neuzusammenstellung, Aktualisierung, Neuverteilung, Planung des Push-Images, Planung der Wartung und Änderung des Standard-Images für einen Desktop-Pool und eine Farm.	Desktop-Pool, Farm
Computer verwalten	Ausführen aller computer- und sitzungsbezogenen Vorgänge.	Computer
Persistente Festplatten verwalten	Durchführen aller Horizon Composer-Vorgänge für persistente Festplatten, einschließlich Verknüpfen, Trennen und Importieren von persistenten Festplatten.	Persistente Festplatte
Farmer, Desktop- und Anwendungspools verwalten	Hinzufügen, Ändern und Löschen von Farmen. Hinzufügen, Ändern, Löschen und Berechtigung erteilen für Desktop- und Anwendungspools. Hinzufügen und Entfernen von Maschinen.	Desktop-Pool, Anwendungspool, Farm

Tabelle 7-8. Objektspezifische Berechtigungen (Fortsetzung)

Berechtigung	Benutzerfähigkeiten	Objekt
Sitzungen verwalten	Trennen und Abmelden von Sitzungen und Senden von Nachrichten an Benutzer.	Sitzung
Neustartvorgang verwalten	Zurücksetzen virtueller Maschinen oder Neustarten virtueller Desktops.	Computer

Interne Berechtigungen

Einige der vordefinierten Administratorrollen können interne Berechtigungen enthalten. Beim Erstellen benutzerdefinierter Rollen können keine internen Berechtigungen ausgewählt werden.

Die folgende Tabelle zeigt die internen Berechtigungen sowie die vordefinierten Rollen, die diese Berechtigungen enthalten.

Tabelle 7-9. Interne Berechtigungen

Berechtigung	Beschreibung	Vordefinierte Rollen
Vollständig (Nur Lesezugriff)	Gewährt Lesezugriff auf alle Einstellungen.	Administratoren (Nur Lesezugriff)
Bestandsliste verwalten (Nur Lesezugriff)	Gewährt Lesezugriff auf Bestandslistenobjekte.	Bestandslistenadministratoren (Nur Lesezugriff)
Globale Konfiguration und Globale Richtlinien verwalten (Nur Lesezugriff)	Gewährt Lesezugriff auf Konfigurationseinstellungen und globale Richtlinien, Administratoren und Rollen ausgenommen.	Administratoren für globale Konfigurationen und Richtlinien (Nur Lesezugriff)

Erforderliche Berechtigungen für häufige Aufgaben

Viele häufig ausgeführte Verwaltungsaufgaben erfordern einen bestimmten Satz an Berechtigungen.

Einige Vorgänge erfordern neben dem Zugriff auf das zu ändernde Objekt Berechtigungen für die Stamm-Zugriffsgruppe.

Berechtigungen für die Pool-Verwaltung

Administratoren müssen über bestimmte Berechtigungen für die Verwaltung von Pools in Horizon Console verfügen.

Die folgende Tabelle listet gängige Pool-Verwaltungsaufgaben sowie die erforderlichen Berechtigungen zur Ausführung der einzelnen Aufgaben auf.

Tabelle 7-10. Aufgaben und Berechtigungen für die Pool-Verwaltung

Aufgabe	Erforderliche Berechtigungen
Aktivieren oder Deaktivieren eines Desktop-Pools.	Farmen und Desktop-Pools aktivieren
Zuweisen oder Entfernen von Benutzerberechtigungen für einen Pool.	Berechtigung für Desktop- und Anwendungspools verleihen

Tabelle 7-10. Aufgaben und Berechtigungen für die Pool-Verwaltung (Fortsetzung)

Aufgabe	Erforderliche Berechtigungen
Hinzufügen eines Pools.	Farmen, Desktop- und Anwendungspools verwalten Hinweis Nicht anwendbar für das Hinzufügen eines nicht verwalteten Desktop-Pools. Der Administrator muss auch über die Rolle „Administratoren für globale Konfigurationen und Richtlinien (Nur Lesezugriff)“ verfügen, um diese Aufgabe ausführen zu können.
Ändern oder Löschen eines Pools.	Farmen, Desktop- und Anwendungspools verwalten Hinweis Nicht anwendbar für das Löschen eines nicht verwalteten Desktop-Pools. Der Administrator muss auch über die Rolle „Administratoren für globale Konfigurationen und Richtlinien (Nur Lesezugriff)“ verfügen, um diese Aufgabe ausführen zu können.
Hinzufügen oder Entfernen von Desktops zu bzw. aus einem Pool.	Farmen, Desktop- und Anwendungspools verwalten Hinweis Nicht anwendbar für das Hinzufügen oder Entfernen nicht verwalteter virtueller Desktops im Desktop-Pool. Der Administrator muss auch über die Rolle „Administratoren für globale Konfigurationen und Richtlinien (Nur Lesezugriff)“ verfügen, um diese Aufgabe ausführen zu können.
Aktualisieren, Neuzusammenstellen, Neuverteilen oder Ändern des standardmäßigen Horizon Console-Images.	Composer-Desktop-Pool-Image verwalten und vCenter-Konfiguration verwalten (schreibgeschützt).
Ändern von Zugriffsgruppen.	Farmen, Desktop- und Anwendungspools verwalten für die Quell- und Zielzugriffsgruppen.

Berechtigungen für die Verwaltung von Maschinen

Administratoren müssen über bestimmte Berechtigungen für die Verwaltung von Maschinen in Horizon Console verfügen.

Die folgende Tabelle listet gängige Verwaltungsaufgaben für Computer sowie die erforderlichen Berechtigungen zur Ausführung der einzelnen Aufgaben auf.

Tabelle 7-11. Aufgaben und Berechtigungen für die Verwaltung von Computern

Aufgabe	Erforderliche Berechtigungen
Entfernen einer virtuellen Maschine.	Computer verwalten oder Farmen, Desktop- und Anwendungspools verwalten Hinweis Nicht anwendbar für das Entfernen nicht verwalteter Desktops oder RDS-Hosts aus dem Desktop-Pool oder der Farm. Der Administrator muss auch über die Rolle „Administratoren für globale Konfigurationen und Richtlinien (Nur Lesezugriff)“ verfügen, um diese Aufgabe ausführen zu können.
Zurücksetzen einer virtuellen Maschine.	Neustartvorgang verwalten
Neustarten eines virtuellen Desktops.	Neustartvorgang verwalten

Tabelle 7-11. Aufgaben und Berechtigungen für die Verwaltung von Computern (Fortsetzung)

Aufgabe	Erforderliche Berechtigungen
Zuweisen oder Entfernen von Besitzrechten.	Computer verwalten
Wechseln in den bzw. Beenden des Wartungsmodus.	Computer verwalten
Trennen oder Abmelden von Sitzungen.	Sitzungen verwalten

Berechtigungen für die Verwaltung persistenter Festplatten

Administratoren müssen über bestimmte Berechtigungen für die Verwaltung persistenter Festplatten in Horizon Console verfügen.

Die folgende Tabelle listet gängige Verwaltungsaufgaben für persistente Festplatten sowie die erforderlichen Berechtigungen zur Ausführung der einzelnen Aufgaben auf. Diese Aufgaben werden auf der Seite „Persistente Festplatten“ in Horizon Console ausgeführt.

Tabelle 7-12. Aufgaben und Berechtigungen für die Verwaltung persistenter Festplatten

Aufgabe	Erforderliche Berechtigungen
Trennen einer Festplatte.	<ul style="list-style-type: none"> ■ Wenn es sich bei der Festplatte um eine sekundäre Festplatte handelt, ist die Berechtigung Persistente Festplatten verwalten erforderlich. ■ Wenn es sich bei der Festplatte um eine primäre Festplatte handelt, sind die Berechtigungen Persistente Festplatten verwalten und Computer verwalten erforderlich. ■ Um eine Festplatte in einem anderen Datenspeicher zu trennen, ist die Berechtigung vCenter-Konfiguration verwalten (schreibgeschützt) auch für den Administrator erforderlich.
Verknüpfen einer Festplatte.	Persistente Festplatten verwalten für die Festplatte und Computer verwalten für den Computer.
Bearbeiten einer Festplatte.	Persistente Festplatten verwalten für die Festplatte und Farmen, Desktop- und Anwendungspools verwalten für den ausgewählten Pool.
Ändern von Zugriffsgruppen.	Persistente Festplatten verwalten für die Quell- und Zielzugriffsgruppen.
Neuerstellen eines Desktops.	Persistente Festplatten verwalten für die Festplatte und Farmen, Desktop- und Anwendungspools verwalten oder Computer verwalten für den letzten Desktop-Pool.
Importieren aus vCenter.	Persistente Festplatten verwalten für die Festplatte und vCenter-Konfiguration verwalten (schreibgeschützt) .
Löschen einer Festplatte.	Persistente Festplatten verwalten für die Festplatte.

Berechtigungen für die Verwaltung von Benutzern und Administratoren

Administratoren müssen über bestimmte Berechtigungen zur Verwaltung von Benutzern und Administratoren in Horizon Console verfügen.

Die folgende Tabelle listet gängige Aufgaben für die Benutzer- und Administratorverwaltung sowie die erforderlichen Berechtigungen zur Ausführung der einzelnen Aufgaben auf. Benutzer werden auf der Seite **Benutzer und Gruppen** in Horizon Console verwaltet. Administratoren werden auf der Seite **Ansicht für globale Administratoren** in Horizon Console verwaltet.

Tabelle 7-13. Aufgaben und Berechtigungen für die Verwaltung von Benutzern und Administratoren

Aufgabe	Erforderliche Berechtigungen
Allgemeine Benutzerinformationen aktualisieren	Globale Konfiguration und globale Richtlinien verwalten
Senden von Nachrichten an Benutzer.	Remote-Sitzungen verwalten auf dem Computer.
Hinzufügen von Administratorbenutzern oder -gruppen.	Rollen und Berechtigungen verwalten
Hinzufügen, Ändern oder Löschen von Administratorberechtigungen.	Rollen und Berechtigungen verwalten
Hinzufügen, Ändern oder Löschen von Administratorrollen.	Rollen und Berechtigungen verwalten

Berechtigungen für Horizon Help Desk Tool-Aufgaben

Horizon Help Desk Tool-Administratoren müssen über bestimmte Berechtigungen zur Durchführung von Fehlerbehebungsaufgaben in Horizon Console verfügen.

Die folgende Tabelle führt die gängigen Aufgaben auf, die der Horizon Help Desk Tool-Administrator durchführen kann, und stellt die für die einzelnen Aufgaben erforderlichen Berechtigungen dar.

Tabelle 7-14. Horizon Help Desk Tool-Aufgaben und -Berechtigungen

Aufgaben	Erforderliche Berechtigungen
Schreibgeschützter Zugriff auf Horizon Help Desk Tool.	Helpdesk verwalten (Nur Lesezugriff)
Verwalten globaler Sitzungen.	Globale Sitzungen verwalten
Kann sich anmelden bei Horizon Console.	Konsoleninteraktion Hinweis Ab Horizon 7 Version 7.10 wird die Berechtigung Konsoleninteraktion neuen Rollen automatisch hinzugefügt und ist nicht Teil der Liste globaler Berechtigungen in Horizon Console.
Ausführen aller computer- und sitzungsbezogenen Befehle.	Computer verwalten
Zurücksetzen oder Neustart von Maschinen.	Neustartvorgang verwalten
Trennen und Abmelden von Sitzungen.	Sitzungen verwalten
Verwaltung von Remoteprozessen und -anwendungen.	Remoteprozesse und -anwendungen verwalten
Remoteunterstützung für den virtuellen Desktop oder den veröffentlichten Desktop.	Remoteunterstützung
Trennen, Abmelden, Zurücksetzen und Neustart für globale Sitzungen.	Helpdesk verwalten (Nur Lesezugriff) und Globale Sitzungen verwalten
Vorgänge zum Zurücksetzen und Neustart für lokale Sitzungen.	Helpdesk verwalten (Nur Lesezugriff) und Neustartvorgang verwalten

Tabelle 7-14. Horizon Help Desk Tool-Aufgaben und -Berechtigungen (Fortsetzung)

Aufgaben	Erforderliche Berechtigungen
Vorgänge zur Remoteunterstützung.	Helpdesk verwalten (Nur Lesezugriff) und Remoteunterstützung
Beenden von Remoteprozessen und -anwendungen.	Helpdesk verwalten (Nur Lesezugriff) und Remoteprozesse und -anwendungen verwalten
Ausführen aller Aufgaben in Horizon Help Desk Tool.	Helpdesk verwalten (Nur Lesezugriff), Globale Sitzungen verwalten, Neustartvorgang verwalten, Remoteunterstützung und Remoteprozesse und -anwendungen verwalten
Remoteunterstützung und Beenden von Remoteprozessen und -anwendungen.	Helpdesk verwalten (Nur Lesezugriff), Remoteunterstützung und Remoteprozesse und -anwendungen verwalten
Vorgänge zum Trennen und Abmelden für lokale Sitzungen.	Helpdesk verwalten (Nur Lesezugriff) und Sitzungen verwalten

Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle

Administratoren müssen über bestimmte Berechtigungen zum Ausführen von allgemeinen Verwaltungsaufgaben und Befehlszeilenprogrammen verfügen.

Die folgende Tabelle zeigt die erforderlichen Berechtigungen, um allgemeine Verwaltungsaufgaben und Befehlszeilenprogramme auszuführen.

Tabelle 7-15. Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle

Aufgabe	Erforderliche Berechtigungen
Hinzufügen oder Löschen einer Zugriffsgruppe	Um eine Zugriffsgruppe löschen zu können, sind die lokale Administratorrolle oder die Administratorrolle in der Stammzugriffsgruppe erforderlich. Die Bestandslistenadministratorrolle oder die lokale Administratorrolle oder die Administratorrolle in der Stammzugriffsgruppe sind erforderlich.
Verwalten von ThinApp-Anwendungen und -Einstellungen in Horizon Administrator	Administratorrolle für die Stammzugriffsgruppe.
Installieren von Horizon Agent auf einer nicht verwalteten Maschine (z. B. auf einem physischen System, einer eigenständigen virtuellen Maschine oder einem RDS-Host)	Agent registrieren
Anzeigen oder Ändern von Konfigurationseinstellungen (Administratoreinstellungen ausgenommen) in Horizon Administrator	Globale Konfiguration und globale Richtlinien verwalten
Ausführen aller PowerShell-Befehle und Befehlszeilenprogramme mit Ausnahme von <code>vdadmin</code> und <code>vdimport</code> .	Direkte Interaktion Hinweis Ab Horizon 7 Version 7.10 wird die Berechtigung „Direkte Interaktion“ neuen Rollen automatisch hinzugefügt und ist nicht in der Liste globaler Berechtigungen in Horizon Console enthalten.

Tabelle 7-15. Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle (Fortsetzung)

Aufgabe	Erforderliche Berechtigungen
Verwenden der Befehle vdmadmin und vdmimport	Administratorrolle für die Stammzugriffsgruppe.
Verwenden des vdmexport-Befehls	Administratorenrolle (Lese- und Schreibzugriff oder nur Lesezugriff) für die Stammzugriffsgruppe.
Schreibgeschützter Zugriff auf die vCenter Server-Konfiguration.	vCenter-Konfiguration verwalten (schreibgeschützt)

Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen

Um die Sicherheit und Verwaltbarkeit Ihrer Horizon 7-Umgebung zu verbessern, sollten bei der Verwaltung von Administratorbenutzern und -gruppen empfohlene Vorgehensweisen befolgt werden.

- Erstellen Sie neue Benutzergruppen in Active Directory und weisen Sie diesen Gruppen Administrationsrollen zu. Vermeiden Sie es, in Windows integrierte Gruppen oder andere vorhandene Gruppen zu verwenden, die möglicherweise Benutzer enthalten, die keine Horizon 7-Berechtigung benötigen oder haben sollten.
- Halten Sie die Anzahl an Benutzern mit Horizon 7-Administrationsrichtlinien auf ein Minimum begrenzt.
- Da die Administratorenrolle jede Berechtigung besitzt, sollte sie nicht für die alltägliche Verwaltung verwendet werden.
- Vermeiden Sie beim Erstellen von Administratorbenutzern und -gruppen die Verwendung des Namens „Administrator“, da dieser offensichtlich und leicht zu erraten ist.
- Erstellen Sie Zugriffsgruppen, um vertrauliche Desktops und Farmen zu trennen. Delegieren Sie die Verwaltung dieser Zugriffsgruppen an eine eingeschränkte Anzahl an Benutzern.
- Erstellen Sie separate Administratoren, die globale Richtlinien und Horizon 7-Konfigurationseinstellungen ändern können.

Festlegen von Richtlinien in Horizon Console

8

Sie können mithilfe von Horizon Console Richtlinien für Clientsitzungen konfigurieren.

Sie können diese Richtlinien so festlegen, dass sie auf bestimmte Benutzer, bestimmte Desktop-Pools oder auf alle Clientsitzungsbenutzer angewendet werden. Richtlinien, die für bestimmte Benutzer und Desktop-Pools gelten, werden als Richtlinien auf Benutzer- und Desktop-Pool-Ebene bezeichnet. Richtlinien, die sich auf alle Sitzungen und Benutzer auswirken, werden als globale Richtlinien bezeichnet.

Richtlinien auf Benutzerebene erben Einstellungen von äquivalenten Richtlinieneinstellungen für Desktop-Pools. Ähnlich erben Richtlinien auf Desktop-Pool-Ebene Einstellungen von äquivalenten globalen Richtlinieneinstellungen. Eine Richtlinieneinstellung auf Desktop-Pool-Ebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung. Eine Richtlinieneinstellung auf Benutzerebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung oder Richtlinieneinstellungen auf Pool-Ebene.

Richtlinieneinstellungen auf einer niedrigeren Ebene können mehr oder weniger restriktiv sein als die äquivalenten Einstellungen höherer Ebene. Beispiel: Sie können eine globale Richtlinie auf **Verweigern** und die äquivalente Richtlinie auf Desktop-Pool-Ebene auf **Zulassen** oder umgekehrt festlegen.

Hinweis Nur globale Richtlinien sind für veröffentlichte Desktop- und -Anwendungspools verfügbar. Sie können keine Richtlinien auf Benutzerebene oder Poolebene für veröffentlichte Desktop- und Anwendungspools festlegen.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren von globalen Richtlinien](#)

Konfigurieren von globalen Richtlinien

Sie können globale Richtlinien konfigurieren, um das Verhalten aller Clientsitzungsbenutzer zu steuern.

Verfahren

- 1 Wählen Sie in Horizon Console **Einstellungen > Globale Richtlinien** aus.

Im Bereich **Globale Richtlinien** werden die Einstellungen angezeigt, die sich auf alle Clientsitzungen, Desktop-Pools oder Benutzer auswirken.

Tabelle 8-1. Horizon-Richtlinien

Richtlinie	Beschreibung
Multimedia-Umleitung (MMR)	<p>Legt fest, ob MMR für Clientsysteme aktiviert ist.</p> <p>MMR ist ein Windows Media Foundation-Filter, der Multimediadaten von bestimmten Codecs auf Remote-Desktops direkt über einen TCP-Socket an das Clientsystem weiterleitet. Die Daten werden direkt auf dem Clientsystem decodiert, auf dem sie wiedergegeben werden.</p> <p>Der Standardwert lautet Verweigern.</p> <p>Wenn Clientsysteme über unzureichende Ressourcen zum Verarbeiten der lokalen Multimedia-Decodierung verfügen, lassen Sie die Einstellung auf Verweigern.</p> <p>MMR-Daten (Multimedia Redirection, Multimediaumleitung) werden über das Netzwerk ohne anwendungsbasierte Verschlüsselung gesendet und können sensitive Daten enthalten, abhängig vom umgeleiteten Inhalt. Um sicherzustellen, dass diese Daten nicht auf dem Netzwerk nachverfolgt werden können, sollten Sie MMR nur auf einem sicheren Netzwerk verwenden.</p>
USB-Zugriff	<p>Legt fest, ob Remote-Desktops USB-Geräte verwenden können, die mit dem Clientsystem verbunden sind.</p> <p>Der Standardwert lautet Zulassen. Um aus Sicherheitsgründen die Verwendung externer Geräte zu unterbinden, ändern Sie die Einstellung in Verweigern.</p>
PCoIP-Hardwarebeschleunigung	<p>Legt fest, ob die Hardwarebeschleunigung für das PCoIP-Anzeigeprotokoll aktiviert wird und legt die Beschleunigungspriorität fest, die der PCoIP-Benutzersitzung zugewiesen ist.</p> <p>Diese Einstellung hat nur dann Auswirkungen, wenn ein PCoIP-Hardwarebeschleunigungsgerät auf dem physischen Computer vorhanden ist, der den Remote-Desktop hostet.</p> <p>Der Standardwert lautet Zulassen, mit dem Prioritätswert Mittel.</p>

- 2 Klicken Sie auf **Richtlinien bearbeiten**, um die Einstellungen zu ändern.
- 3 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Warten von Horizon 7-Komponenten

9

Um die Verfügbarkeit und den fehlerfreien Betrieb Ihrer Horizon 7-Komponenten sicherzustellen, können Sie verschiedene Wartungsaufgaben ausführen.

Dieses Kapitel enthält die folgenden Themen:

- [Sichern und Wiederherstellen von Horizon 7-Konfigurationsdaten](#)
- [Wiederherstellen von Horizon-Verbindungsserver- und Horizon Composer-Konfigurationsdaten](#)
- [Exportieren von Daten in Horizon Composer-Datenbank](#)
- [Überwachen von Horizon 7-Komponenten](#)
- [Grundlegendes zu Horizon 7-Diensten](#)
- [Ändern des Produktlizenzschlüssels oder der Lizenzmodi in Horizon Console](#)
- [Überwachen der Lizenznutzung](#)
- [Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit](#)
- [Integration des Horizon-Verbindungservers mit Skyline Collector-Appliance](#)

Sichern und Wiederherstellen von Horizon 7-Konfigurationsdaten

Sie können Ihre Horizon 7- und Horizon Composer-Konfigurationsdaten sichern, indem Sie in Horizon Console automatische Sicherungen planen oder ausführen. Sie können Ihre Horizon 7-Konfiguration wiederherstellen, indem Sie die gesicherten View LDAP-Dateien und Horizon Composer-Datenbankdateien manuell importieren.

Sie können die Sicherungs- und Wiederherstellungsfunktionen verwenden, um Horizon 7-Konfigurationsdaten beizubehalten und zu migrieren.

Sichern von Horizon-Verbindungsserver- und Horizon Composer-Daten

Nachdem Sie die anfängliche Konfiguration des Verbindungservers abgeschlossen haben, sollten Sie regelmäßige Sicherungen Ihrer Horizon 7- und Horizon Composer-Konfigurationsdaten planen. Sie können Ihre Horizon 7- und Horizon Composer-Daten mit Horizon Console beibehalten.

Horizon 7 speichert Verbindungsserver-Konfigurationsdaten im View LDAP-Repository. Horizon Composer speichert Konfigurationsdaten für Linked-Clone-Desktops in der Horizon Composer-Datenbank.

Wenn Sie Sicherungen mithilfe von Horizon Console durchführen, sichert Horizon 7 die View LDAP-Konfigurationsdaten und die Horizon Composer-Datenbank. Beide Sicherungsdateisätze werden am selben Speicherort gespeichert. Die View LDAP-Daten werden im verschlüsselten LDAP Data Interchange Format (LDIF) exportiert. Eine Beschreibung des View LDAP finden Sie unter „View LDAP-Verzeichnis“ im Dokument *Horizon 7-Verwaltung*.

Sie können Sicherungen auf verschiedene Arten ausführen.

- Planen Sie automatische Sicherungen unter Verwendung der Horizon 7-Funktion für die Konfigurationssicherung.
- Wenn Sie sofort eine Sicherung durchführen möchten, verwenden Sie die Funktion **Jetzt sichern** in Horizon Console.
- Sie können mit dem Dienstprogramm `vdmexport` einen manuellen Export der View LDAP-Daten durchführen. Dieses Dienstprogramm wird mit jeder Verbindungsserver-Instanz bereitgestellt.

Das Dienstprogramm `vdmexport` kann View LDAP-Daten als verschlüsselte LDIF-Daten, einfachen Text oder einfachen Text mit entfernten Kennwörtern oder anderen vertraulichen Daten exportieren.

Hinweis Das Tool `vdmexport` sichert nur die View LDAP-Daten. Mit diesem Tool werden keine Horizon Console-Datenbankinformationen gesichert.

Weitere Informationen zu `vdmexport` finden Sie unter [Exportieren von Konfigurationsdaten aus Horizon-Verbindungsserver](#).

Es gelten die folgenden Richtlinien für das Sichern von Horizon 7-Konfigurationsdaten:

- Horizon 7 kann Konfigurationsdaten aus einer beliebigen Verbindungsserver-Instanz exportieren.
- Wenn mehrere Verbindungsserver-Instanzen in einer replizierten Gruppe vorhanden sind, müssen Sie die Daten nur aus einer Instanz exportieren. Alle replizierten Instanzen umfassen dieselben Konfigurationsdaten.
- Verlassen Sie sich nicht darauf, dass replizierte Instanzen von Verbindungsserver als Sicherungsmechanismus fungieren. Wenn Horizon 7 Daten in replizierten Instanzen des Verbindungservers synchronisiert, werden die auf einer Instanz verlorenen Daten bei der Datenharmonisierung von allen Mitgliedern der Gruppe entfernt.

- Wenn der Verbindungsserver mehrere vCenter Server-Instanzen mit mehreren Horizon Composer-Diensten verwendet, sichert Horizon 7 alle mit sämtlichen vCenter Server-Instanzen verknüpften Horizon Composer-Datenbanken.

Planen von Horizon 7-Konfigurationssicherungen

Sie können die Sicherung Ihrer Horizon 7-Konfigurationsdaten planen, sodass die Daten in regelmäßigen Abständen gesichert werden. Horizon 7 sichert die Inhalte des View LDAP-Repositorys, in dem die Verbindungsserver-Instanzen ihre Konfigurationsdaten speichern.

Sie können die Konfigurationsdateien sofort sichern, indem Sie die Verbindungsserver-Instanz auswählen und auf **Jetzt sichern** klicken.

Voraussetzungen

Machen Sie sich mit den Sicherungseinstellungen vertraut. Siehe [Sicherungseinstellungen zur Horizon 7-Konfiguration](#).

Verfahren

- 1 Wählen Sie in Horizon Console **Einstellungen > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die zu sichernde Verbindungsserver-Instanz aus und klicken Sie auf **Jetzt sichern**.
- 3 Geben Sie auf der Registerkarte **Sicherung** die Einstellungen für die Horizon 7-Konfigurationssicherung an. Legen Sie beispielsweise die Sicherungshäufigkeit, die maximale Anzahl an Sicherungsdateien sowie den Speicherort für die Sicherungsdateien fest.
- 4 (Optional) Ändern Sie das Kennwort für die Datenwiederherstellung.
 - a Klicken Sie auf **Kennwort für die Datenwiederherstellung ändern**.
 - b Geben Sie das neue Kennwort zweimal ein.
 - c (Optional) Geben Sie eine Kennworterinnerung ein.
 - d Klicken Sie auf **OK**.
- 5 Klicken Sie auf **OK**.

Sicherungseinstellungen zur Horizon 7-Konfiguration

Horizon 7 kann Ihre Verbindungsserver- und Horizon Composer-Konfigurationsdaten in regelmäßigen Abständen sichern. In Horizon Console können Sie die Häufigkeit und andere Aspekte der Sicherungsvorgänge festlegen.

Tabelle 9-1. Sicherungseinstellungen zur Horizon 7-Konfiguration

Einstellung	Beschreibung
Häufigkeit für automatische Sicherungen	<p>Jede Stunde. Sicherungen werden einmal pro Stunde zur vollen Stunde erstellt.</p> <p>Alle 6 Stunden. Sicherungen werden um 24:00 Uhr, 6:00 Uhr, 12:00 Uhr und 18:00 erstellt.</p> <p>Alle 12 Stunden. Sicherungen werden um 24:00 Uhr und um 12:00 Uhr erstellt.</p> <p>Jeden Tag. Sicherungen werden einmal pro Tag um 24:00 Uhr erstellt.</p> <p>Alle 2 Tage. Sicherungen werden am Samstag, Montag, Mittwoch und Freitag jeweils um 24:00 Uhr erstellt.</p> <p>Jede Woche. Sicherungen werden einmal pro Woche am Samstag um 24:00 Uhr erstellt.</p> <p>Alle 2 Wochen. Sicherungen werden jede zweite Woche am Samstag um 24:00 Uhr erstellt.</p> <p>Nie. Es werden keine automatischen Sicherungen ausgeführt.</p>
Sicherungszeitpunkt	Zeitpunkt für die Planung einer Sicherung.
Offset für Sicherungszeitpunkt	Offset für den Zeitpunkt für eine geplante Sicherung.
Maximale Anzahl an Sicherungen	<p>Gibt die Anzahl an Sicherungsdateien an, die auf der Verbindungsserver-Instanz gespeichert werden können. Bei dem hier angegebenen Wert muss es sich um eine Ganzzahl handeln, die größer ist als 0.</p> <p>Wird der angegebene Wert erreicht, wird die älteste Sicherungsdatei von Horizon 7 gelöscht.</p> <p>Diese Einstellung gilt auch für Sicherungsdateien, die mit der Option Jetzt sichern erstellt werden.</p>
Speicherort für Ordner	<p>Standardspeicherort der Sicherungsdateien auf dem Computer, auf dem der Verbindungsserver ausgeführt wird: C:\ProgramData\VMware\VDM\backups</p> <p>Bei Verwendung der Option Jetzt sichern legt Horizon 7 die Sicherungsdateien ebenfalls an diesem Speicherort ab.</p>

Exportieren von Konfigurationsdaten aus Horizon-Verbindungsserver

Sie können die Konfigurationsdaten einer Horizon-Verbindungsserver-Instanz sichern, indem Sie die Inhalte des zugehörigen View LDAP-Repository exportieren.

Verwenden Sie den Befehl `vdmexport`, um die View LDAP-Konfigurationsdaten in eine verschlüsselte LDIF-Datei zu exportieren. Sie können auch die Option `vdmexport -v` (verbatim/wortgetreu) verwenden, um die Daten in eine einfache LDIF-Textdatei zu exportieren, oder die Option `vdmexport -c` (cleansed/ bereinigt), um die Daten als einfachen Text mit entfernten Kennwörtern und anderen vertraulichen Daten zu exportieren.

Sie können den Befehl `vdmexport` auf einer beliebigen Verbindungsserver-Instanz ausführen. Wenn mehrere Verbindungsserver-Instanzen in einer replizierten Gruppe vorhanden sind, müssen Sie die Daten nur aus einer Instanz exportieren. Alle replizierten Instanzen umfassen dieselben Konfigurationsdaten.

Hinweis Der Befehl `vdmexport.exe` sichert nur die View LDAP-Daten. Mit diesem Befehl werden keine Horizon Composer-Datenbankinformationen gesichert.

Voraussetzungen

- Suchen Sie im folgenden Standardpfad nach der ausführbaren Datei `vdmexport.exe`, die zusammen mit Verbindungsserver installiert wird.

`C:\Programme\VMware\VMware View\Server\tools\bin`

- Melden Sie sich bei einer Verbindungsserver-Instanz als Benutzer mit der Rolle „Administrators“ (Administratoren) oder „Administrators (Read only)“ (Administratoren (Nur Lesen)) an.

Verfahren

- 1 Wählen Sie **Start > Eingabeaufforderung** aus.
- 2 Geben Sie an der Eingabeaufforderung den Befehl `vdmexport` ein und leiten Sie die Ausgabe in eine Datei um. Beispiel:

```
vdmexport > Myexport.LDF
```

Die exportierten Daten sind standardmäßig verschlüsselt.

Sie können den Namen der Ausgabedatei als Argument für die Option `-f` angeben. Beispiel:

```
vdmexport -f Myexport.LDF
```

Sie können die Daten in einfachem Textformat (verbatim/wortgetreu) exportieren, indem Sie die Option `-v` verwenden. Beispiel:

```
vdmexport -f Myexport.LDF -v
```

Sie können die Daten in einfachem Textformat mit entfernten Kennwörtern und anderen vertraulichen Daten (cleansed/bereinigt) exportieren, indem Sie die Option `-c` verwenden. Beispiel:

```
vdmexport -f Myexport.LDF -c
```

Hinweis Sie sollten keine bereinigten Sicherungsdaten zur Wiederherstellung einer View LDAP-Konfiguration verwenden. Den bereinigten Konfigurationsdaten fehlen Kennwörter und andere wichtige Informationen.

Weitere Informationen zum Befehl `vdmexport` finden Sie im Dokument *Horizon 7-Integration*.

Nächste Schritte

Sie können die Konfigurationsinformationen vom Verbindungsserver wiederherstellen oder übertragen, indem Sie den Befehl `vdmimport` verwenden.

Weitere Informationen zum Importieren der LDIF-Datei finden Sie unter [Wiederherstellen von Horizon-Verbindungsserver- und Horizon Composer-Konfigurationsdaten](#).

Wiederherstellen von Horizon-Verbindungsserver- und Horizon Composer-Konfigurationsdaten

Sie können die von Horizon 7 gesicherten Verbindungsserver-LDAP-Konfigurationsdateien und die Horizon Composer-Datenbankdateien manuell wiederherstellen.

Sie führen manuell verschiedene Dienstprogramme aus, um die Verbindungsserver- und Horizon Composer-Konfigurationsdaten wiederherzustellen.

Bevor Sie Konfigurationsdaten wiederherstellen, sollten Sie sicherstellen, dass Sie die Konfigurationsdaten in Horizon Console gesichert haben. Siehe [Sichern von Horizon-Verbindungsserver- und Horizon Composer-Daten](#).

Verwenden Sie das Dienstprogramm `vdmimport`, um die Verbindungsserver-Daten aus den LDIF-Sicherungsdateien in das View LDAP-Repository der Verbindungsserver-Instanz zu importieren.

Mit dem Dienstprogramm `SviConfig` können Sie die Horizon Composer-Daten aus den `.svi`-Sicherungsdateien in die Horizon Composer-SQL-Datenbank importieren.

Hinweis Unter bestimmten Umständen müssen Sie die aktuelle Version einer Verbindungsserver-Instanz installieren und die vorhandene Horizon 7-Konfiguration wiederherstellen, indem Sie die Verbindungsserver-LDAP-Konfigurationsdateien importieren. Diese Vorgehensweise kann im Rahmen eines Business Continuity- und Disaster Recovery-Plans (BC/DR), bei dem ein Schritt vorsieht, ein zweites Rechenzentrum mit der bestehenden Horizon 7-Konfiguration einzurichten, oder aus anderen Gründen erforderlich sein. Weitere Informationen finden Sie im Dokument *Horizon 7-Installation*.

Importieren von Konfigurationsdaten in Horizon-Verbindungsserver

Sie können die Konfigurationsdaten einer Verbindungsserver-Instanz wiederherstellen, indem Sie eine Sicherungskopie der in einer LDIF-Datei gespeicherten Daten importieren.

Verwenden Sie den Befehl `vdmimport`, um die Daten aus der LDIF-Datei in das View LDAP-Repository der Verbindungsserver-Instanz zu importieren.

Wenn Sie Ihre View LDAP-Konfiguration mit Horizon Console oder dem Standardbefehl `vdmexport` gesichert haben, ist die exportierte LDIF-Datei verschlüsselt. Sie müssen die LDIF-Datei entschlüsseln, bevor Sie sie importieren können.

Wenn die exportierte LDIF-Datei in einfachem Textformat vorliegt, müssen Sie die Datei nicht entschlüsseln.

Hinweis Importieren Sie eine LDIF-Datei nicht im bereinigten Format, bei dem es sich um einfachen Text mit entfernten Kennwörtern und anderen vertraulichen Daten handelt. Wenn Sie dies tun, fehlen wichtige Konfigurationsinformationen im wiederhergestellten View LDAP-Repository.

Informationen zum Sichern des View LDAP-Repository finden Sie unter [Sichern von Horizon-Verbindungsserver- und Horizon Composer-Daten](#).

Voraussetzungen

- Suchen Sie im folgenden Standardpfad nach der ausführbaren Datei `vdmimport`, die zusammen mit Verbindungsserver installiert wird.

`C:\Programme\VMware\VMware View\Server\tools\bin`

- Melden Sie sich bei einer Verbindungsserver-Instanz als Benutzer mit der Rolle „Administratoren“ an.
- Vergewissern Sie sich, dass Sie das Kennwort für die Datenwiederherstellung kennen. Wenn eine Kennworterinnerung konfiguriert wurde, können Sie die Erinnerung anzeigen, indem Sie den Befehl `vdmimport` ohne Kennwortoption ausführen.

Verfahren

- 1 Beenden Sie alle Instanzen von Horizon Composer, indem Sie den VMware Horizon Composer-Windows-Dienst auf den Servern beenden, auf denen Horizon Composer ausgeführt wird.
- 2 Deinstallieren Sie alle Instanzen von Horizon-Verbindungsserver.

Deinstallieren Sie sowohl VMware Horizon-Verbindungsserver als auch die AD LDS-Instanz „VMwareVDMDS“.
- 3 Installieren Sie eine Instanz von Verbindungsserver.
- 4 Stoppen Sie die Verbindungsserver-Instanz, indem Sie den Windows-Dienst „VMware Horizon Verbindungsserver“ stoppen.
- 5 Klicken Sie auf **Start > Eingabeaufforderung**.
- 6 Entschlüsseln Sie die verschlüsselte LDIF-Datei.

Geben Sie an der Eingabeaufforderung den Befehl `vdmimport` ein. Geben Sie die Option `-d`, die Option `-p` mit dem Kennwort zur Datenwiederherstellung und die Option `-f` mit einer vorhandenen verschlüsselten LDIF-Datei gefolgt von einem Namen für die entschlüsselte LDIF-Datei an. Beispiel:

Wenn Sie sich an das Kennwort für die Datenwiederherstellung nicht mehr erinnern können, geben Sie den Befehl ohne die Option `-p` ein. Das Dienstprogramm zeigt die Kennworterinnerung an und fordert Sie auf, das Kennwort einzugeben.
- 7 Importieren Sie die entschlüsselte LDIF-Datei, um die View LDAP-Konfiguration wiederherzustellen.

Geben Sie die Option `-f` mit der entschlüsselten LDIF-Datei an. Beispiel:
- 8 Deinstallieren Sie den Verbindungsserver.

Deinstallieren Sie nur das Paket „VMware Horizon-Verbindungsserver“.
- 9 Installieren Sie den Verbindungsserver neu.
- 10 Melden Sie sich bei Horizon Console an und validieren Sie, dass die Konfiguration korrekt ist.
- 11 Starten Sie die Horizon Composer-Instanzen.
- 12 Installieren Sie die Replikatserverinstanzen neu.

Der Befehl `vdmimport` aktualisiert das View LDAP-Repository in Verbindungsserver mit den Konfigurationsdaten aus der LDIF-Datei. Weitere Informationen zum Befehl `vdmimport` finden Sie im Dokument *Horizon 7-Installation*.

Hinweis Stellen Sie sicher, dass die Konfiguration, die gerade wiederhergestellt wird, mit den virtuellen Maschinen übereinstimmt, die vCenter Server und Horizon Composer bekannt sind, falls letzter verwendet wird. Stellen Sie bei Bedarf die Horizon Composer-Konfiguration von einer Sicherung wieder her. Siehe [Wiederherstellen einer Horizon Composer-Datenbank](#). Nachdem Sie die Horizon Composer-Konfiguration wiederherstellen, müssen Sie möglicherweise manuell Inkonsistenzen auflösen, falls sich die virtuellen Maschinen in vCenter Server seit der Sicherung der Horizon Composer-Konfiguration geändert haben.

Wiederherstellen einer Horizon Composer-Datenbank

Sie können die Sicherungsdateien für Ihre Horizon Composer-Konfiguration in die Horizon Composer-Datenbank importieren, die Linked-Clone-Informationen speichert.

Mithilfe des Befehls `SviConfig restoredata` können Sie die Horizon Composer-Datenbank nach einem Systemausfall wiederherstellen oder die Horizon Composer-Konfiguration in einen früheren Zustand zurückversetzen.

Wichtig Nur erfahrene Horizon Composer-Administratoren sollten das Dienstprogramm `SviConfig` verwenden. Mit diesem Dienstprogramm lassen sich Fehler im Zusammenhang mit dem Horizon Composer-Dienst behandeln.

Voraussetzungen

Ermitteln Sie den Speicherort der Sicherungsdateien für die Horizon Composer-Datenbank. Standardmäßig speichert Horizon 7 die Sicherungsdateien auf Laufwerk C: des Verbindungsserver-Computers im Verzeichnis `C:\ProgramData\VMware\VDM\backups`.

Horizon Composer-Sicherungsdateien folgen einer Namenskonvention mit Datumsstempel und `.svi`-Suffix.

`Backup-Jahr_Monat_Tag-Nummer-vCenter_Server-Name_Domänenname.svi`

Beispiel: `Backup-20090304000010-foobar_test_org.svi`

Machen Sie sich mit den `SviConfig restoredata`-Parametern vertraut:

- **DsnName** – Der DSN für die Verbindung mit der Datenbank. Der Parameter `DsnName` ist verbindlich und kann keine leere Zeichenfolge enthalten.
- **Username** – Der Benutzername für die Verbindung mit der Datenbank. Wenn dieser Parameter nicht angegeben wird, wird die Windows-Authentifizierung verwendet.
- **Password** – Das Kennwort des Benutzers, der eine Verbindung mit der Datenbank herstellt. Wenn dieser Parameter nicht angegeben und die Windows-Authentifizierung nicht verwendet wird, werden Sie zu einem späteren Zeitpunkt zur Eingabe des Kennworts aufgefordert.
- **BackupFilePath** – Der Pfad zur Horizon Composer-Sicherungsdatei.

Die Parameter DsnName und BackupFilePath sind erforderlich und können keine leeren Zeichenfolgen enthalten. Die Parameter Username und Password sind optional.

Verfahren

- 1 Kopieren Sie die Horizon Composer-Sicherungsdateien vom Verbindungsserver-Computer an einen Speicherort, auf den von dem Computer zugegriffen werden kann, auf dem der VMware Horizon Composer-Dienst installiert ist.
- 2 Beenden Sie auf dem Computer, auf dem Horizon Composer installiert ist, den VMware Horizon Composer-Dienst.
- 3 Öffnen Sie eine Windows-Eingabeaufforderung und navigieren Sie zur ausführbaren SviConfig-Datei.

Die Datei befindet sich im Ordner der Horizon Composer-Anwendung. Der Standardpfad lautet C:\Programme (x86)\VMware\VMware View Composer\sviconfig.exe.

- 4 Führen Sie den Befehl SviConfig restoredata aus.

```
sviconfig -operation=restoredata
          -DsnName=Ziel-DSN
          -Username=Benutzername_des_Datenbankadministrators
          -Password=Kennwort_des_Datenbankadministrators
          -BackupFilePath=Pfad_zur_View_Composer-Sicherungsdatei
```

Beispiel:

```
sviconfig -operation=restoredata -dsnnname=LinkedClone
          -username=Admin -password=Pass
          -backupfilepath="C:\Program Files (x86)\VMware\VMware View
Composer\Backup-20090304000010-foobar_test_org.SVI"
```

- 5 Starten Sie den VMware Horizon Composer-Dienst.

Nächste Schritte

Ergebniscodes zur Ausgabe des Befehls SviConfig restoredata finden Sie unter [Ergebniscodes für das Wiederherstellen der Horizon Console-Datenbank](#).

Ergebniscodes für das Wiederherstellen der Horizon Console-Datenbank

Wenn Sie eine Horizon Console-Datenbank wiederherstellen, zeigt der Befehl SviConfig restoredata einen Ergebniscode an.

Tabelle 9-2. Restoredata-Ergebniscodes

Code	Beschreibung
0	Vorgang erfolgreich abgeschlossen.
1	Angegebener DSN wurde nicht gefunden.
2	Angegebene Anmeldeinformationen für Datenbankadministrator sind ungültig.

Tabelle 9-2. Restoredata-Ergebniscodes (Fortsetzung)

Code	Beschreibung
3	Treiber für die Datenbank wird nicht unterstützt.
4	Unerwartetes Problem ist aufgetreten und der Befehl konnte nicht abgeschlossen werden.
14	Der VMware Horizon Console-Dienst wird von einer anderen Anwendung verwendet. Beenden Sie den Dienst, bevor Sie den Befehl ausführen.
15	Während des Wiederherstellungsvorgangs ist ein Problem aufgetreten. Einzelheiten sind in der angezeigten Protokollausgabe aufgeführt.

Exportieren von Daten in Horizon Composer-Datenbank

Sie können die Daten aus Ihrer Horizon Composer-Datenbank in eine Datei exportieren.

Wichtig Das Dienstprogramm SviConfig sollte nur von erfahrenen Horizon Composer-Administratoren verwendet werden.

Voraussetzungen

Standardmäßig speichert Horizon 7 die Sicherungsdateien auf Laufwerk C: des Verbindungsserver-Computers im Verzeichnis C:\ProgramData\VMware\VDM\backups.

Machen Sie sich mit den SviConfig exportdata-Parametern vertraut:

- DsnName – Der DSN für die Verbindung mit der Datenbank. Wenn dieser Wert nicht angegeben wird, werden DSN, Benutzername und Kennwort aus der Serverkonfigurationsdatei abgerufen.
- Username – Der Benutzername für die Verbindung mit der Datenbank. Wenn dieser Parameter nicht angegeben wird, wird die Windows-Authentifizierung verwendet.
- Password – Das Kennwort des Benutzers, der eine Verbindung mit der Datenbank herstellt. Wenn dieser Parameter nicht angegeben und die Windows-Authentifizierung nicht verwendet wird, werden Sie zu einem späteren Zeitpunkt zur Eingabe des Kennworts aufgefordert.
- OutputFilePath – Der Pfad zur Ausgabedatei.

Verfahren

- 1 Beenden Sie auf dem Computer, auf dem Horizon Composer installiert ist, den VMware Horizon Composer-Dienst.
- 2 Öffnen Sie eine Windows-Eingabeaufforderung und navigieren Sie zur ausführbaren SviConfig-Datei.

Die Datei befindet sich im Ordner der Horizon Composer-Anwendung.

Horizon-Composer-installation-directory\sviconfig.exe

3 Führen Sie den Befehl `SviConfig exportdata` aus.

```
sviconfig -operation=exportdata
          -DsnName=Ziel-DSN
          -Username=Benutzername_des_Datenbankadministrators
          -Password=Kennwort_des_Datenbankadministrators
          -OutputFilePath=Pfad_zur_Horizon_Composer-Ausgabedatei
```

Beispiel:

```
sviconfig -operation=exportdata -dsname=LinkedClone
          -username=Admin -password=Pass
          -outputfilepath="C:\Program Files\VMware\VMware View
          Composer\Export-20090304000010-foobar_test_org.SVI"
```

Nächste Schritte

Exportergebniscodes des Befehls `SviConfig exportdata` finden Sie unter [Ergebniscodes für den Export der Horizon Composer-Datenbank](#).

Ergebniscodes für den Export der Horizon Composer-Datenbank

Beim Export einer Horizon Composer-Datenbank zeigt der `SviConfig exportdata` -Befehl einen Exitcode an.

Tabelle 9-3. Exportdata ExitStatus-Codes

Code	Beschreibung
0	Der Datenexport wurde erfolgreich beendet.
1	Der angegebene DSN wurde nicht gefunden.
2	Die angegebenen Anmeldeinformationen sind ungültig.
3	Der Treiber für die angegebene Datenbank wird nicht unterstützt.
4	Es ist ein unerwartetes Problem aufgetreten.
18	Verbindung zum Datenbankserver kann nicht hergestellt werden.
24	Die Ausgabedatei kann nicht geöffnet werden.

Überwachen von Horizon 7-Komponenten

Sie können den Status der Horizon 7- und vSphere-Komponenten in Ihrer Horizon 7-Bereitstellung problemlos über das Horizon Console-Dashboard überwachen.

Horizon Console zeigt Überwachungsinformationen zu Verbindungsserver-Instanzen, zur Ereignisdatenbank, zu Gateways, Horizon Composer-Diensten, Datenspeichern, vCenter Server-Instanzen und Domänen an.

Hinweis Horizon 7 kann keine Statusinformationen zu Kerberos-Domänen sammeln. Horizon Console zeigt den Status von Kerberos-Domänen als unbekannt an, selbst wenn eine Domäne konfiguriert wurde und fehlerfrei arbeitet.

Verfahren

1 Navigieren Sie in Horizon Console zu **Monitor > Dashboard**.

2 Klicken Sie im Bereich **Systemzustand** auf **Anzeigen**.

Im Bereich „Details“ werden der Name, die Version und weitere Informationen zu den einzelnen Problemen angezeigt.

- Ein grünes Häkchen weist darauf hin, dass für eine Komponente keine Probleme vorliegen.
- Ein rotes Ausrufezeichen weist darauf hin, dass eine Komponente nicht verfügbar ist oder nicht funktioniert.
- Ein gelbes Ausrufezeichen weist darauf hin, dass sich eine Komponente in einem Warnzustand befindet.
- Ein Fragezeichen weist darauf hin, dass der Status einer Komponente unbekannt ist.

3 Treffen Sie eine Auswahl, um weitere Informationen zu einem Problem anzuzeigen.

Option	Bezeichnung
Komponenten	<p>Zeigt Informationen zu DienstkompONENTEN an.</p> <p>Klicken Sie auf die Registerkarten Verbindungsserver, Gateway-Server, Ereignisdatenbank, View Composer Server oder True SSO, um Informationen zu DienstkompONENTEN anzuzeigen und Aufgaben zur Fehlerbehebung durchzuführen.</p> <p>Wählen Sie eine Komponente aus, um die folgenden Aufgaben auszuführen:</p> <ul style="list-style-type: none"> ■ Zeigen Sie den Status, den Namen, die Version und andere Details an. ■ Wenn Sie einen Verbindungsserver auswählen, klicken Sie auf die Registerkarte Dienststatus anzeigen, um Informationen zu Gateway-Diensten anzuzeigen. ■ Wenn Sie einen Verbindungsserver auswählen, klicken Sie auf die Registerkarte Sitzungsdetails anzeigen, um Informationen zu Verbindungsserver-Sitzungen anzuzeigen.
RDS-Farmen	<p>Zeigt Informationen zu Farmen an. Klicken Sie auf eine Farm-ID, um weitere Informationen zur Farm anzuzeigen, einschließlich der RDS-Hosts, die zur Farm gehören.</p>
vSphere	<p>Zeigt Informationen zu Komponenten im Zusammenhang mit vSphere an.</p> <p>Klicken Sie auf die Registerkarten Datenspeicher, ESX-Hosts und vCenter Server, um Informationen über die einzelnen Komponenten anzuzeigen.</p>

Option	Bezeichnung
Andere Komponenten	<p>Klicken Sie auf die Registerkarten Domänen, SAML 2.0 und Lizenzdienst, um weitere Informationen zu den einzelnen Komponenten anzuzeigen. Dieser Abschnitt gilt auch für Horizon Composer.</p> <p>Hinweis Wenn ein SAML 2.0-Authentifikator eine Warnung aufgrund eines nicht vertrauenswürdigen Zertifikats zeigt, können Sie auf den Zertifikatlink klicken, um das Zertifikat zu akzeptieren und zu validieren.</p>
Remote-Pods	<p>Zeigt Informationen zu Horizon 7-Remote-Pods an.</p> <p>Hinweis Dieser Abschnitt wird nur angezeigt, wenn die Cloud-Pod-Architektur-Funktion aktiviert ist.</p>

- Im Bereich **Sitzungen** können Sie Balkendiagramme anzeigen, die die Anzahl der aktiven, getrennten oder im Leerlauf befindlichen Sitzungen von virtuellen Desktops, veröffentlichten Desktops und veröffentlichten Anwendungen anzeigen.
- Klicken Sie im Bereich **Sitzungen** auf **Ansicht**, um Sitzungen anzuzeigen.
Auf der Seite „Sitzungen“ werden Informationen zu den Sitzungen angezeigt.
- Klicken Sie im Bereich **Arbeitslast** auf **Ansicht**, um Datenspeicher anzuzeigen.
Sie können einen Datenspeicher auswählen, um zusätzliche Informationen wie die aktuelle Nutzung des Datenspeichers anzuzeigen. Horizon Console zeigt eine Warnung an, wenn der freie Speicherplatz für einen Datenspeicher unter einen Schwellenwert rutscht. Wenn Desktop-Pools mit einem ausgewählten Datenspeicher verknüpft sind, können Sie die Informationen für die Desktop-Pools anzeigen, wenn Sie den Datenspeicher auswählen. In der Spalte **Andere Datenspeicher** werden Informationen zu Desktop-Pools oder Farmen angezeigt, die sich über mehrere Datenspeicher erstrecken.

Überwachen des Auslastungsstatus des Horizon-Verbindungsservers

Sie können die Auslastung eines Verbindungsservers im Horizon Console-Dashboard überwachen. Für jeden Verbindungsserver können Sie den Prozentsatz der CPU-Nutzung und der Arbeitsspeichernutzung, die Anzahl der Anzeigeprotokollsitzungen, Verbindungsserver-Verbindungssitzungen oder den Schwellenwert für die maximale Anzahl der Sitzungen, die mit einem Verbindungsserver verbunden werden können, anzeigen. Sie können auch die Anzahl der verbundenen Sitzungen für einen RDS-Host anzeigen.

Verfahren

- Navigieren Sie in Horizon Console zu **Monitor > Dashboard**.

2 Klicken Sie im Bereich **Systemzustand** auf **Anzeigen**.

Im Bereich **Komponenten** wird auf der Registerkarte **Verbindungsserver** in der Spalte **Sitzungen** der Prozentsatz der Verbindungsserver-Sitzungen für die einzelnen Verbindungsserver angezeigt. In der Spalte **CPU-Nutzung** wird angezeigt, wie viel Prozent der CPU jeder Verbindungsserver verbraucht. In der Spalte **Arbeitsspeichernutzung** wird der Prozentsatz des benötigten Arbeitsspeichers für jeden Verbindungsserver angezeigt.

Hinweis Wenn der Verbindungsserver nicht mit einer sicheren Gateway-Verbindung mit sicherem Tunnel über HTTP(s), PCoIP Secure Gateway-Verbindung und Blast Secure Gateway-Verbindung konfiguriert ist, zeigt Horizon Console keinen Prozentsatz der Verbindungsserver-Sitzungen an und zeigt die Anzahl der Verbindungsserver-Sitzungen stattdessen als Liste an.

3 Wählen Sie einen Verbindungsserver aus und klicken Sie auf **Sitzungsdetails anzeigen**, um die Verbindungsserver-Sitzungen, die maximale Anzahl der Verbindungsserver-Sitzungen und die Anzeigeprotokoll-Sitzungen anzuzeigen.

Hinweis Wenn der Verbindungsserver nicht mit einer sicheren Gateway-Verbindung mit sicherem Tunnel über HTTP(s), PCoIP Secure Gateway-Verbindung und Blast Secure Gateway-Verbindung konfiguriert ist, zeigt Horizon Console nicht den maximalen Schwellenwert für Sitzungen an, da kein Schwellenwert für die Anzahl an Sitzungen existiert, die eine Verbindung zum Verbindungsserver herstellen können.

4 Um die Anzahl der Sitzungen auf einem RDS-Host anzuzeigen, klicken Sie im Bereich **Komponenten** auf **RDS-Farmen** und klicken Sie auf eine Farm-ID.

In der Spalte „Sitzungen“ wird die Anzahl der Sitzungen auf einem RDS-Host angezeigt.

Überwachen von Diensten auf dem Horizon-Verbindungsserver

Sie können die auf einem Verbindungsserver ausgeführten Gateway-Dienstkomponenten im Horizon Console-Dashboard überwachen. Gateway-Dienstkomponenten umfassen eine sichere Gateway-Verbindung, die mit sicherer Tunnelverbindung über HTTP(s), PCoIP Gateway- und Blast Secure Gateway-Verbindungen konfiguriert ist.

Verfahren

1 Navigieren Sie in Horizon Console zu **Monitor > Dashboard**.

2 Klicken Sie im Bereich **Systemzustand** auf **Anzeigen**.

3 Wählen Sie einen Verbindungsserver und anschließend die Option **Dienststatus anzeigen** aus.

Im Dialogfeld **Gateway-Dienststatus** werden der Status der Gateway-Dienstkomponenten sowie die verwendeten Gateway-Dienstkomponenten angezeigt.

Hinweis Die nicht aktivierten Dienstkomponenten werden abgeblendet dargestellt.

Grundlegendes zu Horizon 7-Diensten

Der Betrieb von Verbindungsserver-Instanzen und Sicherheitsservern hängt von verschiedenen Diensten ab, die auf dem System ausgeführt werden. Diese Systeme werden automatisch gestartet und beendet, aber gelegentlich kann es erforderlich sein, den Betrieb dieser Dienste manuell anzupassen.

Sie verwenden das Microsoft Windows-Tool „Dienste“ zum Beenden oder Starten von Horizon 7-Diensten. Wenn Sie die Horizon 7-Dienste auf einem Verbindungsserver-Host oder einem Sicherheitsserver beenden, können die Endbenutzer erst wieder eine Verbindung zu ihren Remote-Desktops bzw. Anwendungen herstellen, wenn Sie die Dienste neu starten. Ein Neustart eines Dienstes kann erforderlich sein, wenn der Dienst nicht mehr ausgeführt wird oder die Horizon 7-Funktionalität eingeschränkt ist.

Beenden und Starten der Horizon 7-Dienste

Der Betrieb von Verbindungsserver-Instanzen und Sicherheitsservern hängt von verschiedenen Diensten ab, die auf dem System ausgeführt werden. Sie werden möglicherweise manchmal diese Dienste bei der Fehlerbehebung mit dem Betrieb von Horizon 7 manuell beenden und starten müssen.

Wenn Sie Horizon 7-Dienste beenden, können Endbenutzer keine Verbindung mehr zu ihren Remote-Desktops und Remoteanwendungen herstellen. Sie sollten einen solchen Vorgang daher im Rahmen einer geplanten Systemwartung durchführen oder die Endbenutzer warnen, dass ihre Desktops und Anwendungen temporär nicht zur Verfügung stehen werden.

Hinweis Beenden Sie nur den VMware Horizon View Connection Server-Dienst auf einem Verbindungsserver-Host oder den VMware Horizon View-Sicherheitsserver-Dienst auf einem Sicherheitsserver. Beenden Sie keine anderen Komponentendienste.

Voraussetzungen

Machen Sie sich mit den Diensten vertraut, die auf Verbindungsserver-Hosts und Sicherheitsservern ausgeführt werden, wie unter [Dienste auf einem Verbindungsserver-Host](#) und [Dienste auf einem Sicherheitsserver](#) beschrieben.

Verfahren

- 1 Starten Sie das Windows-Tool Services (Dienste), indem Sie an der Eingabeaufforderung **services.msc** eingeben.
- 2 Wählen Sie den VMware Horizon View Connection Server-Dienst auf einem Verbindungsserver-Host oder den VMware Horizon View-Sicherheitsserver-Dienst auf einem Sicherheitsserver aus und klicken Sie je nach gewünschtem Vorgang auf **Beenden**, **Neustarten** oder **Starten**.
- 3 Stellen Sie sicher, dass sich der Status des aufgeführten Dienstes wie erwartet ändert.

Dienste auf einem Verbindungsserver-Host

Der Betrieb von Horizon 7 hängt von verschiedenen Diensten ab, die auf einem Verbindungsserver-Host ausgeführt werden.

Tabelle 9-4. Horizon Verbindungsserver-Hostdienste

Dienstname	Starttyp	Beschreibung
VMware Horizon View Blast Secure Gateway	Automatisch	Stellt sichere HTML Access- und Blast Extreme-Dienste bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zum Verbindungsserver über ein Blast Secure Gateway herstellen.
VMware Horizon View-Verbindungsserver	Automatisch	Stellt Verbindungs-Broker-Dienste bereit. Dieser Dienst muss immer ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework-, Nachrichtenbus-, Sicherheits-Gateway- und Webdienste gestartet oder beendet. Dieser Dienst führt keinen Start des VMware VDMDS-Dienstes oder des VMware Horizon View-Skripthostdienstes durch bzw. beendet diese Dienste nicht.
VMware Horizon View Framework-Komponente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View Message Bus-Komponente	Manuell	Stellt Dienste für die Nachrichtenübermittlung zwischen den Horizon 7-Komponenten bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View PCoIP Secure Gateway	Manuell	Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zum Verbindungsserver über ein PCoIP Secure Gateway herstellen.
VMware Horizon View-Skripthost	Deaktiviert	Bietet Unterstützung für Drittanbieterskripts, die beim Löschen von virtuellen Maschinen ausgeführt werden. Dieser Dienst ist standardmäßig deaktiviert. Sie sollten diesen Dienst aktivieren, wenn Sie Skripts ausführen möchten.
VMware Horizon View Sicherheits-Gateway-Komponente	Manuell	Stellt gängige Gateway-Dienste bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View Web-Komponente	Manuell	Stellt Webdienste bereit. Dieser Dienst muss immer ausgeführt werden.
VMwareVDMDS	Automatisch	Stellt LDAP-Verzeichnisdienste bereit. Dieser Dienst muss immer ausgeführt werden. Während Upgrade-Vorgängen von Horizon 7 stellt dieser Dienst sicher, dass vorhandene Daten korrekt migriert werden.

Dienste auf einem Sicherheitsserver

Der Betrieb von Horizon 7 hängt von verschiedenen Diensten ab, die auf einem Sicherheitsserver ausgeführt werden.

Tabelle 9-5. Dienste auf einem Sicherheitsserver

Dienstname	Starttyp	Beschreibung
VMware Horizon View Blast Secure Gateway	Automatisch	Stellt sichere HTML Access- und Blast Extreme-Dienste bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu diesem Sicherheitsserver über ein Blast Secure Gateway herstellen.
VMware Horizon View-Sicherheitsserver	Automatisch	Stellt Sicherheitsserverdienste bereit. Dieser Dienst muss immer ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework- und Sicherheits-Gateway-Dienste gestartet oder beendet.

Tabelle 9-5. Dienste auf einem Sicherheitsserver (Fortsetzung)

Dienstname	Starttyp	Beschreibung
VMware Horizon View Framework-Komponente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View PCoIP Secure Gateway	Manuell	Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu diesem Sicherheitsserver über ein PCoIP Secure Gateway herstellen.
VMware Horizon View Security Gateway-Komponente	Manuell	Stellt gängige Gateway-Dienste bereit. Dieser Dienst muss immer ausgeführt werden.

Ändern des Produktlizenzschlüssels oder der Lizenzmodi in Horizon Console

Wenn die aktuelle Lizenz auf einem System abläuft oder Sie auf Horizon 7-Funktionen zugreifen möchten, die derzeit nicht lizenziert sind, können Sie mithilfe von Horizon Console den Produktlizenzschlüssel ändern. Basierend auf Ihrer Horizon 7-Bereitstellung auf VMware Horizon Cloud Service können Sie entweder eine unbefristete Lizenz oder eine Abonnementlizenz für Horizon 7 erhalten. Sie können Horizon Console verwenden, um den Lizenzmodus für einen Pod von einer Abonnementlizenz zu einer unbefristeten Lizenz zu ändern und umgekehrt.

Sie können eine Lizenz zu Horizon 7 hinzufügen, während Horizon 7 ausgeführt wird. Ein Neustart des Systems ist nicht erforderlich und der Zugriff auf Desktops und Anwendungen wird nicht unterbrochen.

Voraussetzungen

- Für den erfolgreichen Einsatz von Horizon 7 und Add-On-Funktionen, wie beispielsweise Horizon Composer und veröffentlichte Anwendungen, müssen Sie einen gültigen Produktlizenzschlüssel erwerben.
- Um eine Abonnementlizenz zu verwenden, stellen Sie sicher, dass Sie Horizon 7 für eine Abonnementlizenz aktiviert haben. Weitere Informationen finden Sie im Dokument *Horizon 7-Installation*. Im Bereich **Lizenzierung** werden Informationen über die Abonnementlizenz für den Horizon 7-Pod angezeigt.

Verfahren

- 1 Wählen Sie in Horizon Console die Optionen **Einstellungen > Produktlizenzierung und -verwendung** aus.

Im Bereich **Lizenzierung** werden die ersten und die letzten fünf Zeichen des aktuellen Lizenzschlüssels dargestellt.

- 2 Um den Lizenzschlüssel zu bearbeiten, klicken Sie auf **Lizenz bearbeiten**, geben Sie die Seriennummer der Lizenz ein und klicken Sie auf **OK**.

Im Bereich **Lizenzierungseinstellungen** werden die aktualisierten Lizenzinformationen angezeigt.

- 3 (Optional) Um von einer Abonnementlizenz zu einer unbefristeten Lizenz für einen Horizon 7-Pod zu wechseln, klicken Sie auf **Unbefristete Lizenz verwenden** und dann auf **OK**.

Im Bereich **Lizenzierungseinstellungen** werden die aktualisierten Lizenzinformationen angezeigt.

- 4 (Optional) Um von einer unbefristeten Lizenz zu einer Abonnementlizenz für einen Horizon 7-Pod zu wechseln, klicken Sie auf **Abonnementlizenz verwenden** und dann auf **OK**. Der VMware Horizon Cloud Service-Administrator kann dann den Horizon 7-Pod für eine Abonnementlizenz aktivieren.

Im Bereich **Lizenzierungseinstellungen** werden die aktualisierten Lizenzinformationen angezeigt.

- 5 Überprüfen Sie das Ablaufdatum der Lizenz.

- 6 Überprüfen Sie, ob die Lizenzen für Desktops, die Remote-Ausführung von Anwendungen sowie Horizon Composer aktiviert oder deaktiviert sind, je nach der VMware Horizon 7-Edition, zu deren Verwendung Ihre Produktlizenz Sie berechtigt.

Nicht alle Funktionen von VMware Horizon 7 sind in allen Editionen verfügbar. Einen Funktionsvergleich der einzelnen Editionen finden Sie unter <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

- 7 Stellen Sie sicher, dass das Lizenznutzungsmodell dem für Ihre Produktlizenz verwendeten Modell entspricht.

Die Nutzung wird anhand der Anzahl benannter oder gleichzeitiger Benutzer ermittelt, abhängig von der Edition und der Nutzungsvereinbarung für Ihre Produktlizenz.

Überwachen der Lizenznutzung

In Horizon Console können Sie die aktiven Benutzer überwachen, die gleichzeitig mit Horizon 7 verbunden sind. Im Bereich **Nutzungseinstellungen** werden die aktuellen und höchsten historischen Nutzungszahlen angezeigt. Mithilfe dieser Anzeige können Sie die Verwendung Ihrer Produktlizenzierungen überblicken. Sie können auch die historischen Nutzungsdaten zurücksetzen und mit den aktuellen Daten erneut beginnen.

Horizon 7 bietet zwei Modelle für Nutzungslizenzen, eines für benannte und eines für gleichzeitige Benutzer. Horizon 7 ermittelt die benannten und gleichzeitigen Benutzer in Ihrer Umgebung, unabhängig von Ihrer Produktlizenzedition oder Ihrer Nutzungsvereinbarung.

Für benannte Benutzer ermittelt Horizon 7 die Anzahl eindeutiger Benutzer, die auf die Horizon 7-Umgebung zugegriffen haben. Wenn ein benannter Benutzer mehrere Einzelbenutzer-Desktops, veröffentlichte Desktops und veröffentlichte Anwendungen ausführt, wird er nur einmal gezählt.

Für benannte Benutzer wird in der Spalte **Aktuell** im Bereich **Nutzungseinstellungen** die Anzahl der Benutzer seit der ersten Konfiguration Ihrer Horizon 7-Bereitstellung oder seit dem letzten Zurücksetzen der Anzahl benannter Benutzer angezeigt. Die Spalte **Höchste** gilt nicht für benannte Benutzer.

Für gleichzeitige Benutzer ermittelt Horizon 7 Verbindungen von Einzelbenutzer-Desktops pro Sitzung. Wenn ein gleichzeitiger Benutzer mehrere Einzelbenutzer-Desktops ausführt, wird jede verbundene Desktop-Sitzung separat gezählt.

Für gleichzeitige Benutzer werden die Verbindungen von veröffentlichten Desktops und veröffentlichten Anwendungen pro Benutzer ermittelt. Wenn ein gleichzeitiger Benutzer mehrere Sitzungen veröffentlichter Desktops und veröffentlichter Anwendungen ausführt, wird dieser nur einmal gezählt, auch wenn unterschiedliche veröffentlichte Desktops oder veröffentlichte Anwendungen auf unterschiedlichen RDS-Hosts gehostet werden. Führt ein gleichzeitiger Benutzer einen Einzelbenutzer-Desktop und zusätzliche veröffentlichte Desktops und veröffentlichte Anwendungen aus, wird auch dieser Benutzer nur einmal gezählt.

Für gleichzeitige Benutzer wird in der Spalte **Höchste** im Bereich **Nutzungseinstellungen** die höchste Anzahl gleichzeitiger Benutzer von Desktop-Sitzungen sowie von veröffentlichten Desktops und veröffentlichten Anwendungen seit der ersten Konfiguration Ihrer Horizon 7-Bereitstellung oder seit dem letzten Zurücksetzen des höchsten Werts angezeigt.

Sie können die Anzahl der gemeinsamen Sitzungen (Zusammenarbeitssitzungen) und der mit einer Sitzung verbundenen Sitzungsteilnehmer überwachen.

- **Active – Zusammenarbeitssitzungen:** die Anzahl der Sitzungen, für die ein Sitzungsbesitzer einen oder mehrere Benutzer zur Teilnahme eingeladen hat. Beispiel: John hat zwei Personen eingeladen, an seiner Sitzung teilzunehmen, Mary hat eine Person zur Teilnahme an ihrer Sitzung eingeladen. Der Wert dieser Zeile beträgt 2, unabhängig davon, ob eine eingeladene Person an der Sitzung teilnimmt.
- **Active – Teilnehmer insgesamt:** die Gesamtzahl der Benutzer, die mit einer gemeinsamen Sitzung verbunden sind, einschließlich Sitzungsbesitzer und aller Sitzungsteilnehmer. Beispiel: John hat zwei Personen eingeladen, und nur eine Person nimmt an der Sitzung teil. Mary hat eine Person eingeladen, die nicht an der Sitzung teilnimmt. Der Wert dieser Zeile beträgt 3: Die gemeinsame Sitzung von John verfügt über einen primären und einen sekundären Teilnehmer, während die gemeinsame Sitzung von Mary einen primären und keinen sekundären Teilnehmer aufweist. Da der Sitzungsbesitzer mitgezählt wird, ist sichergestellt, dass die Gesamtzahl der Teilnehmer immer größer oder gleich der Gesamtzahl der gemeinsamen Sitzungen ist.

Zurücksetzen der Daten zur Lizenznutzung

Sie können in Horizon Console die historischen Daten zur Produktnutzung zurücksetzen und mit den aktuellen Daten erneut beginnen.

Ein Administrator mit dem Recht **Globale Konfiguration und Richtlinien verwalten** kann die Einstellungen **Höchsten Wert zurücksetzen** und **Wert benannter Benutzer zurücksetzen** auswählen. Um den Zugriff auf diese Einstellungen einzuschränken, sollte dieses Recht nur Administratoren gewährt werden.

Voraussetzungen

Machen Sie sich mit der Nutzung der Produktlizenz vertraut. Siehe [Überwachen der Lizenznutzung](#).

Verfahren

- 1 Wählen Sie in Horizon Console die Optionen **Einstellungen > Produktlizenzierung und -verwendung** aus.

- 2 (Optional) Wählen Sie im Fensterbereich **Nutzung** die Option **Höchsten Wert zurücksetzen**.
Die höchste historische Anzahl gleichzeitiger Verbindungen wird auf die aktuelle Anzahl zurückgesetzt.
- 3 (Optional) Wählen Sie im Fensterbereich **Nutzung** die Option **Wert benannter Benutzer zurücksetzen**.

Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit

Sie können Horizon 7 konfigurieren, um beim Programm von VMware zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) mitzumachen.

Informationen über die Art der Daten, die VMware über das CEIP erfasst, und darüber, wie VMware diese Daten verwendet, finden Sie im „Trust & Assurance Center“ unter <http://www.vmware.com/trustvmware/ceip.html>.

Informationen zum Konfigurieren der Datenfreigabe in Horizon Client finden Sie im entsprechenden Installations- und Einrichtungshandbuch für Horizon Client. Für Windows-Clients finden Sie weitere Informationen beispielsweise im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*. Informationen zum Konfigurieren der Datenfreigabe in HTML Access finden Sie im Dokument *VMware Horizon HTML Access Installations- und Einrichtungshandbuch*.

Verfahren

- 1 Wählen Sie in Horizon Console die Optionen **Einstellungen > Produktlizenzierung und -verwendung**.
- 2 Wählen Sie die Registerkarte **Programm zur Gewährleistung der Benutzerfreundlichkeit** und klicken Sie auf **Einstellungen bearbeiten** aus.
- 3 Um am CEIP teilzunehmen, wählen Sie **Machen Sie mit beim Programm von VMware zur Verbesserung der Benutzerfreundlichkeit** aus.
Wenn Sie diese Option nicht auswählen, können Sie nicht am CEIP teilnehmen.
- 4 (Optional) Wählen Sie Ihren geographischen Standort, Ihre Branche oder die Anzahl der Mitarbeiter in Ihrer Organisation aus.
- 5 Klicken Sie auf **OK**.

Integration des Horizon-Verbindungsservers mit Skyline Collector-Appliance

Sie können den Horizon-Verbindungsserver für die Integration mit der Skyline Collector-Appliance konfigurieren, die der technische Support von VMware zur Diagnose und Behebung von Problemen mit Horizon 7 verwendet. Die Skyline Collector-Appliance ruft Verbindungsserver-Protokolle für den zur Protokollerfassung konfigurierten Benutzer mit Horizon 7-Administratorberechtigungen ab.

Verfahren

- 1 Erstellen Sie in Horizon Console eine benutzerdefinierte Rolle mit dem Namen „Protokollerfassende Administratoren“ mit der Berechtigung zum Erfassen von Betriebsprotokollen. Weitere Informationen finden Sie unter [Hinzufügen einer benutzerdefinierten Rolle in Horizon Console](#).
- 2 Fügen Sie eine Beschreibung für die benutzerdefinierte Rolle hinzu.
- 3 Fügen Sie einen neuen Benutzer mit Administratorberechtigungen hinzu und wählen Sie die Rolle „Bestandslistenadministrator (schreibgeschützt)“ und die benutzerdefinierte Rolle „Protokollerfassender Administrator“ für den Benutzer.

Die Skyline Collector-Appliance kann die Verbindungsserver-Protokolle für diesen Benutzer mit Administratorrechten abrufen, um Horizon 7-Probleme zu diagnostizieren und zu beheben.

Erste Schritte mit JMP Integrated Workflow

10

Machen Sie sich mit den allgemeinen JMP Integrated Workflow-Konzepten vertraut und führen Sie die Aufgaben für die ersten Schritte mit den JMP Integrated Workflow-Funktionen aus.

Dieses Kapitel enthält die folgenden Themen:

- [Informationen zu JMP Integrated Workflow](#)
- [Erste Schritte mit dem integrierten JMP-Arbeitsablauf](#)

Informationen zu JMP Integrated Workflow

Mit den Funktionen des integrierten Arbeitsablaufs von VMware HorizonJMP (Just-in-Time Management Platform) können Sie über eine einzelne Konsole die Desktop-Arbeitsumgebungen für Benutzer oder Benutzergruppen definieren und verwalten.

Eine Desktop-Arbeitsumgebung wird durch Definieren einer JMP-Zuweisung erstellt, die Informationen zu den VMware Horizon-Desktop-Pools, VMware App Volumes-AppStacks und VMware Dynamic Environment Manager-Einstellungen enthält. Nach dem Absenden einer JMP-Zuweisung kommuniziert die JMP-Automatisierungs-Engine mit dem Horizon 7-, App Volumes- und Dynamic Environment Manager-System, um den Benutzer für einen Desktop zu berechtigen.

Sie können bestehende JMP-Zuweisungen auf der Registerkarte **Zuweisungen (JMP)** in Horizon Console verwalten. Sie können die jeweiligen Komponentenzuweisungen auch an der entsprechenden JMP-Komponentenkonsole ändern. Beispielsweise können Änderungen an den Desktop-Pools, die in einer JMP-Zuweisung definiert wurden, auch durch Auswählen von **Bestands- > Desktops** von Horizon Console geändert werden.

Wenn eine JMP-Zuweisung in Horizon Console geöffnet wird, wird der aktuelle Status der einzelnen Komponenten in der JMP-Zuweisung validiert, um sicherzustellen, dass die Komponenten den erwarteten Status aufweisen. Bei Unterschieden werden die betroffenen Bereiche an der Konsole hervorgehoben und Sie können entweder den aktuellen Status akzeptieren oder die Zuweisung ändern, um den gewünschten Status zu erreichen und den Benutzer neu zu berechtigen.

Die JMP Integrated Workflow-Funktionen stehen in Horizon Console nach Installation und Konfiguration von VMware HorizonJMP Server zur Verfügung. Weitere Informationen finden Sie unter [Erste Schritte mit dem integrierten JMP-Arbeitsablauf](#) und *VMware Horizon JMP Server Installations- und Einrichtungshandbuch*.

Hinweis Die JMP Integrated Workflow-Funktionen unterstützen VMware Cloud[®] auf AWS nicht, da App Volumes VMware Cloud nicht unterstützt.

Erste Schritte mit dem integrierten JMP-Arbeitsablauf

Bevor Sie die JMP Integrated Workflow-Funktionen verwenden können, müssen Sie JMP Server installieren und einrichten und die JMP-Einstellungen konfigurieren.

Voraussetzungen

Sehen Sie sich die Voraussetzungen und die Systemanforderungen für alle Technologiekomponenten an, die Sie installieren möchten.

Verfahren

- 1 Richten Sie gegebenenfalls die benötigten Administratorbenutzer und -gruppen in Active Directory ein.

Weitere Informationen finden Sie unter „Vorbereiten von Active Directory“ im Dokument *Horizon 7-Installation*. Die Active Directory-Informationen werden für die Konfiguration der JMP-Einstellungen benötigt.

- 2 Richten Sie den Microsoft SQL Server ein und vergewissern Sie sich, dass die Anmeldedaten, die Sie während der Installation von JMP Server verwenden möchten, erstellt wurden. Weitere Informationen finden Sie unter „Datenbankanforderungen für JMP Server“ im Dokument *VMware Horizon JMP Server Installations- und Einrichtungshandbuch*.

- 3 Installieren und Einrichten von VMware Horizon 7 Version 7.5 oder höher.

Siehe das Dokument *Horizon 7-Installation*.

- 4 (Optional) Installieren Sie VMware App Volumes 2.14, und richten Sie es ein. Es bietet Funktionen für die Anwendungsbereitstellung in Echtzeit.

Weitere Details finden Sie im Dokument *Installationshandbuch zu VMware App Volumes*.

- 5 (Optional) Installieren Sie VMware Dynamic Environment Manager 9.2.1 für die kontextuelle Richtlinienverwaltung, und richten Sie ihn entsprechend ein.

Siehe das Dokument *Installieren und Konfigurieren von VMware Dynamic Environment Manager*.

- 6 Rufen Sie die CA-signierten SSL-Zertifikate ab, die für JMP Server verwendet werden müssen, um die sichere Kommunikation mit anderen Servern im Netzwerk Ihrer Organisation sicherzustellen.

- 7 Installieren Sie JMP Server und konfigurieren Sie die SSL-Zertifikate für den JMP Server für die Kommunikation mit den anderen Servern, die für die Funktionen der JMP Integrated Workflow erforderlich sind.

Weitere Informationen finden Sie unter *VMware Horizon JMP Server Installations- und Einrichtungshandbuch*.

- 8 Konfigurieren Sie die JMP-Einstellungen zum ersten Mal. Ausführliche Informationen dazu finden Sie unter [Erstmaliges Konfigurieren der JMP-Einstellungen](#).

Nächste Schritte

Nach erfolgreichem Abschluss der oben genannten Aufgaben können Sie nun eine JMP-Zuweisung erstellen. Weitere Informationen finden Sie unter [Erstellen einer JMP-Zuweisung](#).

Verwalten von JMP-Einstellungen

11

Nach der Installation von JMP Server müssen Sie die JMP-Einstellungen mit den erforderlichen Anmeldedaten konfigurieren, bevor Sie JMP-Zuweisungen erstellen und die JMP Integrated Workflow-Funktionen verwenden. Sie haben die Möglichkeit, die internen JMP-Einstellungen zu bearbeiten und gegebenenfalls neue Einstellungsinformationen hinzuzufügen.

Dieses Kapitel enthält die folgenden Themen:

- [Erstmaliges Konfigurieren der JMP-Einstellungen](#)
- [Verwalten von JMP-Einstellungen](#)

Erstmaliges Konfigurieren der JMP-Einstellungen

Vor dem Erstellen von JMP-Zuweisungen müssen Sie die JMP-Einstellungen mit Horizon Console konfigurieren. Sie müssen die Anmeldedaten für die Active Directory-Domäne angeben, in der Sie Desktop-Arbeitsumgebungen für Benutzer oder Benutzergruppen zuweisen. Sie können optional die Anmeldedaten für App Volumes-AppStacks und die Dynamic Environment Manager-Konfigurationsdateifreigabe verwenden, wenn Sie JMP-Zuweisungen erstellen.

Voraussetzungen

- Vergewissern Sie sich, dass der VMware HorizonJMP Server erfolgreich installiert wurde und dass Sie seine URL kennen. Weitere Informationen finden Sie unter *VMware Horizon JMP Server Installations- und Einrichtungshandbuch*.
- Rufen Sie die Anmeldedaten des Administratorkontos für Horizon 7 Version 7.5 oder höher ab, die Sie für JMP Server verwenden möchten.
- Rufen Sie die Active Directory-Anmeldedaten ab, die für den JMP Server verwendet werden müssen.
- Wenn Sie den JMP-Zuweisungen Anwendungen zuweisen, müssen Sie sicherstellen, dass Sie über die URL und die Anmeldedaten des Administratorkontos verfügen, die für die VMware App Volumes-Manager-Instanz verwendet werden müssen. Wenn die App Volumes-Manager-Instanzen, die Sie verwenden möchten, von einem Lastausgleichsdienst verwaltet werden, rufen Sie die URL für den Lastausgleichsdienst ab und verwenden Sie sie beim Konfigurieren der App Volumes-Manager-Informationen.

- Wenn Sie eine VMware Dynamic Environment Manager-Konfigurationsdateifreigabe verwenden möchten, rufen Sie deren UNC-Pfad und die erforderlichen Anmeldedaten des Administratorkontos ab, um darauf zuzugreifen.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.

- 2 Geben Sie die JMP Server-Informationen ein.

- a Klicken Sie auf der Registerkarte **JMP-Server** auf **JMP-Server hinzufügen**.
- b Geben Sie die JMP Server-URL im Format `https://jmp.yourcompany.com` ein.
- c Klicken Sie auf **Speichern**.

Die JMP Server-URL wird validiert. Wenn Sie die Meldung **JMP-Server nicht erreichbar** erhalten, überprüfen Sie, ob JMP Server korrekt konfiguriert ist und ob der JMP Server erreichbar ist.

- 3 Geben Sie die Kontoinformationen für den Horizon 7-Verbindungsserver Version 7.5 oder höher ein, den Sie für JMP Server verwenden möchten.

- a Klicken Sie auf die Registerkarte **Horizon 7**.
- b Geben Sie den Wert für die **Verbindungsserver-URL** ein, falls er nicht automatisch eingetragen wird. Diese URL ist mit der URL des Horizon 7-Verbindungservers identisch, mit dem Horizon Console verbunden ist.
- c Geben Sie den Benutzernamen und das Kennwort für Ihr Horizon 7-Dienst-Konto ein.
- d Geben Sie im Textfeld **Domäne des Dienstkontos** einen gültigen Namen ein, der für die JMP-Zuweisungen verwendet werden soll, die Sie erstellen. Drücken Sie anschließend die **Eingabetaste**.
- e Klicken Sie auf **Speichern**.

- 4 Geben Sie die Informationen für das Active Directory ein, das Sie für die JMP-Zuweisungen verwenden möchten.

- a Klicken Sie auf die Registerkarte **Active Directory**.
- b Klicken Sie auf **Neu**.
- c Wählen Sie im Textfeld **NETBIOS-Name** in der Liste der verfügbaren NetBIOS-Domännennamen einen Namen aus.

Die Textfelder „DNS-Domänenname“ und „Kontext“ werden mit Standardwerten aktualisiert.

- d Vergewissern Sie sich, dass der Standardwert, der im Textfeld **DNS-Domänenname** hinzugefügt wurde, der korrekte Wert ist. Geben Sie optional einen anderen vollqualifizierten Active Directory-Domännennamen ein. Beispiel: `mycompany.com`.
- e Wählen Sie im Abschnitt **Protokoll** das von Active Directory verwendete Protokoll aus.
- f Geben Sie in den Textfeldern **Bind-Benutzername** und **Bind-Kennwort** die Anmeldedaten für das Konto des Benutzers mit Bind Distinguished Name (DN) ein. Beispiel: **Administrator**.

- g Ändern Sie den Wert im Textfeld **Kontext**, wenn Sie einen anderen Wert als den Standardwert verwenden möchten.

Dieser Wert wird als Stamm für die Active Directory-Datensuche verwendet.

- h (Optional) Klicken Sie auf **Erweiterte Eigenschaften** und ändern Sie den Standardwert für die Portnummer.

Der Standardwert für den Port basiert auf dem Protokoll, das Sie vorher ausgewählt haben. Sie können den Portwert ändern oder das Textfeld leer lassen.

- i Geben Sie optional im Textfeld **Domänencontroller** mindestens einen Hostnamen oder eine IP-Adresse für die Verarbeitung des Active Directory-Datenverkehrs ein.

Beispiel: `adserver.mycompany.com`, `10.111.XXX.XXX`. Wenn das Textfeld leer bleibt, wird der Wert im Textfeld **DNS-Domänenname** verwendet.

- j Klicken Sie auf **Speichern**.

- 5 Wenn Sie App Volumes-AppStacks beim Erstellen von JMP-Zuweisungen verwenden möchten, konfigurieren Sie den App Volumes-Manager, den Sie verwenden möchten.

- a Klicken Sie auf die Registerkarte **App Volumes**.

- b Klicken Sie auf **Neu**.

- c Geben Sie im Textfeld **Name** einen Namen ein, der der App Volumes-Instanz zugewiesen werden soll. Wenn Sie das Textfeld leer lassen, wird der Wert verwendet, den Sie im Textfeld **App Volumes Server-URL** eingegeben haben.

- d Geben Sie eine gültige URL für den App Volumes-Manager ein, mit der der JMP Server-Pod verknüpft werden soll.

Wichtig Wenn der App Volumes-Manager, den Sie verwenden möchten, über einen Lastausgleichsdienst verwaltet wird, geben Sie die URL für diesen Lastausgleichsdienst ein.

- e Geben Sie die Anmeldedaten für das Administratorkonto des App Volumes-Managers oder Lastausgleichsdiensts ein, mit denen Ihr JMP Server auf Ihren App Volumes-Manager zugreifen kann.

- f Geben Sie den Domännennamen für das Konto des App Volumes-Manager-Diensts an, der für die JMP-Zuweisungen verwendet werden soll.

- g (Optional) Wenn Sie mehr als einen App Volumes-Manager registrieren, geben Sie anhand der Umschaltfläche an, ob der App Volumes-Manager, den Sie hinzufügen, der Standardserver zum Erstellen von JMP-Zuweisungen ist. Sie können die gewünschte Instanz beim Erstellen einer JMP-Zuweisung ändern.

- h Klicken Sie auf **Speichern**.

- 6 Wenn Sie eine Dynamic Environment Manager-Konfigurationsdateifreigabe beim Erstellen von JMP-Zuweisungen verwenden möchten, fügen Sie die entsprechenden Informationen den JMP-Einstellungen hinzu.

- a Klicken Sie auf die Registerkarte **UEM**.
- b Klicken Sie auf **Neu**.
- c Geben Sie im Textfeld **UNC-Pfad für Dateifreigabe** einen Wert im Format `\\Dateiservername\Pfadname-der-UEM-Konfigurationsdateifreigabe` ein. Beispiel: `\\DateiServer\UEMConfig`.

Wichtig Schließen Sie Allgemein nicht in den UNC-Pfad der Dateifreigabe ein, den Sie eingeben.

- d Geben Sie die Anmeldedaten für das Dynamic Environment Manager-Administratorkonto ein, die zum Herstellen einer Verbindung zur Dynamic Environment Manager-Konfigurationsdateifreigabe verwendet werden sollen.
- e Wählen Sie in der **Active Directory**-Liste den Domänennamen aus, der für die Dynamic Environment Manager-Konfigurationsdateifreigabe verwendet werden soll.

Hinweis Ein Active Directory kann jeweils nur mit einer Dynamic Environment Manager-Konfigurationsdateifreigabe verknüpft werden.

- f Klicken Sie auf **Speichern**.

Nächste Schritte

Nach der erfolgreichen Konfiguration der ersten JMP-Einstellungen können Sie nun die JMP-Zuweisungen erstellen. Weitere Informationen finden Sie unter [Erstellen einer JMP-Zuweisung](#).

Verwalten von JMP-Einstellungen

Mit Horizon Console können Sie die Informationen für eine JMP-Einstellung ändern, hinzufügen oder löschen.

- Verschaffen Sie sich die erforderlichen Informationen zum Ändern der spezifischen JMP-Einstellung.
- Zum Ändern der JMP-Einstellungen müssen Sie über die erforderlichen Verwaltungsrechte verfügen.

Bearbeiten der JMP Server-Einstellungen

Mit Horizon Console können Sie die bestehenden JMP Server-Einstellungen ändern.

Voraussetzungen

- Verschaffen Sie sich die erforderlichen Informationen zum Ändern der spezifischen JMP Server-Einstellungen.
- Vergewissern Sie sich, dass Sie über die entsprechenden Verwaltungsrechte zum Anmelden bei Horizon Console und zum Ändern der JMP Server-Einstellungen verfügen.

Verfahren

- 1 Wählen Sie in Horizon Console die Option **JMP-Konfiguration** aus.
- 2 Klicken Sie im Bereich „JMP-Einstellungen“ auf die Registerkarte **JMP Server**.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Geben Sie eine neue **JMP Server-URL** ein.
- 5 Klicken Sie auf **Speichern**.

Die neue JMP Server-URL wird validiert. Falls sie ungültig ist, wird eine Fehlermeldung angezeigt.

Bearbeiten der Anmeldedaten für Horizon 7

Ändern Sie mit Horizon Console die bestehenden Anmeldedaten des Horizon 7-Verbindungservers.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.
- 2 Klicken Sie auf die Registerkarte **Horizon 7**.
- 3 Klicken Sie auf **Anmeldedaten bearbeiten**.
- 4 Geben Sie unter **Benutzername für Dienstkonto** einen neuen Benutzernamen ein, falls erforderlich.
- 5 Geben Sie unter **Kennwort für Dienstkonto** ein neues Kennwort ein, falls erforderlich.
- 6 Ändern Sie den Wert für **Domäne des Dienstkontos**, falls erforderlich.
- 7 Klicken Sie auf **Speichern**.

Bearbeiten der Horizon-Verbindungsserver-URL

Wenn Sie die bestehenden JMP-Zuweisungen mit einer anderen Horizon Connection Server verknüpfen möchten, dann müssen Sie die Horizon Connection Server-URL ändern, die mit den JMP Server-Einstellungen registriert ist, die mit diesen JMP-Zuweisungen verknüpft ist.

In Horizon Console ist keine Benutzeroberfläche vorhanden, auf der Sie die Horizon Connection Server-Informationen ändern könnten. Sie müssen stattdessen SQL Server Management Studio verwenden, um die bestehende Horizon Connection Server-Host-URL in den JMP-Einstellungen zu ändern.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die entsprechenden Systemadministratorrechte verfügen, um sich bei einer SQL Server Management Studio-Sitzung anmelden und auf die SQL Server-Datenbank zugreifen zu können, die Sie für JMP Server erstellt haben.
- Sichern Sie Ihre SQL Server-Datenbank, bevor Sie mit den Datenbankänderungen fortfahren.

Verfahren

- 1 Wenn Sie aktuell bei einer Horizon Console-Sitzung angemeldet sind, melden Sie sich ab.

- 2 Melden Sie sich bei einer SQL Server Management Studio-Sitzung als Sysadmin (SA) oder über ein Benutzerkonto mit SA-Rechten an.
- 3 Vergewissern Sie sich, dass die Horizon Connection Server-Host-URL, die Sie als Ersatz verwenden möchten, nicht bereits bei einer anderen JMP Server-Instanz registriert ist.

Wenn beispielsweise die URL für den neuen Horizon Connection Server-Host `new-horizon-host.com` lautet, prüfen Sie mit der folgenden SQL-Anweisung, ob sie bereits registriert ist.

```
SELECT * from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

- 4 Wenn diese SQL-Anweisung keine Ergebnisse zurück gibt, fahren Sie mit dem nächsten Schritt fort. Löschen Sie andernfalls mit der folgenden Anweisung die Informationen für den bestehenden Horizon Connection Server-Host.

```
DELETE from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

- 5 Aktualisieren Sie die bestehenden JMP Server-Einstellungen mit den folgenden Anweisungen. Dabei ist `new-horizon-server-host.com` die URL des neuen Horizon Connection Server-Host und `old-horizon-host.com` die URL des aktuell registrierten Horizon Connection Server-Host.

```
UPDATE xms_service_endpoints
SET host = 'new-horizon-host.com', is_available = 1
WHERE service_id = (SELECT id FROM xms_services WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com')
AND host = 'old-horizon-host.com'

UPDATE xms_services
SET [name] = 'horizon-https://new-horizon-host.com', host = 'new-horizon-host.com'
WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com'
```

- 6 Melden Sie sich bei Horizon Console mit der neuen Horizon Connection Server-URL an und prüfen Sie, ob der neue Horizon Connection Server-Host nun mit den bestehenden JMP-Zuweisungen verknüpft ist, die vorher mit dem alten Horizon Connection Server-Host verknüpft waren.

Hinzufügen von Active Directory-Domänen

Über Horizon Console können Sie nach dem Festlegen der ersten Active Directory-Domäne noch weitere hinzufügen.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.
- 2 Klicken Sie auf die Registerkarte **Active Directory** und anschließend auf **Hinzufügen**.

- 3 Wählen Sie im Textfeld **NETBIOS-Name** in der Liste der verfügbaren NetBIOS-Domännennamen einen Namen aus.

Die Textfelder „DNS-Domänenname“ und „Kontext“ werden mit Standardwerten aktualisiert.

- 4 Überprüfen Sie im Textfeld **DNS-Domänenname** ob nach Aktualisierung des NETBIOS-Namens der Standardwert hinzugefügt wurde. Geben Sie optional einen anderen vollqualifizierten Active Directory-Domännennamen ein. Beispiel: `mycompany.com`.

- 5 Wählen Sie im Abschnitt **Protokoll** das von Active Directory verwendete Protokoll aus.

- 6 Geben Sie in den Textfeldern **Bindungsbenutzername** und **Bindungskennwort** die Anmeldedaten für das Konto des Benutzers mit Bindungs-DN (z. B. Administrator) ein.

- 7 Ändern Sie den Wert im Textfeld **Kontext**, wenn Sie einen anderen Wert als den Standardwert verwenden möchten.

- 8 (Optional) Klicken Sie auf **Erweiterte Eigenschaften** und ändern Sie den Standardwert für die Portnummer.

Der Standardwert für den Port basiert auf dem Protokoll, das Sie vorher ausgewählt haben. Sie können den Portwert ändern oder das Textfeld leer lassen.

- 9 Geben Sie optional im Textfeld **Domänencontroller** mindestens einen Hostnamen oder eine IP-Adresse für die Verarbeitung des Active Directory-Datenverkehrs ein.

- 10 Klicken Sie auf **Speichern**.

Informationen zur neu hinzugefügten Active Directory--Domäne finden Sie in der Active Directory-Tabelle.

Bearbeiten der Informationen zur Active Directory-Domäne

Wenn sich seit der ersten Konfiguration der JMP-Einstellungen bestimmte Informationen geändert haben, können Sie die Informationen zu den Einstellungen der Active Directory-Domäne mit Horizon Console ändern.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.
- 2 Klicken Sie auf die Registerkarte **Active Directory**.
- 3 Wählen Sie eine der Zeilen in der Tabelle der Active Directory-Domänen aus und klicken Sie auf **Bearbeiten**.
- 4 Ändern Sie die Active Directory-Informationen, die aktualisiert werden müssen.
- 5 Klicken Sie auf **Speichern**.

Löschen der Informationen der Active Directory-Domäne

Verwenden Sie Horizon Console, wenn Sie die Einstellungsinformationen einer Active Directory (AD)-Domäne löschen müssen.

Sie können nur Informationen zu einer registrierten Active Directory-Domäne aus einer JMP-Einstellung löschen, wenn diese Domäne nicht bereits von bestehenden JMP-Zuweisungen verwendet wird.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.
- 2 Klicken Sie auf die Registerkarte **Active Directory**.
- 3 Wählen Sie die Tabellenzeile für die Active Directory-Domäne aus, die Sie aus den JMP-Einstellungen löschen möchten.
- 4 Wenn das Dialogfeld zum Bestätigen des Löschvorgangs erscheint, lesen Sie die Meldung und klicken Sie auf **Löschen**, um zu bestätigen, dass Sie die Informationen zu dieser Active Directory-Domäne löschen möchten.

Sie wird entfernt, falls keine JMP-Zuweisungen vorhanden sind, die die Active Directory-Domäne verwenden.

Ein Dialogfeld mit einer Warnung wird angezeigt, wenn die Active Directory-Domäne von einer JMP-Zuweisung verwendet wird. Die Warnmeldung enthält die Liste der JMP-Zuweisungen, die die Active Directory-Domäne verwenden. Sie können die Domäneninformationen erst löschen, nachdem die Domäne aus den JMP-Zuweisungen entfernt wurde oder diese JMP-Zuweisungen, die die Domäne verwenden, gelöscht wurden.

Hinzufügen von Informationen zu App Volumes

Fügen Sie über Horizon Console Informationen für weitere App Volumes-Manager hinzu, die beim Erstellen von JMP-Zuweisungen nützlich sind.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.
- 2 Klicken Sie auf die Registerkarte **App Volumes** und anschließend auf **Hinzufügen**.
Das Dialogfeld **App Volumes-Instanz hinzufügen** wird angezeigt.
- 3 Geben Sie im Textfeld **Name** einen eindeutigen Namen ein, der der App Volumes-Instanz hinzugefügt werden soll. Wenn Sie das Textfeld leer lassen, wird der Wert verwendet, den Sie im Textfeld **App Volumes Server-URL** eingegeben haben.
- 4 Geben Sie im Textfeld **App Volumes Server-URL** eine gültige URL für den App Volumes-Manager ein, den Sie mit Ihrem JMP Server verknüpfen möchten. Wenn der hinzugefügte App Volumes-Manager über einen Lastausgleichsdienst verwaltet wird, geben Sie die URL für diesen Lastausgleichsdienst ein.

Hinweis Wenn die hinzugefügten App Volumes-Manager mit verschiedenen SQL-Datenbanken verbunden sind, dann werden Informationen zum App Volumes-Manager auf der Registerkarte App Volumes angezeigt. Wenn die App Volumes-Manager mit derselben SQL-Datenbank verbunden sind, dann werden nur die Informationen zum vorher registrierten App Volumes-Manager auf der Registerkarte App Volumes angezeigt.

- 5 Geben Sie den Benutzernamen und das Kennwort des App Volumes-Administrators ein, den Ihr JMP Server für den Zugriff zu Ihrem App Volumes-Manager verwenden kann.
- 6 Geben Sie den Domännennamen für das Konto des App Volumes-Diensts an, der für die JMP-Zuweisungen verwendet wird.
- 7 Klicken Sie auf die Umschaltfläche, um den aktuell hinzugefügten App Volumes-Manager zum Standardserver für den App Volumes-Manager zu machen, der beim Erstellen von JMP-Zuweisungen verwendet wird. Sie können den gewünschten Server beim Erstellen einer JMP-Zuweisung ändern.
Die Umschaltfläche wird blau und erhält ein **Ja**-Label.
- 8 Klicken Sie auf **Speichern**.

Bearbeiten der Informationen zur App Volumes-Instanz

Wenn Sie die bestehenden Informationen zur App Volumes-Instanz, die von den JMP-Zuweisungen verwendet wird, ändern müssen, können Sie dies mit Horizon Console erledigen.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.
- 2 Klicken Sie auf die Registerkarte **App Volumes** und wählen Sie die Tabellenzeile für die App Volumes-Instanz aus, die Sie ändern möchten.
- 3 Klicken Sie auf **Bearbeiten**.
Das Dialogfeld **App Volumes-Instanz hinzufügen** wird angezeigt.
- 4 Ändern Sie die Informationen zur App Volumes-Instanz, die aktualisiert werden müssen.
- 5 Klicken Sie auf **Speichern**.

Löschen der Informationen zur App Volumes-Instanz

Verwenden Sie Horizon Console, wenn Sie die Informationen der bestehenden Einstellungen zu einer App Volumes-Instanz löschen müssen.

Sie können nur Informationen zu einer registrierten App Volumes-Instanz aus einer JMP-Einstellung löschen, wenn diese Instanz nicht bereits von JMP-Zuweisungen verwendet wird.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.
- 2 Klicken Sie auf die Registerkarte **App Volumes**.
- 3 Wählen Sie die Tabellenzeile für die App Volumes-Instanz aus, die Sie aus den JMP-Einstellungen löschen möchten.
- 4 Klicken Sie auf **Löschen**, um zu bestätigen, dass Sie die Informationen zu dieser App Volumes-Instanz löschen möchten.

Sie wird entfernt, falls keine JMP-Zuweisungen vorhanden sind, die die App Volumes-Instanz verwenden.

Ein Dialogfeld mit einer Warnung wird angezeigt, wenn die App Volumes-Instanz von einer JMP-Zuweisung verwendet wird. Die Warnmeldung enthält die Liste der JMP-Zuweisungen, von denen die App Volumes-Instanz verwendet wird. Sie können die Informationen zur App Volumes-Instanz erst löschen, nachdem die Instanz aus den JMP-Zuweisungen entfernt wurde oder diese JMP-Zuweisungen, die die Instanz verwenden, gelöscht wurden.

Hinzufügen von Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe

Verwenden Sie Horizon Console, wenn Sie eine weitere Dynamic Environment Manager-Konfigurationsdateifreigabe nach Festlegen der ersten hinzufügen müssen.

Sie können pro AD-Domäne nur eine Dynamic Environment Manager-Konfigurationsdateifreigabe hinzufügen. Die Konfigurationsdateifreigabe, die Sie hinzufügen möchten, darf nicht dieselbe IP- oder DNS-Adresse haben wie die Konfigurationsdateifreigaben, die bereits in Ihren JMP-Servereinstellungen vorhanden sind.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.

- 2 Klicken Sie auf der Registerkarte **UEM** auf **Hinzufügen**.

Das Dialogfeld **UEM-Dateifreigabe hinzufügen** wird angezeigt.

- 3 Geben Sie im Textfeld **UNC-Pfad für Dateifreigabe** einen Wert im Format `\\<Servername>\<Pfadname>-der-UEM-Konfigurationsdateifreigabe` ein.

Wenn beispielsweise der Speicherort der Konfigurationsdateifreigabe `\\<IP-Adresse>\uemshare\config\general\FlexRepository\..` lautet, müssen Sie in das Textfeld **UNC-Pfad für Dateifreigabe** den Pfad `\\<IP-Adresse>\uemshare\config` eingeben.

- 4 Geben Sie den Dynamic Environment Manager-Benutzernamen und das Kennwort ein, das zum Verbinden mit der Dynamic Environment Manager-Konfigurationsdateifreigabe erforderlich ist.
- 5 Wählen Sie in der **Active Directory**-Liste den Domännennamen aus, der für die Dynamic Environment Manager-Konfigurationsdateifreigabe verwendet werden soll.

Hinweis Ein Active Directory kann jeweils nur mit einer Dynamic Environment Manager-Konfigurationsdateifreigabe verknüpft werden.

- 6 Klicken Sie auf **Speichern**.

Die Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe werden zu den JMP-Einstellungen hinzugefügt und eine neue Zeile wird zur Tabelle auf der Registerkarte **UEM** hinzugefügt.

Bearbeiten der Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe

Verwenden Sie den Horizon Console, falls Sie die bestehenden Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe ändern müssen, die von den JMP-Zuweisungen verwendet werden.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.
- 2 Klicken Sie auf die Registerkarte **UEM** und wählen Sie in der Tabelle der bestehenden Informationen die Zeile für die Dynamic Environment Manager-Konfigurationsdateifreigabe aus, die Sie ändern möchten.
- 3 Klicken Sie auf **Bearbeiten**.

Das Dialogfeld **UEM-Dateifreigabe bearbeiten** wird angezeigt.
- 4 Ändern Sie die Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe, die aktualisiert werden müssen.
- 5 Klicken Sie auf **Speichern**.

Löschen der Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe

Verwenden Sie Horizon Console, wenn Sie die Informationen der bestehenden Einstellungen zu einer Dynamic Environment Manager-Konfigurationsdateifreigabe löschen müssen.

Sie können nur Informationen zu einer registrierten Dynamic Environment Manager-Konfigurationsdateifreigabe aus einer JMP-Einstellung löschen, wenn diese Instanz nicht bereits von JMP-Zuweisungen verwendet wird.

Verfahren

- 1 Klicken Sie in Horizon Console auf **JMP-Konfiguration**.
- 2 Klicken Sie auf die Registerkarte **UEM**.
- 3 Wählen Sie die Tabellenzeile mit den Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe aus, die Sie aus den JMP-Einstellungen löschen möchten.
- 4 Klicken Sie auf **Löschen**, um zu bestätigen, dass Sie die Informationen zu dieser Dynamic Environment Manager-Konfigurationsdateifreigabe löschen möchten.

Sie wird entfernt, falls keine JMP-Zuweisungen vorhanden sind, die die Dynamic Environment Manager-Konfigurationsdateifreigabe verwenden.

Ein Dialogfeld mit einer Warnung wird angezeigt, wenn die Dynamic Environment Manager-Konfigurationsdateifreigabe von einer JMP-Zuweisung verwendet wird. Die Warnmeldung enthält die Liste der JMP-Zuweisungen, von denen die Dynamic Environment Manager-Konfigurationsdateifreigabe verwendet wird. Sie können die Informationen zur Dynamic Environment Manager-Konfigurationsdateifreigabe erst löschen, nachdem sie aus den JMP-Zuweisungen entfernt wurde oder diese JMP-Zuweisungen, die die Konfigurationsdateifreigabe verwenden, gelöscht wurden.

Verwalten von JMP-Zuweisungen

12

Nach Installation von JMP Server und Konfiguration der JMP-Einstellungen können Sie mit den JMP Integrated Workflow-Funktionen JMP-Zuweisungen erstellen, ändern, duplizieren oder löschen.

Sie müssen zunächst JMP Server installieren und die JMP-Einstellungen konfigurieren, bevor Sie JMP-Zuweisungen erstellen. Weitere Informationen hierzu finden Sie in *VMware Horizon JMP Server Installations- und Einrichtungshandbuch* und [Erstmaliges Konfigurieren der JMP-Einstellungen](#).

Vergewissern Sie sich, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie JMP-Zuweisungen erstellen, bearbeiten, duplizieren oder löschen.

- Vergewissern Sie sich, dass die Horizon 7-Instanz, die mit der JMP-Einstellung registriert ist, aktiv ist und ausgeführt wird.
- Stellen Sie sicher, dass mindestens eine Active Directory-Domäne mit der JMP-Einstellung registriert ist.
- Vergewissern Sie sich, dass die App Volumes-Instanz, die Sie mit der JMP-Einstellung registriert haben, aktiv ist und ausgeführt wird.
- Vergewissern Sie sich, dass die Dynamic Environment Manager-Konfigurationsdateifreigabe, die in der JMP-Einstellung definiert ist, aktiv ist und ausgeführt wird.

Hinweis Globale Berechtigungen werden nicht unterstützt.

Wenn Sie versuchen, eine JMP-Zuweisung zu erstellen, zu bearbeiten, zu duplizieren oder zu löschen, erhalten Sie möglicherweise eine Meldung, die Sie darauf hinweist, dass die versuchte Aktion nicht erfolgreich durchgeführt wurde. Möglicherweise treten Probleme auf, wenn Sie versuchen, eine der zugrunde liegenden JMP-Technologiekomponenten zu erreichen, woraufhin die Zuweisungsvalidierung nicht erfolgreich durchgeführt wird. Auf dem Bildschirm mit der JMP-Zuweisungsübersicht können Sie versuchen, das Problem zu beheben. Wählen Sie dazu eine der folgenden Optionen aus.

- Klicken Sie auf **Bearbeiten**, um die Probleme manuell zu beheben.
- Klicken Sie auf **Reparieren**, wenn der JMP-Server versuchen soll, die bei der aktuellen JMP-Zuweisung gefundenen Probleme zu beheben.
- Klicken Sie auf **Löschen erzwingen**, um die JMP-Zuweisung vollständig zu entfernen.

Dieses Kapitel enthält die folgenden Themen:

- [Erstellen einer JMP-Zuweisung](#)

- [Bearbeiten einer JMP-Zuweisung](#)
- [Duplizieren einer JMP-Zuweisung](#)
- [Löschen einer JMP-Zuweisung](#)

Erstellen einer JMP-Zuweisung

Mit Horizon Console können Sie JMP-Zuweisungen erstellen, mit denen Sie Desktop-Arbeitsumgebungen für Benutzer oder Benutzergruppen erstellen.

Sie wählen zur Definition einer JMP-Zuweisung die Einstellungen für Horizon Desktop-Pools, App Volumes AppStacks und User Environment Manager aus.

Voraussetzungen

Vergewissern Sie sich, dass die in [Kapitel 12 Verwalten von JMP-Zuweisungen](#) angegebenen Voraussetzungen erfüllt sind.

Verfahren

- 1 Klicken Sie auf der Horizon Console auf **Zuweisungen (JMP)**.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie im Assistenten für neue Zuweisungen auf der Registerkarte **Benutzer** einige Zeichen neben der Active Directory-Dropdownliste ein und wählen Sie die Benutzer oder Benutzergruppen aus, die zur neuen JMP-Zuweisung hinzugefügt werden sollen.

Ihre Auswahl wird im Abschnitt „Ausgewählte Benutzer/Gruppen“ hinzugefügt.
- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Registerkarte **Desktops** den Desktop-Pool aus, den Sie zur JMP-Zuweisung hinzufügen möchten. Klicken Sie anschließend auf **Weiter**.
- 6 Aktivieren Sie auf der Registerkarte **Anwendungen** das Kontrollkästchen neben dem Namen der Anwendung, die Sie zur JMP-Zuweisung hinzufügen möchten. Klicken Sie nach Ihrer Auswahl auf **Weiter**.
- 7 Legen Sie auf der Registerkarte **Benutzerumgebung** fest, ob Sie die JMP-Zuweisung mit einer der verfügbaren Benutzerumgebungseinstellungen konfigurieren möchten.
 - Wenn **UEM-Einstellungen deaktivieren?** auf **Nein** festgelegt ist, wird durch Klicken auf **Überspringen** die User Environment Manager-Zuweisungsdatei nicht in der User Environment Manager-Konfigurationsdateifreigabe gespeichert. Alle User Environment Manager-Einstellungen werden auf die Arbeitsumgebungen der virtuellen Desktops angewendet. Diese wurden für die Benutzer erstellt, die die JMP-Zuweisungen verwenden, die Sie aktuell erstellen.
 - Wenn **UEM-Einstellungen deaktivieren?** auf **Nein** festgelegt ist, wählen Sie die Einstellungen der Benutzerumgebung aus, die auf die JMP-Zuweisung, die gerade erstellt wird, angewendet

werden sollen. Durch Klicken auf **Weiter** wird die User Environment Manager-Zuweisungsdatei mit den ausgewählten Benutzerumgebungseinstellungen erstellt. Die ausgewählten Einstellungen werden auf die Arbeitsumgebungen der virtuellen Desktops angewendet. Diese wurden für die Benutzer erstellt, die die JMP-Zuweisungen verwenden, die Sie aktuell erstellen.

- Wenn **UEM-Einstellungen deaktivieren?** auf **Ja** festgelegt ist, wird die Liste der verfügbaren Benutzerumgebungseinstellungen aus der Ansicht gelöscht. Wenn Sie auf **Weiter** klicken, wird eine leere Zuweisungsdatei in die User Environment Manager-Konfigurationsdateifreigabe geschrieben. Durch Deaktivieren der User Environment Manager-Einstellungen wird sichergestellt, dass keine Benutzerumgebungseinstellungen auf die Arbeitsumgebungen der virtuellen Desktops angewendet werden. Diese wurden für die Benutzer erstellt, die die JMP-Zuweisungen verwenden, die Sie aktuell erstellen.
- 8 Akzeptieren Sie auf der Registerkarte **Definitionen** den Standardnamen für die JMP-Zuweisung oder ersetzen Sie den Namen durch einen anderen. Optional können Sie eine Beschreibung hinzufügen.
 - 9 Wählen Sie in der Dropdownliste **AppStack verknüpfen** den Zeitpunkt aus, zu dem der AppStack an die JMP-Zuweisung angehängt werden soll. Klicken Sie anschließend auf **Weiter**.
 - 10 Überprüfen Sie auf der Registerkarte **Übersicht** die Details für die neue Zuweisung. Wenn Sie diese akzeptieren, klicken Sie auf **Absenden**. Klicken Sie auf **Zurück**, falls Änderungen erforderlich sind und nehmen Sie diese vor.

Die neue JMP-Zuweisung wird in die Warteschlange zum Speichern in der JMP-Datenbank gestellt und zur Liste der Zuweisungen im Bereich „JMP-Zuweisungen“ hinzugefügt. Nach erfolgreichem Hinzufügen zur der JMP-Zuweisung ändert sich der Status und wird nicht mehr als „Ausstehend“ angegeben. Sie kann nun in der Liste der JMP-Zuweisungen ausgewählt und bearbeitet, dupliziert oder gelöscht werden.

Sie können unter Verwendung der folgenden Informationen auch die Zuweisungen oder Berechtigungen überprüfen, die für die neue JMP-Zuweisung erstellt wurden.

- Um Informationen zum für die JMP-Zuweisung erstellten Horizon-Desktop-Pool zu überprüfen, verwenden Sie Horizon Console. Wählen Sie **Bestand > Desktops** und suchen Sie den durch JMP Server erstellten Desktop-Pool.
- Verwenden Sie die App Volumes-Verwaltungskonsole, um die für die neue JMP-Zuweisung durch JMP Server erstellten AppStacks-Informationen anzuzeigen. Wählen Sie **Volumes > AppStacks** und suchen Sie die durch JMP Server erstellten AppStacks.
- Um die Einstellungen für die Benutzerumgebung zu überprüfen, die Sie für die JMP-Zuweisung konfiguriert haben, verwenden Sie die Dynamic Environment Manager-Verwaltungskonsole und klicken Sie auf die Registerkarte **Benutzerumgebung**. Wählen Sie im linken Bereich die Einstellung der Benutzerumgebung, die von der JMP-Zuweisung verwendet wird, und klicken Sie im daraufhin angezeigten Dialogfeld auf die Registerkarte **Zuordnungen**, um die JMP-Zuweisungsinformationen für diese Benutzerumgebungseinstellung anzuzeigen.

Bearbeiten einer JMP-Zuweisung

Es kann vorkommen, dass Sie eine bestehende JMP-Zuweisung ändern müssen, weil Komponenten geändert wurden, die zu deren Definition verwendet wurden. An der Horizon Console können Sie die erforderlichen Änderungen an der JMP-Zuweisung vornehmen.

Voraussetzungen

- Vergewissern Sie sich, dass die in [Kapitel 12 Verwalten von JMP-Zuweisungen](#) angegebenen Voraussetzungen erfüllt sind.
- Die JMP-Zuweisung, die Sie bearbeiten möchten, darf nicht den Status „Ausstehend“ aufweisen.

Verfahren

- 1 Klicken Sie auf der Horizon Console auf **Zuweisungen (JMP)**.
- 2 Wählen Sie die zu bearbeitende JMP-Zuweisung aus, indem Sie entweder das Kontrollkästchen aktivieren oder den Namen der JMP-Zuweisung in der Liste auswählen.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Ändern Sie die aktuellen Einstellungen im Assistenten „Zuweisung bearbeiten“.

Klicken Sie auf **Abbrechen**, wenn Sie den Bearbeitungsprozess unterbrechen möchten.

- a Wenn Sie aktuell ausgewählte Benutzer oder Gruppen entfernen möchten, klicken Sie auf das Symbol zum Löschen (**X**).
- b Klicken Sie auf **Weiter**.
- c Wählen Sie auf der Registerkarte **Desktops** einen Desktop-Pool aus, der zur JMP-Zuweisung hinzugefügt werden soll. Klicken Sie auf **Weiter**.
- d Wählen Sie auf der Registerkarte **Anwendungen** die verfügbaren Anwendungen aus, die zur JMP-Zuweisung hinzugefügt werden sollen. Alternativ können Sie auch die Auswahl der vorher ausgewählten Anwendungen aufheben. Klicken Sie auf **Weiter**.

- e Legen Sie auf der Registerkarte **Benutzerumgebung** fest, ob Sie die JMP-Zuweisung mit einer der verfügbaren Benutzerumgebungseinstellungen konfigurieren möchten.
 - Wenn **UEM-Einstellungen deaktivieren?** auf **Nein** festgelegt ist, wird durch Klicken auf **Überspringen** die User Environment Manager-Zuweisungsdatei nicht in der User Environment Manager-Konfigurationsdateifreigabe gespeichert. Alle User Environment Manager-Einstellungen werden auf die Arbeitsumgebungen der virtuellen Desktops angewendet. Diese wurden für die Benutzer erstellt, die die JMP-Zuweisungen verwenden, die Sie aktuell bearbeiten.
 - Wenn **UEM-Einstellungen deaktivieren?** auf **Nein** festgelegt ist, wählen Sie die Einstellungen der Benutzerumgebung aus, die auf die JMP-Zuweisung, die gerade erstellt wird, angewendet werden sollen. Durch Klicken auf **Weiter** wird die User Environment Manager-Zuweisungsdatei mit den ausgewählten Benutzerumgebungseinstellungen erstellt. Die ausgewählten Einstellungen werden auf die Arbeitsumgebungen der virtuellen Desktops angewendet. Diese wurden für die Benutzer erstellt, die die JMP-Zuweisungen verwenden, die Sie aktuell bearbeiten.
 - Wenn **UEM-Einstellungen deaktivieren?** auf **Ja** festgelegt ist, wird die Liste der verfügbaren Benutzerumgebungseinstellungen aus der Ansicht gelöscht. Wenn Sie auf **Weiter** klicken, wird eine leere Zuweisungsdatei in die User Environment Manager-Konfigurationsdateifreigabe geschrieben. Durch Deaktivieren der User Environment Manager-Einstellungen wird sichergestellt, dass keine Benutzerumgebungseinstellungen auf die Arbeitsumgebungen der virtuellen Desktops angewendet werden. Diese wurden für die Benutzer erstellt, die die JMP-Zuweisungen verwenden, die Sie aktuell bearbeiten.
- f Ändern Sie gegebenenfalls auf der Registerkarte **Definitionen** die aktuellen Werte unter **Name**, **Beschreibung** oder geben Sie einen neuen Zeitpunkt zum Anhängen des AppStack an die JMP-Zuweisung an.
- g Klicken Sie auf **Weiter**.
- h Prüfen Sie die Übersicht der vorgenommenen Änderungen und klicken Sie auf **Absenden**, um die Änderungen zu speichern.

Wenn der Vorgang erfolgreich ausgeführt wurde, werden die Änderungen gespeichert. Wenn Probleme auftreten, erhalten Sie zusätzliche Informationen und werden informiert, welche möglichen Aktionen Sie durchführen können.

Duplizieren einer JMP-Zuweisung

Sie können JMP-Zuweisungen schneller erstellen, indem Sie bestehende ähnliche JMP-Zuweisungen duplizieren.

Voraussetzungen

- Vergewissern Sie sich, dass die in [Kapitel 12 Verwalten von JMP-Zuweisungen](#) angegebenen Voraussetzungen erfüllt sind.

- Die JMP-Zuweisung, die Sie duplizieren möchten, darf nicht den Status „Ausstehend“ oder „Fehler“ aufweisen.

Verfahren

- 1 Wählen Sie auf der Horizon Console **Zuweisungen (JMP)** aus.
- 2 Wählen Sie die JMP-Zuweisung aus, die Sie duplizieren möchten, und klicken Sie auf **Duplizieren**.
- 3 Ändern Sie im Assistenten „Neue Zuweisung“ die duplizierte JMP-Zuweisung nach Bedarf.
 - a Wählen Sie neue Benutzer oder Gruppen aus oder entfernen Sie beliebige der aktuell ausgewählten Benutzer oder Gruppen. Klicken Sie auf **Weiter**.
 - b Wählen Sie im Bereich „Desktops“ einen neuen Desktop-Pool aus oder entfernen Sie beliebige der Desktop-Pools, die in der duplizierten JMP-Zuweisung enthalten waren. Klicken Sie auf **Weiter**.
 - c Wählen Sie weitere Anwendungen für die neue JMP-Zuweisung aus und heben Sie die Auswahl von Anwendungen auf, die aktuell ausgewählt sind. Klicken Sie auf **Weiter**.
 - d Wählen Sie im Bereich „Benutzerumgebung“ die Einstellung des User Environment Managers aus, die auf die neue JMP-Zuweisung angewendet werden soll. Klicken Sie auf **Weiter**.
 - e Ersetzen Sie im Bereich „Definitionen“ den erstellten Standardnamen, falls gewünscht. Fügen Sie eine Beschreibung hinzu und geben Sie an, wann der AppStack an die neue JMP-Zuweisung angehängt werden soll.
 - f Klicken Sie auf **Weiter** und sehen Sie sich die Übersicht der Details der neuen JMP-Zuweisung an.
 - g Wenn die Informationen Ihren Vorstellungen entsprechen, klicken Sie auf **Absenden**. Klicken Sie andernfalls auf **Zurück**, um Änderungen vorzunehmen.

Die neue JMP-Zuweisung wird validiert, was einige Zeit in Anspruch nehmen kann. Nach erfolgreicher Validierung wird die neu erstellte JMP-Zuweisung zur Liste im Bereich „JMP-Zuweisungen“ hinzugefügt. Wenn Sie den Mauszeiger über den Namen bewegen, sehen Sie, dass die Zuweisung den Status „Ausstehend“ aufweist. Der Status ändert sich erst nach dem erfolgreichen Speichern in der JMP-Datenbank. Wenn die JMP-Zuweisung nicht mehr den Status „Ausstehend“ aufweist, können Sie weitere Aktionen für die Zuweisung durchführen.

Löschen einer JMP-Zuweisung

Verwenden Sie Horizon Console zum Löschen einer JMP-Zuweisung.

Wenn eine JMP-Zuweisung gelöscht wird, dann werden auch die Horizon-Poolberechtigungen, die AppStack-Zuweisungen und die UEM-Berechtigung gelöscht, die mit der JMP-Zuweisung verknüpft sind. Wenn die von der JMP-Zuweisung verwendete Horizon-Poolberechtigung oder AppStack-Zuweisung jedoch bereits vor Erstellung der JMP-Zuweisung vorhanden waren, dann werden sie nicht gelöscht. Nach dem Löschen einer JMP-Zuweisung wird diese nicht mehr auf Benutzer oder Desktops angewendet.

Voraussetzungen

- Prüfen Sie, ob die in [Kapitel 12 Verwalten von JMP-Zuweisungen](#) angegebenen Voraussetzungen erfüllt sind.
- Die JMP-Zuweisung, die Sie löschen möchten, darf nicht den Status „Ausstehend“ aufweisen.

Verfahren

- 1 Klicken Sie in Horizon Console auf **Zuweisungen (JMP)**.
- 2 Wählen Sie im Bereich „JMP-Zuweisungen“ eine oder mehrere JMP-Zuweisungen aus und klicken Sie auf **Löschen**.
- 3 Klicken Sie im Bestätigungsdialogfeld auf **Löschen**, um zu bestätigen, dass Sie die Zuweisung dauerhaft löschen möchten.

Bei erfolgreicher Löschung wird die Horizon-Poolberechtigung von der JMP-Datenbank und aus der Liste im Bereich „JMP-Zuweisungen“ entfernt.

Die JMP-Zuweisung wird nicht gelöscht, wenn der Löschvorgang teilweise fehlschlägt. Durch Klicken auf die Statusanzeigen erhalten Sie weitere Informationen dazu, weshalb der Vorgang fehlgeschlagen ist.

Konfigurieren der Ereignisberichterstattung in Horizon Console

13

Sie können eine Ereignisdatenbank erstellen, um Informationen zu Horizon 7-Ereignissen aufzuzeichnen. Wenn Sie einen Syslog-Server verwenden, können Sie den Verbindungsserver darüber hinaus so konfigurieren, dass Ereignisse an einen Syslog-Server gesendet werden oder eine Flatfiledatei mit Ereignissen im Sys Log-Format erstellt wird.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen einer Datenbank und eines Datenbankbenutzers für Horizon 7-Ereignisse in Horizon Console](#)
- [Vorbereiten einer SQL Server-Datenbank für die Ereignisberichterstellung in Horizon Console](#)
- [Konfigurieren der Ereignisdatenbank in Horizon Console](#)
- [Konfigurieren der Ereignisprotokollierung in Datei oder Syslog-Server in Horizon Console](#)
- [Überwachen von Ereignissen in Horizon 7](#)

Hinzufügen einer Datenbank und eines Datenbankbenutzers für Horizon 7-Ereignisse in Horizon Console

Sie erstellen eine Ereignisdatenbank, indem Sie sie zu einem vorhandenen Datenbankserver hinzufügen. Anschließend können Sie mithilfe von Berichtssoftware die Ereignisse in der Datenbank analysieren.

Stellen Sie den Datenbankserver für die Ereignisdatenbank auf einem dedizierten Server bereit, sodass die Aktivitäten der Ereignisprotokollierung weder die Bereitstellung noch andere Aktivitäten, die für Horizon 7-Bereitstellungen wichtig sind, beeinträchtigen.

Hinweis Sie müssen für diese Datenbank keine ODBC-Datenquelle erstellen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen unterstützten Microsoft SQL Server- oder Oracle-Datenbankserver auf einem System verfügen, auf das eine Verbindungsserver-Instanz zugreifen kann.

Aktuelle Informationen zu unterstützten Datenbanken finden Sie in den VMware Produkt-Interoperabilität-Matrizen unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. Nachdem Sie für **Lösung-/Datenbank-Interoperabilität** das Produkt und die Version ausgewählt haben, um für den Schritt „Datenbank hinzufügen“ eine Liste mit allen unterstützten Datenbanken anzuzeigen, wählen Sie **Beliebig** aus und klicken Sie auf **Hinzufügen**.

- Stellen Sie sicher, dass Sie über die erforderlichen Datenbankberechtigungen zum Erstellen einer Datenbank und eines Benutzers auf dem Datenbankserver verfügen.
- Wenn Sie nicht mit dem Verfahren zum Erstellen von Datenbanken auf Microsoft SQL Server-Datenbankservern vertraut sind, finden Sie weitere Informationen unter „Hinzufügen einer View Composer-Datenbank zu SQL Server“ im Dokument *Horizon 7-Installation*.
- Wenn Sie nicht mit dem Verfahren zum Erstellen von Datenbanken auf Oracle-Datenbankservern vertraut sind, finden Sie weitere Informationen unter „Hinzufügen einer View Composer-Datenbank zu Oracle 12c oder 11g“ im Dokument *Horizon 7-Installation*.

Verfahren

- 1 Fügen Sie dem Server eine Datenbank hinzu und geben Sie ihr einen beschreibenden Namen, z. B. „Horizon-Ereignisse“.

Geben Sie für eine Oracle 12c- oder Oracle 11g-Datenbankinstanz eine Oracle-Systemkennung (SID) ein, die Sie beim Konfigurieren der Ereignisdatenbank in Horizon Console verwenden.

- 2 Fügen Sie einen Benutzer für diese Datenbank hinzu, der über Berechtigungen zum Erstellen von Tabellen, Ansichten und Oracle-Triggern und -Sequenzen verfügt und die Berechtigung zum Ausführen von Lese- und Schreiboperationen für diese Objekte besitzt.

Verwenden Sie für eine Microsoft SQL Server-Datenbank nicht das Sicherheitsmodell der integrierten Windows-Authentifizierung als Authentifizierungsmethode. Stellen Sie sicher, dass Sie als Authentifizierungsmethode die SQL Server-Authentifizierung verwenden.

Die Datenbank wird erstellt, das Schema jedoch nicht. Dieses wird erst angelegt, wenn Sie die Datenbank in Horizon Console konfigurieren.

Nächste Schritte

Folgen Sie den Anweisungen unter [Konfigurieren der Ereignisdatenbank in Horizon Console](#).

Vorbereiten einer SQL Server-Datenbank für die Ereignisberichterstellung in Horizon Console

Bevor Sie Horizon Console zum Konfigurieren einer Ereignisdatenbank auf dem Microsoft SQL Server verwenden können, müssen Sie die richtigen TCP/IP-Eigenschaften konfigurieren und sicherstellen, dass der Server die SQL Server-Authentifizierung nutzt.

Voraussetzungen

- Erstellen einer SQL Server-Datenbank für die Ereignisberichterstellung. Siehe [Hinzufügen einer Datenbank und eines Datenbankbenutzers für Horizon 7-Ereignisse in Horizon Console](#).

- Stellen Sie sicher, dass Sie über die erforderlichen Datenbankberechtigungen zum Konfigurieren der Datenbank verfügen.
- Stellen Sie sicher, dass der Datenbankserver die SQL Server-Authentifizierungsmethode nutzt. Verwenden Sie nicht die Windows-Authentifizierung.

Verfahren

- 1 Öffnen Sie den SQL Server-Konfigurations-Manager und erweitern Sie **Netzwerkconfiguration von SQL Server YYYY**.
- 2 Wählen Sie **Protokolle für Servername** aus.
- 3 Klicken Sie in der Liste der Protokolle mit der rechten Maustaste auf **TCP/IP** und wählen Sie **Eigenschaften**.
- 4 Setzen Sie die Eigenschaft **Aktiviert** auf **Ja**.
- 5 Stellen Sie sicher, dass ein Port zugewiesen ist, oder weisen Sie ggf. einen Port zu.
Informationen zu statischen und dynamischen Ports sowie ihrer Zuweisung finden Sie in der Online-Hilfe zum SQL Server-Konfigurations-Manager.
- 6 Stellen Sie sicher, dass dieser Port nicht von einer Firewall blockiert ist.

Nächste Schritte

Verbinden Sie mittels Horizon Console die Datenbank mit dem Verbindungsserver. Folgen Sie den Anweisungen unter [Konfigurieren der Ereignisdatenbank in Horizon Console](#).

Konfigurieren der Ereignisdatenbank in Horizon Console

Die Ereignisdatenbank speichert Informationen zu Horizon 7-Ereignissen nicht in einer Protokolldatei, sondern in Form von Einträgen in einer Datenbank.

Sie konfigurieren eine Ereignisdatenbank nach der Installation einer Verbindungsserver-Instanz. Sie müssen nur einen Host in einer Verbindungsserver-Gruppe konfigurieren. Die verbleibenden Hosts in der Gruppe werden automatisch konfiguriert.

Hinweis Für die Sicherheit der Datenbankverbindung zwischen der Verbindungsserver-Instanz und einer externen Datenbank ist der Administrator verantwortlich, auch wenn der Ereignisdatenverkehr auf Informationen über den Zustand der Horizon 7-Umgebung beschränkt ist. Wenn Sie zusätzliche Sicherheitsmaßnahmen ergreifen möchten, können Sie diesen Kanal durch IPSec oder ein anderes Hilfsmittel schützen. Sie können die Datenbank auch lokal auf dem Verbindungsserver-Computer bereitstellen.

Sie können die Ereignisse in den Datenbanktabellen unter Verwendung von Microsoft SQL Server oder Oracle-Datenbankberichttools untersuchen. Weitere Informationen finden Sie im Dokument *Horizon 7-Integration*.

Sie können auch Horizon 7-Ereignisse im Format SysLog generieren, damit Analysesoftware von Drittanbietern auf die Ereignisdaten zugreifen kann. Sie verwenden den Befehl `vdmadmin` in Verbindung mit der Option `-I`, um Horizon 7-Ereignismeldungen in den Ereignisprotokolldateien im Format SysLog aufzuzeichnen. Siehe „Generieren von Horizon 7-Ereignisprotokollmeldungen im Syslog-Format mit der Option `-I`“ im Dokument *Horizon 7-Verwaltung*.

Voraussetzungen

Sie benötigen die folgenden Informationen, um eine Ereignisdatenbank zu konfigurieren:

- Den DNS-Namen oder die IP-Adresse des Datenbankservers.
- Typ des Datenbankservers: Microsoft SQL Server oder Oracle.
- Die Portnummer, die für den Zugriff auf den Datenbankserver verwendet wird. Standardmäßig wird Port 1521 für Oracle und Port 1433 für SQL Server verwendet. Wenn es sich beim SQL Server-Datenbankserver um eine benannte Instanz handelt oder Sie SQL Server Express verwenden, müssen Sie möglicherweise die Portnummer ermitteln. Informationen zum Herstellen einer Verbindung mit einer benannten Instanz von SQL Server finden Sie im Microsoft KB-Artikel unter <http://support.microsoft.com/kb/265808>.
- Der Name der Ereignisdatenbank, die Sie auf dem Datenbankserver erstellt haben. Siehe [Hinzufügen einer Datenbank und eines Datenbankbenutzers für Horizon 7-Ereignisse in Horizon Console](#).

Wenn Sie die Ereignisdatenbank in Horizon Console konfigurieren, müssen Sie für eine Oracle 12c- oder 11g-Datenbank die Oracle-Systemkennung (SID) als Datenbanknamen verwenden.

- Den Benutzernamen und das Kennwort des Benutzers, den Sie für diese Datenbank erstellt haben. Siehe [Hinzufügen einer Datenbank und eines Datenbankbenutzers für Horizon 7-Ereignisse in Horizon Console](#).

Verwenden Sie die SQL Server-Authentifizierung für diesen Benutzer. Verwenden Sie nicht das Sicherheitsmodell der integrierten Windows-Authentifizierung als Authentifizierungsmethode.

- Ein Präfix für die Tabellen in der Ereignisdatenbank, beispielsweise `VE_`. Das Präfix ermöglicht eine gemeinsame Verwendung der Datenbank durch die Horizon 7-Installationen.

Hinweis Die eingegebenen Zeichen müssen für die verwendete Datenbanksoftware zulässig sein. Die Syntax des Präfixes wird nicht überprüft, wenn Sie Daten in das Dialogfeld eingeben. Wenn Sie Zeichen eingeben, die für die verwendete Datenbanksoftware unzulässig sind, tritt ein Fehler auf, wenn der Verbindungsserver versucht, eine Verbindung mit dem Datenbankserver herzustellen. Dieser Fehler und mögliche andere Fehlermeldungen, die bei einem ungültigen Datenbanknamen auftreten, werden in der Protokolldatei aufgezeichnet.

Verfahren

- 1 Wählen Sie in Horizon Console die Optionen **Einstellungen > Ereigniskonfiguration** aus.
- 2 Klicken Sie im Abschnitt **Ereignisdatenbank** auf **Bearbeiten**, geben Sie die erforderlichen Informationen in die dafür vorgesehenen Felder ein und klicken Sie auf **OK**.

Um die Ereignisdatenbank-Informationen zu löschen, klicken Sie auf **Löschen**.

- 3 (Optional) Klicken Sie im Fenster „Ereigniseinstellungen“ auf **Bearbeiten**, ändern Sie den Wert für die Anzeigedauer von Ereignissen sowie die Anzahl der Tage zur Klassifizierung von neuen Ereignissen und klicken Sie auf **OK**.

Diese Einstellungen beziehen sich auf den Zeitraum, in dem die Ereignisse auf der Horizon Console-Oberfläche angezeigt werden. Nach Ablauf dieses Zeitraums stehen die Ereignisse nur in den Verlaufsdatenbanktabellen zur Verfügung.

- 4 Wählen Sie **Überwachung > Ereignisse** aus, um zu prüfen, ob die Verbindung mit der Ereignisdatenbank erfolgreich hergestellt wurde.

Tritt bei der Verbindungsherstellung ein Fehler auf, wird eine Fehlermeldung angezeigt. Wenn Sie SQL Express oder eine benannte Instanz von SQL Server verwenden, müssen Sie möglicherweise die richtige Portnummer ermitteln, wie in den Voraussetzungen erwähnt.

Konfigurieren der Ereignisprotokollierung in Datei oder Syslog-Server in Horizon Console

Sie können Horizon 7-Ereignisse im Syslog-Format generieren, damit Analysesoftware auf die Ereignisdaten zugreifen kann.

Sie müssen nur einen Host in einer Verbindungsserver-Gruppe konfigurieren. Die verbleibenden Hosts in der Gruppe werden automatisch konfiguriert.

Wenn Sie die dateibasierte Protokollierung von Ereignissen aktivieren, werden Ereignisse in einer lokalen Protokolldatei gesammelt. Bei Angabe einer Dateifreigabe werden diese Protokolldateien auf diese Freigabe verschoben.

- Die maximale Größe des lokalen Verzeichnisses für Ereignisprotokolle (einschließlich geschlossene Protokolldateien) beträgt 300 MB. Bei Überschreiten dieser Größe werden die ältesten Dateien gelöscht. Das Standardziel der Syslog-Ausgabe ist %PROGRAMDATA%\VMware\VDM\events\.
- Verwenden Sie einen UNC-Pfad für langfristige Ereignisaufzeichnungen, wenn Sie nicht über einen Syslog-Server oder eine Ereignisdatenbank verfügen oder wenn Ihr aktueller Syslog-Server Ihre Anforderungen nicht erfüllt.

Alternativ können Sie einen `vdmadmin`-Befehl verwenden, um die dateibasierte Protokollierung von Ereignissen im Syslog-Format zu konfigurieren. Weitere Informationen finden Sie im Thema zum Generieren von Horizon 7-Ereignisprotokollmeldungen im Syslog-Format unter Verwendung der Option `-I` des Befehls `vdmadmin` im Dokument *Horizon 7-Verwaltung*.

Wichtig Syslog-Daten werden beim Senden an einen Syslog-Server innerhalb des Netzwerks ohne softwarebasierte Verschlüsselung übertragen und enthalten möglicherweise sensible Daten (z. B. Benutzernamen). VMware empfiehlt die Implementierung einer Sicherheitsmaßnahme auf Verbindungsebene, z. B. IPsec, um zu verhindern, dass diese Daten im Netzwerk überwacht werden können.

Voraussetzungen

Um einen Verbindungsserver so zu konfigurieren, dass Ereignisse im Syslog-Format aufgezeichnet und/oder an einen Syslog-Server gesendet werden, benötigen Sie die folgenden Informationen:

- Wenn ein Syslog-Server das System an einem UDP-Port auf Horizon 7-Ereignisse überwachen soll, benötigen Sie den DNS-Namen oder die IP-Adresse des Syslog-Servers sowie die UDP-Portnummer. Die standardmäßige UDP-Portnummer lautet 514.
- Wenn Protokolle in einem Flatfileformat erfasst werden sollen, benötigen Sie den UNC-Pfad zur Dateifreigabe und zum Ordner, in dem die Protokolldateien gespeichert werden sollen. Außerdem benötigen Sie den Benutzernamen, den Domännennamen und das Kennwort eines Kontos mit Schreibberechtigungen für die Dateifreigabe.

Verfahren

- 1 Wählen Sie in Horizon Console die Optionen **Einstellungen > Ereigniskonfiguration** aus.
- 2 (Optional) Um den Verbindungsserver so zu konfigurieren, dass Ereignisse an einen Syslog-Server gesendet werden, klicken Sie im Bereich **Syslog** unter **An Syslog-Server senden** auf **Hinzufügen** und geben Sie den Servernamen oder die IP-Adresse und die UDP-Portnummer an.
- 3 (Optional) Wählen Sie im Bereich **Ereignisse in Dateisystem** aus, ob Ereignisprotokollmeldungen generiert und im Syslog-Format in Protokolldateien gespeichert werden sollen.

Option	Beschreibung
Always	Ereignisprotokollmeldungen werden immer im Syslog-Format generiert und in Protokolldateien gespeichert.
Bei Fehler in Datei protokollieren (Standard)	Überwachungsereignisse werden in einer Protokolldatei gespeichert, wenn beim Schreiben von Ereignissen in die Ereignisdatenbank oder auf den Syslog-Server ein Problem auftritt. Diese Option ist standardmäßig aktiviert.
Nie	Ereignisprotokollmeldungen werden niemals im Syslog-Format generiert und in Protokolldateien gespeichert.

Wenn Sie keinen UNC-Pfad zu einer Dateifreigabe angeben, werden die Protokolldateien lokal gespeichert.

- 4 (Optional) Um die Horizon 7-Ereignisprotokollmeldungen auf einer Dateifreigabe zu speichern, klicken Sie unter **An Speicherort kopieren** auf **Hinzufügen** und geben Sie den UNC-Pfad zur Dateifreigabe und zu dem Ordner an, in dem die Protokolldateien gespeichert werden sollen. Geben Sie dabei auch den Benutzernamen, den Domännennamen und das Kennwort eines Kontos mit Schreibberechtigungen für die Dateifreigabe an.

Beispiel für einen UNC-Pfad:

```
\\syslog-server\folder\file
```

Überwachen von Ereignissen in Horizon 7

In der Ereignisdatenbank werden Informationen zu Ereignissen gespeichert, die im Verbindungsserver-Host oder in der Verbindungsserver-Gruppe, in Horizon Agent und in Horizon Console, auftreten. Sie werden im Dashboard über die Anzahl der Ereignisse benachrichtigt. Auf der Seite **Ereignisse** können Sie die Ereignisse im Detail untersuchen.

Hinweis Ereignisse werden in der Horizon Console-Benutzeroberfläche für einen begrenzten Zeitraum angezeigt. Nach Ablauf dieses Zeitraums stehen die Ereignisse nur in den Verlaufsdatenbanktabellen zur Verfügung. Sie können die Ereignisse in den Datenbanktabellen unter Verwendung von Microsoft SQL Server oder Oracle-Datenbankberichttools untersuchen. Weitere Informationen finden Sie im Dokument *Horizon 7-Integration*.

Hinweis Wenn die Ereignisdatenbank nicht mehr verfügbar ist, führt Horizon 7 die Überwachung der Ereignisse in diesem Zeitraum der fehlenden Verfügbarkeit durch und speichert die Ereignisse in der Ereignisdatenbank, sobald diese wieder verfügbar ist. Sie müssen die Ereignisdatenbank und den Verbindungsserver neu starten, um diese Ereignisse in der Horizon Console-Benutzeroberfläche anzeigen zu können.

Neben der Überwachung von Ereignissen in Horizon Console können Sie Horizon 7-Ereignisse im SysLog-Format generieren, damit die Analysesoftware auf die Ereignisdaten zugreifen kann. Siehe [Konfigurieren der Ereignisprotokollierung in Datei oder Syslog-Server in Horizon Console](#) und „Generieren von Horizon 7-Ereignisprotokollmeldungen im Syslog-Format mit der Option -l“ im Dokument *Horizon 7-Installation*.

Wenn Sie eine Ereignisdatenbank für mehrere Verbindungsserver konfigurieren, zeigt Horizon Console die Ereignisse für alle Verbindungsserver auf der Seite **Ereignisse** an. Horizon Console filtert Ereignisse basierend auf den von Ihnen durchgeführten Aufgaben und zeigt diese Ereignisse auf relevanten Seiten wie den Seiten **Desktop-Pools** oder **Anwendungspools** an.

Voraussetzungen

Erstellen und konfigurieren Sie die Ereignisdatenbank. Die erforderlichen Schritte sind im Dokument *Horizon 7-Installation* beschrieben.

Verfahren

- 1 Wählen Sie in Horizon Console die Optionen **Überwachen > Ereignisse** aus.
- 2 (Optional) Auf der Seite **Ereignisse** können Sie den Zeitraum der Ereignisse auswählen, die Ereignisse filtern und die aufgelisteten Ereignisse nach einer oder mehreren Spalten sortieren.

Nächste Schritte

Navigieren Sie in Horizon Console zu einem Desktop- oder Anwendungspool, einer virtuellen Maschine, einer persistenten Festplatte, einem Benutzer oder einer Gruppe und klicken Sie auf die Registerkarte **Ereignisse**, um bestimmte Ereignisse anzuzeigen.

Horizon 7-Ereignismeldungen

Horizon 7 zeigt ein Ereignis an, wenn sich der Systemstatus ändert oder ein Problem ermittelt wird. Basierend auf den in den Ereignismeldungen enthaltenen Informationen können Sie die entsprechende Maßnahme ergreifen.

Die folgende Tabelle zeigt die von Horizon 7 gemeldeten Ereignistypen.

Tabelle 13-1. Von Horizon 7 angezeigte Ereignistypen

Ereignistyp	Beschreibung
Audit Failure or Audit Success (Überwachungsfehler oder Überwachungserfolg)	Zeigt das Fehlschlagen oder den Erfolg einer Änderung an, die ein Administrator oder Benutzer am Verhalten oder an der Konfiguration von Horizon 7 vornimmt.
Fehler	Zeigt einen fehlgeschlagenen Horizon 7-Vorgang an.
Information	Zeigt normale Vorgänge innerhalb von Horizon 7 an.
Warnung	Zeigt kleinere Probleme bei Vorgängen oder Konfigurationseinstellungen an, die zu schwerwiegenden Problemen führen könnten.

Für Überwachungsfehler, Fehler oder Warnungen müssen möglicherweise Maßnahmen ergriffen werden. Wenn Überwachungserfolge oder Informationen angezeigt werden, sind keine Schritte erforderlich.

Verwenden des Horizon Help Desk Tool in Horizon Console

14

Horizon Help Desk Tool ist eine Webanwendung, mit der Sie den Status von Horizon 7-Benutzersitzungen abrufen und eine Fehlerbehebung sowie Wartungsvorgänge durchführen können.

In Horizon Help Desk Tool können Sie Benutzersitzungen zur Fehlerbehebung suchen und Vorgänge für die Desktop-Wartung wie den Neustart oder das Zurücksetzen von Desktops durchführen.

Um Horizon Help Desk Tool konfigurieren zu können, müssen die folgenden Anforderungen erfüllt sein:

- Lizenz für Horizon Enterprise Edition oder Horizon Apps Advanced Edition für Horizon 7. Informationen zur Prüfung, ob Sie über die richtige Lizenz verfügen, finden Sie im Dokument *Horizon 7-Verwaltung*.
- Eine Ereignisdatenbank zum Speichern von Informationen zu Horizon 7-Komponenten. Weitere Informationen zur Konfiguration einer Ereignisdatenbank finden Sie im Dokument *Horizon 7-Verwaltung*.
- Die Rolle „Helpdesk-Administrator“ oder „Helpdesk-Administrator (Nur Lesezugriff)“ zum Anmelden bei Horizon Help Desk Tool. Weitere Informationen zu diesen Rollen finden Sie im Dokument *Horizon 7-Verwaltung*.
- Aktivieren Sie den Zeitprofiler auf jeder Verbindungsserver-Instanz zur Anzeige der Anmeldesegmente.

Mit dem folgenden Befehl `vdadmin` aktivieren Sie den Zeitprofiler auf jeder Verbindungsserver-Instanz:

```
vdadmin -I -timingProfiler -enable
```

Mit dem folgenden Befehl `vdadmin` aktivieren Sie den Zeitprofiler auf einer Verbindungsserver-Instanz, die einen Verwaltungsport verwendet:

```
vdadmin -I -timingProfiler -enable -server {ip/server}
```

Dieses Kapitel enthält die folgenden Themen:

- [Starten des Horizon Help Desk Tool an der Horizon Console](#)
- [Fehlerbehebung bei Benutzern in Horizon Help Desk Tool](#)
- [Sitzungsdetails für das Horizon Help Desk Tool](#)

- [Sitzungsprozesse für das Horizon Help Desk Tool](#)
- [Anwendungsstatus für Horizon Help Desk Tool](#)
- [Fehlerbehebung bei Desktop- oder Anwendungssitzungen in Horizon Help Desk Tool](#)

Starten des Horizon Help Desk Tool an der Horizon Console

Das Horizon Help Desk Tool ist in der Horizon Console enthalten. Sie können nach einem Benutzer suchen, für den Sie im Horizon Help Desk Tool Probleme beheben möchten.

Verfahren

- 1 Sie können mit dem Textfeld „Benutzersuche“ nach einem Benutzernamen suchen oder direkt zum Horizon Help Desk Tool navigieren.
 - Geben Sie an der Horizon Console einen Benutzernamen im Textfeld „Benutzersuche“ ein.
 - Wählen Sie **Überwachen > Helpdesk** aus und geben Sie einen Benutzernamen in das Textfeld „Benutzersuche“ ein.

An der Horizon Console wird eine Liste der Benutzer in den Suchergebnissen angezeigt. Die Suche kann bis zu 100 übereinstimmende Ergebnisse zurückgeben.

- 2 Wählen Sie einen Benutzernamen aus.

Die Benutzerinformationen werden in einer Benutzerkarte angezeigt.

Nächste Schritte

Um Probleme zu beheben, klicken Sie auf die verwandten Registerkarten in der Benutzerkarte.

Fehlerbehebung bei Benutzern in Horizon Help Desk Tool

In Horizon Help Desk Tool können Sie in einer Benutzerkarte grundlegende Benutzerinformationen anzeigen. Durch Klicken auf Registerkarten auf der Benutzerkarte erhalten Sie weitere Details zu bestimmten Komponenten.

Benutzerdetails werden manchmal in Tabellen angezeigt. Sie können diese Benutzerdetails nach Spalten sortieren.

- Um eine Spalte in aufsteigender Reihenfolge zu sortieren, klicken Sie einmal auf die Spalte.
- Um eine Spalte in absteigender Reihenfolge zu sortieren, klicken Sie zweimal auf die Spalte.
- Um die Spalte nicht zu sortieren, klicken Sie dreimal auf die Spalte.

Grundlegende Benutzerinformationen

Zeigt grundlegende Benutzerinformationen an wie z. B. Benutzername, Telefonnummer und E-Mail-Adresse sowie den Verbindungsstatus des Benutzers (verbunden oder getrennt). Wenn der Benutzer über eine Desktop- oder Anwendungssitzung verfügt, ist der Status des Benutzers „Verbunden“. Wenn der Benutzer über keine Desktop- oder Anwendungssitzung verfügt, ist der Status des Benutzers „Getrennt“.

Durch Klicken auf die E-Mail-Adresse können Sie dem Benutzer eine E-Mail senden.

Sie können durch Klicken auf die Telefonnummer eine Skype for Business-Sitzung öffnen, um den Benutzer für eine Kontaktaufnahme zur Fehlerbehebung anzurufen.

Hinweis Die Skype for Business-Informationen werden für Linux-Desktop-Benutzer nicht angezeigt.

Sitzungen

Die Registerkarte **Sitzungen** zeigt Informationen zu den Desktop- oder Anwendungssitzungen an, mit denen der Benutzer verbunden ist.

Sie können mit dem Textfeld **Filter** Desktop- oder Anwendungssitzungen filtern.

Hinweis Auf der Registerkarte **Sitzungen** werden keine Informationen zu Sitzungen angezeigt, die das Microsoft RDP-Anzeigeprotokoll verwenden, oder zu Sitzungen, die auf virtuelle Maschinen aus vSphere Client oder ESXi zugreifen.

Die Registerkarte **Sitzungen** enthält die folgenden Informationen:

Tabelle 14-1. Registerkarte „Sitzungen“

Option	Beschreibung
Status	<p>Zeigt Informationen zum Status der Desktop- oder Anwendungssitzung an.</p> <ul style="list-style-type: none"> ■ Wenn die Sitzung verbunden ist, wird der Status „Grün“ angezeigt. ■ L, wenn es sich bei der Sitzung um eine lokale Sitzung handelt oder um eine Sitzung, die im lokalen Pod ausgeführt wird.
Computername	<p>Name der Desktop- oder Anwendungssitzung. Klicken Sie auf den Namen, um die Sitzungsinformationen auf einer Karte anzuzeigen.</p> <p>Um weitere Informationen anzuzeigen, klicken Sie auf die Registerkarten in der Sitzungskarte:</p> <ul style="list-style-type: none"> ■ Die Registerkarte Details zeigt die Benutzerinformationen wie z. B. die VM-Informationen und die CPU- bzw. Arbeitsspeicherauslastung an. ■ Die Registerkarte Prozesse zeigt Informationen zu den Prozessen an, die CPU und Arbeitsspeicher betreffen. ■ Die Registerkarte Anwendungen zeigt die Details zu den ausgeführten Anwendungen an. <p>Hinweis Für Linux-Desktopsitzungen kann nicht auf die Registerkarte Anwendungen zugegriffen werden.</p>
Protokoll	Das Anzeigeprotokoll für die Desktop- oder Anwendungssitzung.
Typ	Zeigt an, ob es sich beim Desktop um einen veröffentlichten Desktop, einen Desktop einer virtuellen Maschine oder eine Anwendung handelt.
Verbindungszeitpunkt	Der Zeitpunkt, an dem die Sitzung mit Verbindungsserver verbunden wurde.
Sitzungsdauer	Der Zeitraum, in dem die Sitzung mit dem Verbindungsserver verbunden war.

Desktops

Die Registerkarte **Desktops** zeigt Informationen zu den veröffentlichten oder virtuellen Desktops an, für die der Benutzer über Berechtigungen verfügt.

Tabelle 14-2. Desktops

Option	Beschreibung
Status	<p>Zeigt Informationen zum Status des Desktop-Sitzung an.</p> <ul style="list-style-type: none"> ■ Wenn die Sitzung verbunden ist, wird der Status „Grün“ angezeigt.
Name des Desktop-Pools	Name des Desktop-Pools für die Sitzung. Zeigt Linux als Desktop-Pool für eine Linux-Desktop-Sitzung an.

Tabelle 14-2. Desktops (Fortsetzung)

Option	Beschreibung
Desktop-Typ	<p>Zeigt an, ob es sich beim Desktop um einen veröffentlichten Desktop oder um einen Desktop einer virtuellen Maschine handelt.</p> <p>Hinweis Wenn die Sitzung in einem anderen Pod im Pod-Verbund ausgeführt wird, werden nicht alle Informationen angezeigt.</p>
Typ	<p>Zeigt Informationen zum Typ der Desktop-Berechtigung an.</p> <ul style="list-style-type: none"> ■ „Lokal“ für eine lokale Berechtigung.
vCenter	<p>Zeigt den Namen der virtuellen Maschine in vCenter Server an.</p> <p>Hinweis Wenn die Sitzung in einem anderen Pod im Pod-Verbund ausgeführt wird, werden nicht alle Informationen angezeigt.</p>
Standardprotokoll	<p>Das standardmäßige Anzeigeprotokoll für die Desktop- oder Anwendungssitzung.</p>

Anwendungen

Die Registerkarte **Anwendungen** enthält Informationen zu den veröffentlichten Anwendungen, für die der Benutzer über Berechtigungen verfügt.

Hinweis Im Rahmen von Linux-Desktopsitzungen kann nicht auf die Registerkarte **Anwendungen** zugegriffen werden.

Tabelle 14-3. Anwendungen

Option	Beschreibung
Status	<p>Zeigt Informationen zum Status der Anwendungssitzung an.</p> <ul style="list-style-type: none"> ■ Wenn die Sitzung verbunden ist, wird der Status „Grün“ angezeigt.
Anwendungen	<p>Zeigt die Namen der veröffentlichten Anwendungen im Anwendungspool an.</p>
Farm	<p>Name der Farm, die den RDS-Host enthält, mit dem die Sitzung verbunden ist.</p> <p>Hinweis Im Falle einer globalen Anwendungsberechtigung wird in dieser Spalte die Anzahl der Farmen in der globalen Anwendungsberechtigung angezeigt.</p>
Typ	<p>Zeigt Informationen zum Typ der Anwendungsberechtigung an.</p> <ul style="list-style-type: none"> ■ „Lokal“ für eine lokale Berechtigung.
Veröffentlicher	<p>Name des Softwareherstellers der veröffentlichten Anwendung.</p>

Aktivitäten

Die Registerkarte **Aktivitäten** zeigt die Ereignisprotokollinformationen über die Aktivitäten des Benutzers an. Sie können Aktivitäten zeitlich filtern, indem Sie z. B. als Zeitraum die letzten 12 Stunden oder die letzten 30 Tage angeben, oder nach Administratorname filtern. Klicken Sie auf **Nur Helpdesk-Ereignisse**, um nur nach Horizon Help Desk Tool-Aktivitäten zu filtern. Klicken Sie auf das Symbol „Aktualisieren“, um das Ereignisprotokoll zu aktualisieren. Klicken Sie auf das Symbol „Export“, um das Ereignisprotokoll in eine Datei zu exportieren.

Hinweis Die Ereignisprotokollinformationen werden nicht für Benutzer in einer Cloud-Pod-Architektur-Umgebung angezeigt.

Tabelle 14-4. Aktivitäten

Option	Beschreibung
Uhrzeit	<p>Ermöglicht die Auswahl eines Zeitraums. Standardmäßig sind die letzten 12 Stunden ausgewählt.</p> <ul style="list-style-type: none"> ■ Letzte 12 Stunden ■ Letzte 24 Stunden ■ Letzte 7 Tage ■ Letzte 30 Tage ■ Alle
Administratoren	Name des Administratorbenutzers.
Meldung	Zeigt Meldungen für einen Benutzer oder Administrator zu den von ihm durchgeführten Aktivitäten an.
Ressourcenname	Zeigt Informationen zum Namen des Desktop-Pools oder der virtuellen Maschine an, für die die Aktivität ausgeführt wurde.

Sitzungsdetails für das Horizon Help Desk Tool

Die Sitzungsdetails werden auf der Registerkarte **Details** angezeigt, wenn Sie in der Option **Computernamen** auf der Registerkarte **Sitzungen** auf den jeweiligen Benutzernamen klicken. Sie können die Details für Horizon Client, für den veröffentlichten oder virtuellen Desktop und CPU- bzw. Arbeitsspeicherdetails anzeigen.

Horizon Client

Zeigt Informationen an, die vom Horizon Client-Typ abhängig sind. Sie enthalten Details wie den Benutzernamen, die Horizon Client-Version sowie die IP-Adresse und das Betriebssystem des Clientcomputers.

Hinweis Wenn Sie für Horizon Agent ein Upgrade durchgeführt haben, müssen Sie auch Horizon Client auf die aktuelle Version aktualisieren. Andernfalls wird keine Version für Horizon Client angezeigt. Weitere Informationen zum Upgrade von Horizon Client finden Sie im Dokument *Horizon 7-Upgrades*.

VM

Zeigt Informationen zu virtuellen oder veröffentlichten Desktops an.

Tabelle 14-5. VM-Details

Option	Beschreibung
Computername	Name der Desktop- oder Anwendungssitzung.
Agent-Version	Version von Horizon Agent.
Betriebssystemversion	Betriebssystemversion.
Verbindungsserver	Der Verbindungsserver, mit dem die Sitzung verbunden ist.
Pool	Der Name des Desktop- oder Anwendungspools. Zeigt Linux für einen Linux-Desktop-Pool an.
vCenter	Die IP-Adresse von vCenter Server.
Sitzungsstatus	<p>Status der Desktop- oder Anwendungssitzung. Der Sitzungsstatus kann „Leerlauf“, „Aktiv“ oder „Verbindung getrennt“ lauten. Wenn der Benutzer eine Minute lang nicht aktiv ist, wird der Sitzungsstatus zu Leerlauf geändert. Das Statussymbol erhält eine grüne Umrandung für „Leerlauf“, wird vollständig grün für „Aktiv“ und grau für „Verbindung getrennt“.</p> <p>Hinweis Linux-Desktop-Sitzungen zeigen den Leerlauf-Status nicht an.</p>
Sitzungsdauer	Der Zeitraum, in dem die Sitzung mit dem Verbindungsserver verbunden war.
Statusdauer	Der Zeitraum, in dem für eine Sitzung ein bestimmter Status gültig war.
Anmeldezeitpunkt	Der Zeitpunkt, an dem sich der Benutzer bei der Sitzung angemeldet hat.
Anmeldedauer	Der Zeitraum, in dem der Benutzer bei der Sitzung angemeldet war.
Gateway-/Proxyname	Name des Sicherheitsservers, der Unified Access Gateway-Appliance oder des Lastausgleichsdiensts. Diese Informationen werden 30 bis 60 Sekunden nach dem Herstellen einer Verbindung mit der Sitzung angezeigt.
Gateway-/Proxy-IP	IP-Adresse des Sicherheitsservers, der Unified Access Gateway-Appliance oder des Lastausgleichsdiensts. Diese Informationen werden 30 bis 60 Sekunden nach dem Herstellen einer Verbindung mit der Sitzung angezeigt.
Farm	Die Farm von RDS-Hosts für die veröffentlichte Desktop- oder Anwendungssitzung.

Kennzahlen zur Benutzererfahrung

Zeigt Leistungsdetails für eine virtuelle oder veröffentlichte Desktop-Sitzung an, die das PCoIP- oder VMware Blast-Anzeigeprotokoll verwendet. Klicken Sie zum Anzeigen dieser Leistungsdetails auf **Mehr**. Klicken Sie zum Aktualisieren dieser Details auf das Symbol „Aktualisieren“.

Tabelle 14-6. PCoIP-Anzeigeprotokolldetails

Option	Beschreibung
TX-Bandbreite	Die Übertragungs-Bandbreite für eine PCoIP-Sitzung in Kilobits pro Sekunde.
Frame-Rate	Die Frame-Rate für eine PCoIP-Sitzung in Kilobits pro Sekunde.
Paketverlust	Prozentsatz des Paketverlusts in einer PCoIP-Sitzung.
Skype-Status	<p>Der Status von Skype for Business in einer PCoIP-Sitzung.</p> <ul style="list-style-type: none"> ■ Optimiert ■ Fallback ■ Optimiert (Versionen sind unterschiedlich) ■ Fallback (Versionen sind unterschiedlich) ■ Verbindung wird hergestellt ■ Verbindung getrennt ■ Nicht definiert <p>Diese Option wird für Linux-Desktop-Sitzungen als „Nicht verfügbar“ angezeigt.</p>

Tabelle 14-7. Blast-Anzeigeprotokolldetails

Option	Beschreibung
Frame-Rate	Die Frame-Rate für eine Blast-Sitzung in Frames pro Sekunde.
Skype-Status	<p>Der Status von Skype for Business in einer Blast-Sitzung.</p> <ul style="list-style-type: none"> ■ Optimiert ■ Fallback ■ Optimiert (Versionen sind unterschiedlich) ■ Fallback (Versionen sind unterschiedlich) ■ Verbindung wird hergestellt ■ Verbindung getrennt ■ Nicht definiert <p>Diese Option wird für Linux-Desktop-Sitzungen als „Nicht verfügbar“ angezeigt.</p>
Blast-Sitzungszähler	<ul style="list-style-type: none"> ■ Geschätzte Bandbreite (Uplink). Geschätzte Bandbreite für ein Uplink-Signal. ■ Paketverlust (Uplink). Prozentsatz des Paketverlusts für ein Uplink-Signal.
Blast-Imagezähler	<ul style="list-style-type: none"> ■ Gesendete Byte. Gesamtzahl der Bytes der Bildverarbeitungsdaten, die für eine Blast-Sitzung gesendet wurden. ■ Empfangene Byte. Gesamtzahl der Bytes der Bildverarbeitungsdaten, die für eine Blast-Sitzung empfangen wurden.

Tabelle 14-7. Blast-Anzeigeprotokolldetails (Fortsetzung)

Option	Beschreibung
Blast-Audiozähler	<ul style="list-style-type: none"> ■ Gesendete Byte. Gesamtzahl der Bytes der Audiodaten, die für eine Blast-Sitzung gesendet wurden. ■ Empfangene Byte. Gesamtzahl der Bytes der Audiodaten, die für eine Blast-Sitzung empfangen wurden.
Blast-CDR-Zähler	<ul style="list-style-type: none"> ■ Gesendete Byte. Gesamtzahl der Bytes der Daten der Clientlaufwerksumleitung, die für eine Blast-Sitzung gesendet wurden. ■ Empfangene Byte. Gesamtzahl der Bytes der Daten der Clientlaufwerksumleitung, die für eine Blast-Sitzung empfangen wurden.

CPU- und Arbeitsspeicherauslastung sowie Netzwerk- und Festplattenleistung

Zeigt Diagramme für die Auslastung von CPU und Arbeitsspeicher des virtuellen oder veröffentlichten Desktops oder der Anwendung sowie die Netzwerk- oder Festplattenleistung für das PCoIP- oder Blast-Anzeigeprotokoll an.

Hinweis Nach dem Start oder Neustart von Horizon Agent am Desktop zeigen die Leistungsdiagramme möglicherweise die Zeitachse nicht sofort an. Die Zeitachse erscheint nach wenigen Minuten.

Tabelle 14-8. CPU-Auslastung

Option	Beschreibung
Sitzungs-CPU	CPU-Auslastung der aktuellen Sitzung.
Host-CPU	CPU-Auslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.

Tabelle 14-9. Speicherauslastung

Option	Beschreibung
Sitzungsarbeitsspeicher	Arbeitsspeicherauslastung der aktuellen Sitzung.
Hostarbeitsspeicher	Arbeitsspeicherauslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.

Tabelle 14-10. Netzwerkleistung

Option	Beschreibung
Latenz	<p>Zeigt ein Diagramm der Latenz für die PCoIP- oder Blast-Sitzung an.</p> <p>Für das Blast-Anzeigeprotokoll ist die Latenzzeit die Roundtripzeit in Millisekunden. Der Leistungsindikator, der diese Latenzzeit verfolgt, ist VMware Blast-Sitzungszähler > RTT.</p> <p>Für das PCoIP-Anzeigeprotokoll ist die Latenzzeit die Roundtrip-Latenzzeit in Millisekunden. Der Leistungsindikator, der diese Latenzzeit verfolgt, ist Netzwerkstatistik für PCoIP-Sitzung > Roundtrip-Latenz.</p>

Tabelle 14-11. Festplattenleistung

Option	Beschreibung
Lesen	Die Anzahl der Eingang/Ausgang (E/A)-Lesevorgänge pro Sekunde.
Schreiben	Die Anzahl der E/A-Schreibvorgänge pro Sekunde.
Festplattenlatenz	Zeigt ein Diagramm für die Festplattenlatenz an. Die Festplattenlatenz ist die Zeit in Millisekunden der Eingang/Ausgang-Vorgänge pro Sekunde (Input/Output Operations Per Second, IOPS), die von den Windows-Leistungsindikatoren abgerufen wurden.
Durchschnittliche Lesedauer	Die durchschnittliche Anzahl der zufälligen E/A-Lesevorgänge pro Sekunde.
Durchschnittliche Schreibdauer	Die durchschnittliche Anzahl der zufälligen E/A-Schreibvorgänge pro Sekunde.
Durchschnittliche Latenz	Die durchschnittliche Latenzzeit in Millisekunden von den IOPS-Daten, die von den Windows-Leistungsindikatoren abgerufen wurden.

Segmente der Sitzungsanmeldung

Zeigt die Segmente für die Anmeldungsdauer und -nutzung an, die während der Anmeldung erstellt werden.

Tabelle 14-12. Segmente der Sitzungsanmeldung

Option	Beschreibung
Anmeldedauer	Die Anmeldedauer wird ermittelt von dem Zeitpunkt, an dem der Benutzer auf den Desktop- oder Anwendungspool klickt, bis zu dem Zeitpunkt, an dem Windows Explorer startet.
Zeitpunkt der Sitzungsanmeldung	Der Zeitraum, in dem der Benutzer bei der Sitzung angemeldet war.
Anmeldesegmente	<p>Zeigt die Segmente an, die während der Anmeldung erstellt werden.</p> <ul style="list-style-type: none"> ■ Brokering. Der gesamte Zeitraum, in dem der Verbindungsserver eine Verbindung für eine Sitzung herstellt oder trennt. Der Wert wird ermittelt von dem Zeitpunkt, an dem der Benutzer auf den Desktop-Pool klickt, bis zu dem Zeitpunkt, an dem die Tunnelverbindung eingerichtet ist. Enthält die Zeitangaben für Verbindungsserver-Vorgänge wie z. B. die Benutzerauthentifizierung, die Computerauswahl und die Computervorbereitung für die Einrichtung der Tunnelverbindung. ■ GPO laden. Der gesamte Zeitraum für die Verarbeitung der Windows-Gruppenrichtlinie. Zeigt 0 an, wenn keine globale Richtlinie konfiguriert ist. ■ Profil laden. Der gesamte Zeitraum für die Verarbeitung des Windows-Benutzerprofils. ■ Interaktiv. Der gesamte Zeitraum, in dem Horizon Agent eine Verbindung für eine Sitzung herstellt oder trennt. Der Wert wird ermittelt von dem Zeitpunkt, ab dem PCoIP oder Blast Extreme die Tunnelverbindung verwendet, bis zu dem Zeitpunkt, an dem Windows Explorer startet. ■ Protokoll der Verbindung. Gesamtzeit für die Erstellung des PCoIP- oder Blast-Protokolls der Verbindung während des Anmeldevorgangs. ■ Anmeldeskript. Gesamtzeit für die Ausführung des Anmeldeskripts vom Start bis zur Fertigstellung. ■ Authentifizierung. Gesamtzeit für den Verbindungsserver zur Authentifizierung der Sitzung. ■ Start der VM. Gesamtzeit zum Starten einer virtuellen Maschine. Dieser Zeitraum beinhaltet das Starten des Betriebssystems, das Fortsetzen einer angehaltenen Maschine und die Zeit, bis Horizon Agent signalisiert, dass es für eine Verbindung bereit ist.

Verwenden Sie die folgenden Richtlinien für die Anwendung der Informationen in Anmeldesegmenten zur Fehlerbehebung:

- Wenn es sich bei der Sitzung um eine neue Sitzung eines virtuellen Desktops handelt, werden alle Anmeldesegmente angezeigt. Wenn keine globale Richtlinie konfiguriert ist, ist die Anmeldesegmentzeit für **GPO laden** gleich 0.

- Wenn es sich bei der Sitzung eines virtuellen Desktops um eine Sitzung handelt, die nach einer Trennung erneut verbunden wurde, werden die Anmeldesegmente **Anmeldedauer**, **Interaktiv** und **Brokering** angezeigt.
- Wenn es sich bei der Sitzung um eine Sitzung eines veröffentlichten Desktops handelt, werden die Anmeldesegmente **Anmeldedauer**, **GPO laden** oder **Profil laden** angezeigt. Die Anmeldesegmente **GPO laden** und **Profil laden** werden für neue Sitzungen angezeigt. Wenn diese Anmeldesegmente für neue Sitzungen nicht eingeblendet werden, müssen Sie den RDS-Host neu starten.
- Wenn es sich bei der Sitzung um eine Linux-Desktop-Sitzung handelt, werden die Segmente **GPO laden** und **Profil laden** nicht angezeigt.
- Die Anmeldedaten sind möglicherweise nicht sofort verfügbar, wenn die Verbindung mit der Desktop-Sitzung hergestellt wird. Die Anmeldedaten erscheinen nach wenigen Minuten.

Sitzungsprozesse für das Horizon Help Desk Tool

Die Sitzungsprozesse werden auf der Registerkarte **Prozesse** angezeigt, wenn Sie in der Option **Computernamen** auf der Registerkarte **Sitzungen** auf einen Benutzernamen klicken.

Prozesse

Für jede Sitzung können Sie weitere ausführliche Informationen zu den Prozessen anzeigen, die CPU und Arbeitsspeicher betreffen. Wenn Sie feststellen, dass die CPU- und die Arbeitsspeicherauslastung für eine Sitzung ungewöhnlich hoch ist, können Sie die Details zum jeweiligen Prozess auf der Registerkarte **Prozesse** einsehen.

Für RDS-Host-Sitzungen zeigt die Registerkarte **Prozesse** die aktuellen RDS-Host-Sitzungsprozesse, die durch den aktuellen Benutzer oder den aktuellen Systemprozess gestartet wurden.

Tabelle 14-13. Sitzungsprozessdetails

Option	Beschreibung
Prozessname	Name des Sitzungsprozesses. Beispiel: chrome.exe.
CPU	CPU-Auslastung durch den Prozess in Prozent.
Arbeitsspeicher	Arbeitsspeicherauslastung durch den Prozess in KB.
Laufwerk	IOPS des Speicherdatenträgers. Wurde mit der folgenden Formel berechnet: (Gesamte E/A-Bytes zum aktuellen Zeitpunkt) – (Gesamte E/A-Bytes eine Sekunde vor dem aktuellen Zeitpunkt). Diese Berechnung kann einen Wert von 0 KB pro Sekunde ergeben, wenn im Task-Manager ein positiver Wert angezeigt wird.
Benutzername	Name des Benutzers, der für den Prozess zuständig ist.
Host-CPU	CPU-Auslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.
Hostarbeitsspeicher	Arbeitsspeicherauslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.

Tabelle 14-13. Sitzungsprozessdetails (Fortsetzung)

Option	Beschreibung
Prozesse	Anzahl der Prozesse in der virtuellen Maschine
Aktualisieren	Mit dem Symbol „Aktualisieren“ wird die Liste der Prozesse aktualisiert.
Prozess beenden	<p>Beendet einen aktuell ausgeführten Prozess.</p> <p>Hinweis Um einen Prozess beenden zu können, müssen Sie über die Rolle „Helpdesk-Administrator“ verfügen.</p> <p>Um einen Prozess zu beenden, wählen Sie diesen aus und klicken Sie auf die Schaltfläche Prozess beenden.</p> <p>Kritische Prozesse wie Windows-Kernprozesse, die unter Umständen auf der Registerkarte Prozesse aufgeführt werden, können nicht beendet werden. Wenn Sie einen kritischen Prozess beenden, zeigt Horizon Help Desk Tool eine Meldung, die besagt, dass der Systemprozess nicht beendet werden kann.</p>

Anwendungsstatus für Horizon Help Desk Tool

Der Status und die Details einer Anwendung werden auf der Registerkarte **Anwendungen** angezeigt, wenn Sie in der Option **Computername** auf der Registerkarte **Sitzungen** auf einen Benutzernamen klicken. Im Rahmen von Linux-Desktopsitzungen kann nicht auf die Registerkarte **Anwendungen** zugegriffen werden.

Anwendungen

Für jede Anwendung können Sie den aktuellen Status und weitere Details anzeigen.

Sie können einen Anwendungsprozess für den Endbenutzer beenden. Um einen Anwendungsprozess zu beenden, klicken Sie auf **Anwendung beenden** und dann auf **OK**, um die Änderung zu bestätigen.

Hinweis Das Beenden des Anwendungsprozesses kann fehlschlagen, wenn bei der Anwendung eine Benutzerinteraktion, z. B. nicht gespeicherte Daten, aussteht oder andere Ausnahmen vorliegen. Allerdings wird von Horizon Help Desk Tool keine Erfolgs- oder Fehlermeldung angezeigt, wenn Sie eine Anwendung beenden.

Tabelle 14-14. Anwendungsdetails

Option	Beschreibung
Anwendung	Name der Anwendung.
Beschreibung	Beschreibung der Anwendung.
Status	Status der Anwendung. Zeigt an, ob die Anwendung ausgeführt wird.
Host-CPU	CPU-Auslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.

Tabelle 14-14. Anwendungsdetails (Fortsetzung)

Option	Beschreibung
Hostarbeitsspeicher	Arbeitsspeicherauslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.
Anwendungen	Liste der ausgeführten Anwendungen.
Aktualisieren	Mit dem Symbol „Aktualisieren“ wird die Liste der Anwendungen aktualisiert.

Fehlerbehebung bei Desktop- oder Anwendungssitzungen in Horizon Help Desk Tool

Sie können in Horizon Help Desk Tool Fehlerbehebungen für Desktop- oder Anwendungssitzungen basierend auf dem Verbindungsstatus eines Benutzers durchführen.

Voraussetzungen

- Starten Sie Horizon Help Desk Tool.

Verfahren

- 1 Klicken Sie auf der Benutzerkarte auf die Registerkarte **Sitzungen**.

Eine Karte mit Leistungsinformationen wird angezeigt, die die CPU- sowie die Arbeitsspeicherauslastung und Informationen zu Horizon Client sowie zum virtuellen oder veröffentlichten Desktop enthält.

2 Wählen Sie eine Option für die Fehlerbehebung aus.

Option	Aktion
Nachricht senden	<p>Sendet eine Nachricht an den Benutzer auf dem veröffentlichten oder virtuellen Desktop. Sie können den Schweregrad der Nachricht durch Angabe von „Warnung“, „Info“ oder „Fehler“ auswählen.</p> <p>Klicken Sie auf Nachricht senden, geben Sie den Schweregrad und die Nachrichtendetails ein und klicken Sie auf Absenden.</p>
Remoteunterstützung	<p>Sie können Tickets für eine Remoteunterstützung für verbundene Desktop- oder Anwendungssitzungen generieren. Administratoren haben die Möglichkeit, mit dem Ticket für die Remoteunterstützung die Desktop-Probleme des Benutzers und die Fehlerbehebung zu steuern.</p> <p>Hinweis Diese Funktion ist für Linux-Desktop-Benutzer nicht verfügbar.</p> <p>Klicken Sie auf Remoteunterstützung und laden Sie die Helpdesk-Ticket-Datei herunter. Öffnen Sie das Ticket und warten Sie, bis es vom Benutzer auf dem Remote-Desktop akzeptiert wird. Sie können das Ticket nur auf einem Windows-Desktop öffnen. Nachdem der Benutzer das Ticket akzeptiert hat, können Sie mit dem Benutzer einen Chat starten und die Steuerung des Benutzer-Desktops anfordern.</p> <p>Hinweis Die Funktion der Helpdesk-Remoteunterstützung basiert auf der Microsoft-Remoteunterstützung. Sie müssen die Microsoft-Remoteunterstützung installieren und die Funktion der Remoteunterstützung auf dem veröffentlichten Desktop aktivieren. Die Helpdesk-Remoteunterstützung startet eventuell nicht, wenn bei der Microsoft-Remoteunterstützung Probleme mit der Verbindung oder mit dem Upgrade bestehen. Weitere Informationen finden Sie in der Dokumentation zur Microsoft-Remoteunterstützung auf der Microsoft-Website.</p>
Neustarten	<p>Initiiert den Windows-Neustart auf dem virtuellen Desktop. Diese Funktion ist nicht für Sitzungen veröffentlichter Desktops oder Anwendungen verfügbar.</p> <p>Klicken Sie auf VDI neu zu starten.</p>
Verbindung trennen	<p>Trennt die Desktop- oder Anwendungssitzung.</p> <p>Klicken Sie auf Mehr > Trennen.</p>
Abmelden	<p>Initiiert den Abmeldevorgang für einen veröffentlichten bzw. virtuellen Desktop oder den Abmeldevorgang für eine Anwendungssitzung.</p> <p>Klicken Sie auf Mehr > Abmelden.</p>
Zurücksetzen	<p>Initiiert das Zurücksetzen der virtuellen Maschine. Diese Funktion ist nicht für Sitzungen veröffentlichter Desktops oder Anwendungen verfügbar.</p> <p>Klicken Sie auf Mehr > VM zurücksetzen.</p> <p>Hinweis Nicht gespeicherte Änderungen des Benutzers können verloren gehen.</p>

Verwenden des Befehls „vdmadmin“

15

Über die Befehlszeilenschnittstelle `vdmadmin` kann eine Vielzahl von Verwaltungsaufgaben für eine Verbindungsserver-Instanz ausgeführt werden.

Mithilfe von `vdmadmin` ist das Ausführen von Verwaltungsaufgaben möglich, die nicht über die Benutzeroberfläche ausgeführt werden können oder die automatisch über Skripts ausgeführt werden müssen.

- **Verwendung des Befehls „vdmadmin“**

Die Syntax des Befehls `vdmadmin` bestimmt seine Ausführung.

- **Konfigurieren der Protokollierung in Horizon Agent mithilfe der Option „-A“**

Sie können mit dem Befehl `vdmadmin` mit der Option `-A` die Protokollierung durch Horizon Agent konfigurieren.

- **Außerkräftsetzen von IP-Adressen mithilfe der Option „-A“**

Sie können den Befehl `vdmadmin` mit der Option `-A` verwenden, um die von einer Horizon Agent-Instanz angegebene IP-Adresse außer Kraft zu setzen.

- **Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F“**

Mithilfe des Befehls `vdmadmin` können über die Option `-F` die fremden Sicherheitsprinzipale (Foreign Security Principals, FSPs) von Windows-Benutzern in Active Directory aktualisiert werden, die für die Verwendung eines Desktops berechtigt sind.

- **Auflisten und Anzeigen von Systemüberwachungen mithilfe der Option „-H“**

Mithilfe der Option `-H` des Befehls `vdmadmin` können die vorhandenen Systemüberwachungen angezeigt werden, um Instanzen für Horizon 7-Komponenten zu überwachen und die Einzelheiten für eine bestimmte Systemüberwachung oder eine bestimmte Überwachungsinstanz anzuzeigen.

- **Auflisten und Anzeigen von Berichten zum Horizon 7-Betrieb unter Verwendung der Option „-I“**

Sie können den Befehl `vdmadmin` mit der Option `-I` verwenden, um die verfügbaren Berichte zum Horizon 7-Betrieb aufzulisten und die Ergebnisse beim Ausführen eines dieser Berichte anzuzeigen.

- **Generieren von Horizon 7-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-I“**

Sie können den Befehl `vdadmin` zusammen mit der Option `-I` verwenden, um Horizon 7-Ereignismeldungen in den Ereignisprotokolldateien im Format Syslog aufzuzeichnen. Viele Analyseprodukte von Drittanbietern erfordern Flatfile-Syslog-Daten als Eingabe für die Analysevorgänge.

- **Zuweisen von dedizierten Computern unter Verwendung der Option „-L“**

Mithilfe des Befehls `vdadmin` können Sie über die Option `-L` Benutzern Computer aus einem dedizierten Pool zuweisen.

- **Anzeigen von Informationen zu Maschinen mithilfe der Option „-M“**

Sie können den Befehl `vdadmin` mit der Option `-M` verwenden, um Informationen zur Konfiguration virtueller Maschinen oder physischer Computer anzuzeigen.

- **Rückgewinnung von Datenträgerplatz auf virtuellen Maschinen mithilfe der Option „-M“**

Sie können den Befehl `vdadmin` zusammen mit der Option `-M` verwenden, um eine virtuelle Linked-Clone-Maschine für die Rückgewinnung von Datenträgerplatz zu markieren. Horizon 7 weist den ESXi-Host an, Datenträgerplatz auf der Linked-Clone-Betriebssystemfestplatte zurückzugewinnen, ohne darauf zu warten, dass der ungenutzte Platz auf der Betriebssystemfestplatte den maximalen Grenzwert erreicht, der in Horizon Administrator angegeben ist.

- **Konfigurieren von Domänenfiltern mithilfe der Option „-N“**

Sie können den Befehl `vdadmin` mit der Option `-N` zum Steuern der Domänen verwenden, die Horizon 7 für die Endbenutzer zur Verfügung stellt.

- **Konfigurieren von Domänenfiltern**

Domänenfilter können Sie zur Einschränkung der Anzahl der Domänen, die eine Verbindungsserver-Instanz oder ein Sicherheitsserver den Endbenutzern zur Verfügung stellt, konfigurieren.

- **Anzeigen der Maschinen und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“**

Sie können den Befehl `vdadmin` mit den Optionen `-O` und `-P` verwenden, um die virtuellen Maschinen und Richtlinien von Benutzern anzuzeigen, die nicht länger zur Verwendung des Systems berechtigt sind.

- **Konfigurieren von Clients im Kiosk-Modus mithilfe der Option „-Q“**

Unter Verwendung des Befehls `vdadmin` mit der Option `-Q` können Standardwerte festgelegt und Konten für Clients im Kiosk-Modus erstellt werden, um die Authentifizierung für diese Clients zu aktivieren und Informationen zu ihrer Konfiguration anzuzeigen.

- **Anzeigen des ersten Benutzers einer Maschine mithilfe der Option „-R“**

Sie können den Befehl `vdadmin` mit der Option `-R` verwenden, um die anfängliche Zuweisung einer verwalteten virtuellen Maschine zu ermitteln. Bei Verlust von LDAP-Daten wird diese Information z. B. möglicherweise benötigt, um eine Neuzuweisung von virtuellen Maschinen zu Benutzern durchzuführen.

- [Entfernen des Eintrags für eine Verbindungsserver-Instanz oder einen Sicherheitsserver mithilfe der Option „-S“](#)

Sie können den Befehl `vdmadmin` mit der Option `-S` verwenden, um den Eintrag für eine Verbindungsserver-Instanz oder einen Sicherheitsserver aus der Horizon 7-Konfiguration zu entfernen.

- [Bereitstellen sekundärer Anmeldeinformationen für Administratoren mithilfe der Option „-T“](#)

Sie können mithilfe des `vdmadmin`-Befehls und der `-T`-Option sekundäre Active Directory-Anmeldeinformationen für Administrationsbenutzer bereitstellen.

- [Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U“](#)

Sie können den Befehl `vdmadmin` mit der Option `-U` verwenden, um detaillierte Informationen zu Benutzern anzuzeigen.

- [Entsperren oder Sperren von virtuellen Maschinen mithilfe der Option „-V“](#)

Sie können den Befehl `vdmadmin` mit der Option `-V` verwenden, um virtuelle Maschinen im Datacenter zu sperren oder zu entsperren.

- [Ermitteln und Lösen von Konflikten bei LDAP-Einträgen und LDAP-Schemas mithilfe der Option „-X“](#)

Sie können den Befehl `vdmadmin` mit der Option `-X` verwenden, um Konflikte bei LDAP-Einträgen und LDAP-Schemas auf replizierten Verbindungsserver-Instanzen in einer Gruppe zu ermitteln und zu lösen. Mit dieser Option lassen sich auch LDAP-Schemakonflikte in einer Cloud-Pod-Architektur-Umgebung ermitteln und lösen.

Verwendung des Befehls „vdmadmin“

Die Syntax des Befehls `vdmadmin` bestimmt seine Ausführung.

Verwenden Sie den Befehl `vdmadmin` an einer Windows-Eingabeaufforderung mit dem folgenden Format.

```
vdmadmin Befehlsoption [Zusatzoption Argument] ...
```

Welche Zusatzoptionen verwendet werden können, hängt von der Befehlsoption ab.

Der Pfad zur ausführbaren Datei des Befehls `vdmadmin` lautet standardmäßig `C:\Programme\VMware\VMware View\Server\tools\bin`. Damit Sie den Pfad nicht in die Befehlszeile eingeben müssen, fügen Sie diesen zur Umgebungsvariable `PATH` hinzu.

- [Authentifizierung für den Befehl „vdmadmin“](#)

Um eine angegebene Aktion erfolgreich auszuführen, muss der Befehl `vdmadmin` als Benutzer mit der Rolle **Administrators (Administratoren)** ausgeführt werden.

- [Ausgabeformat des Befehls „vdmadmin“](#)

Bei einigen Optionen des Befehls `vdmadmin` können Sie das Format der Ausgabeinformationen angeben.

■ Optionen des Befehls „vdmadmin“

Über die Befehlsoptionen des Befehls `vdmadmin` wird der Vorgang angegeben, der ausgeführt werden soll.

Authentifizierung für den Befehl „vdmadmin“

Um eine angegebene Aktion erfolgreich auszuführen, muss der Befehl `vdmadmin` als Benutzer mit der Rolle **Administrators (Administratoren)** ausgeführt werden.

Sie können einem Benutzer die Rolle **Administratoren** mithilfe von Horizon Administrator zuweisen. Siehe [#unique_9](#).

Wenn Sie als Benutzer ohne ausreichende Berechtigungen angemeldet sind, können Sie die Option `-b` verwenden, um den Befehl als Benutzer mit der Rolle **Administrators (Administratoren)** auszuführen. Voraussetzung dafür ist, dass Sie das Kennwort dieses Benutzers kennen. Sie können die Option `-b` angeben, um den Befehl `vdmadmin` als der angegebene Benutzer in der angegebenen Domäne auszuführen. Für die Option `-b` gelten folgende äquivalente Verwendungsmöglichkeiten:

```
-b
Benutzername
Domäne [Kennwort | *]
```

```
-b
Benutzername@Domäne [Kennwort | *]
```

```
-b
Domäne\Benutzername [Kennwort | *]
```

Wenn Sie ein Sternchen (*) anstelle eines Kennworts festlegen, werden Sie zur Eingabe des Kennworts aufgefordert und der `vdmadmin`-Befehl hinterlässt keine sensitiven Kennwörter in der Befehlszeilenhistorie.

Mit Ausnahme der Optionen `-b` und `-R` kann die Option `-T` mit sämtlichen Befehlsoptionen verwendet werden.

Ausgabeformat des Befehls „vdmadmin“

Bei einigen Optionen des Befehls `vdmadmin` können Sie das Format der Ausgabeinformationen angeben.

Die folgende Tabelle zeigt einige Optionen des Befehls `vdmadmin` für die Ausgabeformatierung.

Tabelle 15-1. Optionen für die Auswahl des Ausgabeformats

Option	Beschreibung
-csv	Formatiert die Ausgabe als kommagetrennte Werte.
-n	Zeigt die Ausgabe unter Verwendung von ASCII (UTF-8)-Zeichen an. Dies ist der Standardzeichensatz für kommagetrennte Werte und Ausgaben im Textformat.
-w	Zeigt die Ausgabe unter Verwendung von Unicode (UTF-16)-Zeichen an. Dies ist der Standardzeichensatz für XML-Ausgaben.
-xml	Formatiert die Ausgabe als XML.

Optionen des Befehls „vdmadmin“

Über die Befehlsoptionen des Befehls `vdmadmin` wird der Vorgang angegeben, der ausgeführt werden soll.

Die folgende Tabelle zeigt die Befehlsoptionen, die Sie mit dem Befehl `vdmadmin` zum Steuern und Untersuchen des Betriebs von Horizon 7 verwenden können.

Tabelle 15-2. Optionen des Befehls „vdmadmin“

Option	Beschreibung
-A	Verwaltet die von Horizon Agent in seinen Protokolldateien aufgezeichneten Informationen. Siehe Konfigurieren der Protokollierung in Horizon Agent mithilfe der Option „-A“ . Überschreibt die von Horizon Agent übermittelte IP-Adresse. Siehe Außerkräftsetzen von IP-Adressen mithilfe der Option „-A“ .
-C	Legt den Namen einer Verbindungsserver-Gruppe fest. Siehe #unique_186 .
-F	Aktualisiert die fremden Sicherheitsprinzipale (FSPs) in Active Directory für alle oder die angegebenen Benutzer. Siehe Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F“ .
-H	Zeigt Informationen zum Zustand für Horizon 7-Dienste an. Siehe Auflisten und Anzeigen von Systemüberwachungen mithilfe der Option „-H“ .
-I	Generiert Berichte zu Horizon 7-Vorgängen. Siehe Auflisten und Anzeigen von Berichten zum Horizon 7-Betrieb unter Verwendung der Option „-I“ .
-L	Weist einem Benutzer einem dedizierten Desktop zu oder entfernt eine solche Zuweisung. Siehe Zuweisen von dedizierten Computern unter Verwendung der Option „-L“ .
-M	Zeigt Informationen zu einer virtuellen Maschine oder einem physischen Computer an. Siehe Anzeigen von Informationen zu Maschinen mithilfe der Option „-M“ .
-N	Konfiguriert die Domänen, die eine Verbindungsserver-Instanz oder -Gruppe für Horizon Client verfügbar macht. Siehe Konfigurieren von Domänenfiltern mithilfe der Option „-N“ .
-O	Zeigt die Remote-Desktops an, die Benutzern zugewiesen sind, die nicht länger über Berechtigungen für diese Desktops verfügen. Siehe Anzeigen der Maschinen und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“ .
-P	Zeigt die Benutzerrichtlinien für Remote-Desktops von Benutzern an, die nicht über Berechtigungen verfügen. Siehe Anzeigen der Maschinen und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“ .

Tabelle 15-2. Optionen des Befehls „vdmadmin“ (Fortsetzung)

Option	Beschreibung
-Q	Konfiguriert das Konto in Active Directory und in Horizon 7 ein Client-Gerät im Kiosk-Modus. Siehe Konfigurieren von Clients im Kiosk-Modus mithilfe der Option „-Q“ .
-R	Gibt den ersten Benutzer an, der auf einen Remote-Desktop zugegriffen hat. Siehe Anzeigen des ersten Benutzers einer Maschine mithilfe der Option „-R“ .
-S	Entfernt einen Konfigurationseintrag für eine Verbindungsserver-Instanz aus der Konfiguration von Horizon 7. Siehe Entfernen des Eintrags für eine Verbindungsserver-Instanz oder einen Sicherheitsserver mithilfe der Option „-S“ .
-T	Stellt die sekundären Active Directory-Anmeldeinformationen für Administratorbenutzer bereit. Siehe Bereitstellen sekundärer Anmeldeinformationen für Administratoren mithilfe der Option „-T“ .
-U	Zeigt Informationen zu einem Benutzer an, einschließlich Remote-Desktop-Berechtigungen und ThinApp-Zuweisungen sowie Administratorrollen. Siehe Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U“ .
-V	Entsperrt oder sperrt virtuelle Maschinen. Siehe Entsperren oder Sperren von virtuellen Maschinen mithilfe der Option „-V“ .
-X	Ermittelt und löst Konflikte bei LDAP-Einträgen auf replizierten Verbindungsserver-Instanzen. Siehe Ermitteln und Lösen von Konflikten bei LDAP-Einträgen und LDAP-Schemas mithilfe der Option „-X“ .

Konfigurieren der Protokollierung in Horizon Agent mithilfe der Option „-A“

Sie können mit dem Befehl `vdmadmin` mit der Option `-A` die Protokollierung durch Horizon Agent konfigurieren.

Syntax

```
vdadmin
-A [-b authentication_arguments] -getDCT-outfile local_file -d desktop -m machine
```

```
vdadmin
-A [-b authentication_arguments] -getlogfile logfile-outfile local_file -d desktop -m machine
```

```
vdadmin
-A [-b authentication_arguments] -getloglevel [-xml] -d desktop [-m machine]
```

```
vdadmin
-A [-b authentication_arguments] -getstatus [-xml] -d desktop [-m machine]
```

```
vdadmin
-A [-b authentication_arguments] -getversion [-xml] -d desktop [-m machine]
```

```
vdadmin
-A [-b authentication_arguments] -list [-xml] [-w | -n] -d desktop -m machine
```

```
vdadmin
-A [-b authentication_arguments] -setloglevel level -d desktop [-m machine]
```

Nutzungshinweise

Um den technischen Support von VMware bei der Fehlerbehebung für Horizon Agent zu unterstützen, können Sie ein DCT-Paket (Data Collection Tool) erstellen. Darüber hinaus können Sie die Protokollierungsebene ändern, die Version und den Status von Horizon Agent anzeigen und einzelne Protokolldateien auf der lokalen Festplatte speichern.

Optionen

Die folgende Tabelle zeigt die verfügbaren Optionen zum Konfigurieren der Protokollierung in Horizon Agent.

Tabelle 15-3. Optionen zum Konfigurieren der Protokollierung in Horizon Agent

Option	Beschreibung
-d Desktop	Gibt den Desktop-Pool an.
-getDCT	Erstellt ein DCT-Paket (Data Collection Tool) und speichert es in einer lokalen Datei.

Tabelle 15-3. Optionen zum Konfigurieren der Protokollierung in Horizon Agent (Fortsetzung)

Option	Beschreibung
<code>-getlogfile <i>Protokolldatei</i></code>	Gibt den Namen der Protokolldatei an, für die eine Kopie gespeichert werden soll.
<code>-getloglevel</code>	Zeigt die aktuelle Protokollierungsebene von Horizon Agent an.
<code>-getstatus</code>	Zeigt den Status von Horizon Agent an.
<code>-getversion</code>	Zeigt die Version von Horizon Agent an.
<code>-list</code>	Listet die Protokolldateien für Horizon Agent auf.
<code>-m <i>Computer</i></code>	Gibt die Maschine innerhalb eines Desktop-Pools an.
<code>-outfile <i>lokale_Datei</i></code>	Gibt den Namen der lokalen Datei an, in der ein DCT-Paket oder die Kopie einer Protokolldatei gespeichert werden soll.
<code>-setloglevel <i>Ebene</i></code>	Legt die Protokollierungsebene von Horizon Agent fest. <div> <div>debug</div> <div>Protokolliert Fehler-, Warnungs- und Debugging-Ereignisse.</div> </div> <div> <div>normal</div> <div>Protokolliert Fehler- und Warnungsereignisse.</div> </div> <div> <div>trace</div> <div>Protokolliert Fehler-, Informations- und Debugging-Ereignisse.</div> </div>

Beispiele

Zeigen Sie die Protokollierungsebene von Horizon Agent für die Maschine „machine1“ im Desktop-Pool „dtpool2“ an.

```
vdadmin -A -d dtpool2 -m machine1 -getloglevel
```

Legen Sie die Protokollierungsebene von Horizon Agent für die Maschine „machine1“ im Desktop-Pool „dtpool2“ fest.

```
vdadmin -A -d dtpool2 -m machine1 -setloglevel debug
```

Zeigen Sie die Liste der Horizon Agent-Protokolldateien für die Maschine „machine1“ im Desktop-Pool „dtpool2“ an.

```
vdadmin -A -d dtpool2 -m machine1 -list
```

Speichern Sie eine Kopie der Horizon Agent-Protokolldatei `log-2009-01-02.txt` für die Maschine „machine1“ im Desktop-Pool „dtpool2“ unter dem Namen `C:\mycopiedlog.txt`.

```
vdadmin -A -d dtpool2 -m machine1 -getlogfile log-2009-01-02.txt -outfile C:\mycopiedlog.txt
```

Zeigen Sie die Version von Horizon Agent für die Maschine „machine1“ im Desktop-Pool „dtpool2“ an.

```
vdmadmin -A -d dtpool2 -m machine1 -getversion
```

Zeigen Sie den Status von Horizon Agent für die Maschine „machine1“ im Desktop-Pool „dtpool2“ an.

```
vdmadmin -A -d dtpool2 -m machine1 -getstatus
```

Erstellen Sie das DCT-Paket für die Maschine „machine1“ im Desktop-Pool „dtpool2“ und schreiben Sie es in die .zip-Datei C:\myfile.zip.

```
vdmadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

Außerkräftsetzen von IP-Adressen mithilfe der Option „-A“

Sie können den Befehl `vdmadmin` mit der Option `-A` verwenden, um die von einer Horizon Agent-Instanz angegebene IP-Adresse außer Kraft zu setzen.

Syntax

```
vdmadmin
-A [-bauthentication_arguments] -override-ip_or_dns-ddesktop-mmachine
```

```
vdmadmin
-A [-bauthentication_arguments] -override-list-ddesktop-mmachine
```

```
vdmadmin
-A [-bauthentication_arguments] -override-r-ddesktop [-mmachine]
```

Nutzungshinweise

Eine Horizon Agent-Instanz gibt die ermittelte IP-Adresse der Maschine, auf der sie ausgeführt wird, an die Verbindungsserver-Instanz zurück. In sicheren Konfigurationen, in denen die Verbindungsserver-Instanz den von der Horizon Agent-Instanz bereitgestellten Wert nicht als vertrauenswürdig einstuft, können Sie den von der Horizon Agent-Instanz bereitgestellten Wert außer Kraft setzen und die IP-Adresse festlegen, welche die verwaltete Maschine verwenden soll. Wenn die von der Horizon Agent-Instanz angegebene Adresse einer Maschine nicht mit der definierten Adresse übereinstimmt, kann nicht über Horizon Client auf die Maschine zugegriffen werden.

Optionen

Die folgende Tabelle zeigt die verfügbaren Optionen zum Außerkräftsetzen von IP-Adressen.

Tabelle 15-4. Optionen für das Außerkraftsetzen von IP-Adressen

Option	Beschreibung
<code>-d Desktop</code>	Gibt den Desktop-Pool an.
<code>-i IP_oder_DNS</code>	Gibt die IP-Adresse oder den auflösbaren Domännennamen in DNS an.
<code>-m Computer</code>	Gibt den Namen der Maschine in einem Desktop-Pool an.
<code>-override</code>	Gibt einen Vorgang zum Außerkraftsetzen von IP-Adressen an.
<code>-r</code>	Entfernt eine außer Kraft gesetzte IP-Adresse.

Beispiele

Setzen Sie die IP-Adresse für die Maschine `machine2` im Desktop-Pool `dtpool2` außer Kraft.

```
vdadmin -A -override -i 10.20.54.165 -d dtpool2 -m machine2
```

Zeigen Sie die IP-Adressen an, die für die Maschine `machine2` im Desktop-Pool `dtpool2` definiert wurden.

```
vdadmin -A -override -list -d dtpool2 -m machine2
```

Entfernen Sie die IP-Adressen, die für die Maschine `machine2` im Desktop-Pool `dtpool2` definiert wurden.

```
vdadmin -A -override -r -d dtpool2 -m machine2
```

Entfernen Sie die IP-Adressen, die für die Desktops im Desktop-Pool `dtpool3` definiert wurden.

```
vdadmin -A -override -r -d dtpool3
```

Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F“

Mithilfe des Befehls `vdadmin` können über die Option `-F` die fremden Sicherheitsprinzipale (Foreign Security Principals, FSPs) von Windows-Benutzern in Active Directory aktualisiert werden, die für die Verwendung eines Desktops berechtigt sind.

Syntax

```
vdadmin
-F [-bauthentication_arguments] [-udomain\user]
```

Nutzungshinweise

Wenn Sie Domänen außerhalb Ihrer lokalen Domänen als vertrauenswürdig einstufen, lassen Sie den Zugriff auf die Ressourcen der lokalen Domänen durch Sicherheitsprinzipale in den externen Domänen zu. In Active Directory werden Sicherheitsprinzipale in vertrauenswürdigen externen Domänen durch fremde Sicherheitsprinzipale repräsentiert. Wenn Sie die Liste der vertrauenswürdigen externen Domänen ändern, kann die Aktualisierung der fremden Sicherheitsprinzipale erforderlich sein.

Options (Optionen)

Die Option `-u` gibt den Namen und die Domäne des Benutzers an, dessen FSP aktualisiert werden soll. Wenn Sie diese Option nicht festlegen, werden über den Befehl die FSPs aller Benutzer in Active Directory aktualisiert.

Beispiele

Aktualisieren Sie den fremden Sicherheitsprinzipal des Benutzers **Jim** in der Domäne **EXTERNAL**.

```
vdadmin -F -u EXTERNAL\Jim
```

Aktualisieren Sie die fremden Sicherheitsprinzipale aller Benutzer in Active Directory.

```
vdadmin -F
```

Auflisten und Anzeigen von Systemüberwachungen mithilfe der Option „-H“

Mithilfe der Option `-H` des Befehls `vdadmin` können die vorhandenen Systemüberwachungen angezeigt werden, um Instanzen für Horizon 7-Komponenten zu überwachen und die Einzelheiten für eine bestimmte Systemüberwachung oder eine bestimmte Überwachungsinstanz anzuzeigen.

Syntax

```
vdadmin
-H [-b Authentifizierungsargumente] -list-xml [-w | -n]
```

```
vdadmin
-H [-b Authentifizierungsargumente] -list-monitorid Monitor-ID -xml [-w | -n]
```

```
vdadmin
-H [-b Authentifizierungsargumente] -monitorid Monitor-ID -instanceid Instanz-ID -xml [-w | -n]
```


Nutzungshinweise

Die folgende Tabelle zeigt die von Horizon 7 hinsichtlich des Zustands der Komponenten verwendeten Systemüberwachungen.

Tabelle 15-5. Systemüberwachungen

Überwachungsfunktion	Beschreibung
CBMonitor	Überwacht den Zustand von Verbindungsserver-Instanzen.
DBMonitor	Überwacht den Zustand der Ereignisdatenbank.
DomainMonitor	Überwacht den Zustand der lokalen Domäne und aller vertrauenswürdigen Domänen des Verbindungsserver-Hosts.
SGMonitor	Überwacht den Zustand von Sicherheits-Gateway-Diensten und Sicherheitsservern.
VCMonitor	Überwacht den Zustand von vCenter Server-Instanzen.

Wenn eine Komponente über mehrere Instanzen verfügt, erstellt Horizon 7 eine separate Überwachungsinstanz für die Überwachung jeder einzelnen Komponenteninstanz.

Der Befehl gibt sämtliche Informationen zu Systemüberwachungen und Überwachungsinstanzen im XML-Format aus.

Optionen

Die folgende Tabelle zeigt die verfügbaren Optionen zum Auflisten und Anzeigen von Systemüberwachungen.

Tabelle 15-6. Optionen für das Auflisten und Anzeigen von Systemüberwachungen

Option	Beschreibung
<code>-instanceid <i>Instanzen-ID</i></code>	Gibt eine Systemüberwachungsinstanz an.
<code>-list</code>	Zeigt die vorhandenen Systemüberwachungen an, wenn keine Systemüberwachungs-ID angegeben wird.
<code>-list -monitorid <i>Monitor-ID</i></code>	Zeigt die Überwachungsinstanzen für die angegebene Systemüberwachungs-ID an.
<code>-monitorid <i>Monitor-ID</i></code>	Gibt eine Systemüberwachungs-ID an.

Beispiele

Listen Sie alle vorhandenen Systemüberwachungen im XML-Format mit Unicode-Zeichen auf.

```
vdadmin -H -list -xml
```

Listen Sie alle Instanzen der vCenter-Überwachung (VCMonitor) im XML-Format mit ASCII-Zeichen auf.

```
vdadmin -H -list -monitorid VCMonitor -xml -n
```

Zeigen Sie den Zustand einer angegebenen vCenter-Überwachungsinstanz an.

```
vdmin -H -monitorid VCMonitor -instanceid 4aec2c99-4879-96b2-de408064d035 -xml
```

Auflisten und Anzeigen von Berichten zum Horizon 7-Betrieb unter Verwendung der Option „-l“

Sie können den Befehl `vdmin` mit der Option `-l` verwenden, um die verfügbaren Berichte zum Horizon 7-Betrieb aufzulisten und die Ergebnisse beim Ausführen eines dieser Berichte anzuzeigen.

Syntax

```
vdmin
-l [-b Authentifizierungsargumente] -list [-xml] [-w | -n]
```

```
vdmin
-l [-b Authentifizierungsargumente] -report Bericht -view Ansicht [-startdate JJJJ-MM-TT-HH:mm:ss] [-enddate JJJJ-MM-TT-HH:mm:ss] [-w | -n] -xml | -csv
```

Nutzungshinweise

Sie können den Befehl zum Anzeigen der verfügbaren Berichte und Ansichten sowie zum Anzeigen der Informationen verwenden, die Horizon 7 für einen angegebenen Bericht oder eine angegebene Ansicht aufgezeichnet hat.

Sie können den Befehl `vdmin` auch mit der Option `-l` verwenden, um Horizon 7-Protokollmeldungen im `syslog`-Format zu erzeugen. Siehe [Generieren von Horizon 7-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-l“](#).

Optionen

Die folgende Tabelle zeigt die verfügbaren Optionen zum Auflisten und Anzeigen von Berichten und Ansichten.

Tabelle 15-7. Optionen für das Auflisten und Anzeigen von Berichten und Ansichten

Option	Beschreibung
<code>-enddate jjjj-MM-tt-HH:mm:ss</code>	Gibt das Enddatum des Zeitraums an, für den Informationen angezeigt werden sollen.
<code>-list</code>	Zeigt eine Liste der verfügbaren Berichte und Ansichten an.
<code>-report Bericht</code>	Gibt einen Bericht an.
<code>-startdate jjjj-MM-tt-HH:mm:ss</code>	Gibt das Startdatum des Zeitraums an, für den Informationen angezeigt werden sollen.
<code>-view Ansicht</code>	Gibt eine Ansicht an.

Beispiele

Listen Sie die verfügbaren Berichte und Ansichten im XML-Format mit Unicode-Zeichen auf.

```
vdadmin -I -list -xml -w
```

Zeigen Sie eine Liste der Benutzerereignisse seit dem 1. August 2010 im CSV-Format mit ASCII-Zeichen an.

```
vdadmin -I -report events -view user_events -startdate 2010-08-01-00:00:00 -csv -n
```

Generieren von Horizon 7-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-I“

Sie können den Befehl `vdadmin` zusammen mit der Option `-I` verwenden, um Horizon 7-Ereignismeldungen in den Ereignisprotokolldateien im Format SysLog aufzuzeichnen. Viele Analyseprodukte von Drittanbietern erfordern Flatfile-SysLog-Daten als Eingabe für die Analysevorgänge.

Syntax

```
vdadmin
-I
-eventSyslog
-disable
```

```
vdadmin
-I
-eventSyslog
-enable
-localOnly
```

```
vdadmin
-I
-eventSyslog
-enable
-path
Pfad
```

```
vdadmin
-I
-eventSyslog
-enable
-path
```

```

Pfad
-user
Domänenname\Benutzername
-password
Kennwort

```

Nutzungshinweise

Sie können den Befehl verwenden, um Horizon 7-Ereignisprotokollmeldungen im Syslog-Format zu generieren. Horizon 7-Ereignisprotokollmeldungen werden in einer Syslog-Datei in Schlüssel-Wert-Paaren formatiert, sodass die Protokolldaten für Analysesoftware zugänglich wird.

Sie können auch den Befehl `vdadmin` zusammen mit der Option `-I` verwenden, um die verfügbaren Berichte und Ansichten aufzulisten sowie die Inhalte eines bestimmten Berichts anzuzeigen. Siehe [Auflisten und Anzeigen von Berichten zum Horizon 7-Betrieb unter Verwendung der Option „-I“](#).

Optionen

Sie können die Option `eventSyslog` deaktivieren oder aktivieren. Sie können die Syslog-Ausgabe auf das lokale System oder an einen anderen Ort lenken. In Horizon 7 5.2 oder höher wird eine direkte UDP-Verbindung zu einem Syslog-Server unterstützt. Weitere Informationen finden Sie unter „Konfigurieren der Ereignisprotokollierung für Syslog-Server“ im Dokument *Horizon 7-Installation*.

Tabelle 15-8. Optionen zum Generieren von Horizon 7-Ereignisprotokollmeldungen im Syslog-Format

Option	Beschreibung
<code>-disable</code>	Deaktiviert die Syslog-Protokollierung.
<code>-e -enable</code>	Aktiviert die Syslog-Protokollierung.
<code>-eventSyslog</code>	Gibt an, dass Horizon 7-Ereignisse im Syslog-Format generiert werden.
<code>-localOnly</code>	Speichert die Syslog-Ausgabe nur auf dem lokalen System. Wenn Sie die Option <code>-localOnly</code> verwenden, lautet das Standardziel der Syslog-Ausgabe <code>%PROGRAMDATA%\VMware\VDM\events\</code> .
<code>-password Kennwort</code>	Gibt das Kennwort für den Benutzer an, der den Zugriff auf den angegebenen Zielpfad für die Syslog-Ausgabe autorisiert.
<code>-path</code>	Legt den Ziel-UNC-Pfad für die Syslog-Ausgabe fest.
<code>-u -user Domänenname\Benutzername</code>	Gibt die Domäne und den Benutzernamen an, die bzw. der auf den Zielpfad für die Syslog-Ausgabe zugreifen kann.

Beispiele

Deaktivieren der Generierung von Horizon 7-Ereignissen im Syslog-Format:

```
vdadmin -I -eventSyslog -disable
```

Leiten der Syslog-Ausgabe von Horizon 7-Ereignissen nur auf das lokale System:

```
vdadmin -I -eventSyslog -enable -localOnly
```

Leiten der Syslog-Ausgabe von Horizon 7-Ereignissen auf einen angegebenen Pfad:

```
vdadmin -I -eventSyslog -enable -path Pfad
```

Leiten der Syslog-Ausgabe von Horizon 7-Ereignissen auf einen angegebenen Pfad, der Zugriff durch einen autorisierten Domänenbenutzer erfordert:

```
vdadmin -I -eventSyslog -enable -path \\logserver\share\ViewEvents -user mydomain\myuser
-passwd mypassword
```

Zuweisen von dedizierten Computern unter Verwendung der Option „-L“

Mithilfe des Befehls `vdadmin` können Sie über die Option `-L` Benutzern Computer aus einem dedizierten Pool zuweisen.

Syntax

```
vdadmin
-L [-bAuthentifizierungsargumente] -dDesktop-m Computer-uDomäne\Benutzer
```

```
vdadmin
-L [-bAuthentifizierungsargumente] -dDesktop [-mComputer | -uDomäne\Benutzer] -r
```

Nutzungshinweise

Horizon 7 weist Benutzern Computer zu, wenn sich diese zum ersten Mal mit einem dedizierten Desktop-Pool verbinden. Unter bestimmten Umständen kann es sinnvoll sein, Benutzern Computer bereits vorab zuzuweisen. Zum Beispiel sollen die Systemumgebungen möglicherweise vorbereitet werden, bevor die Benutzer erstmalig eine Verbindung herstellen. Nachdem ein Benutzer eine Verbindung mit einem Remote-Desktop herstellt, der von Horizon 7 aus einem dedizierten Pool zugewiesen wird, bleibt die virtuelle Maschine, die den Desktop hostet, während der gesamten Lebensdauer der virtuellen Maschine diesem Benutzer zugewiesen. Sie können einen Benutzer einem einzelnen Computer in einem dedizierten Pool zuweisen.

Sie können einen Computer einem beliebigen berechtigten Benutzer zuweisen. Dies kann notwendig sein, wenn Sie nach dem Verlust von View LDAP-Daten auf einer Verbindungsserver-Instanz eine Wiederherstellung durchführen oder wenn Sie den Besitz einer bestimmten Computer ändern möchten.

Nachdem ein Benutzer eine Verbindung mit einem Remote-Desktop herstellt, der von Horizon 7 aus einem dedizierten Pool zugewiesen wird, bleibt der Remote-Desktop während der gesamten Lebensdauer der virtuellen Maschine, die den Desktop hostet, diesem Benutzer zugewiesen. Möglicherweise möchten Sie die Zuweisung eines Computers zu einem Benutzer entfernen, wenn ein Benutzer nicht mehr für die Organisation tätig ist, nicht länger auf den Desktop zugreifen muss oder einen Desktop in einem anderen Desktop-Pool verwenden wird. Es ist auch möglich, die Zuweisungen für sämtliche Benutzer zu entfernen, die auf einen Desktop-Pool zugreifen.

Hinweis Der Befehl `vdadmin -L` weist persistenten View Composer-Festplatten keine Besitzrechte zu. Verwenden Sie die Menüoption **Benutzer zuweisen** in Horizon Administrator, um Benutzern Linked-Clone-Desktops mit persistenten Festplatten zuzuweisen.

Wenn Sie `vdadmin -L` verwenden, um einem Benutzer einen Linked-Clone-Desktop mit einer persistenten Festplatte zuzuweisen, können in bestimmten Situationen unerwartete Ergebnisse auftreten. Wenn Sie beispielsweise eine persistente Festplatte trennen und diese zur Neuerstellung eines Desktops verwenden, wird der neu erstellte Desktop nicht dem Besitzer des ursprünglichen Desktops zugewiesen.

Optionen

Die folgende Tabelle zeigt die Optionen an, die Sie für die Zuweisung eines Benutzers zu einem Desktop oder zum Entfernen einer Zuweisung festlegen können.

Tabelle 15-9. Optionen für die Zuweisung dedizierter Desktops

Option	Beschreibung
<code>-d Desktop</code>	Legt den Namen des Desktop-Pools fest.
<code>-m Computer</code>	Legt den Namen der virtuellen Maschine fest, die den Remote-Desktop hostet.
<code>-r</code>	Entfernt eine Zuweisung für einen bestimmten Benutzer oder entfernt die gesamten Zuweisungen für eine bestimmte Maschine.
<code>-u Domäne\Benutzer</code>	Legt den Anmeldenamen und die Domäne des Benutzers fest.

Beispiele

Weisen Sie die Maschine „machine2“ im Desktop-Pool „dtpool1“ dem Benutzer „Jo“ in der Domäne „CORP“ zu.

```
vdadmin -L -d dtpool1 -m machine2 -u CORP\Jo
```

Entfernen Sie die Zuweisungen für den Benutzer Jo in der Domäne CORP für Desktops im Pool dtpool1.

```
vdadmin -L -d dtpool1 -u Corp\Jo -r
```

Entfernen Sie sämtliche Benutzerzuweisungen für die Maschine „machine1“ im Desktop-Pool „dtpool3“.

```
vdadmin -L -d dtpool3 -m machine1 -r
```

Anzeigen von Informationen zu Maschinen mithilfe der Option „-M“

Sie können den Befehl `vdadmin` mit der Option `-M` verwenden, um Informationen zur Konfiguration virtueller Maschinen oder physischer Computer anzuzeigen.

Syntax

```
vdadmin
-M [-b authentication_arguments] [-m machine | [-u domain\user] [-d desktop]] [-xml | -csv] [-w
| -n]
```

Nutzungshinweise

Dieser Befehl zeigt Informationen zur zugrunde liegenden virtuellen Maschine oder zum zugrunde liegenden physischen Computer eines Remote-Desktops an.

- Anzeigename der Maschine.
- Name des Desktop-Pools.
- Status der Maschine.

Als Maschinenstatus kann einer der folgenden Werte angezeigt werden: `UNDEFINED`, `PRE_PROVISIONED`, `CLONING`, `CLONINGERROR`, `CUSTOMIZING`, `READY`, `DELETING`, `MAINTENANCE`, `ERROR`, `LOGOUT`.

Der Befehl zeigt nicht alle dynamischen Maschinenstati an, wie beispielsweise `Connected` (Verbunden) oder `Disconnected` (Verbindung getrennt), die in Horizon Administrator angezeigt werden.

- SID des zugewiesenen Benutzers.
- Kontoname des zugewiesenen Benutzers.
- Domänenname des zugewiesenen Benutzers.
- Gegebenenfalls der Bestandslistenpfad der virtuellen Maschine.
- Erstellungsdatum der Maschine.
- Gegebenenfalls der Vorlagenpfad der Maschine.
- Gegebenenfalls die vCenter Server-URL.

Optionen

Die folgende Tabelle zeigt die verfügbaren Optionen zum Angeben der Maschine, für die Details angezeigt werden sollen.

Tabelle 15-10. Optionen für das Anzeigen von Informationen zu Maschinen

Option	Beschreibung
<code>-d Desktop</code>	Legt den Namen des Desktop-Pools fest.
<code>-m Computer</code>	Legt den Namen der virtuellen Maschine fest.
<code>-u Domäne\Benutzer</code>	Legt den Anmeldenamen und die Domäne des Benutzers fest.

Beispiele

Zeigen Sie Informationen zum zugrunde liegenden Computer für den Remote-Desktop im Pool `dtpool2` an, der dem Benutzer `Jo` in der Domäne `CORP` zugewiesen ist, und legen Sie für die Ausgabe das XML-Format mit ASCII-Zeichen fest.

```
vdmadmin -M -u CORP\Jo -d dtpool2 -xml -n
```

Zeigen Sie Informationen zur Maschine `machine3` an und legen Sie für die Ausgabe das CSV-Format fest.

```
vdmadmin -M -m machine3 -csv
```

Rückgewinnung von Datenträgerplatz auf virtuellen Maschinen mithilfe der Option „-M“

Sie können den Befehl `vdmadmin` zusammen mit der Option `-M` verwenden, um eine virtuelle Linked-Clone-Maschine für die Rückgewinnung von Datenträgerplatz zu markieren. Horizon 7 weist den ESXi-Host an, Datenträgerplatz auf der Linked-Clone-Betriebssystemfestplatte zurückzugewinnen, ohne darauf zu warten, dass der ungenutzte Platz auf der Betriebssystemfestplatte den maximalen Grenzwert erreicht, der in Horizon Administrator angegeben ist.

Syntax

```
vdmadmin
-M [-b authentication_arguments] -d desktop-m machine-markForSpaceReclamation
```

Nutzungshinweise

Mit dieser Option können Sie eine Rückgewinnung von Datenträgerplatz auf einer bestimmten virtuellen Maschine zu Demonstrations- oder Fehlerbehebungs Zwecken initiieren.

Die Rückgewinnung von Datenträgerplatz findet nicht statt, wenn Sie diesen Befehl ausführen, während eine Ausfallzeit gilt.

Die folgenden Voraussetzungen müssen erfüllt sein, bevor Sie Datenträgerplatz mit dem Befehl `vdmadmin` mit der Option `-M` zurückgewinnen können:

- Vergewissern Sie sich, dass Horizon 7 vCenter Server und ESXi Version 5.1 oder höher verwendet.

- Überprüfen Sie, dass VMware Tools, die mit vSphere Version 5.1 oder höher geliefert werden, auf der virtuellen Maschine installiert sind.
- Überprüfen Sie, dass die virtuelle Maschine die virtuelle Hardwareversion 9 oder höher aufweist.
- Stellen Sie in Horizon Administrator sicher, dass die Option **Zurückgewinnung von Datenträgerplatz** für vCenter Server ausgewählt ist. Siehe [#unique_203](#).
- Stellen Sie in Horizon Administrator sicher, dass die Option **VM-Datenträgerplatz zurückgewinnen** für den Desktop-Pool ausgewählt wurde. Weitere Informationen finden Sie unter „Rückgewinnen von Datenträgerplatz auf View Composer-Linked-Clones“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.
- Überprüfen Sie, dass die virtuelle Maschine eingeschaltet ist, bevor Sie den Vorgang zur Rückgewinnung von Speicherplatz initiieren.
- Überprüfen Sie, dass keine Ausfallperiode wirksam ist. Weitere Informationen finden Sie unter „Festlegen der Speicherbeschleunigung und von Ausfallzeiten der Rückgewinnung von Speicherplatz für View Composer-Linked-Clones“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Optionen

Tabelle 15-11. Optionen für die Rückgewinnung von Datenträgerplatz auf virtuellen Maschinen

Option	Beschreibung
<code>-d Desktop</code>	Legt den Namen des Desktop-Pools fest.
<code>-m Computer</code>	Legt den Namen der virtuellen Maschine fest.
<code>-MarkForSpaceReclamation</code>	Markiert die virtuelle Maschine für die Rückgewinnung von Datenträgerplatz.

Beispiel

Markiert die virtuelle Maschine `machine3` im Desktop-Pool `pool1` für die Rückgewinnung von Datenträgerplatz.

```
vdmadmin -M -d pool1 -m machine3 -markForSpaceReclamation
```

Konfigurieren von Domänenfiltern mithilfe der Option „-N“

Sie können den Befehl `vdmadmin` mit der Option `-N` zum Steuern der Domänen verwenden, die Horizon 7 für die Endbenutzer zur Verfügung stellt.

Syntax

```
vdmadmin
```

```
-N [-b Authentifizierungsargumente] -domains {-exclude | -include | -search} -domain Domäne-add [-s
Verbindungsserver]
```

```
vdmadmin
-N [-b Authentifizierungsargumente] -domains-list [-w | -n] [-xml]
```

```
vdmadmin
-N [-b Authentifizierungsargumente] -domains-list-active [-w | -n] [-xml]
```

```
vdmadmin
-N [-b Authentifizierungsargumente] -domains {-exclude | -include | -search} -domain Domäne-remove
[-s Verbindungsserver]
```

```
vdmadmin
-N [-b Authentifizierungsargumente] -domains {-exclude | -include | -search} -removeall [-s
Verbindungsserver]
```

Nutzungshinweise

Geben Sie die Option `-exclude`, `-include` oder `-search` an, um einen Vorgang auf die Ausschlussliste, die Aufnahmeliste oder die Ausschlussliste für die Suche anzuwenden.

Wenn Sie eine Domäne zu einer Ausschlussliste für die Suche hinzufügen, wird die Domäne bei einer automatisierten Domänensuche ausgeschlossen.

Beim Hinzufügen einer Domäne zu einer Aufnahmeliste wird die Domäne in die Ergebnisse der Suche aufgenommen.

Wenn Sie eine Domäne zu einer Ausschlussliste hinzufügen, wird die Domäne aus den Ergebnissen der Suche ausgeschlossen.

Optionen

Die folgende Tabelle zeigt die verfügbaren Optionen zum Konfigurieren von Domänenfiltern.

Tabelle 15-12. Optionen für die Konfiguration von Domänenfiltern

Option	Beschreibung
<code>-add</code>	Fügt eine Domäne zu einer Liste hinzu.
<code>-domain Domäne</code>	Gibt die Domäne für die Filterung an. Verwenden Sie zum Angeben von Domänen nicht den DNS-Namen, sondern den NetBIOS-Namen.
<code>-domains</code>	Gibt einen Domänenfiltervorgang an.
<code>-exclude</code>	Gibt einen Vorgang für eine Ausschlussliste an.
<code>-include</code>	Gibt einen Vorgang für eine Aufnahmeliste an.

Tabelle 15-12. Optionen für die Konfiguration von Domänenfiltern (Fortsetzung)

Option	Beschreibung
<code>-list</code>	Zeigt die Domänen an, die in der Ausschlussliste für die Suche, in der Ausschlussliste und in der Aufnahmeliste für die einzelnen Verbindungsserver-Instanzen und für die Verbindungsserver-Gruppe konfiguriert sind.
<code>-list -active</code>	Zeigt die verfügbaren Domänen für die Verbindungsserver-Instanz an, auf welcher der Befehl ausgeführt wird.
<code>-remove</code>	Entfernt eine Domäne aus einer Liste.
<code>-removeall</code>	Entfernt alle Domänen aus einer Liste.
<code>-s <i>Verbindungsserver</i></code>	Gibt an, dass der Vorgang für die Domänenfilter einer Verbindungsserver-Instanz ausgeführt wird. Die Verbindungsserver-Instanz kann über den Namen oder die IP-Adresse angegeben werden. Wenn Sie diese Option nicht angeben, werden Änderungen an der Suchkonfiguration für alle Verbindungsserver-Instanzen innerhalb der Gruppe übernommen.
<code>-search</code>	Gibt einen Vorgang für eine Ausschlussliste für die Suche an.

Beispiele

Fügen Sie die Domäne FARDOM zur Ausschlussliste für die Suche für die Verbindungsserver-Instanz csvr1 hinzu.

```
vdmadmin -N -domains -search -domain FARDOM -add -s csvr1
```

Fügen Sie die Domäne NEARDOM zur Ausschlussliste für eine Verbindungsserver-Gruppe hinzu.

```
vdmadmin -N -domains -exclude -domain NEARDOM -add
```

Zeigen Sie die Konfiguration für die Domänensuche auf beiden Verbindungsserver-Instanzen in der Gruppe und für die Gruppe an.

```
C:\ vdmadmin -N -domains -list
```

```
Domain Configuration
```

```
=====
```

```
Cluster Settings
```

```
Include:
```

```
Exclude:
```

```
Search :
```

```
FARDOM
```

```
DEPTX
```

```
Broker Settings: CONSVR-1
```

```
Include:
```

```
(*)Exclude:
```

```
YOURDOM
```

```
Search :
```

```
Broker Settings: CONSVR-2
  Include:
  Exclude:
  Search :
```

Horizon 7 schränkt die Domänensuche auf allen Verbindungsserver-Hosts in der Gruppe ein, indem die Domänen „FARDOM“ und „DEPTX“ ausgeschlossen werden. Die Zeichen (*) neben der Ausschlussliste für „CONSVR-1“ zeigen an, dass Horizon 7 die Domäne „YOURDOM“ aus den Ergebnissen der Domänensuche auf „CONSVR-1“ ausschließt.

Zeigen Sie die Domänenfilter im XML-Format mit ASCII-Zeichen an.

```
vdadmin -N -domains -list -xml -n
```

Zeigen Sie die Domänen an, die für Horizon 7 auf der lokalen Verbindungsserver-Instanz verfügbar sind.

```
C:\ vdadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: FARDOM DNS:fardom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

Zeigen Sie die verfügbaren Domänen im XML-Format mit ASCII-Zeichen an.

```
vdadmin -N -domains -list -active -xml -n
```

Entfernen Sie die Domäne NEARDOM aus der Ausschlussliste für eine Verbindungsserver-Gruppe.

```
vdadmin -N -domains -exclude -domain NEARDOM -remove
```

Entfernen Sie sämtliche Domänen aus der Aufnahmeliste für die Verbindungsserver-Instanz csvr1.

```
vdadmin -N -domains -include -removeall -s csvr1
```

Konfigurieren von Domänenfiltern

Domänenfilter können Sie zur Einschränkung der Anzahl der Domänen, die eine Verbindungsserver-Instanz oder ein Sicherheitsserver den Endbenutzern zur Verfügung stellt, konfigurieren.

Horizon 7 ermittelt die für den Zugriff verfügbaren Domänen, indem – beginnend mit der Domäne, in der sich eine Verbindungsserver-Instanz oder ein Sicherheitsserver befindet – die vorhandenen Vertrauensbeziehungen durchlaufen werden. Bei einer kleinen, gut verbundenen Gruppe von Domänen kann Horizon 7 schnell eine vollständige Liste der vorhandenen Domänen erstellen. Liegt jedoch eine

große Anzahl an Domänen oder eine weniger gute Verbindung zwischen den Domänen vor, steigt der zur Ermittlung der Domänen benötigte Zeitaufwand. Die Horizon 7-Suchergebnisse können Domänen enthalten, die Sie Benutzern nicht anbieten möchten, wenn sich diese bei ihren Remote-Desktops anmelden.

Wenn Sie den Wert des Windows-Registrierungsschlüssels zum Steuern der rekursiven Domänenenumeration (HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum) zuvor auf false gesetzt haben, ist die rekursive Domänensuche deaktiviert und die Verbindungsserver-Instanz verwendet nur die primäre Domäne. Löschen Sie zum Verwenden der Domänenfilterungsfunktion den Registrierungsschlüssel oder setzen Sie seinen Wert auf true. Starten Sie das System anschließend neu. Dieser Schritt muss für jede Verbindungsserver-Instanz ausgeführt werden, auf der dieser Schlüssel festgelegt ist.

Die folgende Tabelle zeigt die Typen von Domänenlisten, die Sie zur Konfiguration der Domänenfilterung angeben können.

Tabelle 15-13. Typen von Domänenlisten

Domänenlistentyp	Beschreibung
Ausschlussliste für die Suche	Gibt die Domänen an, die Horizon 7 während einer automatisierten Suche durchlaufen kann. Bei der Suche werden Domänen ignoriert, die in der Ausschlussliste für die Suche enthalten sind. Es wird nicht versucht, Domänen zu ermitteln, denen die ausgeschlossenen Domänen vertrauen. Die primäre Domäne kann nicht aus der Suche ausgeschlossen werden.
Ausschlussliste	Gibt die Domänen an, die Horizon 7 aus den Ergebnissen einer Domänensuche ausschließt. Die primäre Domäne kann nicht ausgeschlossen werden.
Aufnahmeliste	Gibt die Domänen an, die Horizon 7 nicht aus den Ergebnissen einer Domänensuche ausschließt. Mit Ausnahme der primären Domäne werden alle anderen Domänen entfernt.

Bei der automatisierten Domänensuche wird eine Liste mit Domänen abgerufen. Dabei werden die in der Ausschlussliste für die Suche angegebenen Domänen sowie Domänen, denen diese ausgeschlossenen Domänen vertrauen, ausgeschlossen. Horizon 7 wählt die erste nicht leere Ausschluss- oder Aufnahmeliste mit dieser Reihenfolge aus.

- 1 Die für die Verbindungsserver-Instanz konfigurierte Ausschlussliste.
- 2 Die für die Verbindungsserver-Gruppe konfigurierte Ausschlussliste.
- 3 Die für die Verbindungsserver-Instanz konfigurierte Aufnahmeliste.
- 4 Die für die Verbindungsserver-Gruppe konfigurierte Aufnahmeliste.

Horizon 7 wendet lediglich die erste ausgewählte Liste auf die Suchergebnisse an.

Wenn Sie eine Domäne in die Aufnahmeliste aufnehmen, deren Domänencontroller nicht verfügbar ist, nimmt Horizon 7 diese Domäne nicht in die Liste aktiver Domänen auf.

Die primäre Domäne, zu der eine Verbindungsserver-Instanz oder ein Sicherheitsserver gehört, kann nicht ausgeschlossen werden.

Beispiel für die Filterung zum Einschließen von Domänen

Sie können mithilfe einer Aufnahmeliste Domänen angeben, die Horizon 7 nicht aus den Ergebnissen einer Domänensuche ausschließt. Mit Ausnahme der primären Domäne werden alle anderen Domänen entfernt.

Eine Verbindungsserver-Instanz ist mit der primären Domäne MYDOM verbunden und verfügt über eine Vertrauensbeziehung mit der Domäne YOURDOM. Die Domäne YOURDOM verfügt über eine Vertrauensbeziehung mit der Domäne DEPTX.

Zeigen Sie die derzeit aktiven Domänen für die Verbindungsserver-Instanz an.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: FARDOM DNS: fardom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

Die Domänen DEPTY und DEPTZ sind in der Liste enthalten, da sie vertrauenswürdige Domänen der Domäne DEPTX sind.

Geben Sie an, dass die Verbindungsserver-Instanz neben der primären Domäne MYDOM nur die Domänen YOURDOM und DEPTX verfügbar machen soll.

```
vdmadmin -N -domains -include -domain YOURDOM -add
```

```
vdmadmin -N -domains -include -domain DEPTX -add
```

Zeigen Sie die derzeit aktiven Domänen an, nachdem die Domänen YOURDOM und DEPTX aufgenommen wurden.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

Horizon 7 wendet die Aufnahmeliste auf die Ergebnisse einer Domänensuche an. Wenn die Domänenhierarchie sehr komplex ist oder die Netzwerkverbindungen zu einigen Domänen eine geringe Leistung bieten, wird die Domänensuche möglicherweise langsam ausgeführt. Verwenden Sie in diesen Fällen stattdessen die Ausschlussliste für die Suche.

Beispiel für die Filterung zum Ausschließen von Domänen

Sie können in einer Ausschlussliste die Domänen angeben, die Horizon 7 aus den Ergebnissen einer Domänensuche ausschließt.

Eine Gruppe aus zwei Verbindungsserver-Instanzen, CONSVR-1 und CONSVR-2, ist mit der primären Domäne MYDOM verbunden und verfügt über eine Vertrauensbeziehung mit der Domäne YOURDOM. Die Domäne YOURDOM verfügt über eine Vertrauensbeziehung mit den Domänen DEPTX und FARDOM.

Die Domäne FARDOM befindet sich an einem geografisch entfernten Standort und die Netzwerkkonnektivität mit dieser Domäne wird über eine langsame Verbindung mit hoher Latenz hergestellt. Benutzer in der Domäne FARDOM müssen nicht auf die Verbindungsserver-Gruppe in der Domäne MYDOM zugreifen können.

Zeigen Sie die derzeit aktiven Domänen für ein Mitglied der Verbindungsserver-Gruppe an.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: FARDOM DNS:fardom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

Bei den Domänen DEPTY und DEPTZ handelt es sich um vertrauenswürdige Domänen der Domäne DEPTX.

Zum Verbessern der Verbindungsleistung für Horizon Client schließen Sie die Domäne FARDOM aus der Suche der Verbindungsserver-Gruppe aus.

```
vdmadmin -N -domains -search -domain FARDOM -add
```

Der Befehl zeigt die derzeit aktiven Domänen an, nachdem die Domäne FARDOM aus der Suche ausgeschlossen wurde.

```
C:\ vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

Erweitern Sie die Ausschlussliste für die Suche, um die Domäne DEPTX sowie all ihre als vertrauenswürdig eingestuft Domänen aus der Domänensuche für alle Verbindungsserver-Instanzen einer Gruppe auszuschließen. Schließen Sie zudem die Domäne YOURDOM aus den verfügbaren Domänen auf CONSVR-1 aus.

```
vdadmin -N -domains -search -domain DEPTX -add
vdadmin -N -domains -exclude -domain YOURDOM -add -s CONSVR-1
```

Zeigen Sie die neue Konfiguration für die Domänensuche an.

```
C:\ vdadmin -N -domains -list
```

```
Domain Configuration
```

```
=====
```

```
Cluster Settings
```

```
Include:
```

```
Exclude:
```

```
Search :
```

```
FARDOM
```

```
DEPTX
```

```
Broker Settings: CONSVR-1
```

```
Include:
```

```
(*)Exclude:
```

```
YOURDOM
```

```
Search :
```

```
Broker Settings: CONSVR-2
```

```
Include:
```

```
Exclude:
```

```
Search :
```

Horizon 7 schränkt die Domänensuche auf allen Verbindungsserver-Hosts in der Gruppe ein, indem die Domänen „FARDOM“ und „DEPTX“ ausgeschlossen werden. Die Zeichen (*) neben der Ausschlussliste für „CONSVR-1“ zeigen an, dass Horizon 7 die Domäne „YOURDOM“ aus den Ergebnissen der Domänensuche auf „CONSVR-1“ ausschließt.

Zeigen Sie auf CONSVR-1 die derzeit aktiven Domänen an.

```
C:\ vdadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

Zeigen Sie auf CONSVR-2 die derzeit aktiven Domänen an.

```
C:\ vdadmin -N -domains -list -active
```

```
Domain Information (CONSVR-2)
```

```
=====
```


Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com

Domain: YOURDOM DNS:yourdom.mycorp.com

Anzeigen der Maschinen und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“

Sie können den Befehl `vdmadmin` mit den Optionen `-O` und `-P` verwenden, um die virtuellen Maschinen und Richtlinien von Benutzern anzuzeigen, die nicht länger zur Verwendung des Systems berechtigt sind.

Syntax

```
vdmadmin
-O [-b Authentifizierungsargumente] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath Pfad]]
```

```
vdmadmin
-P [-b Authentifizierungsargumente] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath Pfad]]
```

Nutzungshinweise

Wenn Sie die Berechtigungen eines Benutzers für eine persistente virtuelle Maschine oder ein physisches System aufheben, wird die verknüpfte Remote-Desktop-Zuweisung nicht automatisch entfernt. Dies kann akzeptabel sein, wenn ein Benutzerkonto temporär gesperrt wird oder sich der Benutzer in einem Sabbatjahr befindet. Bei erneuter Aktivierung der Berechtigung kann der Benutzer dieselbe virtuelle Maschine wie zuvor weiterverwenden. Wenn ein Benutzer nicht mehr in der Organisation beschäftigt ist, können andere Benutzer nicht auf die virtuelle Maschine zugreifen und die Maschine wird als verwaist betrachtet. Zudem sollten die Richtlinien geprüft werden, die nicht berechtigten Benutzern zugewiesen sind.

Optionen

Die folgende Tabelle zeigt die verfügbaren Optionen zum Anzeigen der virtuellen Maschinen und Richtlinien nicht berechtigter Benutzer auf.

Tabelle 15-14. Optionen für das Anzeigen der Maschinen und Richtlinien nicht berechtigter Benutzer

Option	Beschreibung
<code>-ld</code>	Sortiert die Einträge der Ausgabe nach Maschine.
<code>-lu</code>	Sortiert die Einträge der Ausgabe nach Benutzer.

Tabelle 15-14. Optionen für das Anzeigen der Maschinen und Richtlinien nicht berechtigter Benutzer (Fortsetzung)

Option	Beschreibung
<code>-noxslt</code>	Gibt an, dass das standardmäßige Stylesheet nicht auf die XML-Ausgabe angewendet wird.
<code>-xsltpath <i>Pfad</i></code>	Gibt den Pfad zum Stylesheet an, das zur Umwandlung der XML-Ausgabe verwendet wird.

Tabelle 15-15. XSL-Stylesheets zeigt die verfügbaren Stylesheets, um die XML-Ausgabe in das HTML-Format umzuwandeln. Die Stylesheets befinden sich im Verzeichnis `C:\Programme\VMware\VMware View\server\etc`.

Tabelle 15-15. XSL-Stylesheets

Name der Stylesheet-Datei	Beschreibung
<code>unentitled-machines.xml</code>	Zur Umwandlung von Berichten mit einer Liste nicht berechtigter virtueller Maschinen, die nach Benutzer oder nach System gruppiert und derzeit einem Benutzer zugewiesen sind. Dies ist das standardmäßige Stylesheet.
<code>unentitled-policies.xml</code>	Zur Umwandlung von Berichten mit einer Liste von virtuellen Maschinen, denen Richtlinien auf Benutzerebene zugewiesen sind, die auf nicht berechnete Benutzer angewendet werden.

Beispiele

Zeigen Sie die nicht berechtigten Benutzern zugewiesenen virtuellen Maschinen an und legen Sie eine Gruppierung nach virtueller Maschine sowie die Ausgabe im Textformat fest.

```
vdmadmin -O -ld
```

Zeigen Sie die nicht berechtigten Benutzern zugewiesenen virtuellen Maschinen an und legen Sie eine Gruppierung nach Benutzer sowie die Ausgabe im XML-Format mit ASCII-Zeichen fest.

```
vdmadmin -O -lu -xml -n
```

Wenden Sie Ihr eigenes Stylesheet `C:\tmp\unentitled-users.xml` an und legen Sie die Speicherung der Ausgabe in der Datei `uu-output.html` fest.

```
vdmadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xml" > uu-output.html
```

Zeigen Sie die Benutzerrichtlinien an, die den virtuellen Maschinen nicht berechtigter Benutzer zugewiesen sind, und legen Sie eine Gruppierung nach Desktop sowie die Ausgabe im XML-Format mit Unicode-Zeichen fest.

```
vdmadmin -P -ld -xml -w
```

Wenden Sie Ihr eigenes Stylesheet C:\tmp\unentitled-policies.xml an und legen Sie die Speicherung der Ausgabe in der Datei up-output.html fest.

```
vdmadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xml" > up-output.html
```

Konfigurieren von Clients im Kiosk-Modus mithilfe der Option „-Q“

Unter Verwendung des Befehls vdmadmin mit der Option -Q können Standardwerte festgelegt und Konten für Clients im Kiosk-Modus erstellt werden, um die Authentifizierung für diese Clients zu aktivieren und Informationen zu ihrer Konfiguration anzuzeigen.

Syntax

```
vdmadmin
-Q
-clientauth
-add [-b Authentifizierungsargumente] -domain Domänenname-clientid Client-ID [-password
"Kennwort" | -genpassword] [-ou DM] [-expirepassword | -noexpirepassword] [-groupGruppenname | -nogroup]
[-description "Beschreibungstext"]
```

```
vdmadmin
-Q
-disable [-bAuthentifizierungsargumente] -sVerbindungsserver
```

```
vdmadmin
-Q
-enable [-bAuthentifizierungsargumente] -sVerbindungsserver [-requirepassword]
```

```
vdmadmin
-Q
-clientauth
-getdefaults [-b Authentifizierungsargumente] [-xml]
```

```
vdmadmin
-Q
-clientauth
-list [-b Authentifizierungsargumente] [-xml]
```

```
vdmadmin
-Q
```

```
-clientauth
-remove [-b Authentifizierungsargumente] -domain Domänenname-clientid Client-ID
```

```
vdmadmin
-Q
-clientauth
-removeall [-b Authentifizierungsargumente] [-force]
```

```
vdmadmin
-Q
-clientauth
-setdefaults [-b Authentifizierungsargumente] [-ou DN] [ -expirepassword | -noexpirepassword ]
[-group Gruppenname | -nogroup]
```

```
vdmadmin
-Q
-clientauth
-update [-b Authentifizierungsargumente] -domain Domänenname-clientid Client-ID [-password
"Kennwort" | -genpassword] [-description "Beschreibungstext"]
```

Nutzungshinweise

Der Befehl `vdmadmin` muss für eine der Verbindungsserver-Instanzen in der Gruppe mit der Verbindungsserver-Instanz ausgeführt werden, welche die Clients zum Herstellen einer Verbindung mit ihren Remote-Desktops verwenden.

Wenn Sie Standardwerte für die Ablaufzeit von Kennwörtern und die Active Directory-Gruppenmitgliedschaft konfigurieren, werden diese Einstellungen von allen Verbindungsserver-Instanzen innerhalb einer Gruppe verwendet.

Beim Hinzufügen von Clients im Kiosk-Modus erstellt Horizon 7 ein Benutzerkonto für den Client in Active Directory. Wenn Sie einen Namen für einen Client angeben, muss dieser Name mit der Zeichenfolge „custom-“ oder einer der anderen Zeichenfolgen beginnen, die Sie in ADAM definieren können. Außerdem darf diese Zeichenfolge nicht länger als 20 Zeichen lang sein. Verwenden Sie einen angegebenen Namen nicht mit mehreren Clientgeräten.

Unter `pae-ClientAuthPrefix`, einem Attribut mit mehreren Werten, können Sie alternative Präfixe für „custom“ angeben, und zwar unter `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` in ADAM in einer Verbindungsserver-Instanz. Vermeiden Sie, diese Präfixe bei normalen Benutzerkonten zu verwenden.

Wenn Sie keinen Namen für den Client angeben, generiert Horizon 7 einen Namen aus der für das Clientgerät angegebenen MAC-Adresse. So wird z. B. für die MAC-Adresse 00:10:db:ee:76:80 der Kontoname `cm-00_10_db_ee_76_80` generiert. Diese Konten können Sie nur mit Verbindungsserver-Instanzen verwenden, die für die Authentifizierung von Clients aktiviert wurden.

Einige Thin Clients lassen zur Verwendung mit dem Kiosk-Modus nur Kontennamen zu, die mit der Zeichenfolge „custom-“ oder „cm-“ beginnen.

Ein automatisch generiertes Kennwort umfasst 16 Zeichen, mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen sowie eine Zahl und kann sich wiederholende Zeichen enthalten. Wenn ein sichereres Kennwort erforderlich ist, muss das Kennwort über die Option `-password` angegeben werden.

Wenn Sie die Option `-group` zur Angabe einer Gruppe verwenden oder zuvor eine Standardgruppe festgelegt haben, fügt Horizon 7 das Clientkonto zu dieser Gruppe hinzu. Durch Angabe der Option `-nogroup` können Sie verhindern, dass das Konto zu einer Gruppe hinzugefügt wird.

Wenn Sie eine Verbindungsserver-Instanz für die Authentifizierung von Clients im Kiosk-Modus aktivieren, können Sie optional festlegen, dass Clients ein Kennwort bereitstellen müssen. Bei Deaktivierung der Authentifizierung können Clients keine Verbindung zu ihren Remote-Desktops herstellen.

Wenngleich die Authentifizierung für eine einzelne Verbindungsserver-Instanz aktiviert oder deaktiviert wird, gelten die anderen Einstellungen für die Clientauthentifizierung für alle Verbindungsserver-Instanzen innerhalb einer Gruppe. Ein Client muss nur einmal hinzugefügt werden, damit alle Verbindungsserver-Instanzen in einer Gruppe Anforderungen von diesem Client akzeptieren.

Wenn Sie beim Aktivieren der Authentifizierung die Option `-requirepassword` angeben, kann die Verbindungsserver-Instanz keine Clients authentifizieren, die über automatisch generierte Kennwörter verfügen. Wenn Sie die Konfiguration einer Verbindungsserver-Instanz ändern und diese Option angeben, können diese Clients nicht authentifiziert werden und der Fehler `Unknown username or bad password` (Unbekannter Benutzername oder falsches Kennwort) wird ausgegeben.

Optionen

Die folgende Tabelle zeigt die verfügbaren Optionen für die Konfiguration von Clients im Kiosk-Modus.

Tabelle 15-16. Optionen für die Konfiguration von Clients im Kiosk-Modus

Option	Beschreibung
<code>-add</code>	Fügt ein Konto für einen Client im Kiosk-Modus hinzu.
<code>-clientauth</code>	Gibt einen Vorgang zur Konfiguration der Authentifizierung für einen Client im Kiosk-Modus an.
<code>-clientid</code> <i>Client-ID</i>	Gibt den Namen oder die MAC-Adresse des Clients an.
<code>-description</code> " <i>description_text</i> "	Erstellt eine Beschreibung des Kontos für das Clientgerät in Active Directory.
<code>-disable</code>	Deaktiviert die Authentifizierung von Clients im Kiosk-Modus auf einer angegebenen Verbindungsserver-Instanz.
<code>-domain</code> <i>Domänenname</i>	Gibt die Domäne des Kontos für das Clientgerät an.
<code>-enable</code>	Aktiviert die Authentifizierung von Clients im Kiosk-Modus auf einer angegebenen Verbindungsserver-Instanz.

Tabelle 15-16. Optionen für die Konfiguration von Clients im Kiosk-Modus (Fortsetzung)

Option	Beschreibung
<code>-expirepassword</code>	Gibt an, dass die Ablaufzeit für Kennwörter der Clientkonten mit der Ablaufzeit für die Verbindungsserver-Gruppe übereinstimmt. Wenn für die Gruppe keine Ablaufzeit definiert ist, laufen Kennwörter nicht ab.
<code>-force</code>	Deaktiviert die Bestätigungsmeldung beim Entfernen eines Kontos für einen Client im Kiosk-Modus.
<code>-genpassword</code>	Generiert ein Kennwort für das Clientkonto. Dies ist das Standardverhalten, wenn weder <code>-password</code> noch <code>-genpassword</code> angegeben wird.
<code>-getdefaults</code>	Ruft die Standardwerte für das Hinzufügen von Clientkonten ab.
<code>-group <i>Gruppenname</i></code>	Gibt den Namen der Standardgruppe an, zu der Clientkonten hinzugefügt werden. Der Name der Gruppe muss als der Prä-Windows 2000-Gruppenname aus Active Directory angegeben werden.
<code>-list</code>	Zeigt Informationen zu Clients im Kiosk-Modus sowie zu Verbindungsserver-Instanzen an, auf denen die Authentifizierung von Clients im Kiosk-Modus aktiviert ist.
<code>-noexpirepassword</code>	Gibt an, dass das Kennwort für ein Konto nicht abläuft.
<code>-nogroup</code>	Beim Hinzufügen eines Kontos für einen Client gibt diese Option an, dass das Clientkonto nicht zur Standardgruppe hinzugefügt wird. Beim Festlegen der Standardwerte für Clients löscht diese Option die Einstellung für die Standardgruppe.
<code>-ou <i>DN</i></code>	Gibt den Distinguished Name der Organisationseinheit an, zu der Clientkonten hinzugefügt werden. Beispiel: OU=kiosk-ou,DC=myorg,DC=com Hinweis Die Konfiguration einer Organisationseinheit kann nicht über die Option <code>-setdefaults</code> geändert werden.
<code>-password "<i>Kennwort</i>"</code>	Gibt ein explizites Kennwort für das Clientkonto an.
<code>-remove</code>	Entfernt das Konto für einen Client im Kiosk-Modus.
<code>-removeall</code>	Entfernt die Konten aller Clients im Kiosk-Modus.
<code>-requirepassword</code>	Gibt an, dass Clients im Kiosk-Modus Kennwörter bereitstellen müssen. Horizon 7 akzeptiert für neue Verbindungen keine generierten Kennwörter.
<code>-s <i>Verbindungsserver</i></code>	Gibt den NetBIOS-Namen der Verbindungsserver-Instanz an, für welche die Authentifizierung von Clients im Kiosk-Modus aktiviert oder deaktiviert werden soll.
<code>-setdefaults</code>	Legt die Standardwerte für das Hinzufügen von Clientkonten fest.
<code>-update</code>	Aktualisiert ein Konto für einen Client im Kiosk-Modus.

Beispiele

Legen Sie die Standardwerte für die Organisationseinheit, den Ablauf von Kennwörtern sowie die Gruppenmitgliedschaft von Clients fest.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

Rufen Sie die aktuellen Standardwerte für Clients im Textformat ab.

```
vdmadmin -Q -clientauth -getdefaults
```

Rufen Sie die aktuellen Standardwerte für Clients im XML-Format ab.

```
vdmadmin -Q -clientauth -getdefaults -xml
```

Fügen Sie ein Konto für einen Client, der über die MAC-Adresse angegeben wird, zur Domäne MYORG hinzu und verwenden Sie die Standardeinstellungen für die Gruppe „kc-grp“.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

Fügen Sie ein Konto für einen Client, der über die MAC-Adresse angegeben wird, zur Domäne MYORG hinzu und verwenden Sie ein automatisch generiertes Kennwort.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -group kc-grp
```

Fügen Sie ein Konto für einen benannten Client hinzu und geben Sie ein Kennwort zur Verwendung mit dem Client an.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Aktualisieren Sie ein Konto für einen Client und geben Sie ein neues Kennwort sowie eine Beschreibung an.

```
vdmadmin -Q -clientauth -update -domain MYORG -clientid custom-Terminal21 -password "Secret1!" -description "Foyer Entry Workstation"
```

Entfernen Sie das Konto für einen Kiosk-Client, der über seine MAC-Adresse angegeben wird, aus der Domäne MYORG.

```
vdmadmin -Q -clientauth -remove -domain MYORG -clientid 00:10:db:ee:54:12
```

Entfernen Sie die Konten aller Clients, ohne eine Bestätigungsmeldung für den Entfernungsvorgang anzuzeigen.

```
vdmadmin -Q -clientauth -removeall -force
```

Aktivieren Sie die Authentifizierung von Clients für die Verbindungsserver-Instanz „csvr-2“. Clients mit automatisch generierten Kennwörtern können sich ohne Angabe eines Kennworts authentifizieren.

```
vdmadmin -Q -enable -s csvr-2
```

Aktivieren Sie die Authentifizierung von Clients für die Verbindungsserver-Instanz csvr-3 und legen Sie fest, dass die Clients ihre Kennwörter für Horizon Client bereitstellen müssen. Clients mit automatisch generierten Kennwörtern können sich nicht authentifizieren.

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

Deaktivieren Sie die Authentifizierung von Clients für die Verbindungsserver-Instanz „csvr-1“.

```
vdmadmin -Q -disable -s csvr-1
```

Zeigen Sie Informationen zu Clients im Textformat an. Der Client „cm-00_0c_29_0d_a3_e6“ verfügt über ein automatisch generiertes Kennwort, sodass dieses Kennwort nicht durch den Endbenutzer oder über ein Anwendungsskript für Horizon Client angegeben werden muss. Der Client cm-00_22_19_12_6d_cf verfügt über ein explizit angegebenes Kennwort, sodass der Endbenutzer dieses Kennwort angeben muss. Die Verbindungsserver-Instanz CONSVR2 akzeptiert Authentifizierungsanforderungen von Clients mit automatisch generierten Kennwörtern. CONSVR1 akzeptiert keine Authentifizierungsanforderungen von Clients im Kiosk-Modus.

```
C:\ vdmadmin -Q -clientauth -list
Client Authentication User List
=====
GUID           : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID       : cm-00_0c_29_0d_a3_e6
Domain         : myorg.com
Password Generated: true

GUID           : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID       : cm-00_22_19_12_6d_cf
Domain         : myorg.com
Password Generated: false

Client Authentication Connection Servers
=====
Common Name           : CONSVR1
Client Authentication Enabled : false
Password Required     : false

Common Name           : CONSVR2
Client Authentication Enabled : true
Password Required     : false
```


Anzeigen des ersten Benutzers einer Maschine mithilfe der Option „-R“

Sie können den Befehl `vdmadmin` mit der Option `-R` verwenden, um die anfängliche Zuweisung einer verwalteten virtuellen Maschine zu ermitteln. Bei Verlust von LDAP-Daten wird diese Information z. B. möglicherweise benötigt, um eine Neuzuweisung von virtuellen Maschinen zu Benutzern durchzuführen.

Hinweis Der Befehl `vdmadmin` mit der Option `-R` kann nur auf virtuellen Maschinen vor View Agent 5.1 angewendet werden. Auf virtuellen Maschinen, auf denen View Agent 5.1 oder eine höhere Version und Horizon Agent 7.0 oder eine höhere Version ausgeführt wird, funktioniert diese Option nicht. Verwenden Sie die Ereignisdatenbank, um den ersten Benutzer einer virtuellen Maschine zu identifizieren und zu ermitteln, welche Benutzer sich bei der Maschine angemeldet haben.

Syntax

```
vdmadmin  
-R  
-i  
network_address
```

Nutzungshinweise

Die Option `-b` kann nicht verwendet werden, um diesen Befehl als Benutzer mit Administratorrechten auszuführen. Sie müssen als Benutzer mit der Rolle **Administrator** angemeldet sein.

Optionen

Die Option `-i` gibt die IP-Adresse der virtuellen Maschine an.

Beispiele

Zeigen Sie den ersten Benutzer an, der über die IP-Adresse 10.20.34.120 auf die virtuelle Maschine zugegriffen hat.

```
vdmadmin -R -i 10.20.34.120
```

Entfernen des Eintrags für eine Verbindungsserver-Instanz oder einen Sicherheitsserver mithilfe der Option „-S“

Sie können den Befehl `vdmadmin` mit der Option `-S` verwenden, um den Eintrag für eine Verbindungsserver-Instanz oder einen Sicherheitsserver aus der Horizon 7-Konfiguration zu entfernen.

Syntax

```
vdmin  
-S [-b Authentifizierungsargumente] -r-s Server
```

Nutzungshinweise

Um Hochverfügbarkeit zu gewährleisten, ermöglicht Horizon 7 die Konfiguration einer oder mehrerer Verbindungsserver-Replikatinstanzen in einer Verbindungsserver-Gruppe. Wenn Sie eine Verbindungsserver-Instanz in einer Gruppe deaktivieren, bleibt der Eintrag für den Server in der Horizon 7-Konfiguration erhalten.

Sie können auch den Befehl `vdmin` mit der Option `-S` verwenden, um einen Sicherheitsserver aus Ihrer Horizon 7-Umgebung zu entfernen. Sie müssen diese Option nicht verwenden, wenn Sie beabsichtigen, einen Sicherheitsserver zu aktualisieren oder neu zu installieren, ohne ihn permanent zu entfernen.

Führen Sie die folgenden Schritte aus, um den Eintrag dauerhaft zu entfernen:

- 1 Deinstallieren Sie die Verbindungsserver-Instanz oder den Sicherheitsserver vom Windows Server-Computer, indem Sie das Verbindungsserver-Installationsprogramm ausführen.
- 2 Entfernen Sie die ADAM-Instanz `VMwareVDMDS` vom Windows Server-Computer, indem Sie das Dienstprogramm `Add/Remove Programs (Software)` ausführen.
- 3 Verwenden Sie den Befehl `vdmin` auf einer anderen Verbindungsserver-Instanz, um den Eintrag für die deinstallierte Verbindungsserver-Instanz oder den Sicherheitsserver aus der Konfiguration zu entfernen.

Wenn Sie Horizon 7 auf den entfernten Systemen erneut installieren möchten, ohne die Horizon 7-Konfiguration der ursprünglichen Gruppe zu replizieren, starten Sie vor der erneuten Installation alle Verbindungsserver-Hosts in der ursprünglichen Gruppe neu. Dadurch wird verhindert, dass die erneut installierten Verbindungsserver-Instanzen die Konfigurationsaktualisierungen ihrer ursprünglichen Gruppe erhalten.

Optionen

Die Option `-s` gibt den NetBIOS-Namen der Verbindungsserver-Instanz oder des Sicherheitsservers an, die bzw. der entfernt werden soll.

Beispiele

Entfernen Sie den Eintrag für die Verbindungsserver-Instanz `connsvr3`.

```
vdmin -S -r -s connsvr3
```

Bereitstellen sekundärer Anmeldeinformationen für Administratoren mithilfe der Option „-T“

Sie können mithilfe des `vdmadmin`-Befehls und der `-T`-Option sekundäre Active Directory-Anmeldeinformationen für Administrationsbenutzer bereitstellen.

Syntax

```
vdmadmin
-T [-b Authentifizierungsargumente] -domainauth
{-add | -update | -remove | -removeall | -list} -ownerDomäne\Benutzer-userDomäne\Benutzer
[-passwordKennwort]
```

Nutzungshinweise

Wenn Ihre Benutzer und Gruppen sich in einer Domäne mit einer Ein-Weg-Vertrauensstellung mit der Verbindungsserver-Domäne befinden, müssen Sie für Administrationsbenutzer sekundäre Anmeldeinformationen in Horizon Administrator bereitstellen. Administratoren müssen für den Zugriff auf Domänen mit einer Ein-Weg-Vertrauensstellung über sekundäre Anmeldeinformationen verfügen. Bei Domänen mit einer Ein-Weg-Vertrauensstellung kann es sich um eine externe Domäne oder um eine Domäne in einer transitiven Gesamtstruktur-Vertrauensstellung handeln.

Sekundäre Anmeldedaten sind nur für Horizon Administrator-Sitzungen erforderlich und nicht für Desktop- und Anwendungssitzungen von Endbenutzern. Nur Administrationsbenutzer benötigen sekundäre Anmeldeinformationen.

Mit dem `vdmadmin`-Befehl können Sie sekundäre Anmeldeinformationen auf einer Benutzerbasis konfigurieren. Es ist nicht möglich, global gültige sekundäre Anmeldeinformationen zu konfigurieren.

Für eine Gesamtstruktur-Vertrauensstellung konfigurieren Sie in der Regel sekundäre Anmeldeinformationen nur für die Gesamtstruktur-Stammdomäne. Der Verbindungsserver hat dann die Möglichkeit, die untergeordneten Domänen in der Gesamtstruktur-Vertrauensstellung einzeln zu benennen.

Die Sperrung und Deaktivierung des Active Directory-Kontos sowie die Überprüfung der Anmeldezeiten können nur durchgeführt werden, wenn sich ein Benutzer bei einer Domäne mit einer Ein-Weg-Vertrauensstellung zum ersten Mal anmeldet.

Die PowerShell-Verwaltung und die Smartcard-Authentifizierung von Benutzern wird für Domänen mit einer Ein-Weg-Vertrauensstellung nicht unterstützt. Die SAML-Authentifizierung von Benutzern wird für Domänen mit einer Ein-Weg-Vertrauensstellung nicht unterstützt.

Konten mit sekundären Anmeldeinformationen erfordern die im Folgenden aufgeführten Berechtigungen. Ein Standardbenutzerkonto muss standardmäßig über diese Berechtigungen verfügen.

- Inhalt auflisten
- Alle Eigenschaften lesen

- Berechtigungen lesen
- tokenGroupsGlobalAndUniversal lesen (implizit enthalten in „Alle Eigenschaften lesen“)

Einschränkungen

- Die PowerShell-Verwaltung und die Smartcard-Authentifizierung von Benutzern in Domänen mit einer Ein-Weg-Vertrauensstellung wird nicht unterstützt.
- Die SAML-Authentifizierung von Benutzern wird für Domänen mit einer Ein-Weg-Vertrauensstellung nicht unterstützt.

Optionen

Tabelle 15-17. Optionen für die Bereitstellung von sekundären Anmeldeinformationen

Option	Beschreibung
<code>-add</code>	Fügt sekundäre Anmeldeinformationen für das Besitzerkonto hinzu. Mit einer Windows-Anmeldung wird überprüft, ob die angegebenen Anmeldeinformationen gültig sind. Für den Benutzer wird in View LDAP ein fremder Sicherheitsprinzipal (FSP, Foreign Security Principal) erstellt.
<code>-update</code>	Aktualisiert die sekundären Anmeldeinformationen für das Besitzerkonto. Mit einer Windows-Anmeldung wird überprüft, ob die aktualisierten Anmeldeinformationen gültig sind.
<code>-list</code>	Stellt die Sicherheitsanmeldeinformationen für das Besitzerkonto dar. Kennwörter werden nicht angezeigt.
<code>-remove</code>	Entfernt Sicherheitsanmeldeinformationen des Besitzerkontos.
<code>-removeall</code>	Entfernt alle Sicherheitsanmeldeinformationen des Besitzerkontos.

Beispiele

Fügt sekundäre Anmeldeinformationen für das angegebene Besitzerkonto hinzu. Mit einer Windows-Anmeldung wird überprüft, ob die angegebenen Anmeldeinformationen gültig sind.

```
vdmadmin -T -domainauth -add -owner Domäne\Benutzer -user Domäne\Benutzer -password Kennwort
```

Aktualisiert die sekundären Anmeldeinformationen für das angegebene Besitzerkonto. Mit einer Windows-Anmeldung wird überprüft, ob die aktualisierten Anmeldeinformationen gültig sind.

```
vdmadmin -T -domainauth -update -owner Domäne\Benutzer -user Domäne\Benutzer -password Kennwort
```

Entfernt sekundäre Anmeldeinformationen für das angegebene Besitzerkonto.

```
vdmadmin -T -domainauth -remove -owner Domäne\Benutzer -user Domäne\Benutzer
```

Entfernt alle sekundären Anmeldeinformationen für das angegebene Besitzerkonto.

```
vdmadmin -T -domainauth -removeall -owner Domäne\Benutzer
```

Stellt alle sekundären Anmeldeinformationen für das angegebene Besitzerkonto dar. Kennwörter werden nicht angezeigt.

```
vdmadmin -T -domainauth -list -owner Domäne\Benutzer
```

Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U“

Sie können den Befehl `vdmadmin` mit der Option `-U` verwenden, um detaillierte Informationen zu Benutzern anzuzeigen.

Syntax

```
vdmadmin
-U [-b authentication_arguments] -u domain\user [-w | -n] [-xml]
```

Nutzungshinweise

Der Befehl zeigt Informationen zu einem Benutzer aus Active Directory und Horizon 7 an.

- Active Directory-Informationen zum Konto des Benutzers.
- Mitgliedschaft in Active Directory-Gruppen.
- Computer-Berechtigungen, einschließlich Computer-ID, Anzeigename, Beschreibung, Ordner und Informationen dazu, ob ein Computer deaktiviert wurde.
- ThinApp-Zuweisungen.
- Administratorrollen, u. a. die Administratorrechte eines Benutzers sowie die Ordner, für die diese Rechte gelten.

Optionen

Die Option `-u` gibt den Namen und die Domäne des Benutzers an.

Beispiele

Zeigen Sie Informationen zum Benutzer Jo in der Domäne CORP im XML-Format mit ASCII-Zeichen an.

```
vdmadmin -U -u CORP\Jo -n -xml
```

Entsperren oder Sperren von virtuellen Maschinen mithilfe der Option „-V“

Sie können den Befehl `vdmadmin` mit der Option `-V` verwenden, um virtuelle Maschinen im Datacenter zu sperren oder zu entsperren.

Syntax

```
vdmadmin
-V [-bAuthentifizierungsargumente] -e-dDesktop-mComputer [-m Computer] ...
```

```
vdmadmin
-V [-bAuthentifizierungsargumente] -e-vcdnvCenter-DN-vmpath Pfad_Bestandsliste
```

```
vdmadmin
-V [-b Authentifizierungsargumente] -p-d Desktop -m Computer [-mComputer] ...
```

```
vdmadmin
-V [-bAuthentifizierungsargumente] -p-vcdnvCenter-DN-vmpath Pfad_Bestandsliste
```

Nutzungshinweise

Sie sollten ausschließlich den Befehl `vdmadmin` zum Entsperren oder Sperren einer virtuellen Maschine verwenden, wenn ein Problem dazu geführt hat, dass sich ein Remote-Desktop in einem fehlerhaften Zustand befindet. Verwenden Sie den Befehl nicht zur Verwaltung von Remote-Desktops, die ordnungsgemäß funktionieren.

Wenn ein Remote-Desktop gesperrt ist und der Eintrag für die zugehörige virtuelle Maschine nicht mehr in ADAM vorhanden ist, können Sie den Bestandslistenpfad der virtuellen Maschine und den vCenter Server über die Optionen `-vmpath` und `-vcdn` angeben. Mithilfe von vCenter Client können Sie den Bestandslistenpfad einer virtuellen Maschine für einen Remote-Desktop unter `Home/Bestandsliste/VMs` und `Vorlagen` ermitteln. Sie können in ADAM das Dienstprogramm ADSI-Editor verwenden, um den Distinguished Name der vCenter Server-Instanz unter der Überschrift `OU=Properties` zu suchen.

Optionen

Die folgende Tabelle zeigt die Optionen, die Sie zum Entsperren oder Sperren von virtuellen Maschinen angeben können.

Tabelle 15-18. Optionen für das Entsperren oder Sperren von virtuellen Maschinen

Option	Beschreibung
<code>-d Desktop</code>	Gibt den Desktop-Pool an.
<code>-e</code>	Entsperrt eine virtuelle Maschine.

Tabelle 15-18. Optionen für das Entsperren oder Sperren von virtuellen Maschinen (Fortsetzung)

Option	Beschreibung
<code>-m Computer</code>	Legt den Namen der virtuellen Maschine fest.
<code>-p</code>	Sperrt eine virtuelle Maschine.
<code>-vcdn vCenter_dn</code>	Gibt den Distinguished Name der vCenter Server-Instanz an.
<code>-vmopath inventory_path</code>	Legt den Bestandslistenpfad der virtuellen Maschine fest.

Beispiele

Entsperren Sie die virtuellen Maschinen `machine1` und `machine2` im Desktop-Pool `dtpool3`.

```
vdadmin -V -e -d dtpool3 -m machine1 -m machine2
```

Sperren Sie die virtuelle Maschine `machine3` im Desktop-Pool `dtpool3`.

```
vdadmin -V -p -d dtpool3 -m machine3
```

Ermitteln und Lösen von Konflikten bei LDAP-Einträgen und LDAP-Schemas mithilfe der Option „-X“

Sie können den Befehl `vdadmin` mit der Option `-x` verwenden, um Konflikte bei LDAP-Einträgen und LDAP-Schemas auf replizierten Verbindungsserver-Instanzen in einer Gruppe zu ermitteln und zu lösen. Mit dieser Option lassen sich auch LDAP-Schemakonflikte in einer Cloud-Pod-Architektur-Umgebung ermitteln und lösen.

Syntax

```
vdadmin
-X [-bAuthentifizierungsargumente] -collisions [-resolve]
vdadmin-X [-bAuthentifizierungsargumente] -schemacollisions [-resolve] [-global]
```

Nutzungshinweise

Wenn auf mindestens zwei Verbindungsserver-Instanzen die gleichen LDAP-Einträge erstellt wurden, kann dies zu Integritätsproblemen von LDAP-Daten in Horizon 7 führen. Diese können auftreten, wenn ein Upgrade durchgeführt wird, wenn die LDAP-Replikation nicht verwendet wird. Auch wenn Horizon 7 in regelmäßigen Abständen nach dieser Fehlerbedingung sucht, können Sie den Befehl `vdadmin` auf den Verbindungsserver-Instanzen in der Gruppe ausführen, um Konflikte bei LDAP-Einträgen manuell zu ermitteln und diese zu lösen.

LDAP-Schemakonflikte können auch während einer Aktualisierung auftreten, wenn die LDAP-Replikation nicht betriebsbereit ist. Da Horizon 7 diese Fehlerbedingung nicht prüft, müssen Sie den Befehl `vdadmin` zur Ermittlung und Lösung von LDAP-Schemakonflikten manuell ausführen.

Optionen

Die folgende Tabelle enthält die Optionen, die für die Ermittlung und Lösung von Konflikten bei LDAP-Einträgen festgelegt werden können.

Tabelle 15-19. Optionen zum Ermitteln und Lösen von Konflikten bei LDAP-Einträgen

Option	Beschreibung
<code>-collisions</code>	Legt einen Vorgang zur Ermittlung von Konflikten bei LDAP-Einträgen in einer Verbindungsserver-Gruppe fest.
<code>-resolve</code>	Löst alle LDAP-Konflikte in der LDAP-Instanz. Wenn Sie diese Option nicht festlegen, listet der Befehl nur die von ihm ermittelten Probleme auf.

Die folgende Tabelle enthält die Optionen, für die Ermittlung und Behebung von LDAP-Schemakonflikten festgelegt werden können.

Tabelle 15-20. Optionen zum Ermitteln und Lösen von LDAP-Schemakonflikten

Option	Beschreibung
<code>-schemacollisions</code>	Legt einen Vorgang zur Ermittlung von LDAP-Schemakonflikten in einer Verbindungsserver-Gruppe oder in einer Cloud-Pod-Architektur-Umgebung fest.
<code>-resolve</code>	Löst alle LDAP-Schemakonflikte in der LDAP-Instanz. Wenn Sie diese Option nicht festlegen, listet der Befehl nur die von ihm ermittelten Probleme auf.
<code>-global</code>	Wendet die Konfliktprüfung und -lösung für die globale LDAP-Instanz in einer Cloud-Pod-Architektur-Umgebung an. Wenn Sie diese Option nicht festlegen, wird die Prüfung für die lokale LDAP-Instanz ausgeführt.

Beispiele

Ermitteln von Konflikten bei LDAP-Einträgen in einer Verbindungsserver-Gruppe.

```
vdadmin -X -collisions
```

Ermitteln und Lösen von Konflikten bei LDAP-Einträgen in der lokalen LDAP-Instanz.

```
vdadmin -X -collisions -resolve
```

Ermitteln und Lösen von LDAP-Schemakonflikten in der globalen LDAP-Instanz.

```
vdadmin -X -schemacollisions -resolve -global
```