

Horizon 7-Verwaltung

MÄRZ 2020

VMware Horizon 7 7.12



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 © 2014–2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Horizon 7-Verwaltung 11

1 Verwenden von Horizon Administrator 12

- Horizon Administrator und Horizon-Verbindungsserver 12
- Anmelden bei Horizon Administrator 13
- Tipps zur Verwendung der Horizon Administrator-Oberfläche 14
- Fehlerbehebung bei der Textanzeige in Horizon Administrator 16

2 Konfigurieren von Horizon-Verbindungsserver 18

- Konfigurieren von vCenter Server und View Composer 18
 - Erstellen eines Benutzerkontos für View Composer-AD-Vorgänge 18
 - Hinzufügen von vCenter Server-Instanzen zu Horizon 7 20
 - Konfigurieren von View Composer-Einstellungen 22
 - Konfigurieren von View Composer-Domänen 23
 - Zulassen, dass vSphere Speicherplatz auf virtuellen Linked-Clone-Maschinen freigibt 24
 - Konfigurieren der View-Speicherbeschleunigung für vCenter Server 26
 - Grenzwerte für parallele Vorgänge für vCenter Server und View Composer 28
 - Einstellen der Anzahl paralleler Vorgänge zum Ändern des Betriebszustands, um Remote-Desktop-Anmeldungsüberlastungen zu unterstützen 29
 - Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats 30
 - Entfernen einer vCenter Server-Instanz aus Horizon 7 32
 - Entfernen von View Composer aus Horizon 7 33
 - Konflikte bei eindeutigen IDs für vCenter Server 34
- Sichern von Horizon-Verbindungsserver 34
- Konfigurieren der Einstellungen für Clientsitzungen 34
 - Festlegen von Optionen für Clientsitzungen und -verbindungen 35
 - Ändern des Kennworts für die Datenwiederherstellung 35
 - Globale Einstellungen für Clientsitzungen 36
 - Globale Sicherheitseinstellungen für Clientsitzungen und -verbindungen 40
 - Sicherheitsmodus für Nachrichten für Horizon 7-Komponenten 42
 - Konfigurieren des sicheren Tunnels und des PCoIP Secure Gateway 46
 - Konfigurieren des Blast-Sicherheitsgateways 47
 - Verschieben von TLS-Verbindungen auf Zwischenserver 49
 - Konfigurieren des Gateway-Standorts für einen Horizon-Verbindungsserver- oder Sicherheitsserver-Host 52
- Deaktivieren oder Aktivieren von Horizon-Verbindungsserver 52
- Bearbeiten der externen URLs 53
- Beitreten oder Verlassen des Programms zur Verbesserung der Benutzerfreundlichkeit 55

[View LDAP-Verzeichnis](#) 55

3 Einrichten der Smartcard-Authentifizierung 57

[Anmelden über eine Smartcard](#) 58

[Konfigurieren der Smart Card-Authentifizierung auf dem Horizon-Verbindungsserver](#) 59

[Anfordern der Zertifizierungsstellenzertifikate](#) 59

[Anfordern des CA-Zertifikats von Windows](#) 60

[Hinzufügen des CA-Zertifikats zu einer Server-Vertrauensspeicherdatei](#) 61

[Ändern von Horizon-Verbindungsserver-Konfigurationseigenschaften](#) 62

[Konfigurieren von Smartcard-Einstellungen in Horizon Administrator](#) 63

[Konfigurieren der Smartcard-Authentifizierung auf Drittanbieterlösungen](#) 67

[Vorbereiten von Active Directory für die Smartcard-Authentifizierung](#) 67

[Hinzufügen von UPNs für Smartcard-Benutzer](#) 68

[Hinzufügen des Stammzertifikats zum Enterprise NTAAuth-Speicher](#) 69

[Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen](#) 69

[Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen](#) 71

[Überprüfen der Smartcard-Authentifizierungskonfiguration](#) 72

[Verwenden der Smartcard-Zertifikatsperrüberprüfung](#) 73

[Anmelden bei Verwendung der Überprüfung von Zertifikatsperrlisten](#) 74

[Anmelden bei Verwendung der OCSP-Zertifikatsperrüberprüfung](#) 74

[Konfigurieren der Überprüfung von Zertifikatsperrlisten](#) 75

[Konfigurieren der OCSP-Zertifikatsperrüberprüfung](#) 76

[Eigenschaften der Smartcard-Zertifikatsperrüberprüfung](#) 77

4 Einrichten anderer Typen der Benutzerauthentifizierung 78

[Verwenden der zweistufigen Authentifizierung](#) 78

[Anmeldung unter Verwendung der zweistufigen Authentifizierung](#) 79

[Aktivieren der zweistufigen Authentifizierung in Horizon Administrator](#) 80

[Fehlerbehebung bei Verweigerung des Zugriffs auf RSA SecurID](#) 82

[Fehlerbehebung bei Verweigerung des Zugriffs auf RADIUS](#) 83

[Verwenden der SAML-Authentifizierung](#) 83

[Verwenden der SAML-Authentifizierung zur VMware Identity Manager-Integration](#) 84

[Konfigurieren eines SAML-Authentifikators in Horizon Administrator](#) 85

[Konfigurieren der Proxy-Unterstützung für VMware Identity Manager](#) 87

[Ändern des Ablaufzeitraums der Metadaten von Diensteanbietern auf dem Verbindungsserver](#) 88

[Generieren von SAML-Metadaten für die Verwendung des Verbindungservers als Diensteanbieter](#) 89

[Aspekte der Antwortzeit für mehrere dynamische SAML-Authentifikatoren](#) 89

[Konfigurieren der Workspace ONE-Richtlinien in Horizon Administrator](#) 90

[Konfigurieren der biometrischen Authentifizierung](#) 91

5 Authentifizieren von Benutzern ohne Anforderung von Anmeldeinformationen 92

Bereitstellen eines nicht authentifizierten Zugriffs auf veröffentlichte Anwendungen	93
Erstellen von Benutzern für einen nicht authentifizierten Zugriff	94
Aktivieren des nicht authentifizierten Zugriffs für Benutzer	96
Erteilen von Berechtigungen für Benutzer für einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen	96
Suchen nach Sitzungen mit einem nicht authentifizierten Zugriff	97
Löschen eines Benutzers für einen nicht authentifizierten Zugriff	98
Nicht authentifizierter Zugriff von Horizon Client aus	98
Konfigurieren der Anmeldeverzögerung bei nicht authentifiziertem Zugriff auf veröffentlichte Anwendungen	99
Konfigurieren von Benutzern für die Hybrid-Anmeldung	100
Verwenden der Funktion „Als aktueller Benutzer anmelden“, die mit Windows-basierten Horizon Client-Instanzen verfügbar ist	102
Speichern von Anmeldeinformationen in Horizon Clients für Mobilgeräte und Mac	103
Konfigurieren eines Zeitüberschreitungslimits zum Speichern von Horizon Client-Anmeldeinformationen	104
Einrichten von True SSO	104
Festlegen der Architektur für True SSO	105
Einrichten einer Unternehmenszertifizierungsstelle	108
Erstellen von Zertifikatvorlagen für die Verwendung mit True SSO	110
Installieren und Einrichten eines Registrierungsservers	113
Exportieren des Registrierungsdienst-Clientzertifikats	116
Importieren des Registrierungsdienst-Clientzertifikats in den Registrierungsserver	117
Konfigurieren der SAML-Authentifizierung für die Verwendung von True SSO	119
Konfigurieren des Horizon-Verbindungsservers für True SSO	121
Befehlszeilenreferenz für die True SSO-Konfiguration	123
Erweiterte Konfigurationseinstellungen für True SSO	128
Identifizieren eines AD-Benutzers ohne Active Directory-UPN	132
Entsperren eines Desktops mit True SSO und Workspace ONE	133
Verwenden des Systemzustand-Dashboards zur Behebung von Fehlern im Zusammenhang mit True SSO	134

6 Konfigurieren der rollenbasierten Verwaltungsdelegierung 139

Grundlegendes zu Rollen und Berechtigungen	139
Verwendung von Zugriffsgruppen zur Delegierung der Verwaltung von Pools und Farmen	140
Unterschiedliche Administratoren für unterschiedliche Zugriffsgruppen	141
Unterschiedliche Administratoren für dieselbe Zugriffsgruppe	141
Grundlegendes zu Berechtigungen	142
Verwalten von Administratoren	143
Erstellen eines Administrators	144
Entfernen eines Administrators	145
Verwalten und Überprüfen von Berechtigungen	146
Hinzufügen einer Berechtigung	146

Löschen einer Berechtigung	147
Überprüfen von Berechtigungen	148
Verwalten und Prüfen von Zugriffsgruppen	149
Hinzufügen einer Zugriffsgruppe	149
Verschieben eines Desktop-Pools oder einer Farm in eine andere Zugriffsgruppe	150
Entfernen einer Zugriffsgruppe	150
Überprüfen der Desktop-Pools, Anwendungspools oder Farmen in einer Zugriffsgruppe	150
Überprüfen der vCenter-VMs in einer Zugriffsgruppe	151
Verwalten von benutzerdefinierten Rollen	151
Hinzufügen einer benutzerdefinierten Rolle	152
Ändern der Berechtigungen in einer benutzerdefinierten Rolle	152
Entfernen einer benutzerdefinierten Rolle	152
Vordefinierte Rollen und Berechtigungen	153
Vordefinierte Administratorrollen	154
Globale Berechtigungen	157
Objektspezifische Berechtigungen	158
Interne Berechtigungen	159
Erforderliche Berechtigungen für häufige Aufgaben	160
Berechtigungen für die Pool-Verwaltung	160
Berechtigungen für die Verwaltung von Maschinen	160
Berechtigungen für die Verwaltung persistenter Festplatten	161
Berechtigungen für die Verwaltung von Benutzern und Administratoren	161
Berechtigungen für Horizon Help Desk Tool-Aufgaben	162
Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle	162
Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen	163

7 Konfigurieren von Richtlinien in Horizon Administrator und Active Directory 165

Festlegen von Richtlinien in Horizon Administrator	165
Konfigurieren globaler Richtlinieneinstellungen	166
Konfigurieren von Richtlinien für Desktop-Pools	166
Konfigurieren von Richtlinien für Benutzer	167
Horizon 7-Richtlinien	167
Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien (ADM) für Horizon 7	168
Horizon 7-ADMX-Vorlagendateien	169
Einstellungen für ADMX-Vorlagen für die Konfiguration des Horizon-Verbindungservers	171
Einstellungen für ADMX-Vorlagen für die allgemeine Horizon 7-Konfiguration	172

8 Warten von Horizon 7-Komponenten 176

Sichern und Wiederherstellen von Horizon 7-Konfigurationsdaten	176
Sichern von Horizon-Verbindungsserver- und View Composer-Daten	177
Wiederherstellen von Horizon-Verbindungsserver- und View Composer-Konfigurationsdaten	180

Exportieren von Daten aus der View Composer-Datenbank	185
Überwachen von Horizon 7-Komponenten	186
Überwachen des Computerstatus	187
Grundlegendes zu Horizon 7-Diensten	188
Beenden und Starten der Horizon 7-Dienste	188
Dienste auf einem Verbindungsserver-Host	189
Dienste auf einem Sicherheitsserver	190
Ändern des Produktlizenzschlüssels	190
Überwachen der Nutzung der Produktlizenz	192
Zurücksetzen der Daten zur Nutzung der Produktlizenz	193
Aktualisieren allgemeiner Benutzerinformationen aus Active Directory	193
Migrieren von View Composer auf eine andere Maschine	194
Anleitungen für die Migration von View Composer	195
Migrieren von View Composer mit einer vorhandenen Datenbank	196
Migrieren von View Composer ohne virtuelle Linked-Clone-Maschinen	198
Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln	199
Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst	200
Aktualisieren der Zertifikate auf einer Verbindungsserver-Instanz, einem Sicherheitsserver oder View Composer	201
Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit	203

9 Verwalten von ThinApp-Anwendungen in Horizon Administrator 204

Horizon 7-Anforderungen für ThinApp-Anwendungen	204
Erfassen und Speichern von Anwendungspaketen	205
Paketieren von Anwendungen	206
Erstellen einer Windows-Netzwerkfreigabe	207
Registrieren eines Anwendungs-Repositorys	207
Hinzufügen von ThinApp-Anwendungen zu Horizon Administrator	208
Erstellen einer ThinApp-Vorlage	209
Zuweisen von ThinApp-Anwendungen zu Maschinen und Desktop-Pools	209
Empfohlene Vorgehensweisen für die Zuweisung von ThinApp-Anwendungen	211
Zuweisen einer ThinApp-Anwendung zu mehreren Computern	211
Zuweisen mehrerer ThinApp-Anwendungen zu einem Computer	212
Zuweisen einer ThinApp-Anwendung zu mehreren Desktop-Pools	213
Zuweisen mehrerer ThinApp-Anwendungen zu einem Desktop-Pool	214
Zuweisen einer ThinApp-Vorlage zu einer Maschine oder zu einem Desktop-Pool	215
Anzeigen von ThinApp-Anwendungszuweisungen	217
Anzeigen von MSI-Paketinformationen	218
Verwalten von ThinApp-Anwendungen in Horizon Administrator	218
Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Computern	219
Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einer Maschine	220
Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Desktop-Pools	220

Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einem Desktop-Pool	221
Entfernen einer ThinApp-Anwendung aus Horizon Administrator	221
Ändern oder Löschen einer ThinApp-Vorlage	222
Entfernen eines Anwendungs-Repository	222
Überwachen von und Fehlerbehebung bei ThinApp-Anwendungen in Horizon Administrator	222
Keine Registrierung eines Anwendungs-Repositorys möglich	223
Kein Hinzufügen von ThinApp-Anwendungen zu Horizon Administrator möglich	223
Kein Zuweisen einer ThinApp-Vorlage möglich	224
ThinApp-Anwendung wird nicht installiert	225
ThinApp-Anwendung wird nicht deinstalliert	225
MSI-Paket ist ungültig	226
ThinApp-Konfigurationsbeispiel	227

10 Einrichten von Clients im Kiosk-Modus 229

Konfigurieren von Clients im Kiosk-Modus	230
Vorbereiten von Active Directory und Horizon 7 für Clients im Kiosk-Modus	231
Festlegen von Standardwerten für Clients im Kiosk-Modus	232
Anzeigen der MAC-Adressen von Clientgeräten	234
Hinzufügen von Konten für Clients im Kiosk-Modus	234
Authentifizierung von Clients im Kiosk-Modus aktivieren	236
Überprüfen der Konfiguration von Clients im Kiosk-Modus	238
Verbinden mit Remote-Desktops über Clients im Kiosk-Modus	239

11 Fehlerbehebung für Horizon 7 242

Verwenden von Horizon Help Desk Tool	242
Prüfen der Horizon Help Desk Tool-Lizenz	243
Konfigurieren des rollenbasierten Zugriffs für Horizon Help Desk Tool	244
Anmelden bei Horizon Help Desk Tool	245
Fehlerbehebung bei Benutzern in Horizon Help Desk Tool	245
Sitzungsdetails für das Horizon Help Desk Tool	249
Sitzungsprozesse für das Horizon Help Desk Tool	253
Anwendungsstatus für das Horizon Help Desk Tool	254
Fehlerbehebung bei Desktop- oder Anwendungssitzungen in Horizon Help Desk Tool	254
Verwenden der VMware-Anmeldeüberwachung	256
Konfigurationseinstellungen der Anmeldeüberwachung	260
Verwenden von VMware Horizon Performance Tracker	261
Konfigurieren von VMware Horizon Performance Tracker	262
Konfigurieren der Gruppenrichtlinieneinstellungen für den Horizon Performance Tracker	263
Ausführen von Horizon Performance Tracker	264
Überwachen des Systemzustands	266
Überwachen von Ereignissen in Horizon 7	266

Horizon 7-Ereignismeldungen	267
Sammeln von Diagnoseinformationen für Horizon 7	268
Erstellen eines Data Collection Tool-Pakets für Horizon Agent	269
Speichern von Diagnoseinformationen für Horizon Client für Windows	270
Sammeln von Diagnoseinformationen für View Composer mithilfe des Supportskripts	270
Sammeln von Diagnoseinformationen für Horizon-Verbindungsserver	271
Sammeln von Diagnoseinformationen für Horizon Agent, Horizon Client oder den Horizon-Verbindungsserver von der Konsole aus	272
Integration des Horizon-Verbindungservers mit Skyline Collector-Appliance	274
Aktualisieren von Supportanfragen	274
Fehlerbehebung einer nicht erfolgreichen Sicherheitsserverkopplung mit Horizon-Verbindungsserver	275
Fehlerbehebung der Horizon 7 Server-Zertifikatsperrüberprüfung	276
Fehlerbehebung bei der Smartcard-Zertifikatsperrüberprüfung	277
Weitere Informationen zur Fehlerbehebung	278

12 Verwenden des Befehls „vdmadmin“ 279

Verwendung des Befehls „vdmadmin“	281
Authentifizierung für den Befehl „vdmadmin“	282
Ausgabeformat des Befehls „vdmadmin“	282
Optionen des Befehls „vdmadmin“	283
Konfigurieren der Protokollierung in Horizon Agent mithilfe der Option „-A“	284
Außerkraftsetzen von IP-Adressen mithilfe der Option „-A“	287
Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F“	288
Auflisten und Anzeigen von Systemüberwachungen mithilfe der Option „-H“	289
Auflisten und Anzeigen von Berichten zum Horizon 7-Betrieb unter Verwendung der Option „-I“	291
Generieren von Horizon 7-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-I“	292
Zuweisen von dedizierten Computern unter Verwendung der Option „-L“	294
Anzeigen von Informationen zu Maschinen mithilfe der Option „-M“	296
Rückgewinnung von Datenträgerplatz auf virtuellen Maschinen mithilfe der Option „-M“	297
Konfigurieren von Domänenfiltern mithilfe der Option „-N“	298
Konfigurieren von Domänenfiltern	301
Beispiel für die Filterung zum Einschließen von Domänen	303
Beispiel für die Filterung zum Ausschließen von Domänen	304
Anzeigen der Maschinen und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“	306
Konfigurieren von Clients im Kiosk-Modus mithilfe der Option „-Q“	308
Anzeigen des ersten Benutzers einer Maschine mithilfe der Option „-R“	314
Entfernen des Eintrags für eine Verbindungsserver-Instanz oder einen Sicherheitsserver mithilfe der Option „-S“	314
Bereitstellen sekundärer Anmeldeinformationen für Administratoren mithilfe der Option „-T“	316
Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U“	318
Entsperren oder Sperren von virtuellen Maschinen mithilfe der Option „-V“	319

Ermitteln und Lösen von Konflikten bei LDAP-Einträgen und LDAP-Schemas mithilfe der Option „-X“ 320

Horizon 7-Verwaltung

Horizon 7-Verwaltung beschreibt die Konfiguration und Verwaltung von VMware Horizon[®] 7. Hierzu zählen u.a. folgende Aufgaben: Konfigurieren des Horizon-Verbindungsservers, Erstellen von Administratoren, Einrichten der Benutzerauthentifizierung, Konfigurieren von Richtlinien und Verwalten von VMware ThinApp[®]-Anwendungen in Horizon Administrator. In diesem Dokument wird außerdem die Wartung und Fehlerbehebung für Horizon 7-Komponenten beschrieben.

Zielgruppe

Diese Informationen richten sich an Benutzer, die VMware Horizon 7 konfigurieren und verwalten möchten. Die bereitgestellten Informationen sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb von Rechenzentren vertraut sind.

Verwenden von Horizon Administrator

1

Horizon Administrator ist die Webschnittstelle, über die Sie Horizon-Verbindungsserver konfigurieren und Ihre Remote-Desktops und -anwendungen verwalten.

Einen Vergleich der Vorgänge, die Sie mit Horizon Administrator, Cmdlets und vdmadmin durchführen können, finden Sie im Dokument *Horizon 7-Integration*.

Dieses Kapitel enthält die folgenden Themen:

- [Horizon Administrator und Horizon-Verbindungsserver](#)
- [Anmelden bei Horizon Administrator](#)
- [Tipps zur Verwendung der Horizon Administrator-Oberfläche](#)
- [Fehlerbehebung bei der Textanzeige in Horizon Administrator](#)

Horizon Administrator und Horizon-Verbindungsserver

Horizon Administrator bietet eine webbasierte Verwaltungsschnittstelle für Horizon 7.

Der Horizon-Verbindungsserver kann über mehrere Instanzen verfügen, die als Replizierungs- oder Sicherheitsserver dienen. Je nach Ihrer Horizon 7-Bereitstellung erhalten Sie eine eigene Horizon Administrator-Oberfläche mit jeder Instanz eines Verbindungsservers.

Wir empfehlen die folgenden Best Practices für die Verwendung von Horizon Administrator mit einem Verbindungsserver:

- Verwenden Sie den Hostnamen und die IP-Adresse des Verbindungsservers für die Anmeldung bei Horizon Administrator. Verwenden Sie die Horizon Administrator-Oberfläche zur Verwaltung des Verbindungsservers und jedes damit verbundenen Sicherheits- oder Replizierungsservers.
- Stellen Sie in einer Pod-Umgebung sicher, dass alle Administratoren den Hostnamen und die IP-Adresse desselben Verbindungsservers für die Anmeldung bei Horizon Administrator verwenden. Für den Zugriff auf eine Horizon Administrator-Webseite dürfen Sie keinesfalls den Hostnamen und die IP-Adresse des Lastausgleichsdienstes verwenden.

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

Hinweis Wenn Sie anstelle von Sicherheitsservern Unified Access Gateway-Appliances benutzen, müssen Sie die Unified Access Gateway-REST-API zur Verwaltung der Unified Access Gateway-Appliances verwenden. Frühere Versionen von Unified Access Gateway wurden als „Access Point“ bezeichnet. Weitere Informationen finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

Anmelden bei Horizon Administrator

Zum Ausführen anfänglicher Konfigurationsaufgaben müssen Sie sich bei Horizon Administrator anmelden. Sie können unter Verwendung einer sicheren Verbindung (TLS) auf Horizon Administrator zugreifen.

Hinweis Horizon Administrator wird Anfang 2020 veraltet sein. Sie können mit der Horizon Console dieselben administrativen Aufgaben durchführen. Weitere Informationen zur Verwendung der Horizon Console finden Sie im Dokument *Verwaltung der VMware Horizon Console*.

Voraussetzungen

- Stellen Sie sicher, dass der Horizon-Verbindungsserver auf einem dedizierten Computer installiert ist.
- Vergewissern Sie sich, dass Sie einen von Horizon Administrator unterstützten Webbrowser verwenden. Informationen zu den Anforderungen für Horizon Administrator 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 zu dem 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 Administrator hängt von der Art Zertifikat ab, die 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 Horizon-Verbindungsserver signiert ist.	Wenn Sie zum ersten Mal eine Verbindung herstellen, zeigt Ihr Webbrowser die Seite Willkommen bei VMware Horizon 7 an.
Das standardmäßige selbst signierte Zertifikat, das mit Horizon-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 Klicken Sie unter Horizon Administrator auf **Start**.

3 Melden Sie sich mit einem Benutzerkonto an, das die Rolle „Administratoren“ besitzt.

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.

Ergebnisse

Nachdem Sie sich bei Horizon Administrator angemeldet haben, können Sie mit der Option **View-Konfiguration > Administratoren** die Liste der Benutzer und Gruppen ändern, die über die Administratorrolle verfügen.

Tipps zur Verwendung der Horizon Administrator-Oberfläche

Sie können mithilfe der Funktionen der Horizon Administrator-Benutzeroberfläche in Horizon-Seiten navigieren, nach Horizon-Objekten suchen sowie Horizon-Objekte filtern und sortieren.

Horizon Administrator umfasst viele gängige Funktionen in der Benutzeroberfläche. So werden Sie z. B. im linken Navigationsbereich auf jeder Seite auf weitere Horizon Administrator-Seiten weitergeleitet. Mit den Suchfiltern können Sie Filterkriterien in Bezug auf die gesuchten Objekte auswählen.

Die folgende Tabelle beschreibt einige weitere Funktionen, die die Verwendung von Horizon Administrator unterstützen.

Tabelle 1-1. Horizon Administrator-Navigations- und Anzeigefunktionen

Horizon Administrator-Funktion	Beschreibung
In Horizon Administrator-Seiten vorwärts und rückwärts navigieren	<p>Klicken Sie auf die Schaltfläche Zurück in Ihrem Browser, um zur vorher angezeigten Horizon Administrator-Seite zurückzukehren. Klicken Sie auf die Schaltfläche Weiter, um zur aktuellen Seite zurückzukehren.</p> <p>Wenn Sie auf die Schaltfläche Zurück des Browsers klicken, während Sie einen Assistenten oder ein Dialogfeld von Horizon Administrator verwenden, kehren Sie zur Hauptseite von Horizon Administrator zurück. Die im Assistenten oder Dialogfeld eingegebenen Informationen gehen dann verloren.</p> <p>In Versionen vor View 5.1 können Sie mit den Schaltflächen Zurück und Weiter Ihres Browsers in Horizon Administrator nicht navigieren. Zur Navigation waren im Horizon Administrator-Fenster eigene Schaltflächen Zurück und Weiter vorgesehen. Diese Schaltflächen wurden in Version 5.1 von View entfernt.</p>
Erstellen von Lesezeichen von Horizon Administrator-Seiten	<p>Sie können in Ihrem Browser Lesezeichen von Horizon Administrator-Seiten erstellen.</p>
Mehrspaltige Sortierung	<p>Sie können Horizon-Objekte mithilfe der mehrspaltigen Sortierung auf unterschiedliche Art und Weise sortieren.</p> <p>Klicken Sie auf eine Überschrift in der obersten Zeile einer Horizon Administrator-Tabelle, um die Horizon-Objekte alphabetisch anhand dieser Überschrift zu sortieren. Beispielsweise können Sie auf der Seite Ressourcen > Computer auf Desktop-Pool klicken, um Desktops nach den Pools zu sortieren, in denen sie enthalten sind. Neben der Überschrift wird die Zahl 1 angezeigt, um anzugeben, dass sie die Spalte für die primäre Sortierung ist. Sie können erneut auf die Überschrift klicken, um die Sortierreihenfolge umzukehren. Dies wird durch einen nach oben oder unten weisenden Pfeil angezeigt.</p> <p>Um die Horizon-Objekte nach einem zweiten Element zu sortieren, markieren Sie eine weitere Überschrift mit der Tastenkombination Strg+Klick.</p> <p>Sie können z. B. in der Tabelle „Computer“ auf Benutzer klicken, um eine zweite Sortierung nach den Benutzern durchzuführen, denen die Desktops zugeordnet sind. Neben der zweiten Überschrift wird die Zahl 2 angezeigt. In diesem Beispiel werden die Desktops nach dem Pool und nach den Benutzern in jedem Pool sortiert.</p> <p>Sie können mit Strg+Klick alle Spalten in einer Tabelle in absteigender Reihenfolge ihrer Bedeutung sortieren.</p> <p>Drücken Sie Strg+Umschalt+Klick, um die Auswahl eines Sortierelements aufzuheben.</p> <p>Sie möchten z.B. die Desktops in einem Pool anzeigen, die sich in einem bestimmten Zustand befinden und in einem bestimmten Datenspeicher gespeichert sind. Sie können Ressourcen > Computer auswählen, auf die Überschrift Datenspeicher klicken und mit Strg+Klick die Überschrift Status auswählen.</p>

Tabelle 1-1. Horizon Administrator-Navigations- und Anzeigefunktionen (Fortsetzung)

Horizon Administrator-Funktion	Beschreibung
Anpassen der Tabellenspalten	<p>Sie können die Anzeige von Horizon Administrator-Tabellenspalten durch Ausblenden von ausgewählten Spalten und Sperren der ersten Spalte anpassen. Mit dieser Funktion können Sie die Anzeige großer Tabellen wie beispielsweise Katalog > Desktop-Pools steuern, die viele Spalten enthalten.</p> <p>Klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift, um ein Kontextmenü anzuzeigen, in dem Sie folgende Aktionen auswählen können:</p> <ul style="list-style-type: none"> ■ Die ausgewählte Spalte ausblenden ■ Spalten anpassen. Ein Dialogfeld zeigt alle Spalten in der Tabelle an. Sie können auswählen, welche Spalten angezeigt oder ausgeblendet werden sollen. ■ Die erste Spalte sperren. Diese Option bewirkt, dass die linke Spalte angezeigt bleibt, während Sie eine Tabelle mit vielen Spalten horizontal verschieben. Beispielsweise bleibt auf der Seite Katalog > Desktop-Pools die Desktop-ID sichtbar, während Sie den Bildschirm horizontal verschieben, um weitere Desktop-Merkmale anzuzeigen.
Auswählen von Horizon-Objekten und Anzeigen von Horizon-Objektdetails	<p>Sie können in Horizon Administrator-Tabellen, die Horizon-Objekte auflisten, ein Objekt auswählen oder Objektdetails anzeigen.</p> <ul style="list-style-type: none"> ■ Um ein Objekt auszuwählen, klicken Sie in der Tabelle in der Objektzeile auf eine beliebige Stelle. Im oberen Bereich der Seite werden die Menüs und Befehle, die das Objekt verwalten, aktiv. ■ Um Objektdetails anzuzeigen, doppelklicken Sie in der Objektzeile auf die linke Zelle. Es wird eine neue Seite in den Objektdetails angezeigt. <p>Klicken Sie beispielsweise auf die Seite Katalog > Desktop-Pools und klicken Sie an eine beliebige Stelle einer einzelnen Zeile im Pool, um die Befehle zu aktivieren, die sich auf den Pool auswirken.</p> <p>Doppelklicken Sie auf die Zelle ID in der linken Spalte, um eine neue Seite anzuzeigen, die Details zum Pool enthält.</p>
Erweitern von Dialogfeldern zur Anzeige von Detailinformationen	<p>Sie können Horizon Administrator-Dialogfelder erweitern, um Detailinformationen wie z. B. Desktop-Namen und Benutzernamen in Tabellenspalten anzuzeigen.</p> <p>Zum Erweitern eines Dialogfelds platzieren Sie die Maus über den Punkten in der rechten unteren Ecke des Dialogfelds und führen Sie eine Ziehoperation aus.</p>
Anzeigen von Kontextmenüs für Horizon-Objekte	<p>Sie können mit der rechten Maustaste auf Horizon-Objekte in Horizon Administrator-Tabellen klicken, um Kontextmenüs anzuzeigen. Ein Kontextmenü ermöglicht Ihnen den Zugriff auf die Befehle, die für das ausgewählte Horizon-Objekt ausgeführt werden können.</p> <p>Sie können beispielsweise auf der Seite Katalog > Desktop-Pools mit der rechten Maustaste auf einen Desktop-Pool klicken, um Befehle wie Hinzufügen, Bearbeiten, Löschen, Bereitstellung deaktivieren (oder aktivieren) usw. anzuzeigen.</p>

Fehlerbehebung bei der Textanzeige in Horizon Administrator

Wenn Ihr Webbrowser auf einem Nicht-Windows-Betriebssystem wie beispielsweise Linux, UNIX oder Mac OS ausgeführt wird, wird der Text in Horizon Administrator nicht ordnungsgemäß angezeigt.

Problem

Der Text in der Benutzeroberfläche von Horizon Administrator ist unleserlich. Es treten beispielsweise Leerzeichen in Wörtern auf.

Ursache

Für Horizon Administrator sind Microsoft-spezifische Schriftarten erforderlich.

Lösung

Installieren Sie Microsoft-spezifische Schriftarten auf Ihrem Computer.

Derzeit werden auf der Microsoft-Website keine Microsoft-Schriftarten bereitgestellt, Sie können die Schriftarten jedoch von unabhängigen Websites herunterladen.

Konfigurieren von Horizon-Verbindungsserver

2

Nachdem Sie Horizon-Verbindungsserver installiert und die Erstkonfiguration durchgeführt haben, können Sie vCenter Server-Instanzen und View 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 View Composer](#)
- [Sichern von Horizon-Verbindungsserver](#)
- [Konfigurieren der Einstellungen für Clientsitzungen](#)
- [Deaktivieren oder Aktivieren von Horizon-Verbindungsserver](#)
- [Bearbeiten der externen URLs](#)
- [Beitreten oder Verlassen des Programms zur Verbesserung der Benutzerfreundlichkeit](#)
- [View LDAP-Verzeichnis](#)

Konfigurieren von vCenter Server und View Composer

Um virtuelle Maschinen als Remote-Desktops zu verwenden, müssen Sie View konfigurieren, um mit vCenter Server zu kommunizieren. Um Linked-Clone-Desktop-Pools zu erstellen und zu verwalten, müssen Sie die View Composer-Einstellungen in Horizon Administrator 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 die View-Speicherbeschleunigung für vCenter Server aktivieren.

Erstellen eines Benutzerkontos für View Composer-AD-Vorgänge

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

Zur Gewährleistung der Sicherheit sollten Sie ein separates Benutzerkonto für View Composer erstellen. 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 für das View Composer-Konto nicht die Berechtigungen eines Domänenadministrators 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 Administrator an, wenn Sie View Composer-Domänen im Assistenten zum Hinzufügen von vCenter Server konfigurieren und Linked-Clone-Desktop-Pools konfigurieren sowie bereitstellen.

Hinzufügen von vCenter Server-Instanzen zu Horizon 7

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 (SSL) 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 View 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*.

- Überprüfen Sie, ob auf dem vCenter Server-Host ein TLS/SSL-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 Zertifikatsspeicher 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 View Composer festlegen. Siehe [Grenzwerte für parallele Vorgänge für vCenter Server und View Composer](#) und [Einstellen der Anzahl paralleler Vorgänge zum Ändern des Betriebszustands, um Remote-Desktop-Anmeldungsüberlastungen zu unterstützen](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- 2 Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen**.
- 3 Geben Sie im Textfeld **Serveradresse** der vCenter Server-Einstellungen den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der vCenter Server-Instanz ein.

Der FQDN umfasst den Hostnamen und den Domänennamen. 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.
- 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 Stellen Sie unter „Erweiterte Einstellungen“ die Grenzwerte für gleichzeitige Vorgänge für vCenter Server- und View Composer-Vorgänge ein.
- 9 Klicken Sie auf **Weiter**, um die Seite „View Composer-Einstellungen“ anzuzeigen.

Nächste Schritte

Konfigurieren Sie die View Composer-Einstellungen.

- Wenn die vCenter Server-Instanz mit einem signierten SSL-Zertifikat konfiguriert ist und der Verbindungsserver dem Stammzertifikat vertraut, zeigt der Assistent „vCenter Server hinzufügen“ die Seite „View 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 View Composer-Einstellungen

Damit Sie View Composer verwenden können, müssen Sie Einstellungen konfigurieren, die es Horizon 7 erlauben, eine Verbindung zum VMware Horizon View Composer-Dienst herzustellen. View 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 VMware Horizon View Composer-Dienst und jeder vCenter Server-Instanz geben. Ein View Composer-Dienst kann jeweils nur mit einer vCenter Server-Instanz zusammenarbeiten. Eine vCenter Server-Instanz kann jeweils nur mit einem VMware Horizon View Composer-Dienst verknüpft werden.

Nach der ersten Horizon 7-Bereitstellung können Sie den VMware Horizon View Composer-Dienst auf einen neuen Host migrieren, um eine wachsende oder sich ändernde Horizon 7-Bereitstellung zu unterstützen. Sie können die ursprünglichen View Composer-Einstellungen in Horizon Administrator bearbeiten, müssen jedoch zusätzliche Schritte ausführen, um sicherzustellen, dass die Migration erfolgreich ist. Siehe [Migrieren von View Composer auf eine andere Maschine](#).

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 View 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](#).
- Stellen Sie sicher, dass dieser VMware Horizon View Composer-Dienst nicht bereits konfiguriert wurde, um eine Verbindung zu einer anderen vCenter Server-Instanz herzustellen.

Verfahren

- 1 Dazu müssen Sie in Horizon Administrator die Seite „vCenter Server-Informationen“ im Assistenten „vCenter Server hinzufügen“ ausfüllen.
 - a Wählen Sie **View-Konfiguration > Server** aus.
 - b Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen** und geben Sie die vCenter Server-Einstellungen an.

- 2 Wählen Sie auf der Seite „View Composer-Einstellungen“ die Option **View Composer nicht verwenden**, wenn Sie View Composer nicht verwenden.

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

- 3 Wenn Sie View Composer verwenden, wählen Sie den Ort des View Composer-Hosts.

Option	Beschreibung
View Composer wird auf demselben Host installiert wie vCenter Server.	<p>a Wählen Sie View Composer wurde zusammen mit vCenter Server installiert.</p> <p>b Vergewissern Sie sich, dass die Portnummer der Portnummer entspricht, die Sie beim Installieren des VMware Horizon View Composer-Dienstes in vCenter Server angegeben haben. Die standardmäßige Portnummer lautet 18443.</p>
View Composer wird auf seinem eigenen separaten Host installiert.	<p>a Wählen Sie Eigenständiger View Composer Server.</p> <p>b Geben Sie im Textfeld für die View Composer-Serveradresse den vollqualifizierten Domännennamen (FQDN) des View Composer-Hosts ein.</p> <p>c Geben Sie den Namen des View Composer-Benutzers ein.</p> <p>Beispiel: domain.com\user oder user@domain.com</p> <p>d Geben Sie das Kennwort des View Composer-Benutzers ein.</p> <p>e Vergewissern Sie sich, dass die Portnummer der Portnummer entspricht, die Sie beim Installieren des VMware Horizon View Composer-Dienstes angegeben haben. Die standardmäßige Portnummer lautet 18443.</p>

- 4 Klicken Sie auf **Weiter**, um die Seite „View Composer-Domänen“ anzuzeigen.

Nächste Schritte

Konfigurieren Sie die View Composer-Domänen.

- Wenn die View Composer-Instanz mit einem signierten TLS-Zertifikat konfiguriert ist und der Verbindungsserver dem Stammzertifikat vertraut, zeigt der Assistent „vCenter Server hinzufügen“ die Seite „View Composer-Domänen“ an.
- Wenn die View Composer-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](#).

Konfigurieren von View Composer-Domänen

Sie müssen eine Active Directory-Domäne konfigurieren, in der View Composer Linked-Clone-Desktops bereitstellt. Es ist möglich, mehrere Domänen für View Composer zu konfigurieren. Nachdem Sie zunächst die vCenter Server- und View Composer-Einstellungen zu View hinzugefügt haben, können Sie weitere View Composer-Domänen durch Bearbeitung der vCenter Server-Instanz in Horizon Administrator hinzufügen.

Voraussetzungen

- Ihr Active Directory-Administrator muss einen View 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 View Composer-AD-Vorgänge](#).
- Überprüfen Sie in Horizon Administrator, ob die Seiten mit den vCenter Server-Informationen und den View Composer-Einstellungen im Assistenten zum Hinzufügen von vCenter Server ausgefüllt wurden.

Verfahren

- 1 Klicken Sie auf der Seite mit den View Composer-Domänen auf **Hinzufügen**, um den View Composer-Benutzer für die Kontoinformationen der AD-Vorgänge hinzuzufügen.
- 2 Geben Sie den Domännennamen der Active Directory-Domäne ein.
Beispiel: **domain.com**
- 3 Geben Sie den Domänenbenutzernamen (einschließlich des Domännennamens) des View Composer-Benutzers ein.
Beispiel: **domain.com\admin**
- 4 Geben Sie das Kontokennwort ein.
- 5 Klicken Sie auf **OK**.
- 6 Um Domänenbenutzerkonten mit Berechtigungen in weiteren Active Directory-Domänen hinzuzufügen, in denen Sie Linked-Clone-Pools bereitgestellt haben, wiederholen Sie die vorangehenden Schritte.
- 7 Klicken Sie auf **Weiter**, um die Seite mit den Speichereinstellungen anzuzeigen.

Nächste Schritte

Aktivieren Sie die Zurückgewinnung von VM-Datenträgerplatz und konfigurieren Sie die View-Speicherbeschleunigung für Horizon 7.

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

In vSphere 5.1 und höher können Sie die Funktion zur Rückgewinnung von Festplattenspeicherplatz für Horizon 7 aktivieren. Mit Einführung von vSphere 5.1 erstellt Horizon 7 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 Rückgewinnung von Datenträgerplatz 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 einer vSphere 5.1- oder neueren Umgebung 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 Administrator 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.
- Dieser Vorgang hat keine Auswirkungen auf persistente View Composer-Festplatten.
- Sie funktioniert nur mit vSphere 5.1 oder höher und nur 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 Führen Sie in Horizon Administrator die Schritte auf den Seiten des Assistenten zum Hinzufügen von vCenter Server-Instanzen aus, die der Seite mit den Speichereinstellungen vorangehen.
 - a Wählen Sie **View-Konfiguration > Server**.
 - b Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen**.
 - c Geben Sie die Informationen für vCenter Server an, legen Sie die View Composer-Einstellungen fest und füllen Sie die Seiten für View Composer-Domänen aus.
- 2 Vergewissern Sie sich auf der Seite **Speichereinstellungen**, das Zurückgewinnung von Datenträgerplatz aktivieren ausgewählt ist.

Die Rückgewinnung von Datenträgerplatz ist standardmäßig ausgewählt, wenn Sie eine frische Installation von Horizon 7 5.2 oder höher durchführen. Sie müssen **Zurückgewinnung von Datenträgerplatz aktivieren** auswählen, wenn Sie ein Upgrade auf Horizon 7 5.2 oder höher von Horizon 7 5.1 oder einer früheren Version durchführen.

Nächste Schritte

Konfigurieren Sie auf der Seite Speichereinstellungen die View-Speicherbeschleunigung.

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

Konfigurieren der View-Speicherbeschleunigung für vCenter Server

In vSphere 5.1 und höher können Sie ESXi-Hosts so konfigurieren, dass Festplattendaten von virtuellen Maschinen gespeichert werden. Diese Funktion, die View-Speicherbeschleunigung, verwendet die CBRC-Funktion (Content Based Read Cache) in ESXi-Hosts. Die View-Speicherbeschleunigung 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 die View-Speicherbeschleunigung 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 Einstellung für die View-Speicherbeschleunigung im vCenter Server-Assistenten in Horizon Administrator wie in dieser Vorgehensweise beschrieben aus.

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

Die View-Speicherbeschleunigung 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 die View-Speicherbeschleunigung 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 die View-Speicherbeschleunigung aktiviert sind.

Die View-Speicherbeschleunigung 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 der View-Speicherbeschleunigung 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 View Composer-Rechte beschrieben werden, die der vCenter Server-Benutzer benötigt.

Verfahren

- 1 Führen Sie in Horizon Administrator die Schritte auf den Seiten des Assistenten zum Hinzufügen von vCenter Server-Instanzen aus, die der Seite mit den Speichereinstellungen vorangehen.
 - a Wählen Sie **View-Konfiguration > Server**.
 - b Klicken Sie auf der Registerkarte **vCenter Server** auf **Hinzufügen**.
 - c Geben Sie die Informationen für vCenter Server an, legen Sie die View Composer-Einstellungen fest und füllen Sie die Seiten für View Composer-Domänen aus.
- 2 Stellen Sie auf der Seite mit den Speichereinstellungen sicher, dass das Kontrollkästchen **View-Speicherbeschleunigung aktivieren** aktiviert ist.
Dieses Kontrollkästchen ist standardmäßig aktiviert.
- 3 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 Cachergröße muss zwischen 100 MB und 2.048 MB betragen.
- 4 Um für einen einzelnen ESXi-Host eine andere Cachergröße anzugeben, wählen Sie einen ESXi-Host aus, und klicken Sie auf **Cachergröße 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**.
- 5 Klicken Sie auf der Seite mit den Speichereinstellungen auf **Weiter**.
- 6 Klicken Sie auf **Fertig stellen**, um die vCenter Server-, View Composer- und Speichereinstellungen zu Horizon 7 hinzuzufügen.

Nächste Schritte

Konfigurieren Sie die Einstellungen für Clientsitzungen und -verbindungen. Siehe [Konfigurieren der Einstellungen für Clientsitzungen](#).

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

Grenzwerte für parallele Vorgänge für vCenter Server und View 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 View Composer ausgeführt werden.

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

Tabelle 2-1. Grenzwerte für parallele Vorgänge für vCenter Server und View 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>
Maximale parallele View Composer-Wartungsvorgänge	<p>Legt die maximale Anzahl an parallelen View Composer-Vorgängen zur Aktualisierung, Neuzusammenstellung und Neuverteilung fest, die auf den Linked Clones ausgeführt werden können, die von dieser View 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>
Maximale parallele View Composer-Bereitstellungsvorgänge	<p>Legt die maximale Anzahl an parallelen Erstellungs- und Löschvorgängen fest, die auf Linked Clones ausgeführt werden können, die von dieser View Composer-Instanz verwaltet werden.</p> <p>Der Standardwert ist 8.</p> <p>Diese Einstellung gilt nur für Linked 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 Einschaltzeit 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 Einschaltzeit während Spitzenzeiten ist. Bei einer vorsichtigen Herangehensweise unterstützt die Standardeinstellung 50 eine Einschaltzeit 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 Einschaltzeit 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 Einschaltzeit während Spitzenzeiten beträgt 16 Desktops pro Minute.

Akzeptieren des Fingerabdrucks eines standardmäßigen TLS-Zertifikats

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

Wenn vCenter Server oder eine View 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 View 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 View Server“ im Dokument *Horizon 7-Installation*.

Als Erstes fügen Sie vCenter Server und View Composer in Horizon Administrator hinzu. Verwenden Sie dazu den Assistenten „vCenter Server hinzufügen“. Wenn ein Zertifikat nicht als vertrauenswürdig eingestuft wird und Sie den Fingerabdruck nicht akzeptieren, können Sie vCenter Server und View Composer 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 View Composer-Zertifikat als nicht vertrauenswürdig eingestuft wird. Gleiches gilt, wenn Sie ein vertrauenswürdiges Zertifikat durch ein nicht vertrauenswürdiges Zertifikat ersetzen.

Auf dem Horizon Administrator-Dashboard ändert sich die Farbe des Symbols für vCenter Server oder View Composer in Rot, und das Dialogfeld „Ungültiges Zertifikat ermittelt“ wird angezeigt. Klicken Sie in Horizon Administrator auf **View-Konfiguration > Server** und bearbeiten Sie den vCenter Server-Eintrag für den View Composer-Dienst. Klicken Sie dann in den vCenter Server-Einstellungen auf **Bearbeiten** und folgen Sie den Eingabeaufforderungen, um das selbstsignierte Zertifikat zu überprüfen und zu akzeptieren.

Gleichermaßen können Sie in Horizon Administrator einen SAML-Authentifikator für die Verwendung durch eine Verbindungsserver-Instanz konfigurieren. Wenn der Verbindungsserver das SAML-Serverzertifikat nicht als vertrauenswürdig einstuft, müssen Sie festlegen, ob der Zertifikatfingerabdruck akzeptiert wird. Wenn Sie den Fingerabdruck nicht akzeptieren, können Sie den SAML-Authentifikator in Horizon 7 nicht konfigurieren. Nach der Konfiguration eines SAML-Authentifikators können Sie ihn im Dialogfeld zum Bearbeiten des Verbindungsservers neu konfigurieren.

Verfahren

- 1 Klicken Sie auf **Zertifikat anzeigen**, wenn Horizon Administrator 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 View Composer-Instanz konfiguriert wurde.
 - a Starten Sie auf dem vCenter Server- oder View Composer-Host das MMC-Snap-In und öffnen Sie den Windows-Zertifikatspeicher.
 - b Navigieren Sie zum vCenter Server- oder View 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 Zertifikatinformationen mit dem Fingerabdruck für die vCenter Server- oder die View 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 View 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 Klicken Sie in Horizon Administrator auf **View-Konfiguration > 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**.

Ergebnisse

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

Entfernen von View Composer aus Horizon 7

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

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

Verfahren

- 1 Entfernen Sie die Desktop-Pools mit Linked Clones, die von View Composer erstellt wurden.
 - a Wählen Sie in Horizon Administrator **Katalog > Desktop-Pools** 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. Die dazugehörigen View Composer-Datenbankeinträge und die Replikate, die von View Composer erstellt wurden, werden auch entfernt.
 - d Wiederholen Sie diese Schritte für jeden Desktop-Pool mit einem Linked Clone, der von View Composer erstellt wurde.
- 2 Wählen Sie **View-Konfiguration > Server** aus.
- 3 Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz, mit der View Composer verknüpft ist, aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Klicken Sie unter „View Composer Server-Einstellungen“ auf **Bearbeiten**, wählen Sie **View Composer nicht verwenden** aus und klicken Sie auf **OK**.

Ergebnisse

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, View Composer auf einem anderen Host zu installieren und Horizon 7 neu zu konfigurieren, um eine Verbindung zum neuen VMware Horizon View Composer-Dienst herzustellen, müssen Sie bestimmte zusätzliche Schritte durchführen. Siehe [Migrieren von View Composer ohne virtuelle Linked-Clone-Maschinen](#).

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

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

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

Konfigurieren der Einstellungen für Clientsitzungen

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.

Festlegen von Optionen für Clientsitzungen und -verbindungen

Sie können globale Einstellungen konfigurieren, um festzulegen, wie die Clientsitzungen und -verbindungen funktionieren sollen.

Die globalen Einstellungen sind keiner einzelnen Verbindungsserver-Instanz zugeordnet. Sie wirken sich auf alle Clientsitzungen aus, die von einer eigenständigen Verbindungsserver-Instanz oder einer Gruppe von replizierten Instanzen verwaltet werden.

Sie können Verbindungsserver-Instanzen auch so konfigurieren, dass direkte, nicht getunnelte Verbindungen zwischen Horizon-Clients und Remote-Desktops verwendet werden. Informationen zur Konfiguration von direkter Verbindung finden Sie unter [Konfigurieren des sicheren Tunnels und des PCoIP Secure Gateway](#).

Voraussetzungen

Machen Sie sich mit den globalen Einstellungen vertraut. Siehe [Globale Einstellungen für Clientsitzungen](#) und [Globale Sicherheitseinstellungen für Clientsitzungen und -verbindungen](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Globale Einstellungen** aus.
- 2 Wählen Sie, ob allgemeine Einstellungen oder Sicherheitseinstellungen konfiguriert werden sollen.

Option	Beschreibung
Allgemeine globale Einstellungen	Klicken Sie im Bereich „Allgemein“ auf Bearbeiten .
Globale Sicherheitseinstellungen	Klicken Sie im Fensterbereich „Sicherheit“ auf Bearbeiten .

- 3 Konfigurieren Sie die globalen Einstellungen.
- 4 Klicken Sie auf **OK**.

Nächste Schritte

Sie können das Kennwort zur Datenwiederherstellung ändern, das während der Installation angegeben wurde. Siehe [Ändern des Kennworts für die Datenwiederherstellung](#).

Ändern des Kennworts für die Datenwiederherstellung

Stellen Sie ein Kennwort für die Datenwiederherstellung bereit, wenn Sie Verbindungsserver Version 5.1 oder höher installieren. Nach der Installation können Sie dieses Kennwort in View Administrator ändern. Das Kennwort ist erforderlich, wenn Sie die View LDAP-Konfiguration aus einem Backup wiederherstellen.

Wenn Sie den Verbindungsserver sichern, wird die View LDAP-Konfiguration in Form verschlüsselter LDIF-Daten exportiert. Um die verschlüsselte Horizon 7-Sicherungskonfiguration wiederherzustellen, müssen Sie das Kennwort für die Datenwiederherstellung angeben.

Das Kennwort muss 1 bis 128 Zeichen umfassen. Befolgen Sie die empfohlenen Vorgehensweisen Ihrer Organisation für das Generieren sicherer Kennwörter.

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Globale Einstellungen** aus.
- 2 Klicken Sie im Bereich „Sicherheit“ auf **Kennwort für die Datenwiederherstellung ändern**.
- 3 Geben Sie das neue Kennwort zweimal ein.
- 4 (Optional) Geben Sie eine Kennwörterinnerung ein.

Ergebnisse

Hinweis Sie können das Kennwort für die Datenwiederherstellung auch ändern, wenn Sie die Sicherung Ihrer Horizon 7-Konfigurationsdaten planen. Siehe [Planen von Horizon 7-Konfigurationssicherungen](#).

Nächste Schritte

Wenn Sie das Dienstprogramm vdmimport zum Wiederherstellen einer Horizon 7-Sicherungskonfiguration verwenden, stellen Sie das neue Kennwort bereit.

Globale Einstellungen für Clientsitzungen

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

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

Tabelle 2-2. Allgemeine globale Einstellungen für Clientsitzungen

Einstellung	Beschreibung
Zeitüberschreitung für View Administrator-Sitzung	<p>Bestimmt, wie lange eine Horizon Administrator-Sitzung im Leerlauf bleibt, bevor die Sitzung abläuft.</p> <hr/> <p>Wichtig Wenn Sie den Zeitüberschreitungszeitpunkt für die Horizon Administrator-Sitzung auf eine hohe Minutenzahl einstellen, steigt das Risiko, dass Horizon Administrator unautorisiert genutzt werden könnte. Seien Sie vorsichtig, wenn Sie zulassen, dass eine Sitzung lange Zeit im Leerlauf bleibt.</p> <hr/> <p>Standardmäßig beträgt die Zeitüberschreitung für die Horizon Administrator-Sitzung 30 Minuten. Sie können als Zeitüberschreitung für eine Sitzung 1 bis 4.320 Minuten (72 Stunden) festlegen.</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>

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

Einstellung	Beschreibung
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> <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>
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>

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

Einstellung	Beschreibung
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. Die Standardeinstellung ist Nach 15 Minuten.</p>
Automatische Status-Updates aktivieren	<p>Legt fest, ob Statusaktualisierungen in der globalen Statusanzeige im oberen linken Bereich von Horizon Administrator mit einem Intervall von wenigen Minuten aktualisiert werden. Die Dashboard-Seite von Horizon Administrator wird ebenfalls mit einem Intervall von wenigen Minuten aktualisiert.</p> <p>Diese Einstellung ist standardmäßig nicht aktiviert.</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>
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 Administrator alle verfügbaren Windows Server-Computer angezeigt, einschließlich der Computer, auf denen Horizon 7-Serverkomponenten installiert sind.</p> <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>

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

Einstellung	Beschreibung
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> <p>Hinweis Diese Funktion ist in Horizon 7 Version 7.0.2 und höher verfügbar.</p>
Mirage-Serverkonfiguration	<p>Ermöglicht Ihnen, die URL eines Mirage-Servers anzugeben, und zwar im Format mirage://Servername:Port bzw. mirages://Servername:Port. <i>Servername</i> ist hier der vollqualifizierte Domänenname. Wenn Sie die Portnummer nicht angeben, wird die standardmäßige Portnummer 8000 verwendet.</p> <p>Hinweis Sie können diese globale Einstellung überschreiben, indem Sie einen Mirage-Server in den Desktop-Pool-Einstellungen angeben.</p> <p>Bei der Festlegung des Mirage-Servers in Horizon Administrator handelt es sich um eine Alternative für die Festlegung des Mirage-Servers, wenn der Mirage-Client installiert wird. Um zu ermitteln, für welche Versionen von Mirage der Server in Horizon Administrator unterstützt wird, lesen Sie die Mirage-Dokumentation unter https://www.vmware.com/support/pubs/mirage_pubs.html.</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 2-2. 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 Clientsitzungen und -verbindungen

Globale Sicherheitseinstellungen legen fest, ob Clients nach Unterbrechungen neu authentifiziert sind, der Nachrichten-Sicherheitsmodus aktiviert ist und IPSec für Sicherheitsserververbindungen verwendet wird.

Für alle Horizon Client-Verbindungen und Horizon Administrator-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. Siehe [Verschieben von TLS-Verbindungen auf Zwischenserver](#).

Tabelle 2-3. 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>Weitere Informationen finden Sie unter Sicherheitsmodus für Nachrichten für Horizon 7-Komponenten.</p> <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. <p>Sie können auch das Befehlszeilendienstprogramm <code>vdmutl</code> zum Überwachen des Fortschritts verwenden. Siehe Konfigurieren des Sicherheitsmodus für JMS-Nachrichten mit dem Dienstprogramm „vdmutl“.</p>
IPSec für Sicherheitsserver-Verbindungen verwenden	<p>Bestimmt, ob Internet Protocol Security (IPSec) für Verbindungen zwischen Sicherheitsservern und Verbindungsserver-Instanzen verwendet wird.</p> <p>Standardmäßig sind sichere Verbindungen (über IPSec) für Sicherheitsserver-Verbindungen aktiviert.</p>

Hinweis Falls Sie aus einer früheren Horizon 7-Version ein Upgrade auf View 5.1 oder höher durchführen, wird die globale Einstellung **SSL für Clientverbindungen anfordern** in Horizon Administrator angezeigt, allerdings nur, wenn die Einstellungen in Ihrer Horizon 7-Konfiguration deaktiviert wurde, bevor Sie das Upgrade durchgeführt haben. Da TLS für alle Horizon Client-Verbindungen und Horizon Administrator-Verbindungen mit Horizon 7 erforderlich ist, wird diese Einstellung nicht bei neuen Installationen von Horizon 7 5.1 oder höher angezeigt und nach einem Upgrade nicht angezeigt, falls die Einstellung bereits in der vorherigen Horizon 7-Konfiguration aktiviert war.

Wenn Sie nach einem Upgrade die Einstellung **SSL für Clientverbindungen anfordern** nicht aktivieren, schlagen HTTPS-Verbindungen von Horizon-Clients fehl, es sei denn, sie stellen eine Verbindung zu einem Zwischengerät her, das so konfiguriert ist, dass weitere Verbindung über HTTP hergestellt werden. Siehe [Verschieben von TLS-Verbindungen auf Zwischenserver](#).

Sicherheitsmodus für Nachrichten für Horizon 7-Komponenten

Sie können den Sicherheitsmodus für Nachrichten festlegen, um den zur Übermittlung von JMS-Nachrichten über Horizon 7-Komponenten verwendeten Sicherheitsmechanismus anzugeben.

Die folgende Tabelle zeigt die Optionen, die Sie zum Konfigurieren des Sicherheitsmodus für Nachrichten auswählen können. Um eine Option festzulegen, wählen Sie die gewünschte Einstellung in der Liste **Sicherheitsmodus für Nachrichten** im Dialogfeld „Globale Einstellungen“ aus.

Tabelle 2-4. Optionen für den Sicherheitsmodus für Nachrichten

Option	Beschreibung
Deaktiviert	Der Sicherheitsmodus für Nachrichten ist deaktiviert.
Gemischt	Der Sicherheitsmodus für Nachrichten ist aktiviert, wird aber nicht erzwungen. Mithilfe dieses Modus können Sie Komponenten in Ihrer Horizon 7-Umgebung erkennen, die eine Version vor Horizon 7 3.0 verwenden. Die vom Verbindungsserver generierten Protokolldateien enthalten Verweise auf diese Komponenten. Diese Einstellung wird nicht empfohlen. Verwenden Sie diese Einstellung nur zum Ermitteln von Komponenten, für die ein Upgrade erforderlich ist.

Tabelle 2-4. Optionen für den Sicherheitsmodus für Nachrichten (Fortsetzung)

Option	Beschreibung
Aktiviert	<p>Der Sicherheitsmodus für Nachrichten ist aktiviert und verwendet eine Kombination aus Nachrichtensignierung und -verschlüsselung. JMS-Nachrichten werden abgelehnt, wenn die Signatur fehlt oder ungültig ist oder wenn eine Nachricht nach dem Signieren geändert wurde.</p> <p>Einige JMS-Nachrichten sind verschlüsselt, da sie vertrauliche Daten wie z. B. Benutzeranmeldeinformationen enthalten. Bei Verwendung der Einstellung Aktiviert können Sie auch IPSec zur Verschlüsselung aller JMS-Nachrichten zwischen Verbindungsserver-Instanzen sowie zwischen Verbindungsserver-Instanzen und Sicherheitsservern verwenden.</p> <p>Hinweis Horizon 7-Komponenten, die eine Version vor 3.0 verwenden, dürfen mit anderen Horizon 7-Komponenten nicht kommunizieren.</p>
Erweitert	<p>SSL wird für alle JMS-Verbindungen verwendet. Die JMS-Zugriffssteuerung ist ebenfalls aktiviert, damit Desktops, Sicherheitsserver und Verbindungsserver-Instanzen nur JMS-Nachrichten zu bestimmten Themen senden und empfangen können.</p> <p>Horizon 7-Komponenten, die älter als Horizon 6, Version 6.1 sind, können nicht mit einer Verbindungsserver 6.1-Instanz kommunizieren.</p> <p>Hinweis Für diesen Modus muss der TCP-Port 4002 zwischen DMZ-basierten Sicherheitsservern und ihren gekoppelten Verbindungsserver-Instanzen geöffnet werden.</p>

Wenn Sie Horizon 7 erstmalig auf einem System installieren, wird der Sicherheitsmodus für Nachrichten auf **Aktiviert** gesetzt. Wenn Sie ein Upgrade für Horizon 7 von einer vorherigen Version durchführen, bleibt der Sicherheitsmodus für Nachrichten unverändert auf der aktuellen Einstellung.

Wichtig Wenn Sie vorhaben, eine aktualisierte Horizon 7-Umgebung von **Aktiviert** in **Erweitert** zu ändern, müssen Sie vorher ein Upgrade für alle Verbindungsserver-Instanzen, Sicherheitsserver und Horizon 7-Desktops auf Horizon 6, Version 6.1 oder höher durchführen. Nachdem Sie die Einstellung in **Erweitert** geändert haben, wird die neue Einstellung phasenweise wirksam.

- 1 Sie müssen einen manuellen Neustart des VMware Horizon View Message Bus-Komponenten-Diensts auf allen Verbindungsserver-Hosts im Pod ausführen oder die Verbindungsserver-Instanzen neu starten.
- 2 Nach dem Neustart der Dienste konfigurieren die Verbindungsserver-Instanzen den Sicherheitsmodus für Nachrichten auf allen Desktops und Sicherheitsservern neu, indem sie den Modus auf **Erweitert** ändern.
- 3 Um den Fortschritt in Horizon Administrator zu überwachen, navigieren Sie zu **View-Konfiguration > Globale Einstellungen**.

Auf der Registerkarte **Sicherheit** wird für die Option **Erweiterter Sicherheitsstatus** der Eintrag **Erweitert** angezeigt, wenn alle Komponenten auf den erweiterten Modus umgestellt wurden.

Alternativ können Sie das Befehlszeilendienstprogramm `vdmutl` zum Überwachen des Fortschritts verwenden. Siehe [Konfigurieren des Sicherheitsmodus für JMS-Nachrichten mit dem Dienstprogramm „vdmutl“](#).

Horizon 7-Komponenten, die älter als Horizon 6 Version 6.1 sind, können nicht mit einer Verbindungsserver 6.1-Instanz kommunizieren, die den erweiterten Modus verwendet.

Wenn Sie vorhaben, eine aktive Horizon 7-Umgebung von **Deaktiviert** in **Aktiviert** oder von **Aktiviert** in **Deaktiviert** zu ändern, wechseln Sie für einen kurzen Zeitraum vor der endgültigen Änderung in den Modus **Gemischt**. Wenn Ihr aktueller Modus beispielsweise **Deaktiviert** lautet, wechseln Sie für einen Tag in den Modus **Gemischt** und danach in **Aktiviert**. Im Modus **Gemischt** werden Signaturen an die Nachrichten angehängt, aber nicht überprüft, wodurch der Wechsel des Nachrichtenmodus in der gesamten Umgebung übernommen werden kann.

Konfigurieren des Sicherheitsmodus für JMS-Nachrichten mit dem Dienstprogramm „vdmutil“

Mit der Befehlszeilenschnittstelle `vdmutil` können Sie den Sicherheitsmechanismus konfigurieren und verwalten, der bei der Übertragung von JMS-Nachrichten zwischen Horizon 7-Komponenten verwendet wird.

Syntax und Speicherort des Dienstprogramms

Der Befehl `vdmutil` bewirkt dasselbe wie der Befehl `lmvutil` aus früheren Versionen von Horizon 7. Darüber hinaus ermöglicht der Befehl `vdmutil` die Festlegung des verwendeten Sicherheitsmodus für Nachrichten sowie die Überwachung des Fortschritts der Umstellung aller Horizon 7-Komponenten auf den erweiterten Modus. Verwenden Sie den Befehl `vdmutil` an einer Windows-Eingabeaufforderung mit dem folgenden Format.

```
vdmutil command_option [additional_option argument] ...
```

Welche Zusatzoptionen verwendet werden können, hängt von der Befehlsoption ab. Dieses Thema befasst sich mit den Optionen für den Sicherheitsmodus für Nachrichten. Informationen zu den anderen Optionen im Zusammenhang mit der Cloud-Pod-Architektur finden Sie im Dokument *Verwalten der Cloud-Pod-Architektur in Horizon 7*.

Der Pfad zur ausführbaren Datei des Befehls `vdmutil` lautet standardmäßig `C:\Programme\VMware\VMware View\Server\tools\bin`. Damit Sie den Pfad nicht in die Befehlszeile eingeben müssen, fügen Sie ihn zur PATH-Umgebungsvariable hinzu.

Authentifizierung

Sie müssen den Befehl als Benutzer mit der Administratorrolle ausführen. Sie können einem Benutzer die Administratorrolle mithilfe von Horizon Administrator zuweisen. Siehe [Kapitel 6 Konfigurieren der rollenbasierten Verwaltungsdelegierung](#).

Der `vdmutil`-Befehl umfasst Optionen zum Angeben des Benutzernamens, der Domäne und des Kennworts für die Authentifizierung.

Tabelle 2-5. vdmutil-Befehlsauthentifizierungsoptionen

Option	Beschreibung
<code>--authAs</code>	Der Name eines Horizon 7-Administratorbenutzers. Verwenden Sie nicht das Format <i>Domäne \Benutzername</i> oder das UPN-Format (Benutzerprinzipalname).
<code>--authDomain</code>	Der vollqualifizierte Domänenname für den in der Option <code>--authAs</code> angegebenen Horizon 7-Administratorbenutzer.
<code>--authPassword</code>	Das Kennwort für den in der Option <code>--authAs</code> angegebenen Horizon 7-Administratorbenutzer. Wenn "*" anstelle eines Kennworts eingegeben wird, fordert der Befehl <code>vdmutil</code> zur Eingabe des Kennworts auf. Vertrauliche Kennwörter werden dann nicht im Befehlsverlauf der Befehlszeile hinterlassen.

Sie müssen die Authentifizierungsoptionen mit allen `vdmutil`-Befehlsoptionen verwenden, mit Ausnahme von `--help` und `--verbose`.

Spezielle Optionen für den Sicherheitsmodus für JMS-Nachrichten

Die folgende Tabelle enthält nur die `vdmutil`-Befehlszeilenoptionen für das Anzeigen, Festlegen oder Überwachen des Sicherheitsmodus für JMS-Nachrichten. Über die `--help`-Befehlszeilenoption erhalten Sie eine Liste der Argumente, die für eine bestimmte Option verwendet werden können.

Der Befehl `vdmutil` gibt 0 zurück, wenn ein Vorgang erfolgreich ist, und einen fehlerspezifischen Code ungleich null, wenn ein Vorgang fehlschlägt. Der Befehl `vdmutil` schreibt Fehlermeldungen in die Standardfehler. Wenn ein Vorgang eine Ausgabe erzeugt oder die ausführliche Protokollierung mithilfe der Option `--verbose` aktiviert ist, schreibt der Befehl `vdmutil` die Ausgabe in die Standardausgabe, und zwar auf Englisch.

Tabelle 2-6. vdmutil-Befehlsoptionen

Option	Beschreibung
<code>--activatePendingConnectionServerCertificates</code>	Aktiviert ein ausstehendes Sicherheitszertifikat für eine Verbindungsserver-Instanz im lokalen Pod.
<code>--countPendingMsgSecStatus</code>	Zählt die Anzahl der Maschinen, die die Umstellung auf den erweiterten Modus bzw. vom erweiterten Modus verhindern.
<code>--createPendingConnectionServerCertificates</code>	Erstellt ein neues ausstehendes Sicherheitszertifikat für eine Verbindungsserver-Instanz im lokalen Pod.
<code>--getMsgSecLevel</code>	Ruft den erweiterten Nachrichten-Sicherheitsstatus für den lokalen Pod ab. Dieser Status ist Teil des Prozesses der Änderung des JMS-Nachrichten-Sicherheitsmodus von Aktiviert in Erweitert für alle Komponenten in einer Horizon 7-Umgebung.
<code>--getMsgSecMode</code>	Ruft den Sicherheitsmodus für Nachrichten für den lokalen Pod ab.
<code>--help</code>	Listet die Optionen des Befehls <code>vdmutil</code> auf. Sie können auch die Option <code>--help</code> mit einem bestimmten Befehl verwenden, z. B. <code>--setMsgSecMode --help</code> .
<code>--listMsgBusSecStatus</code>	Listet den Nachrichtenbus-Sicherheitsstatus für alle Verbindungsserver im lokalen Pod auf.

Tabelle 2-6. vdmutil-Befehlsoptionen (Fortsetzung)

Option	Beschreibung
--listPendingMsgSecStatus	Listet die Maschinen auf, die die Umstellung auf den erweiterten Modus bzw. vom erweiterten Modus verhindern. Standardmäßig auf 25 Einträge beschränkt.
--setMsgSecMode	Legt den Sicherheitsmodus für Nachrichten für den lokalen Pod fest.
--verbose	Aktiviert die ausführliche Protokollierung. Sie können diese Option mit jeder anderen Option kombinieren, um eine detaillierte Befehlsausgabe zu erhalten. Mit dem Befehl <code>vdmutil</code> erhalten Sie eine Standardausgabe.

Konfigurieren des sicheren Tunnels und des PCoIP Secure Gateway

Wenn Benutzer sich mit einem Remote-Desktop verbinden und der sichere Tunnel aktiviert ist, baut Horizon Client eine zweite HTTPS-Verbindung mit dem View-Verbindungsserver- oder Sicherheitsserverhost auf.

Wenn Benutzer sich über das PCoIP-Anzeigeprotokoll mit einem Remote-Desktop verbinden und das PCoIP Secure Gateway aktiviert ist, baut Horizon Client eine weitere sichere Verbindung mit dem Verbindungsserver- oder Sicherheitsserverhost auf.

Hinweis Mit Horizon 6 Version 6.2 und höher können Sie anstelle von Sicherheitsservern Unified Access Gateway-Appliances für den sicheren externen Zugriff auf Horizon 6-Server und -Desktops verwenden. Wenn Sie Unified Access Gateway-Appliances benutzen, müssen Sie die sicheren Gateways auf den Verbindungsserver-Instanzen deaktivieren und diese Gateways auf den Unified Access Gateway-Appliances aktivieren. Weitere Informationen finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

Wenn weder der sichere Tunnel noch das PCoIP Secure Gateway aktiviert sind, wird eine Sitzung direkt zwischen dem Clientsystem und der virtuellen Remote-Desktop-Maschine eingerichtet, und der Verbindungsserver- oder Sicherheitsserverhost werden umgangen. Dieser Verbindungstyp wird als direkte Verbindung bezeichnet.

Wichtig Eine typische Netzwerkkonfiguration, die sichere Verbindungen für externe Clients bereitstellt, umfasst einen Sicherheitsserver. Wenn Sie Horizon Administrator zum Aktivieren oder Deaktivieren des sicheren Tunnels und des PCoIP Secure Gateway auf einem Sicherheitsserver verwenden möchten, müssen Sie die Verbindungsserver-Instanz bearbeiten, die mit dem Sicherheitsserver kombiniert ist.

In einer Netzwerkkonfiguration, bei der externe Clients sich direkt mit einem Verbindungsserver-Host verbinden, aktivieren oder deaktivieren Sie den sicheren Tunnel und das PCoIP Secure Gateway, indem Sie die entsprechende Verbindungsserver-Instanz in Horizon Administrator bearbeiten.

Voraussetzungen

- Wenn Sie das PCoIP Secure Gateway aktivieren möchten, stellen Sie sicher, dass die Verbindungsserver-Instanz und der kombinierte Sicherheitsserver in der Version Horizon 7 4.6 oder höher vorliegen.

- Wenn Sie einen Sicherheitsserver mit einer Verbindungsserver-Instanz kombinieren, auf der Sie das PCoIP Secure Gateway bereits aktiviert haben, stellen Sie sicher, dass der Sicherheitsserver in der Version Horizon 7 4.6 oder höher vorliegt.

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** eine Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 3 Konfigurieren Sie die Verwendung des sicheren Tunnels.

Option	Beschreibung
Aktivieren des sicheren Tunnels	Aktivieren Sie Sichere Tunnelverbindung zum Computer verwenden .
Deaktivieren des sicheren Tunnels	Deaktivieren Sie Sichere Tunnelverbindung zum Computer verwenden .

Der sichere Tunnel ist standardmäßig aktiviert.

- 4 Konfigurieren Sie die Verwendung des PCoIP Secure Gateway.

Option	Beschreibung
Aktivieren des PCoIP Secure Gateway	Aktivieren Sie PCoIP Secure Gateway für PCoIP-Verbindungen zum Computer verwenden .
Deaktivieren des PCoIP Secure Gateway	Deaktivieren Sie PCoIP Secure Gateway für PCoIP-Verbindungen zum Computer verwenden .

Das PCoIP Secure Gateway ist standardmäßig deaktiviert.

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

Konfigurieren des Blast-Sicherheitsgateways

Sie können in Horizon Administrator das Blast-Sicherheitsgateway konfigurieren, um einen sicheren Zugriff auf Remote-Desktops und -anwendungen zu ermöglichen. Der Zugriff erfolgt entweder über HTML Access oder über Clientverbindungen, für die das VMware Blast-Anzeigeprotokoll verwendet wird.

Blast Secure Gateway beinhaltet das BEAT-Netzwerkprotokoll (Blast Extreme Adaptive Transport), das sich dynamisch an die jeweiligen Netzwerkbedingungen wie unterschiedliche Geschwindigkeiten und Paketverluste anpasst.

- Blast Secure Gateway unterstützt das BEAT-Netzwerkprotokoll nur bei der Ausführung auf einer Unified Access Gateway-Appliance.
- Horizon Client-Instanzen mit IPv4 und Horizon Client-Instanzen mit IPv6 können gleichzeitig auf TCP-Port 8443 und auf UDP-Port 8443 (bei BEAT) verarbeitet werden, wenn die Verbindung zu einer Unified Access Gateway-Appliance Version 3.3 oder höher hergestellt wird.

- Horizon Clients mit einer typischen Netzwerkbedingung müssen eine Verbindung mit einem Verbindungsserver mit deaktiviertem BSG, einem Sicherheitsserver mit deaktiviertem BSG oder mit einer höheren Version einer Unified Access Gateway-Appliance als 2.8 herstellen. Wenn Horizon Client eine typische Netzwerkbedingung zur Herstellung einer Verbindung mit einem Verbindungsserver mit aktiviertem BSG, einem Sicherheitsserver mit aktiviertem BSG oder mit einer höheren Version einer Unified Access Gateway-Appliance als 2.8 verwendet, erkennt der Client automatisch diese Netzwerkbedingung und verwendet das TCP-Netzwerk.
- Horizon Clients mit einer schwachen Netzwerkbedingung müssen eine Verbindung mit der Version 2.9 oder höher einer Unified Access Gateway-Appliance (mit aktiviertem UDP-Tunnelserver) herstellen. Wenn Horizon Client eine schwache Netzwerkbedingung zur Herstellung einer Verbindung mit dem Verbindungsserver mit aktiviertem BSG, mit dem Sicherheitsserver mit aktiviertem BSG oder mit einer höheren Version einer Unified Access Gateway-Appliance als 2.8 verwendet, erkennt der Client automatisch diese Netzwerkbedingung und verwendet das TCP-Netzwerk.
- Wenn Horizon Clients eine schwache Netzwerkbedingung zur Herstellung einer Verbindung mit einem Verbindungsserver mit deaktiviertem BSG, mit einem Sicherheitsserver mit deaktiviertem BSG oder mit Version 2.9 oder höher einer Unified Access Gateway-Appliance (ohne aktivierten UDP-Tunnelserver) oder mit Version 2.8 einer Unified Access Gateway-Appliance verwenden, erkennt der Client automatisch diese Netzwerkbedingung und verwendet die typische Netzwerkbedingung.

Weitere Informationen finden Sie in der Dokumentation zu Horizon Client unter <https://docs.vmware.com/de/VMware-Horizon-Client/index.html>.

Hinweis Sie können auch Unified Access Gateway-Appliances statt Sicherheitsserver für den sicheren externen Zugriff auf Horizon 7 Server und Desktops verwenden. Wenn Sie Unified Access Gateway-Appliances benutzen, müssen Sie die sicheren Gateways auf den Verbindungsserver-Instanzen deaktivieren und diese Gateways auf den Unified Access Gateway-Appliances aktivieren. Weitere Informationen finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

Wenn das Blast-Sicherheitsgateway nicht aktiviert ist, verwenden Client-Webbrowser das VMware Blast Extreme-Protokoll, um direkte Verbindungen mit den virtuellen Remote-Desktop-Computern herzustellen, und umgehen somit das Blast-Sicherheitsgateway.

Wichtig Eine typische Netzwerkkonfiguration, die sichere Verbindungen für externe Benutzer bereitstellt, umfasst einen Sicherheitsserver. Zum Aktivieren oder Deaktivieren des Blast-Sicherheitsgateways auf einem Sicherheitsserver müssen Sie die Verbindungsserver-Instanz bearbeiten, die mit dem Sicherheitsserver gekoppelt ist. Wenn externe Benutzer sich direkt mit einem Verbindungsserver-Host verbinden, aktivieren oder deaktivieren Sie das Blast-Sicherheitsgateway, indem Sie die Verbindungsserver-Instanz bearbeiten.

Voraussetzungen

Wenn Benutzer Remote-Desktops über VMware Identity Manager auswählen, müssen Sie überprüfen, ob VMware Identity Manager installiert und für die Verwendung mit dem Verbindungsserver konfiguriert ist. Außerdem muss der Verbindungsserver mit einem SAML 2.0-Authentifizierungsserver gekoppelt sein.

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** eine Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 3 Konfigurieren Sie die Verwendung des Blast-Sicherheitsgateways.

Option	Beschreibung
Aktivieren des Blast Secure Gateway	Aktivieren Sie Blast Secure Gateway für Blast-Verbindungen mit dem Computer verwenden.
Aktivieren des Blast Secure Gateway für HTML Access	Wählen Sie Blast Secure Gateway nur für HTML Access-Blast-Verbindungen mit dem Computer verwenden aus.
Deaktivieren des Blast Secure Gateway	Wählen Sie Blast Secure Gateway nicht verwenden aus.

Das Blast-Sicherheitsgateway ist standardmäßig aktiviert.

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

Verschieben von TLS-Verbindungen auf Zwischenserver

Horizon Client muss HTTPS verwenden, um eine Verbindung zu Horizon 7 herzustellen. Wenn Ihre Horizon-Clients eine Verbindung zu Lastausgleichsdiensten oder anderen Zwischenservern herstellen, die Verbindungen an Verbindungsserver-Instanzen oder Sicherheitsserver weiterreichen, können Sie TLS auf die Zwischenserver verschieben.

Importieren von TLS-Zertifikaten verschiebender Server auf Horizon 7-Servern

Wenn Sie TLS-Verbindungen auf einen Zwischenserver verschieben, müssen Sie das Zertifikat des Zwischenservers auf die Verbindungsserver-Instanzen oder Sicherheitsserver importieren, die eine Verbindung zum Zwischenserver herstellen. Sowohl auf dem verschiebenden Zwischenserver als auch auf jedem verschobenen Horizon 7-Server, der eine Verbindung zum Zwischenserver herstellt, muss sich dasselbe TLS-Serverzertifikat befinden.

Wenn Sie Sicherheitsserver bereitstellen, muss sich sowohl auf dem Zwischenserver als auch auf den Sicherheitsservern, die eine Verbindung zum Zwischenserver herstellen, dasselbe TLS-Zertifikat befinden. Es ist nicht erforderlich, dasselbe TLS-Zertifikat auf Verbindungsserver-Instanzen zu installieren, die an die Sicherheitsserver gekoppelt sind und keine direkte Verbindung zum Zwischenserver herstellen.

Wenn Ihre Bereitstellung keine Sicherheitsserver enthält oder wenn es sich um eine gemischte Netzwerkumgebung mit Sicherheitsservern und Verbindungsserver-Instanzen mit externen Verbindungen handelt, muss sich sowohl auf dem Zwischenserver als auch auf den Verbindungsserver-Instanzen, die eine Verbindung zum Zwischenserver herstellen, dasselbe TLS-Zertifikat befinden.

Wenn das Zertifikat des Zwischenservers nicht auf der Verbindungsserver-Instanz oder dem Sicherheitsserver installiert ist, können Clients ihre Verbindungen zu Horizon 7 nicht validieren. Unter diesen Umständen entspricht der vom Horizon 7-Server gesendete Zertifikatfingerabdruck nicht dem Zertifikat auf dem Zwischenserver, mit dem sich Horizon Client verbindet.

Verwechseln Sie nicht Lastausgleich mit TLS-Verschieben. Das zuvor genannte Erfordernis gilt für alle Geräte, die konfiguriert wurden, TLS-Verschiebungen zu leisten, einschließlich einiger Lastausgleichstypen. Ein reiner Lastenausgleich erfordert jedoch nicht das Kopieren von Zertifikaten zwischen Geräten.

Weitere Informationen zum Importieren von Zertifikaten auf Horizon 7-Server finden Sie unter „Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher“ im Dokument *Horizon 7-Installation*.

Einstellen externer URLs von Horizon 7 Server, sodass sie Clients auf verschiebende TLS-Server verweisen

Wenn TLS auf einen Zwischenserver verschoben wird und Horizon Client-Geräte den sicheren Tunnel nutzen, um sich mit Horizon 7 zu verbinden, müssen Sie die externe URL des sicheren Tunnels auf eine Adresse einstellen, die Clients verwenden können, um auf den Zwischenserver zuzugreifen.

Sie konfigurieren die externen URL-Einstellungen auf der Verbindungsserver-Instanz oder dem Sicherheitsserver, der eine Verbindung zum Zwischenserver herstellt.

Wenn Sie Sicherheitsserver bereitstellen, sind externe URLs für die Sicherheitsserver erforderlich, nicht jedoch für die Verbindungsserver-Instanzen, die mit den Sicherheitsservern gekoppelt werden.

Wenn Sie keine Sicherheitsserver bereitstellen oder über eine heterogene Netzwerkumgebung mit einigen Sicherheitsservern und einigen externen, vorgelagerten Verbindungsserver-Instanzen verfügen, sind externe URLs für alle Verbindungsserver-Instanzen notwendig, die eine Verbindung mit dem Zwischenserver herstellen.

Hinweis Sie können TLS-Verbindungen nicht über ein PCoIP Secure Gateway (PSG) oder Blast Secure Gateway auslagern. Die externe PCoIP-URL und die externe Blast Secure Gateway-URL müssen Clients ermöglichen, eine Verbindung zum Computer herzustellen, der das PSG und Blast Secure Gateway hostet. Setzen Sie die externe PCoIP-URL und die externe Blast-URL nicht zurück, um auf den Zwischenserver zu zeigen – es sei denn, um TLS-Verbindungen zwischen dem Zwischenserver und dem Horizon 7 Server herzustellen.

Weitere Informationen zur Konfiguration von externen URLs finden Sie unter „Konfigurieren externer URLs für PCoIP Secure Gateways und Tunnelverbindungen“ im Dokument *Horizon 7-Installation*.

Zulassen der HTTP-Verbindungen von Zwischenservern

Wenn TLS auf einen Zwischenserver verschoben wird, können Sie Verbindungsserver-Instanzen oder Sicherheitsserver so konfigurieren, dass HTTP-Verbindungen von Zwischengeräten mit Client-Verbindung zugelassen werden. Die Zwischengeräte müssen HTTPS für Horizon Client-Verbindungen akzeptieren.

Um HTTP-Verbindungen zwischen Horizon 7-Servern und Zwischengeräten zuzulassen, müssen Sie die Datei `locked.properties` auf jeder Verbindungsserver-Instanz und jedem Sicherheitsserver konfigurieren, auf denen HTTP-Verbindungen zugelassen sind.

Auch wenn HTTP-Verbindungen zwischen Horizon 7-Servern und Zwischengeräten zugelassen sind, können Sie TLS in Horizon 7 nicht deaktivieren. Die Horizon 7-Server nehmen weiterhin sowohl HTTPS- als auch HTTP-Verbindungen an.

Hinweis Wenn Ihre Horizon-Clients die Smartcard-Authentifizierung verwenden, müssen die Clients direkte HTTPS-Verbindungen zum Verbindungsserver bzw. zum Sicherheitsserver herstellen. Die Smartcard-Authentifizierung unterstützt das Verschieben von TLS nicht.

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 Um das Horizon 7-Serverprotokoll zu konfigurieren, fügen Sie die Eigenschaft `serverProtocol` hinzu, und legen Sie dafür den Wert `http` fest.

Der Wert `http` muss in Kleinbuchstaben eingegeben werden.
- 3 (Optional) Fügen Sie Eigenschaften hinzu, um einen nicht-standardmäßigen HTTP-Überwachungsport und eine Netzwerkschnittstelle auf dem Horizon 7-Server zu konfigurieren.
 - Um den HTTP-Überwachungsport von 80 zu ändern, legen Sie für `serverPortNonTLS` eine andere Portnummer fest, zu der das Zwischengerät per Konfiguration eine Verbindung herstellen soll.
 - Wenn der Horizon 7-Server über mehr als eine Netzwerkschnittstelle verfügt, der Server aber HTTP-Verbindungen nur an einer Schnittstelle überwachen soll, geben Sie für `serverHostNonTLS` die IP-Adresse dieser Netzwerkschnittstelle an.
- 4 Speichern Sie die Datei `locked.properties`.
- 5 Starten Sie den Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Beispiel: `locked.properties`, Datei

Diese Datei lässt Nicht-TLS-HTTP-Verbindungen zu einem Horizon 7-Server zu. Die IP-Adresse der Netzwerkschnittstelle mit Client-Verbindung des Horizon 7-Servers lautet 10.20.30.40. Der Server überwacht HTTP-Verbindungen an Standardport 80. Der Wert `http` muss in Kleinbuchstaben eingegeben werden.

```
serverProtocol=http
serverHostNonTLS=10.20.30.40
```

Konfigurieren des Gateway-Standorts für einen Horizon-Verbindungsserver- oder Sicherheitsserver-Host

Standardmäßig wird der Gateway-Standort bei Horizon-Verbindungsserver-Instanzen auf Intern und bei Sicherheitsservern auf Extern festgelegt. Sie können den vorgegebenen Gateway-Standort ändern, indem Sie die `gatewayLocation`-Eigenschaft in der Datei `locked.properties` festlegen.

Der Gateway-Standort bestimmt den Wert des `ViewClient_Broker_GatewayLocation`-Registrierungsschlüssels in einem Remote-Desktop. Sie können mit diesem Wert in Verbindung mit intelligenten Richtlinien eine Richtlinie erstellen, die nur dann wirksam wird, wenn der Benutzer von innerhalb oder außerhalb des Unternehmensnetzwerks eine Verbindung herstellt. Weitere Informationen dazu finden Sie unter „Verwenden intelligenter Richtlinien“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Verfahren

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im TLS/SSL-Gatewaykonfigurationsordner auf dem Horizon-Verbindungsserver- oder Sicherheitsserver-Host.
 Beispiel: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
 Bei den Eigenschaften in der Datei `locked.properties` wird die Groß-/Kleinschreibung beachtet.
- 2 Fügen Sie die folgende Zeile zur Datei `locked.properties` hinzu:
`gatewayLocation=Wert`
`Wert` kann entweder `External` oder `Internal` lauten. `External` gibt an, dass das Gateway für Benutzer außerhalb des Unternehmensnetzwerks verfügbar ist. `Internal` bedeutet, dass das Gateway nur für Benutzer innerhalb des Unternehmensnetzwerks verfügbar ist.
 Beispiel: `gatewayLocation=External`
- 3 Speichern Sie die Datei `locked.properties`.
- 4 Starten Sie den VMware Horizon-Verbindungsserver- oder den VMware Horizon-Sicherheitsserver-Dienst erneut, damit die Änderungen wirksam werden.

Deaktivieren oder Aktivieren von Horizon-Verbindungsserver

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 Administrator **View-Konfiguration > 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

Sie können zum Bearbeiten von externen URLs für Verbindungsserver-Instanzen und Sicherheitsserver Horizon Administrator verwenden.

Ein Verbindungsserver- oder Sicherheitsserverhost 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- oder Sicherheitsserver-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- oder Sicherheitsserverhost aufbauen. Zur Verwendung des PCoIP Secure Gateway muss ein Clientsystem auf eine IP-Adresse zugreifen können, die dem Client eine Verbindungsherstellung mit dem Verbindungsserver- oder Sicherheitsserverhost 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.

Hinweis Bei einem Sicherheitsserver, der nicht auf Verbindungsserver 4.5 oder höher aktualisiert wurde, können Sie die externen URLs nicht bearbeiten.

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.

Option	Aktion
View-Verbindungsserver-Instanz	Wählen Sie die Verbindungsserver-Instanz auf der Registerkarte Verbindungsserver aus und klicken Sie auf Bearbeiten .
Sicherheitsserver	Wählen Sie den Sicherheitsserver auf der Registerkarte Sicherheitsserver aus und klicken Sie auf Bearbeiten .

- 2 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://view.example.com:443`

Hinweis Sie können die IP-Adresse verwenden, falls Sie auf eine Verbindungsserver-Instanz oder auf einen Sicherheitsserver zugreifen müssen, wenn deren bzw. dessen Hostname nicht aufgelöst werden kann. Der Host, den Sie kontaktieren, passt jedoch nicht zu dem SSL-Zertifikat, das für die Verbindungsserver-Instanz oder für den Sicherheitsserver konfiguriert ist. Dies führt dazu, dass der Zugriff blockiert wird oder weniger sicher ist.

- 3 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 Sicherheitsserver- oder Verbindungsserver-Instanz benötigt.

- 4 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.

- 5 Stellen Sie sicher, dass Clientsysteme mit allen Adressen in diesem Dialogfeld eine Verbindung mit diesem Host herstellen können.
- 6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ergebnisse

Die externen URLs werden sofort aktualisiert. Sie müssen den Verbindungsserver- oder den Sicherheitsserverdienst nicht neu starten, damit die Änderungen wirksam werden.

Beitreten oder Verlassen des Programms zur Verbesserung der Benutzerfreundlichkeit

Wenn Sie den Verbindungsserver mit einer neuen Konfiguration installieren, können Sie an einem Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen. Wenn Sie sich erst nach der Installation für oder gegen eine Teilnahme entscheiden, können Sie mithilfe von Horizon Administrator dem Programm beitreten oder es verlassen.

Wenn Sie an dem Programm teilnehmen, sammelt VMware anonyme Daten zu Ihrer Bereitstellung, um die Reaktionen von VMware auf Benutzeranforderungen zu verbessern. Es werden jedoch keine Daten gesammelt, die Aufschluss über Ihr Unternehmen geben könnten.

Die Liste der Felder, aus denen Daten erfasst werden, einschließlich der Felder, die anonymisiert werden, finden Sie unter [#unique_44](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Produktlizenzierung und -verwendung** aus.
- 2 Klicken Sie im Fensterbereich „Programm zur Verbesserung der Benutzerfreundlichkeit“ auf **Einstellungen bearbeiten**.
- 3 Geben Sie an, ob Sie an dem Programm teilnehmen möchten, indem Sie das Kontrollkästchen **Anonyme Daten an VMware senden** aktivieren oder deaktivieren.
- 4 (Optional) Wenn Sie an dem Programm teilnehmen, können Sie den geografischen Standort, die Art der Geschäftstätigkeit und die Anzahl der Mitarbeiter in Ihrem Unternehmen auswählen.
- 5 Klicken Sie auf **OK**.

View LDAP-Verzeichnis

View LDAP ist das Daten-Repository für alle Horizon 7-Konfigurationsinformationen. View LDAP ist ein eingebettetes LDAP-Verzeichnis (Lightweight Directory Access Protocol), das mit der Verbindungsserver-Installation bereitgestellt wird.

View LDAP umfasst die standardmäßigen LDAP-Verzeichniskomponenten, die in Horizon 7 verwendet werden.

- Horizon 7-Schemadefinitionen
- DIT-Definitionen (Directory Information Tree)
- Zugriffssteuerungslisten (Access Control Lists, ACLs)

View LDAP enthält Verzeichniseinträge, die Horizon 7-Objekte repräsentieren.

- Remote-Desktop-Einträge, die jeden Desktop darstellen, auf den zugegriffen werden kann. Jeder Eintrag enthält Referenzen zu den FSP-Einträgen (Foreign Security Principal) der Windows-Benutzer und -gruppen im Active Directory, die den Desktop nutzen dürfen.

- Remote-Desktop-Pool-Einträge, die mehrere gemeinsam verwaltete Desktops repräsentieren.
- Einträge für virtuelle Maschinen, die die virtuelle vCenter Server-Maschine für jeden Remote-Desktop repräsentieren.
- Horizon 7-Komponenteneinträge, die Konfigurationseinstellungen speichern

View LDAP bietet ferner eine Gruppe von Plug-In-DLLs für Horizon 7, die anderen Horizon 7-Komponenten Automatisierungs- und Benachrichtigungsdienste bereitstellen.

Hinweis Sicherheitsserverinstanzen haben kein View LDAP-Verzeichnis.

LDAP-Replikation

Wenn Sie eine replizierte Verbindungsserver-Instanz installieren, kopiert Horizon 7 die View LDAP-Konfigurationsdaten von der vorhandenen Verbindungsserver-Instanz. Identische View LDAP-Konfigurationsdaten werden auf allen Verbindungsserver-Instanzen in der replizierten Gruppe verwaltet. Werden an einer Instanz Änderungen vorgenommen, werden die aktualisierten Informationen auf die weiteren Instanzen kopiert.

Fällt eine replizierte Instanz aus, setzen die weiteren Instanzen in der Gruppe ihren Betrieb fort. Sobald die ausgefallene Instanz ihren Betrieb wieder aufnimmt, wird ihre Konfiguration mit den Änderungen aktualisiert, die während des Ausfalls durchgeführt wurden. Mit Horizon 7 und höheren Versionen wird alle 15 Minuten eine Überprüfung des Replikationsstatus durchgeführt, um festzustellen, ob jede Instanz mit den anderen Servern in der replizierten Gruppe kommunizieren, und ob jede Instanz LDAP-Aktualisierungen von den anderen Servern in der Gruppe abrufen kann.

Den Replikationsstatus können Sie mit dem Dashboard in Horizon Administrator überprüfen. Wenn für Verbindungsserver-Instanzen ein rotes Symbol im Dashboard angezeigt wird, klicken Sie auf dieses Symbol, und der Replikationsstatus wird eingeblendet. Die Replikation kann aus folgenden Gründen beeinträchtigt sein:

- Eine Firewall blockiert die Kommunikation
- Der VMware VDMDS-Dienst wurde auf der Verbindungsserver-Instanz eventuell angehalten.
- Die VMware VDMDS DSA-Optionen blockieren die Replikationen
- Ein Netzwerkfehler ist aufgetreten

Standardmäßig wird die Replikationsüberprüfung alle 15 Minuten durchgeführt. Mit dem ADSI-Editor können Sie auf einer Verbindungsserver-Instanz das Intervall ändern. Um die Anzahl der Minuten festzulegen, rufen Sie **DC=vdi,DC=vmware,DC=int** auf und bearbeiten Sie das Attribut **pae-ReplicationStatusDataExpiryInMins** des Objekts **CN=Common,OU=Global,OU=Properties**.

Der Wert für das Attribut **pae-ReplicationStatusDataExpiryInMins** muss zwischen zehn und 1440 Minuten (= ein Tag) liegen. Ein Attributwert unter zehn Minuten wird von Horizon 7 ignoriert. Es gilt dann die Einstellung zehn Minuten. Ein Attributwert über 1.440 Minuten wird von Horizon 7 ignoriert. Es gilt dann die Einstellung 1.440 Minuten.

Einrichten der Smartcard-Authentifizierung

3

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](#)
- [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 für Smartcard-Benutzernamen für die Verbindungsserverinstanz in Horizon Administrator 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 dem Verbindungsserver- oder Sicherheitsserverhost Verbindungsserver-Konfigurationseigenschaften geändert werden.

5 [Konfigurieren von Smartcard-Einstellungen in Horizon Administrator](#)

In Horizon Administrator 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.

Nächste Schritte

Fügen Sie das Stammzertifikat oder das Zwischenzertifikat oder beide zu einer Server-Vertrauensspeicherdatei hinzu.

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.

Nächste Schritte

Fügen Sie das CA-Zertifikat einer Server-Vertrauensspeicherdatei hinzu.

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-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 root_certificate -keystore truststorefile.key -storetype JKS
```

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 dem Verbindungsserver- oder Sicherheitsserverhost 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- oder Sicherheitsserver-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- oder Sicherheitsserverdienst 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 Administrator. Sie müssen die Einstellungen für die Smartcard-Authentifizierung für einen Sicherheitsserver nicht konfigurieren. Einstellungen, die auf einer Horizon-Verbindungsserver-Instanz konfiguriert werden, gelten auch für einen gekoppelten Sicherheitsserver.

Konfigurieren von Smartcard-Einstellungen in Horizon Administrator

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

Wenn Sie diese Einstellung auf einer Verbindungsserver-Instanz konfigurieren, werden die Einstellungen auch auf gekoppelte Sicherheitsserver angewandt.

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 Administrator **View-Konfiguration > 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 „View-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 View-Verbindungsserver-Instanz beim Entfernen der Smartcards.	Aktivieren Sie das Kontrollkästchen Benutzersitzungen nach Entfernung der Smartcard trennen .
Benutzer bleiben beim Entfernen der Smartcards weiterhin mit der View-Verbindungsserver-Instanz 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 Administrator anmelden, klicken Sie auf die Registerkarte **Authentifizierung** und wählen Sie aus dem Dropdown-Menü **Smartcard-Authentifizierung für Administratoren** im Abschnitt „View Administration-Authentifizierung“ eine Konfigurationsoption 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 Administrator anzumelden. Wenn die Smartcard-Authentifizierung fehlschlägt, muss der Administrator ein Kennwort angeben.
Erforderlich	Administratoren müssen die Smartcard-Authentifizierung verwenden, wenn sie sich bei Horizon Administrator 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](#).

Konfigurieren der Smartcard-Authentifizierung auf Drittanbieterlösungen

Drittanbieterlösungen wie Lastausgleichsdienste 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 Administrator ein SAML-Authentifikator erstellt werden.

Informationen zur Konfiguration der Smart Card-Authentifizierung auf Unified Access Gateway finden Sie unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

Verfahren

- 1 Erstellen Sie einen SAML-Authentifikator für das Gateway oder den Lastausgleichsdienst eines Drittanbieters.
Siehe [Konfigurieren eines SAML-Authentifikators in Horizon Administrator](#).
- 2 Erweitern Sie den Ablaufzeitraum der Metadaten des Verbindungsservers, 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 Verbindungsservers.
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
```

Ergebnisse

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“.

Ergebnisse

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“.

Ergebnisse

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

Überprüfen der Smartcard-Authentifizierungskonfiguration

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 Administrator.

- a Wählen Sie **View-Konfiguration > 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 der View Agent oder die Horizon Agent-Komponente der 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-Zertifikatsperrüberprüfung

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

Horizon 7 unterstützt die Zertifikatsperrüberprüfung mit Zertifikatsperrlisten und dem Online Certificate Status Protocol (OCSP). Eine Zertifikatsperrliste 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 Zertifikatsperrüberprüfung kann auf einer Verbindungsserver-Instanz oder auf einem Sicherheitsserver konfiguriert werden. Wenn eine Verbindungsserver-Instanz mit einem Sicherheitsserver kombiniert wird, konfigurieren Sie die Zertifikatsperrüberprüfung 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 3-1. Eigenschaften für die Smartcard-Zertifikatsperrüberprüfung](#) listet die Eigenschaften der Datei `locked.properties` für die Zertifikatsperrüberprüfung auf.

Tabelle 3-1. 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

4

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 Authentifizierungscodes.

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 zweistufigen Authentifizierung in Horizon Administrator**

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

- **Fehlerbehebung bei Verweigerung des Zugriffs auf RSA SecurID**

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 zweistufigen Authentifizierung in Horizon Administrator

Sie aktivieren eine Verbindungsserver-Instanz für die RSA SecurID- oder RADIUS-Authentifizierung, indem Sie die Verbindungsserver-Einstellungen in Horizon Administrator 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. Diese Werte geben Sie später in Horizon Administrator ein. Sie können Werte für einen primären und einen sekundären RADIUS-Authentifikator eingeben.

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** den Server aus und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie auf der Registerkarte **Authentifizierung** im Bereich „Erweiterte Authentifizierung“ aus der Dropdown-Liste **2-Faktor-Authentifizierung** **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 in der Dropdown-Liste **SAML-Authentifikator** die Option **Neuen Authentifikator erstellen** und füllen Sie die Seite aus.

- 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.

Ergebnisse

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 Verweigerung des Zugriffs auf RSA SecurID

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 Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** den Verbindungsserver aus und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie auf der Registerkarte **Authentifizierung** die Option **Node Secret löschen**.
- 4 Klicken Sie auf **OK**, um das Knotenkennwort zu löschen.
- 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 **View-Verbindungsserver** aus der Liste aus und deaktivieren Sie das Kontrollkästchen **Knotenkenntwort erstellt**.

Die Option **Knotenkenntwort 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 über VMware Identity Manager ermöglichen möchten, müssen Sie die Desktop- und Anwendungspools als Benutzer mit Administratorrolle für die Stammzugriffsgruppe in Horizon Administrator 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 Administrator

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 Administrator einen SAML-Authentifikator erstellen. Ein SAML-Authentifikator enthält den Vertrauensstellungs- und Metadatenaustausch 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 unter *Bereitstellen und Konfigurieren von Unified Access Gateway*.

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 Lastausgleichsdienstes.
- Wenn Sie Workspace ONE oder VMware Identity Manager verwenden, notieren Sie sich die URL der Connector-Web-Schnittstelle.
- Wenn Sie einen Authentifikator für Unified Access Gateway 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 Wählen Sie in Horizon Administrator **Konfiguration > Server** aus.
- 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 Unified Access Gateway 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 dem Unified Access Gateway 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).

Option	Beschreibung
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.
SAML-Metadaten	(Für statische Authentifikatoren) Metadaten-URL, die Sie generiert und von Unified Access Gateway 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 vertrauenswürdiges Zertifikat für Horizon 7 und VMware Identity Manager oder ein Drittanbietergerät verwenden.

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

- 7 Wählen Sie im Abschnitt „Systemzustand“ auf dem Horizon Administrator-Dashboard **Andere Komponenten > SAML 2.0-Authentifikatoren** aus, wählen Sie den von Ihnen hinzugefügten SAML-Authentifikator aus und prüfen Sie die Details.

Falls die Konfiguration erfolgreich ist, steht der Systemzustand des Authentifikators auf grün. Der Systemzustand eines Authentifikators kann rot formatiert dargestellt werden, wenn das Zertifikat nicht vertrauenswürdig ist, wenn VMware Identity Manager nicht verfügbar ist oder wenn die Metadaten-URL ungültig ist. Falls das Zertifikat nicht vertrauenswürdig ist, sind Sie möglicherweise nicht in der Lage, auf **Überprüfen** zu klicken, um das Zertifikat zu validieren und anzunehmen.

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 Dienst Anbietern 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 Dienst Anbietern 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. Wählen Sie im Abschnitt „Systemzustand“ im Horizon Administrator-Dashboard **Andere Komponenten > SAML 2.0-Authentifikatoren** aus. Wählen Sie anschließend den von Ihnen hinzugefügten SAML-Authentifikator aus und prüfen Sie die Details.

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 Administrator deaktivieren. Erläuterungen zum Deaktivieren eines SAML-Authentifikators finden Sie unter [Konfigurieren eines SAML-Authentifikators in Horizon Administrator](#).

Konfigurieren der Workspace ONE-Richtlinien in Horizon Administrator

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 Administrator Berechtigungen für veröffentlichte Desktops und Anwendungen.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Konfiguration > Server** aus.
- 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.

Ergebnisse

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

Authentifizieren von Benutzern ohne Anforderung von Anmeldeinformationen

5

Nachdem sich Benutzer bei einem Clientgerät oder bei VMware Identity Manager angemeldet haben, können sie eine Verbindung mit einer veröffentlichten Anwendung oder mit einem veröffentlichten Desktop herstellen, ohne erneut zur Eingabe von Active Directory-Anmeldedaten aufgefordert zu werden.

Administratoren können die Konfiguration auf der Grundlage von Benutzeranforderungen einrichten.

- Stellen Sie Benutzern einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen zur Verfügung. Administratoren haben die Möglichkeit, das Setup so zu konfigurieren, dass sich Benutzer bei Horizon Client nicht mit Active Directory (AD)-Anmeldedaten anmelden müssen.
- Verwenden Sie für Windows-basierte Clients die Option „Als aktueller Benutzer anmelden“. Für Windows-basierte Clients kann der Administrator die Installation so konfigurieren, dass die Benutzer keine weiteren Anmeldedaten für die Anmeldung bei einem Horizon-Server eingeben müssen, nachdem sie sich mit AD-Anmeldedaten bei einem Windows-basierten Client angemeldet haben.
- Speichern Sie die Anmeldedaten in mobilen und Mac-Clients. Bei mobilen und Mac-Clients hat der Administrator die Möglichkeit, den Horizon Server so zu konfigurieren, dass die Anmeldeinformationen gespeichert werden. Dank dieser Funktion müssen sich die Benutzer keine AD-Anmeldeinformationen für die einmalige Anmeldung (SSO) merken, nachdem sie diese einmal auf einem mobilen Client oder einem Mac-Client eingegeben haben.
- Konfigurieren Sie True SSO für VMware Identity Manager. Für VMware Identity Manager kann der Administrator True SSO so konfigurieren, dass sich Benutzer, die sich über andere Methoden und nicht mit AD-Anmeldedaten authentifizieren, auch bei einem veröffentlichten Desktop oder einer veröffentlichten Anwendung anmelden können, ohne zur Eingabe von AD-Anmeldedaten aufgefordert zu werden.

Dieses Kapitel enthält die folgenden Themen:

- [Bereitstellen eines nicht authentifizierten Zugriffs auf veröffentlichte Anwendungen](#)
- [Konfigurieren von Benutzern für die Hybrid-Anmeldung](#)
- [Verwenden der Funktion „Als aktueller Benutzer anmelden“, die mit Windows-basierten Horizon Client-Instanzen verfügbar ist](#)
- [Speichern von Anmeldeinformationen in Horizon Clients für Mobilgeräte und Mac](#)
- [Einrichten von True SSO](#)

Bereitstellen eines nicht authentifizierten Zugriffs auf veröffentlichte Anwendungen

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.

Diese Funktion erfordert Horizon Client Version 4.4 oder höher. Für den HTML Access-Client erfordert diese Funktion die Version 4.5 oder höher.

Workflow für die Konfiguration nicht authentifizierter Benutzer

- 1 Erstellen Sie Benutzer für einen nicht authentifizierten Zugriff. Siehe [Erstellen von Benutzern für einen nicht authentifizierten Zugriff](#).
- 2 Aktivieren Sie den nicht authentifizierten Zugriff für Benutzer und richten Sie einen Standardbenutzer für einen nicht authentifizierten Zugriff ein. Siehe [Aktivieren des nicht authentifizierten Zugriffs für Benutzer](#).
- 3 Erteilen Sie nicht authentifizierten Benutzern die Berechtigung für veröffentlichte Anwendungen. Siehe [Erteilen von Berechtigungen für Benutzer für einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen](#).
- 4 Aktivieren Sie den nicht authentifizierten Zugriff aus Horizon Client. Siehe [Nicht authentifizierter Zugriff von Horizon Client aus](#).

Regeln und Richtlinien für die Konfiguration nicht authentifizierter Benutzer

- Eine zweistufige Authentifizierung wie z. B. RSA und RADIUS und eine Smartcard-Authentifizierung werden für den nicht authentifizierten Zugriff nicht unterstützt.
- Eine Smartcard-Authentifizierung und ein nicht authentifizierter Zugriff schließen sich gegenseitig aus. Wenn im Verbindungsserver für die Smartcard-Authentifizierung **Erforderlich** festgelegt ist, ist der nicht authentifizierte Zugriff deaktiviert, auch wenn er zuvor aktiviert war.
- VMware Identity Manager und VMware App Volumes werden für einen nicht authentifizierten Zugriff nicht unterstützt.
- Für diese Funktion wird sowohl das PCoIP- als auch das VMware Blast-Anzeigeprotokoll unterstützt.
- Die Funktion für einen nicht authentifizierten Zugriff überprüft nicht die Lizenzinformationen für RDS-Hosts. Der Administrator muss dafür Gerätelizenzen konfigurieren und anwenden.

- Die Funktion für einen nicht authentifizierten Zugriff speichert keine benutzerspezifischen Daten. Der Benutzer hat die Möglichkeit, die Datenspeicheranforderungen der Anwendung zu überprüfen.
- Sie können mit nicht authentifizierten Anwendungssitzungen keine erneuten Verbindungen herstellen. Wenn ein Benutzer die Verbindung mit einem Client trennt, meldet der RDS-Host die lokale Benutzersitzung automatisch ab.
- Der nicht authentifizierte Zugriff wird nur für veröffentlichte Anwendungen unterstützt.
- Der nicht authentifizierte Zugriff wird für Anwendungen, die von einem Desktop-Pool veröffentlicht werden, nicht unterstützt.
- Der nicht authentifizierte Zugriff wird nicht für einen Sicherheitsserver und nicht für eine Unified Access Gateway-Appliance unterstützt.
- Benutzereinstellungen werden für nicht authentifizierte Benutzer nicht beibehalten.
- Virtuelle Desktops werden für nicht authentifizierte Benutzer nicht unterstützt.
- Wenn der Verbindungsserver mit einem von einer Zertifizierungsstelle signierten Zertifikat konfiguriert und für einen nicht authentifizierten Zugriff aktiviert ist, der Standardbenutzer für einen nicht authentifizierten Zugriff aber nicht konfiguriert ist, zeigt Horizon Administrator für den Verbindungsserver einen roten Status an.
- Die Funktion für einen nicht authentifizierten Zugriff ist nicht anwendbar, wenn die Gruppenrichtlinieneinstellung AllowSingleSignon für den auf einem RDS-Host installierten Horizon Agent deaktiviert ist. Administratoren haben auch die Möglichkeit, den nicht authentifizierten Zugriff mit der Horizon Agent-Gruppenrichtlinieneinstellung UnAuthenticatedAccessEnabled zu deaktivieren oder zu aktivieren. Die Horizon Agent-Gruppenrichtlinieneinstellungen sind in der Vorlagendatei vdm_agent.admx enthalten. Damit diese Richtlinie wirksam wird, muss der RDS-Host neu gestartet werden.

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

- Stellen Sie sicher, dass der Active Directory (AD)-Benutzer, für den Sie einen nicht authentifizierten Zugriff konfigurieren möchten, über einen gültigen Benutzerprinzipalnamen (User Principal Name, UPN) verfügt. Es lässt sich nur ein AD-Benutzer als Benutzer für einen nicht authentifizierten Zugriff konfigurieren.

Hinweis Administratoren können für jedes AD-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.

Verfahren

- 1 Wählen Sie in Horizon Administrator **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.

Der Benutzer muss über einen gültigen UPN verfügen.
- 4 Wählen Sie einen Benutzer aus 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 Klicken Sie auf **Fertig stellen**.

Ergebnisse

Der Verbindungsserver erstellt den Benutzer für einen nicht authentifizierten Zugriff und zeigt die Benutzerdetails inklusive Benutzeralias, Benutzername, Vor- und Nachname, Anzahl der Quell-Pods, Anwendungsberechtigungen und Sitzungen an. Wenn Sie auf die Zahl in der Spalte „Quell-Pods“ klicken, werden Pod-Informationen angezeigt.

Nächste Schritte

Aktivieren Sie im Verbindungsserver den nicht authentifizierten Zugriff für Benutzer. Siehe [Aktivieren des nicht authentifizierten Zugriffs für Benutzer](#).

Aktivieren des nicht authentifizierten Zugriffs für Benutzer

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 Administrator **View-Konfiguration > 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 finden Sie unter „Erstellen von Farmen“ im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Erstellen Sie einen Anwendungspool für veröffentlichte Anwendungen, die auf einer Farm von RDS-Hosts ausgeführt werden. Unter „Erstellen von Anwendungspools“ im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7* finden Sie weitere Erläuterungen dazu.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > Anwendungspools** aus und klicken Sie auf den Namen des Anwendungspools.
- 2 Wählen Sie die Option **Berechtigung hinzufügen** aus dem Dropdown-Menü **Berechtigungen** aus.
- 3 Klicken Sie auf **Hinzufügen**, wählen Sie mindestens ein Suchkriterium aus, klicken Sie auf **Suchen** und aktivieren Sie das Kontrollkästchen **Nicht authentifizierte Benutzer**, 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 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Nach dem Abschluss der Berechtigungserteilung wird neben dem Benutzer für einen nicht authentifizierten Zugriff ein Symbol für den nicht authentifizierten Zugriff angezeigt.

Nächste Schritte

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

Suchen nach Sitzungen mit einem nicht authentifizierten Zugriff

Mit Horizon Administrator können Sie Anwendungssitzungen auflisten oder suchen, zu denen Benutzer für einen nicht authentifizierten Zugriff Verbindungen hergestellt haben. Das Symbol für Benutzer für einen nicht authentifizierten Zugriff wird neben diesen Sitzungen angezeigt, mit denen Benutzer für einen nicht authentifizierten Zugriff verbunden sind.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Überwachung > Sitzungen** aus.
- 2 Klicken Sie auf **Anwendungen**, um nach Anwendungssitzungen zu suchen.
- 3 Wählen Sie Suchkriterien aus und starten Sie die Suche.

In den Suchergebnissen werden Benutzer, Sitzungstyp (Desktop oder Anwendung), Computer, Pool oder Farm, DNS-Name, Client-ID und Sicherheitsgateway angegeben. Weiterhin werden die Startzeit, die Dauer und der Status der Sitzung sowie die letzte Sitzung in den Suchergebnissen angezeigt.

Hinweis „Letzte Sitzung“ bezeichnet die Dauer des letzten Verbindungszeitraums der Sitzung in Millisekunden. Wenn die Sitzung zurzeit verbunden ist, beschreibt dies die Dauer der verbundenen Sitzung. Wenn die Sitzung zurzeit getrennt ist, beschreibt dies die Dauer des vorherigen Verbindungszeitraums.

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.

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 Administrator **Benutzer und Gruppen** aus.
- 2 Klicken Sie auf der Registerkarte **Nicht authentifizierter Zugriff** auf **Löschen**.
- 3 Klicken Sie auf **OK**.

Nächste Schritte

Entfernen Sie die Anwendungsberechtigungen für den Benutzer. Weitere Informationen erhalten Sie unter „Entfernen von Berechtigungen für einen Desktop- oder Anwendungspool“ im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

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 Benutzer für einen nicht authentifizierten Zugriff 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 der Anmeldungsverzögerung bei nicht authentifiziertem Zugriff auf veröffentlichte Anwendungen

Da Benutzer keine Anmeldedaten eingeben, wenn Sie den nicht authentifizierten Zugriff verwenden, können RDS-Hosts von Anforderungen für veröffentlichte Anwendungen überlastet werden. Durch die Anmeldungsverzögerung wird dieses Problem gemindert. Sie können den Grad der Verzögerung anpassen. Sie können auch Clients blockieren, die keine Verzögerung unterstützen.

Voraussetzungen

- Stellen Sie sicher, dass Sie den nicht authentifizierten Zugriff für Benutzer aktiviert haben.
- Stellen Sie sicher, dass Sie über Horizon Client 4.9 oder eine höhere Version verfügen. Wenn Sie Horizon Client Version 4.8 verwenden, kommt es möglicherweise zu gelegentlichen Fehlern, wenn Benutzer sich anonym mit nicht authentifiziertem Zugriff bei Horizon 7 Version 7.6 anmelden, sodass die Anmeldung wiederholt werden muss.

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- 2 Klicken Sie auf die Registerkarte **Verbindungsserver**.
- 3 Klicken Sie auf die Registerkarte **Authentifizierung**.
- 4 Wählen Sie im Dropdown-Menü **Anmeldungsverzögerungsstufe** eine Verzögerungsstufe für Anmeldungen mit nicht authentifiziertem Zugriff aus.

Option	Beschreibung
Niedrig	Legt eine niedrige Verzögerungsstufe für Anmeldungen mit nicht authentifiziertem Zugriff fest. Bei Webbrowsern wie Microsoft Internet Explorer und Microsoft Edge wird empfohlen, die niedrige Verzögerungsstufe festzulegen.
Mittel	Legt eine mittlere Verzögerungsstufe für Anmeldungen mit nicht authentifiziertem Zugriff fest. Standardmäßig festgelegt. Ändern Sie diese Einstellung nicht, wenn Sie Horizon Client Version 4.8 verwenden.
Hoch	Legt eine hohe Verzögerungsstufe für Anmeldungen mit nicht authentifiziertem Zugriff fest. Wenn Sie eine hohe Verzögerungsstufe festlegen, kann das Protokoll dadurch mit der Zeit größer und die Benutzerfreundlichkeit beeinträchtigt werden.

- 5 (Optional) Um zu verhindern, dass Clients, die die Anmeldungsverzögerung nicht unterstützen, sich mit nicht authentifiziertem Zugriff bei Horizon 7 anmelden, wählen Sie **Nicht kompatible Clients blockieren** aus.

Horizon Client-Instanzen vor Version 4.8 sind nicht kompatibel.

6 Klicken Sie auf **OK**.

Nächste Schritte

Melden Sie sich bei Horizon Client mit einem nicht authentifizierten Zugriff an und starten Sie die veröffentlichte Anwendung. Siehe [Nicht authentifizierter Zugriff von Horizon Client aus](#).

Konfigurieren von Benutzern für die Hybrid-Anmeldung

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 7*.
- Überprüfen Sie, ob Sie einen Benutzer mit nicht authentifiziertem Zugriff erstellt haben.
- 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 Administrator **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 **Optionen** **Als 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 Entsperren“ 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 Entsperren“ mit der globalen Richtlinieneinstellung **Remotesitzungen entsperren, 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.

Speichern von Anmeldeinformationen in Horizon Clients für Mobilgeräte und Mac

Administratoren können Verbindungsserver konfigurieren, um zu ermöglichen, dass Horizon Clients für Mobilgeräte und Mac den Benutzernamen, das Kennwort und die Domäneninformationen eines Benutzers speichern.

Bei Horizon Client für Mobilgeräte wird das Kontrollkästchen **Kennwort speichern** durch diese Funktion auf den Anmeldedialogfeldern angezeigt. Bei Horizon Client für Mac wird das Kontrollkästchen **Dieses Kennwort speichern** durch diese Funktion im Anmeldedialogfeld angezeigt.

Wenn Benutzer ihre Anmeldedaten speichern möchten, werden diese Daten bei den nächsten Verbindungen zu den Anmeldefeldern in Horizon Client hinzugefügt.

Zum Aktivieren dieser Funktion müssen Sie einen Wert in View LDAP festlegen, um anzugeben, wie lange Anmeldeinformationen im Client gespeichert werden. Bei Horizon Client für Mac wird diese Funktion nur in der Version 4.1 oder höher unterstützt.

Hinweis Auf Windows-basierten Horizon-Clients entfällt durch die Funktion zur Anmeldung als aktueller Benutzer die Notwendigkeit von Benutzern, Anmeldedaten mehrmals eingeben zu müssen.

Konfigurieren eines Zeitüberschreitungslimits zum Speichern von Horizon Client-Anmeldeinformationen

Sie können ein Zeitüberschreitungslimit konfigurieren, das angibt, wie lange Horizon Client-Anmeldeinformationen auf Mobilgeräten und Mac-Clientsystemen gespeichert werden, indem ein Wert in View LDAP festgelegt wird. Das Zeitüberschreitungslimit wird in Minuten festgelegt. Wenn Sie View LDAP auf einer Verbindungsserver-Instanz ändern, werden diese Änderungen auf alle replizierten Verbindungsserver-Instanzen übertragen.

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 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 Bearbeiten Sie auf im Objekt **OU=Properties, OU=Global, CN=Common** den Attributwert **pae-ClientCredentialCacheTimeout**.

Wenn **pae-ClientCredentialCacheTimeout** nicht bzw. auf **0** festgelegt ist, ist die Funktion deaktiviert. Um diese Funktion zu aktivieren, können Sie die Anzahl der Minuten zur Beibehaltung der Anmeldedaten festlegen oder den Wert auf **-1** setzen, was bedeutet, dass es keine Zeitüberschreitung gibt.

Ergebnisse

Auf dem Verbindungsserver wird die neue Einstellung sofort wirksam. Der Verbindungsserver-Dienst oder der Clientcomputer müssen nicht neu gestartet werden.

Einrichten von True SSO

Mit der True SSO-Funktion (Single Sign-On) müssen Benutzer, nachdem sie sich bei VMware Identity Manager mithilfe einer Smartcard-, RSA SecurID- oder RADIUS-Authentifizierung oder über einen externen Identitätsanbieter mithilfe einer Unified Access Gateway-Appliance angemeldet haben, nicht noch zusätzlich Active Directory-Anmeldedaten für die Verwendung eines virtuellen Desktops, eines veröffentlichten Desktops oder einer veröffentlichten Anwendung eingeben.

Wenn ein Benutzer sich mit den Active Directory-Anmeldeinformationen authentifiziert, ist die True SSO-Funktion nicht erforderlich. Sie können aber die True SSO-Funktion so konfigurieren, dass sie auch in diesem Fall benutzt wird. Dann werden die vom Benutzer eingegebenen AD-Anmeldeinformationen ignoriert und die True SSO-Funktion wird verwendet.

Bei der Herstellung einer Verbindung mit einem virtuellen Desktop oder mit einer veröffentlichten Anwendung können Benutzer auswählen, ob sie den nativen Horizon Client oder HTML Access verwenden möchten.

Für diese Funktion gelten die folgenden Einschränkungen:

- Diese Funktion kann nicht für virtuelle Desktops verwendet werden, die mithilfe des View Agent Direct Connection-Plug-Ins bereitgestellt werden.
- Diese Funktion wird nur in IPv4-Umgebungen unterstützt.

Zur Einrichtung Ihrer Umgebung für die True SSO-Funktion müssen die nachfolgend aufgeführten Aufgaben durchgeführt werden:

- 1 [Festlegen der Architektur für True SSO](#)
- 2 [Einrichten einer Unternehmenszertifizierungsstelle](#)
- 3 [Erstellen von Zertifikatvorlagen für die Verwendung mit True SSO](#)
- 4 [Installieren und Einrichten eines Registrierungsservers](#)
- 5 [Exportieren des Registrierungsdienst-Clientzertifikats](#)
- 6 [Konfigurieren der SAML-Authentifizierung für die Verwendung von True SSO](#)
- 7 [Konfigurieren des Horizon-Verbindungsservers für True SSO](#)

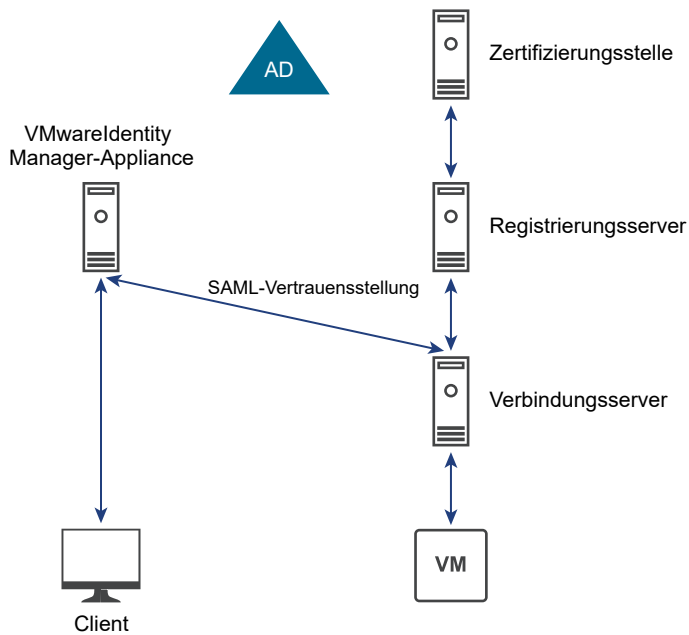
Festlegen der Architektur für True SSO

Damit Sie True SSO verwenden können, müssen Sie über eine Zertifizierungsstelle verfügen oder diese hinzufügen und einen Registrierungsserver erstellen. Diese beiden Server kommunizieren zum Erstellen des kurzlebigen virtuellen Horizon-Zertifikats, das eine Windows-Anmeldung ohne Kennwort ermöglicht. Sie können True SSO in einer einzelnen Domäne, in einer einzelnen Gesamtstruktur mit mehreren Domänen und in einer Installation mit mehreren Gesamtstrukturen sowie mit mehreren Domänen verwenden.

VMware empfiehlt bei Verwendung von True SSO die Verwendung von zwei Zertifizierungsstellen und zwei Registrierungsservern. Die nachfolgend aufgeführten Beispiele veranschaulichen die Anwendung von True SSO in unterschiedlichen Architekturen.

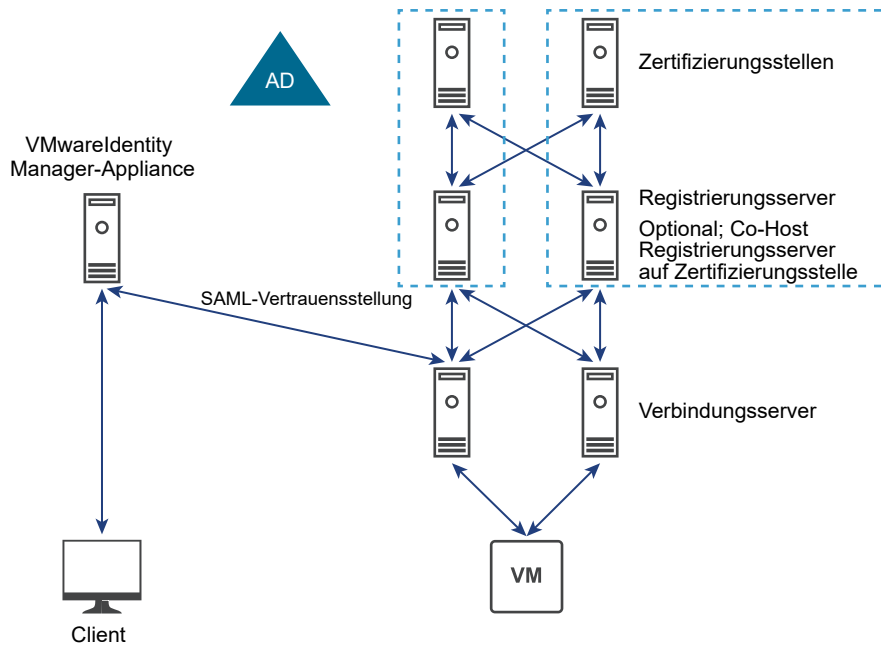
Die nachfolgende Abbildung zeigt eine einfache True SSO-Architektur.

Sehr einfache True SSO-Architektur



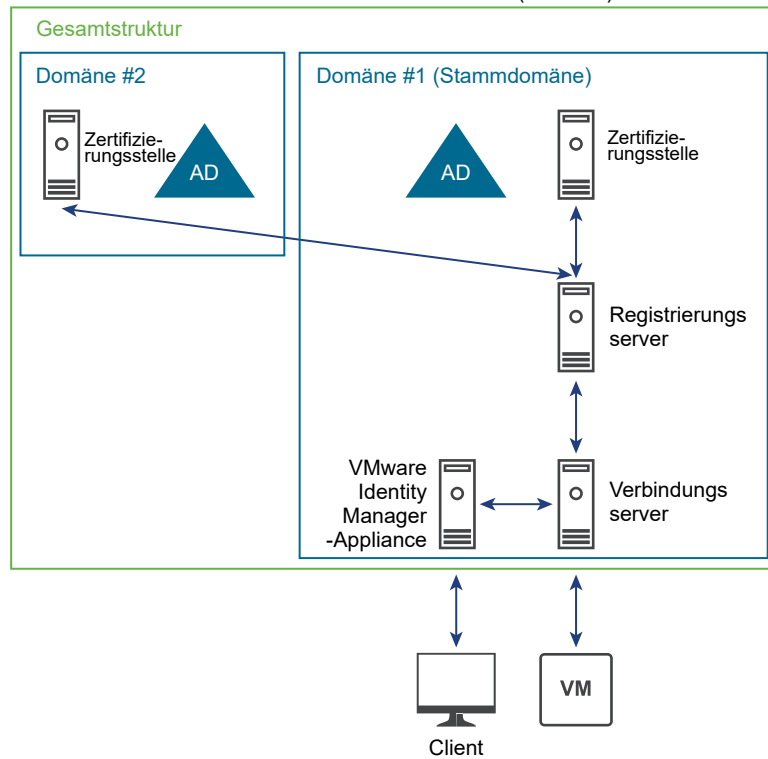
Die nachfolgende Abbildung zeigt die Anwendung von True SSO in einer Architektur mit einer einzelnen Domäne.

Typische HA True SSO-Architektur (einzelne Domäne)



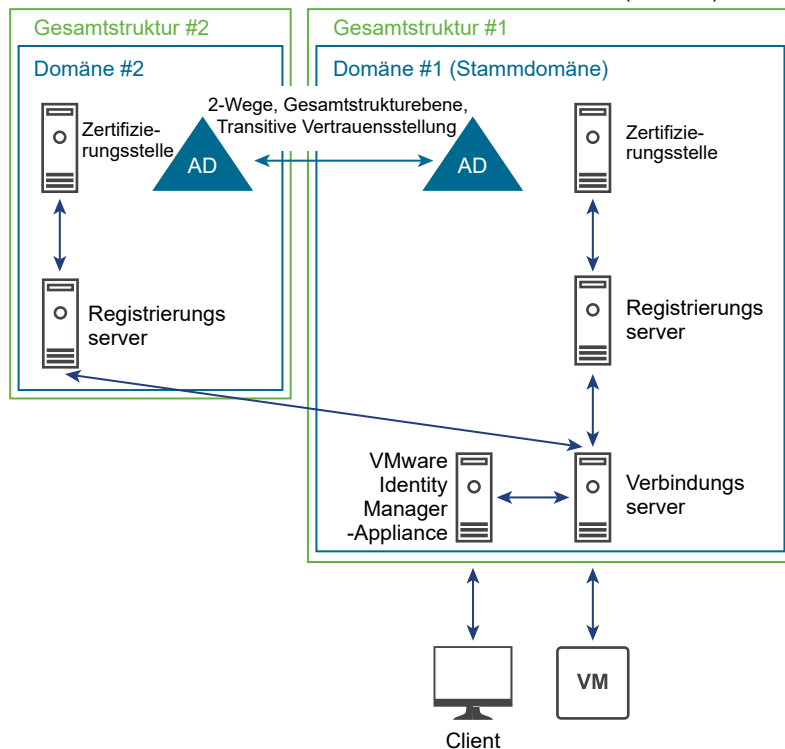
Die nachfolgende Abbildung zeigt die Anwendung von True SSO mit einer einzelnen Gesamtstruktur in einer Architektur mit mehreren Domänen.

True SSO mit einer einzelnen Gesamtstruktur in einer Architektur mit mehreren Domänen (nicht-HA)



Die nachfolgende Abbildung zeigt die Anwendung von True SSO in einer Architektur mit mehreren Gesamtstrukturen.

True SSO-Architektur mit mehreren Gesamtstrukturen (nicht-HA)



Einrichten einer Unternehmenszertifizierungsstelle

Wenn Sie noch keine Zertifizierungsstelle eingerichtet haben, müssen Sie die Rolle der Active Directory-Zertifikatdienste (AD CS) einem Windows-Server hinzufügen und diesen als Unternehmenszertifizierungsstelle konfigurieren.

Wenn Sie bereits über eine eingerichtete Unternehmenszertifizierungsstelle verfügen, stellen Sie sicher, dass die in dieser Vorgehensweise beschriebenen Einstellungen verwendet werden.

Es muss mindestens eine Unternehmenszertifizierungsstelle vorhanden sein. VMware empfiehlt die Verwendung von zwei Registrierungsservern für Failover-Fälle und für den Lastausgleich. Der für die True SSO-Funktion erstellte Registrierungsserver kommuniziert mit der Unternehmenszertifizierungsstelle. Wenn Sie den Registrierungsserver für die Verwendung mehrerer Unternehmenszertifizierungsstellen konfigurieren, wird dieser die verfügbaren Zertifizierungsstellen abwechselnd verwenden. Wenn Sie den Registrierungsserver auf dem Computer installieren, auf dem die Unternehmenszertifizierungsstelle gehostet wird, können Sie den Registrierungsserver so konfigurieren, dass dieser die lokale Zertifizierungsstelle verwendet. Für eine optimale Leistung wird diese Konfiguration empfohlen.

Zu dieser Vorgehensweise gehört auch die Aktivierung einer nicht persistenten Zertifikatverarbeitung. Standardmäßig beinhaltet die Zertifikatverarbeitung das Speichern eines Datensatzes jeder Zertifikatanforderung und des ausgestellten Zertifikats in der Zertifizierungsstellendatenbank. Ein dauerhaft hohes Aufkommen an Anforderungen vergrößert die Zertifizierungsstellendatenbank und nimmt eventuell den gesamten verfügbaren Festplattenspeicher in Anspruch, wenn keine Überwachung stattfindet. Die Aktivierung einer nicht persistenten Zertifikatverarbeitung kann dabei helfen, die Größe der Zertifizierungsstellendatenbank und die Häufigkeit von Aufgaben der Datenbankverwaltung zu beschränken.

Voraussetzungen

- Erstellen Sie eine virtuelle Maschine für Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 oder Windows Server 2019.
- Stellen Sie sicher, dass die virtuelle Maschine Teil der Active Directory-Domäne für die Horizon 7-Bereitstellung ist.
- Stellen Sie sicher, dass eine IPv4-Umgebung verwendet wird. Diese Funktion wird aktuell nicht in einer IPv6-Umgebung unterstützt.
- Stellen Sie sicher, dass das System über eine statische IP-Adresse verfügt.

Verfahren

- 1 Melden Sie sich beim Betriebssystem der virtuellen Maschine als Administrator an und starten Sie Server Manager.

2 Wählen Sie die Einstellungen für das Hinzufügen von Rollen aus.

Betriebssystem	Auswahl
■ Windows Server 2012 R2	a Wählen Sie Rollen und Funktionen hinzufügen aus.
■ Windows Server 2016	b Wählen Sie auf der Seite „Installationstyp auswählen“ Rollenbasierter oder funktionsbasierter Installationstyp aus.
■ Windows Server 2019	c Wählen Sie auf der Seite „Zielserver auswählen“ einen Server aus.
Windows Server 2008 R2	a Wählen Sie in der Navigationsstruktur Rollen aus. b Klicken Sie auf Rollen hinzufügen , um den Assistenten Rolle hinzufügen zu starten.

- 3 Wählen Sie auf der Seite „Serverrollen auswählen“ **Active Directory-Zertifikatdienste** aus.
- 4 Klicken Sie im Assistenten „Rollen und Funktionen hinzufügen“ auf **Funktionen hinzufügen** und lassen Sie das Kontrollkästchen **Verwaltungstools einschließen** aktiviert.
- 5 Bestätigen Sie auf der Seite „Funktionen auswählen“ die Standardeinstellungen.
- 6 Wählen Sie auf der Seite „Rollendienste auswählen“ die Option **Zertifizierungsstelle** aus.
- 7 Folgen Sie den Anweisungen und schließen Sie die Installation ab.
- 8 Klicken Sie nach dem Abschluss der Installation auf der Seite „Installationsstatus“ auf den Link **Active Directory-Zertifikatdienste auf dem Zielserver konfigurieren**, um den Assistenten für die AD/CS-Konfiguration zu öffnen.
- 9 Klicken Sie auf der Seite „Anmeldeinformationen“ auf **Weiter** und vervollständigen Sie die Seiten des Assistenten für die AD/CS-Konfiguration wie in der folgenden Tabelle beschrieben.

Option	Aktion
Rollendienste	Wählen Sie Zertifizierungsstelle aus, und klicken Sie auf Weiter (statt auf Konfigurieren).
Installationstyp	Wählen Sie Unternehmenszertifizierungsstelle aus.
Zertifizierungsstellentyp	Wählen Sie Stammzertifizierungsstelle oder Untergeordnete Zertifizierungsstelle aus. Einige Unternehmen bevorzugen eine PKI-Bereitstellung auf zwei Ebenen. Weitere Informationen finden Sie unter http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx .
Privater Schlüssel	Wählen Sie Neuen privaten Schlüssel erstellen aus.
Kryptografie für Zertifizierungsstelle	Für den Hashalgorithmus können Sie SHA1 , SHA256 , SHA384 oder SHA512 auswählen. Für die Schlüssellänge wählen Sie 1024 , 2048 , 3072 oder 4096 aus. VMware empfiehlt als Mindestwerte für den Schlüssel SHA256 und 2048.
Zertifizierungsstellenname	Übernehmen Sie den Standardnamen oder ändern Sie den Namen.
Gültigkeitsdauer	Übernehmen Sie den Standardwert von fünf Jahren.
Zertifikatdatenbank	Übernehmen Sie die Standardwerte.

- 10 Klicken Sie auf der Seite „Bestätigung“ auf **Konfigurieren**. Wenn der Assistent eine erfolgreiche Konfiguration meldet, schließen Sie den Assistenten.

- 11 Öffnen Sie eine Eingabeaufforderung und geben Sie den folgenden Befehl zur Konfiguration der Zertifizierungsstelle für eine nicht persistente Zertifikatverarbeitung ein.

```
certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

- 12 Geben Sie den folgenden Befehl zum Ignorieren von Offline-Fehlern der Zertifikatswiderrufsliste der Zertifizierungsstelle ein.

```
certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
```

Dieses Attribut ist erforderlich, da das von True SSO verwendete Stammzertifikat in der Regel offline ist und die Zertifikatsperrüberprüfung deshalb zwangsläufig scheitert.

- 13 Geben Sie die folgenden Befehle zum Neustart des Dienstes ein:

```
sc stop certsvc
sc start certsvc
```

Nächste Schritte

Erstellen Sie eine Zertifikatvorlage. Siehe [Erstellen von Zertifikatvorlagen für die Verwendung mit True SSO](#).

Erstellen von Zertifikatvorlagen für die Verwendung mit True SSO

Sie müssen eine Zertifikatvorlage erstellen, die für die Ausstellung von kurzlebigen Zertifikaten verwendet werden kann. Ferner müssen Sie festlegen, welche Computer in der Domäne diesen Zertifikattyp anfordern können.

Sie können mehr als eine Zertifikatvorlage erstellen. Sie können nur eine Vorlage pro Domäne konfigurieren, aber Sie können die Vorlage in mehreren Domänen freigeben. Wenn Sie eine Active Directory-Struktur mit drei Domänen haben und True SSO für alle drei Domänen verwenden möchten, können Sie beispielsweise eine, zwei oder drei Vorlagen konfigurieren. Alle Domänen können die gleiche Vorlage verwenden oder Sie können verschiedene Vorlagen für jede Domäne nutzen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über eine Unternehmenszertifizierungsstelle verfügen, die sich zum Erstellen der Vorlage wie in dieser Vorgehensweise beschrieben eignet. Siehe [Einrichten einer Unternehmenszertifizierungsstelle](#).
- Stellen Sie sicher, dass Active Directory für die Smartcard-Authentifizierung vorbereitet ist. Weitere Informationen finden Sie im Dokument *Horizon 7-Installation*.
- Erstellen Sie in der Domäne und Gesamtstruktur eine Sicherheitsgruppe für die Registrierungsserver, und fügen Sie dieser Gruppe die Computerkonten der Registrierungsserver hinzu.

Verfahren

- 1 Um True SSO zu konfigurieren, melden Sie sich bei dem Computer, den Sie für die Zertifizierungsstelle verwenden, als Administrator im Betriebssystem an und wählen Sie **Verwaltung > Zertifizierungsstelle** aus.
 - a Erweitern Sie den Strukturbaum im linken Fensterbereich, klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen** und wählen Sie **Verwalten** aus.
 - b Klicken Sie mit der rechten Maustaste auf die Vorlage **Smartcard-Anmeldung**, und wählen Sie **Duplizieren** aus.

- c Nehmen Sie auf den dargestellten Registerkarten die folgenden Änderungen vor:

Registerkarte	Aktion
Registerkarte „Kompatibilität“	<ul style="list-style-type: none"> ■ Wählen Sie als Zertifizierungsstelle Windows Server 2008 R2 aus. ■ Wählen Sie als Zertifikatsempfänger Windows 7/Windows Server 2008 R2 aus.
Registerkarte „Allgemein“	<ul style="list-style-type: none"> ■ Ändern Sie den Anzeigenamen der Vorlage in True SS0. ■ Ändern Sie die Gültigkeitsdauer so, dass sie einem typischen Werktag bzw. dem Zeitraum entspricht, in dem der Benutzer voraussichtlich im System angemeldet ist. Damit der Benutzer während der Anmeldungsdauer nicht den Zugriff auf die Netzwerkressource verliert, muss die Gültigkeitsdauer länger sein als der Kerberos-TGT-Erneuerungszeitraum in der Benutzerdomäne. (Die maximale Standardlebensdauer des Tickets beträgt 10 Stunden. Die Standarddomänenrichtlinie finden Sie unter Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Kontorichtlinien > Kerberos-Richtlinie: Max. Gültigkeitsdauer des Benutzertickets.) ■ Ändern Sie den Erneuerungszeitraum auf einen Wert zwischen 50 % und 75 % der Gültigkeitsdauer.
Registerkarte „Anforderungsverarbeitung“	<ul style="list-style-type: none"> ■ Wählen Sie als Zweck Signatur und Smartcard-Anmeldung aus. ■ Wählen Sie Automatische Erneuerung der Smartcards, ... aus.
Registerkarte „Kryptografie“	<ul style="list-style-type: none"> ■ Wählen Sie als Anbieterkategorie Schlüsselspeicheranbieter aus. ■ Wählen Sie als Algorithmusname RSA aus.
Registerkarte „Server“	<p>Wählen Sie Keine Zertifikate und Anforderungen in der Datenbank der Zertifizierungsstelle speichern aus.</p> <p>Wichtig Stellen Sie sicher, dass die Option Sperrinformationen nicht in ausgestellte Zertifikate einschließen deaktiviert ist. (Diese Option wird aktiviert, wenn Sie die erste Option auswählen. Sie müssen sie deshalb gezielt deaktivieren.)</p>
Registerkarte „Ausstellungsvoraussetzungen“	<ul style="list-style-type: none"> ■ Wählen Sie Diese Anzahl an autorisierten Signaturen aus und geben Sie als Wert 1 in das Feld ein. ■ Wählen Sie als Richtlinientyp Anwendungsrichtlinie aus, und setzen Sie die Richtlinie auf Zertifikatsanforderungs-Agent. ■ Wählen Sie unter Erneute Registrierung erfordert Folgendes: die Option Gültiges vorhandenes Zertifikat aus.
Registerkarte „Sicherheit“	<p>Vergeben Sie für die Sicherheitsgruppe, die Sie für die Computerkonten des Registrierungsservers erstellt haben, folgende Berechtigungen: Lesen, Registrieren.</p> <ol style="list-style-type: none"> 1 Klicken Sie auf Hinzufügen. 2 Legen Sie fest, welche Computer Zertifikate registrieren dürfen. 3 Aktivieren Sie für diese Computer die entsprechenden Kontrollkästchen und vergeben Sie diese Berechtigungen: Lesen, Registrieren.

- d Klicken Sie im Dialogfeld „Eigenschaften der neuen Vorlage“ auf **OK**.

- e Schließen Sie das Fenster „Zertifikatvorlagenkonsole“.

- f Klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen** und wählen Sie **Neu > Auszustellende Zertifikatvorlage** aus.

Hinweis Dieser Schritt ist für alle Zertifizierungsstellen erforderlich, die Zertifikate auf der Basis dieser Vorlage ausstellen.

- g Wählen Sie im Fenster „Zertifikatvorlagen aktivieren“ die Vorlage aus, die Sie soeben erstellt haben (z. B. **True SSO**), und klicken Sie auf **OK**.
- 2 Um Registrierungs-Agent-Computer zu konfigurieren, melden Sie sich bei dem Computer, den Sie für die Zertifizierungsstelle verwenden, als Administrator im Betriebssystem an und wählen Sie **Verwaltung > Zertifizierungsstelle** aus.

- a Erweitern Sie den Strukturbaum im linken Fensterbereich, klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen** und wählen Sie **Verwalten** aus.
- b Suchen Sie die Vorlage Registrierungs-Agent-Computer und öffnen Sie sie, und nehmen Sie dann auf der Registerkarte **Sicherheit** die folgende Änderung vor:

Vergeben Sie für die Sicherheitsgruppe, die Sie für die Computerkonten des Registrierungs-servers erstellt haben, folgende Berechtigungen: Lesen, Registrieren.

- 1 Klicken Sie auf **Hinzufügen**.
 - 2 Legen Sie fest, welche Computer Zertifikate registrieren dürfen.
 - 3 Aktivieren Sie für diese Computer die entsprechenden Kontrollkästchen und vergeben Sie diese Berechtigungen: Lesen, Registrieren.
- c Klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen**, und wählen Sie **Neu > Auszustellende Zertifikatvorlage** aus.

Hinweis Dieser Schritt ist für alle Zertifizierungsstellen erforderlich, die Zertifikate auf der Basis dieser Vorlage ausstellen.

- d Wählen Sie im Fenster „Zertifikatvorlagen aktivieren“ die Option **Registrierungs-Agent (Computer)** aus, und klicken Sie auf **OK**.

Nächste Schritte

Erstellen Sie einen Registrierungsdienst. Siehe [Installieren und Einrichten eines Registrierungsservers](#).

Installieren und Einrichten eines Registrierungsservers

Um einen Registrierungsserver zu installieren, führen Sie das Installationsprogramm für den Verbindungsserver aus, und wählen Sie dabei die Option „Horizon 7-Registrierungsserver“ aus. Der Registrierungsserver erfordert kurzlebige Zertifikate für die von Ihnen angegebenen Benutzer. Diese kurzfristigen Zertifikate dienen True SSO als Mechanismus zur Authentifizierung. Damit wird vermieden, dass Benutzer zur Eingabe ihrer Active Directory-Anmeldeinformationen aufgefordert werden.

Sie müssen mindestens einen Registrierungsserver installieren und einrichten. Dieser darf nicht auf demselben Host wie der View-Verbindungsserver installiert werden. VMware empfiehlt die Verwendung von zwei Registrierungsservern für Failover-Fälle und für den Lastausgleich. Wenn Sie über zwei Registrierungsserver verfügen, wird standardmäßig der eine für den normalen Ablauf und der andere für Failover-Fälle verwendet. Sie haben allerdings die Möglichkeit, diese Standardeinstellung so zu ändern, dass der Verbindungsserver abwechselnd Zertifikatanforderungen an beide Registrierungsserver sendet.

Wenn Sie den Registrierungsserver auf dem Computer installieren, auf dem die Unternehmenszertifizierungsstelle gehostet wird, können Sie den Registrierungsserver so konfigurieren, dass dieser die lokale Zertifizierungsstelle verwendet. Für eine optimale Leistung empfiehlt VMware eine Kombination der Konfiguration zur Verwendung der lokalen Zertifizierungsstelle mit der Konfiguration eines Lastausgleichsdienstes für den Registrierungsserver. Dies führt dazu, dass der Verbindungsserver bei Eintreffen einer Zertifikatanforderung die Registrierungsserver alternativ verwendet und jeder Registrierungsserver die Anforderungen mithilfe der lokalen Zertifizierungsstelle verarbeitet. Erläuterungen zu den entsprechenden Konfigurationseinstellungen finden Sie unter [Registrierungsserver-Konfigurationseinstellungen](#) und [Konfigurationseinstellungen für den Verbindungsserver](#).

Voraussetzungen

- Erstellen Sie eine virtuelle Windows Server 2008 R2-, Windows Server 2012 R2- oder Windows Server 2016-Maschine mit mindestens 4 GB Arbeitsspeicher oder verwenden Sie eine virtuelle Maschine, die die Unternehmenszertifizierungsstelle hostet. Verwenden Sie keine Maschine, die als Domänencontroller eingesetzt wird.
- Stellen Sie sicher, dass keine andere View-Komponente wie etwa View-Verbindungsserver, View Composer, Sicherheitsserver, Horizon Client, View Agent oder Horizon Agent auf der virtuellen Maschine installiert ist.
- Stellen Sie sicher, dass die virtuelle Maschine Teil der Active Directory-Domäne für die Horizon 7-Bereitstellung ist.
- Stellen Sie sicher, dass eine IPv4-Umgebung verwendet wird. Diese Funktion wird aktuell nicht in einer IPv6-Umgebung unterstützt.
- VMware empfiehlt eine statische IP-Adresse für das System.
- Stellen Sie sicher, dass Sie sich beim Betriebssystem als Domänenbenutzer mit Administratorrechten anmelden können. Für die Ausführung des Installationsprogramms müssen Sie als Administrator angemeldet sein.

Verfahren

- 1 Auf dem Computer, auf dem der Registrierungsserver verwendet werden soll, fügen Sie zu MMC das Zertifikat-Snap-In hinzu:
 - a Öffnen Sie die Microsoft Management Console und wählen Sie **Datei > Snap-In hinzufügen/entfernen** aus.
 - b Wählen Sie unter **Verfügbare Snap-Ins** **Zertifikate** aus, und klicken Sie auf **Hinzufügen**.

- c Wählen Sie im Fenster „Zertifikat-Snap-In“ **Computerkonto** aus, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
- d Klicken Sie im Fenster „Snap-Ins hinzufügen/entfernen“ auf **OK**.

2 Stellen Sie ein Registrierungs-Agent-Zertifikat aus:

- a Erweitern Sie in der Zertifikatkonsole die Konsolenbaumstruktur, klicken Sie mit der rechten Maustaste auf den Ordner **Persönlich**, und wählen Sie **Alle Aufgaben > Neues Zertifikat anfordern** aus.
- b Im Assistenten zur Zertifikatregistrierung übernehmen Sie die Standardeinstellungen, bis die Seite „Zertifikate anfordern“ angezeigt wird.
- c Auf dieser Seite aktivieren Sie das Kontrollkästchen **Registrierungs-Agent (Computer)** und klicken Sie auf **Registrieren**.
- d Übernehmen Sie die Standardeinstellungen auf den anderen Seiten des Assistenten und klicken Sie auf der letzten Seite auf **Fertig stellen**.

In der Microsoft Management Console wird dann, wenn Sie den Ordner **Persönlich** erweitern und **Zertifikate** im linken Bereich auswählen, ein neues Zertifikat im rechten Bereich dargestellt.

3 Installieren Sie den Registrierungsserver:

- a Laden Sie die View-Verbindungsserver-Installationsdatei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunter.

Unter „Desktop- und Endbenutzer-Computing“ wählen Sie den VMware Horizon-7-Download, der die View-Verbindungsserver-Datei enthält.

Der Dateiname des Installationsprogramms lautet VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe. Hierbei ist xxxxxx die Buildnummer und y.y.y die Versionsnummer.
- b Doppelklicken Sie auf die Installationsdatei, um den Assistenten zu starten, und folgen Sie den Anweisungen, bis die Seite mit den Installationsoptionen angezeigt wird.
- c Wählen Sie **Horizon 7-Registrierungsserver** auf der Seite „Installationsoptionen“. Wählen Sie dann einen Authentifizierungsmodus für die Registrierungsserver-Instanz aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Horizon 7	Konfiguriert den Authentifizierungsmodus für eine Horizon 7-Umgebung.
Horizon Cloud	Konfiguriert den Authentifizierungsmodus für eine Horizon Cloud-Umgebung.

- d Folgen Sie den Anweisungen, um die Installation abzuschließen.

Sie müssen eingehende Verbindungen an Port 32111 (TCP) aktivieren, da der Registrierungsserver sonst nicht funktioniert. Das Installationsprogramm öffnet den Port standardmäßig während der Installation.

Nächste Schritte

- Wenn Sie den Registrierungsserver auf dem Computer installiert haben, auf dem eine Unternehmenszertifizierungsstelle gehostet wird, konfigurieren Sie den Registrierungsserver so, dass dieser die lokale Zertifizierungsstelle verwendet. Siehe [Registrierungsserver-Konfigurationseinstellungen](#). Wenn Sie optional mehr als einen Registrierungsserver installieren und einrichten, konfigurieren Sie die Verbindungsserver für die Aktivierung des Lastausgleichsdienstes zwischen den Registrierungsservern. Siehe [Konfigurationseinstellungen für den Verbindungsserver](#).
- Koppeln Sie die Verbindungsserver mit den Registrierungsservern. Siehe [Exportieren des Registrierungsdienst-Clientzertifikats](#).

Exportieren des Registrierungsdienst-Clientzertifikats

Um eine Kopplung herzustellen, können Sie mit dem MMC-Zertifikat-Snap-In das automatisch generierte, selbstsignierte Registrierungsdienst-Clientzertifikat von einem Verbindungsserver in den Cluster exportieren. Dieses Zertifikat wird als Clientzertifikat bezeichnet, da der Verbindungsserver ein Client des Registrierungsdienstes ist und vom Registrierungsserver bereitgestellt wird.

Der Registrierungsdienst muss dem VMware Horizon-Verbindungsserver vertrauen, wenn dieser die Registrierungsserver auffordert, die kurzlebigen Zertifikate für Active Directory-Benutzer auszustellen. Folglich müssen VMware Horizon-Verbindungsserver-Cluster oder -Pods mit Registrierungsservern kombiniert werden.

Das Registrierungsdienst-Clientzertifikat wird automatisch erstellt, wenn ein Horizon 7- oder höherer Verbindungsserver installiert ist und der VMware Horizon-Verbindungsserver-Dienst gestartet wird. Das Zertifikat wird über View LDAP an die anderen Horizon 7-Verbindungsserver verteilt, die dem Cluster später hinzugefügt werden. Das Zertifikat wird dann in einem benutzerdefinierten Container (VMware Horizon View Certificates\Certificates) im Windows-Zertifikatspeicher auf dem Computer gespeichert.

Voraussetzungen

Stellen Sie sicher, dass Sie einen Horizon 7-Verbindungsserver oder eine höhere Version installiert haben. Weitere Installationsanweisungen finden Sie unter *Horizon 7-Installation*. Weitere Upgradeanweisungen finden Sie unter *Horizon 7-Upgrades*.

Wichtig Kunden können anstelle des vom Verbindungsserver generierten Zertifikats ihre eigenen Zertifikate für die Kopplung verwenden. Dazu platzieren Sie das bevorzugte Zertifikat (und den zugehörigen privaten Schlüssel) in den benutzerdefinierten Container (VMware Horizon View Certificates\Certificates) im Windows-Zertifikatspeicher auf dem Computer des Verbindungsservers. Anschließend müssen Sie den Anzeigenamen des Zertifikats auf **vdm.ec.new** festlegen und den Server neu starten. Die anderen Server im Cluster übernehmen dieses Zertifikat aus LDAP. Anschließend führen Sie die Schritte in der nachstehenden Vorgehensweise aus.

Verfahren

- 1 Fügen Sie auf einem der Verbindungsserver-Computer im Cluster das Zertifikat-Snap-In der MMC hinzu:
 - a Öffnen Sie die Microsoft Management Console, und wählen Sie **Datei > Snap-In hinzufügen/entfernen** aus.
 - b Wählen Sie unter **Verfügbare Snap-Ins** **Zertifikate** aus, und klicken Sie auf **Hinzufügen**.
 - c Wählen Sie im Fenster „Zertifikat-Snap-In“ **Computerkonto** aus, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
 - d Klicken Sie im Fenster „Snap-Ins hinzufügen/entfernen“ auf **OK**.
- 2 Erweitern Sie im linken Bereich der Microsoft Management Console den Ordner **VMware Horizon View Certificates**, und wählen Sie den Ordner **Zertifikate** aus.
- 3 Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf die Zertifikatsdatei mit dem Anzeigenamen **vdm.ec**, und wählen Sie **Alle Aufgaben > Exportieren** aus.
- 4 Übernehmen Sie im Zertifikatexport-Assistenten die Standardeinstellungen, einschließlich des aktivierten Optionsfelds **Nein, privaten Schlüssel nicht exportieren**.
- 5 Wenn Sie dazu aufgefordert werden, die Datei zu benennen, geben Sie als Namen für das Registrierungsdienst-Clientzertifikat beispielsweise **EnrollClient** ein. Folgen Sie den Anweisungen des Assistenten, und exportieren Sie das Zertifikat.

Nächste Schritte

Importieren Sie das Zertifikat in den Registrierungsserver. Siehe [Importieren des Registrierungsdienst-Clientzertifikats in den Registrierungsserver](#).

Importieren des Registrierungsdienst-Clientzertifikats in den Registrierungsserver

Um den Vorgang der Paarbildung abzuschließen, importieren Sie das Registrierungsdienst-Clientzertifikat mithilfe des MMC-Zertifikat-Snap-In in den Registrierungsserver. Sie müssen diesen Vorgang für jeden Registrierungsserver durchführen.

Voraussetzungen

- Stellen Sie sicher, dass Sie einen Horizon 7-Registrierungsserver oder eine neuere Version installiert haben. Siehe [Installieren und Einrichten eines Registrierungsservers](#).

- Stellen Sie sicher, dass Sie über das korrekte Zertifikat für den Import verfügen. Sie können entweder Ihr eigenes Zertifikat oder ein automatisch generiertes, selbstsigniertes Registrierungsdienst-Clientzertifikat von einem Verbindungsserver im Cluster wie unter [Exportieren des Registrierungsdienst-Clientzertifikats](#) beschrieben verwenden.

Wichtig Wenn Sie Ihre eigenen Zertifikate für die Paarbildung verwenden möchten, platzieren Sie das bevorzugte Zertifikat (und den zugehörigen privaten Schlüssel) im benutzerdefinierten Container (VMware Horizon View Certificates\Certificates) des Windows-Zertifikatspeichers auf dem Verbindungsserver-Computer. Anschließend müssen Sie den Anzeigenamen des Zertifikats auf **vdm.ec.new** festlegen und den Server neu starten. Die anderen Server im Cluster übernehmen dieses Zertifikat aus LDAP. Anschließend führen Sie die Schritte in der nachstehenden Vorgehensweise aus.

Wenn Sie über ein eigenes Clientzertifikat verfügen, handelt es sich bei dem Zertifikat, das Sie zum Registrierungsserver kopieren müssen, um das Stammzertifikat, das zum Generieren des Clientzertifikats verwendet wurde.

Verfahren

- 1 Kopieren Sie die jeweilige Zertifikatdatei auf den Computer des Registrierungsservers.

Wenn Sie das automatisch generierte Zertifikat verwenden möchten, kopieren Sie das Registrierungsdienst-Clientzertifikat vom Verbindungsserver. Wenn Sie Ihr eigenes Zertifikat verwenden möchten, kopieren Sie das Stammzertifikat, das zum Generieren des Clientzertifikats verwendet wurde.
- 2 Auf dem Registrierungsserver fügen Sie zu MMC das Zertifikate-Snap-In hinzu.
 - a Öffnen Sie die Microsoft Management Console, und wählen Sie **Datei > Snap-In hinzufügen/entfernen** aus.
 - b Wählen Sie unter **Verfügbare Snap-Ins** **Zertifikate** aus, und klicken Sie auf **Hinzufügen**.
 - c Wählen Sie im Fenster „Zertifikat-Snap-In“ **Computerkonto** aus, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
 - d Klicken Sie im Fenster „Snap-Ins hinzufügen/entfernen“ auf **OK**.
- 3 In der Microsoft Management Console klicken Sie im linken Bereich mit der rechten Maustaste auf den Ordner **VMware Horizon View Enrollment Server Trusted Roots**, und wählen Sie **Alle Aufgaben > Importieren** aus.
- 4 Im Assistenten für den Zertifikatimport folgen Sie den Anweisungen, um zur Zertifikatdatei **EnrollClient** zu wechseln und um diese zu öffnen.
- 5 Folgen Sie den Anweisungen, und übernehmen Sie die Standardwerte, um das Importieren des Zertifikats abzuschließen.

- 6 Klicken Sie das importierte Zertifikat mit der rechten Maustaste an, und fügen Sie einen Anzeigenamen wie z. B. **vdm.ec** (für das Registrierungs-Clientzertifikat) hinzu.

VMware empfiehlt die Verwendung eines Anzeigenamens, der einen Rückschluss auf den Horizon 7-Cluster zulässt. Sie können aber jeden Namen benutzen, mit dem sich das Clientzertifikat einfach identifizieren lässt.

Nächste Schritte

Konfigurieren Sie den SAML-Authentifikator, der zum Delegieren der Authentifizierung bei VMware Identity Manager verwendet wird. Siehe [Konfigurieren der SAML-Authentifizierung für die Verwendung von True SSO](#).

Konfigurieren der SAML-Authentifizierung für die Verwendung von True SSO

Mit der in Horizon 7 eingeführten True SSO-Funktion können sich die Benutzer bei VMware Identity Manager 2.6 und höheren Versionen mithilfe einer Smartcard-, RADIUS- oder RSA SecurID-Authentifizierung anmelden. Sie werden dann nicht mehr zur Eingabe von Active Directory-Anmeldeinformationen aufgefordert, selbst wenn sie einen Remote-Desktop oder eine Remoteanwendung zum ersten Mal starten.

Bei früheren Versionen funktionierte die einmalige Anmeldung (SSO, Single Sign-On) so, dass die Benutzer zur Eingabe ihrer Active Directory-Anmeldedaten aufgefordert wurden, wenn sie zum ersten Mal einen Remote-Desktop oder eine veröffentlichte Anmeldung gestartet haben, sofern sie sich zuvor nicht mit ihren Active Directory-Anmeldedaten authentifiziert hatten. Diese Anmeldeinformationen wurden dann zwischengespeichert, sodass die Benutzer bei nachfolgenden Startvorgängen ihre Anmeldeinformationen nicht erneut eingeben mussten. Bei True SSO werden kurzlebige Zertifikate erstellt und statt der Active Directory-Anmeldeinformationen verwendet.

Das Vorgehen zum Konfigurieren der SAML-Authentifizierung für VMware Identity Manager hat sich nicht geändert, jedoch ist ein zusätzlicher Schritt für True SSO hinzugekommen. Sie müssen VMware Identity Manager so konfigurieren, dass True SSO aktiviert ist.

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

Voraussetzungen

- Stellen Sie sicher, dass die einmalige Anmeldung als globale Einstellung aktiviert ist. Wählen Sie in Horizon Administrator **Konfiguration > Globale Einstellungen** aus und vergewissern Sie sich, dass **Einmalige Anmeldung (Single Sign-On)** auf **Aktiviert** festgelegt ist.
- Stellen Sie sicher, dass VMware Identity Manager installiert und konfiguriert ist. Weitere Informationen finden Sie in der Dokumentation zu VMware Identity Manager unter <https://docs.vmware.com/de/VMware-Identity-Manager/index.html>.
- 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. Weitere Informationen enthält das Thema „Importieren eines Stamm- und Zwischenzertifikats in einen Windows-Zertifikatspeicher“ im Kapitel „Konfigurieren von SSL-Zertifikaten für Horizon 7 Server“ im Dokument *Horizon 7-Installation*.

- Notieren Sie sich den FQDN der VMware Identity Manager-Serverinstanz.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Konfiguration > Server** aus.
- 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** im Dropdown-Menü **Delegierung von Authentifizierung an VMware Horizon (SAML 2.0-Authentifikator)** die Option **Zulässig** oder **Erforderlich** aus.

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
Bezeichnung	Sie können den FQDN der VMware Identity Manager-Serverinstanz verwenden.
Beschreibung	(Optional) Sie können den FQDN der VMware Identity Manager-Serverinstanz verwenden.
Metadaten-URL	URL zum Abrufen aller Informationen, die für den Austausch von SAML-Informationen zwischen dem SAML-Identitätsanbieter und der Horizon-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 diese Zeichenfolge durch den FQDN der VMware Identity Manager-Serverinstanz.
Verwaltungs-URL	URL für den Zugriff auf die Verwaltungskonsole des SAML-Identitätsanbieters (VMware Identity Manager-Instanz). Diese URL hat das Format <code>https://<Identity-Manager-FQDN>:8443</code> .

- 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 vertrauenswürdiges Zertifikat für Horizon 7 und VMware Identity Manager verwenden.

Das Dropdown-Menü **SAML 2.0-Authentifikator** zeigt den neu erstellten Authentifikator an, der nun als ausgewählter Authentifikator festgelegt ist.

- 7 Wählen Sie im Abschnitt „Systemzustand“ auf dem Horizon Administrator-Dashboard **Andere Komponenten > SAML 2.0-Authentifikatoren** aus, wählen Sie den von Ihnen hinzugefügten SAML-Authentifikator aus und prüfen Sie die Details.

Falls die Konfiguration erfolgreich ist, steht der Systemzustand des Authentifikators auf grün. Der Systemzustand eines Authentifikators wird rot dargestellt, wenn das Zertifikat nicht vertrauenswürdig ist, wenn der VMware Identity Manager-Dienst nicht verfügbar ist oder wenn die Metadaten-URL ungültig ist. Falls das Zertifikat nicht vertrauenswürdig ist, sind Sie möglicherweise nicht in der Lage, auf **Überprüfen** zu klicken, um das Zertifikat zu validieren und anzunehmen.

- 8 Melden Sie sich bei der VMware Identity Manager-Verwaltungskonsole an, navigieren Sie zum Desktop-Pool von der Seite **Katalog > Virtuelle Apps** und aktivieren Sie das Kontrollkästchen **True SSO aktiviert**.

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 Dienst Anbietern auf dem Verbindungsserver](#).
- Verwenden Sie die `vdmutl`-Befehlszeilenschnittstelle, um True SSO auf einem Verbindungsserver zu konfigurieren. Siehe [Konfigurieren des Horizon-Verbindungsservers für True SSO](#).

Weitere Informationen zur Funktionsweise der SAML-Authentifizierung finden Sie unter [Verwenden der SAML-Authentifizierung](#).

Konfigurieren des Horizon-Verbindungsservers für True SSO

Mit der Befehlszeilenschnittstelle `vdmutl` können Sie die True SSO-Funktion konfigurieren sowie aktivieren und deaktivieren.

Dieser Vorgang darf nur auf einem einzigen Verbindungsserver im Cluster ausgeführt werden.

Wichtig In dieser Vorgehensweise werden nur die für die Aktivierung von True SSO erforderlichen Befehle verwendet. Eine Liste aller für die Verwaltung von True SSO-Konfigurationen verfügbaren Konfigurationsoptionen und Beschreibungen der einzelnen Optionen finden Sie unter [Befehlszeilenreferenz für die True SSO-Konfiguration](#).

Voraussetzungen

- Stellen Sie sicher, dass Sie den Befehl als Benutzer mit der Administratorrolle ausführen können. Sie können einem Benutzer die Administratorrolle mithilfe von Horizon Administrator zuweisen. Siehe [Kapitel 6 Konfigurieren der rollenbasierten Verwaltungsdelegation](#).
- Stellen Sie sicher, dass Sie den vollqualifizierten Domännennamen (FQDN) der folgenden Server kennen:
 - Verbindungsserver
 - Registrierungsserver

Weitere Informationen finden Sie unter [Installieren und Einrichten eines Registrierungsservers](#).

- Zertifizierungsstelle des Unternehmens

Weitere Informationen finden Sie unter [Einrichten einer Unternehmenszertifizierungsstelle](#).

- Stellen Sie sicher, dass Sie über den Netbios-Namen oder FQDN der Domäne verfügen.
- Stellen Sie sicher, dass eine Zertifikatvorlage erstellt wurde. Siehe [Erstellen von Zertifikatvorlagen für die Verwendung mit True SSO](#).
- Vergewissern Sie sich, dass ein SAML-Authentifikator erstellt wurde, der die Authentifizierung an VMware Identity Manager delegiert. Siehe [Konfigurieren der SAML-Authentifizierung für die Verwendung von True SSO](#).

Verfahren

- 1 Öffnen Sie auf einem Verbindungsserver im Cluster eine Eingabeaufforderung und geben Sie den Befehl zum Hinzufügen eines Registrierungsservers ein.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truessso --environment --add --enrollmentServer enroll-server-fqdn
```

Der Registrierungsserver wird der globalen Liste hinzugefügt.

- 2 Geben Sie den Befehl zum Auflisten der Informationen für diesen Registrierungsserver ein.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truessso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn
```

Die Ausgabe enthält den Namen der Gesamtstruktur, die Angabe, ob das Zertifikat des Registrierungsservers gültig ist, den Namen und die Details der Zertifikatvorlage, die verwendet werden kann, und den allgemeinen Namen der Zertifizierungsstelle. Zur Konfiguration der Domänen, mit denen der Registrierungsserver eine Verbindung herstellen kann, können Sie die Windows-Registrierungseinstellung auf dem Registrierungsserver verwenden. Standardmäßig können Verbindungen mit allen vertrauenswürdigen Domänen hergestellt werden.

Wichtig Sie müssen im nächsten Schritt den allgemeinen Namen (CN) der Zertifizierungsstelle angeben.

- 3 Geben Sie den Befehl zum Erstellen eines True SSO-Connectors mit den Konfigurationsinformationen ein, und aktivieren Sie den Connector.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truessso --create --connector --domain domain-fqdn --template TrueSSO-template-name --primaryEnrollmentServer enroll-server-fqdn --certificateServer ca-common-name --mode enabled
```

In diesem Befehl steht *TrueSSO-template-name* für den Namen der Vorlage, der im vorherigen Schritt ausgegeben wurde, und *ca-common-name* steht für den allgemeinen Namen der Zertifizierungsstelle des Unternehmens, der ebenfalls dieser Ausgabe zu entnehmen ist.

Der True SSO-Konnektor wird in einem Pool oder Cluster für die angegebene Domäne aktiviert. Um True SSO auf der Poolebene zu deaktivieren, führen Sie `vdmUtil --certsso --edit --connector <domain> --mode disabled` aus. Mit einem Gruppenrichtlinienobjekt (`vdm_agent.adm`) können Sie die True SSO-Funktion für eine einzelne virtuelle Maschine deaktivieren.

- 4 Geben Sie den Befehl ein, um zu ermitteln, welche SAML-Authentifikatoren verfügbar sind.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --list --authenticator
```

Authentifikatoren werden erstellt, wenn Sie mit Horizon Administrator die SAML-Authentifizierung zwischen VMware Identity Manager und einem Verbindungsserver konfigurieren.

Die Ausgabe enthält den Namen des Authentifikators und die Angabe, ob True SSO aktiviert ist.

Wichtig Sie müssen im nächsten Schritt den Namen des Authentifikators angeben.

- 5 Geben Sie den Befehl ein, um den Authentifikator für die Verwendung des True SSO-Modus zu aktivieren.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --authenticator --edit --name authenticator-fqdn --truessoMode {ENABLED|ALWAYS}
```

Geben Sie für `--truessoMode` die Option `ENABLED` an, wenn True SSO nur dann verwendet werden soll, wenn bei der Anmeldung des Benutzers bei VMware Identity Manager kein Kennwort angegeben wurde. Wenn in diesem Fall ein Kennwort verwendet und zwischengespeichert wurde, benutzt das System das Kennwort. Legen Sie `--truessoMode` auf `ALWAYS` fest, wenn True SSO selbst dann verwendet werden soll, wenn bei der Anmeldung des Benutzers bei VMware Identity ein Kennwort angegeben wurde.

Nächste Schritte

Überprüfen Sie in Horizon Administrator den Integritätsstatus der True SSO-Konfiguration. Weitere Informationen finden Sie unter [Verwenden des Systemzustand-Dashboards zur Behebung von Fehlern im Zusammenhang mit True SSO](#).

Zum Konfigurieren erweiterter Optionen verwenden Sie die erweiterten Windows-Einstellungen auf dem betreffenden System. Siehe [Erweiterte Konfigurationseinstellungen für True SSO](#).

Befehlszeilenreferenz für die True SSO-Konfiguration

Mit der Befehlszeilenschnittstelle „vdmutil“ können Sie die True SSO-Funktion konfigurieren und verwalten.

Speicherort des Dienstprogramms

Der Pfad zur ausführbaren Datei des Befehls `vdmutil` lautet standardmäßig `C:\Programme\VMware\VMware View\Server\tools\bin`. Damit Sie den Pfad nicht in die Befehlszeile eingeben müssen, fügen Sie ihn zur `PATH`-Umgebungsvariable hinzu.

Syntax und Authentifizierung

Verwenden Sie den Befehl `vdmutil` an einer Windows-Eingabeaufforderung mit dem folgenden Format.

```
vdmutil Authentifizierungsoptionen --truesso Zusatzoptionen und Argumente
```

Welche Zusatzoptionen verwendet werden können, hängt von der Befehlsoption ab. Dieses Thema behandelt die Optionen für die True SSO-Konfiguration (`--truesso`). Es folgt ein Beispiel für den Befehl, mit dem die für True SSO konfigurierten Connectors aufgeführt werden:

```
vdmutil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --list --connector
```

Der `vdmutil`-Befehl umfasst Authentifizierungsoptionen zur Angabe des Benutzernamens, der Domäne und des Kennworts für die Authentifizierung.

Tabelle 5-1. vdmutil-Befehlsauthentifizierungsoptionen

Option	Beschreibung
<code>--authAs</code>	Der Name eines Horizon 7-Administratorbenutzers. Verwenden Sie nicht das Format <i>Domäne \Benutzername</i> oder das UPN-Format (Benutzerprinzipalname).
<code>--authDomain</code>	Der vollqualifizierte Domänenname oder Netbios-Name der Domäne für den mit der Option <code>--authAs</code> angegebenen Horizon 7-Administratorbenutzer.
<code>--authPassword</code>	Das Kennwort für den in der Option <code>--authAs</code> angegebenen Horizon 7-Administratorbenutzer. Wenn "*" anstelle eines Kennworts eingegeben wird, fordert der Befehl <code>vdmutil</code> zur Eingabe des Kennworts auf. Vertrauliche Kennwörter werden dann nicht im Befehlsverlauf der Befehlszeile hinterlassen.

Sie müssen die Authentifizierungsoptionen mit allen `vdmutil`-Befehlsoptionen verwenden, mit Ausnahme von `--help` und `--verbose`.

Ausgabe des Befehls

Der Befehl `vdmutil` gibt 0 zurück, wenn ein Vorgang erfolgreich ist, und einen fehlerspezifischen Code ungleich null, wenn ein Vorgang fehlschlägt. Der Befehl `vdmutil` schreibt Fehlermeldungen in die Standardfehler. Wenn ein Vorgang eine Ausgabe erzeugt oder die ausführliche Protokollierung mithilfe der Option `--verbose` aktiviert ist, schreibt der Befehl `vdmutil` die Ausgabe in die Standardausgabe, und zwar auf Englisch.

Befehle zum Verwalten von Registrierungsservern

Sie müssen für jede Domäne einen Registrierungsserver hinzufügen. Zudem können Sie einen zweiten Registrierungsserver hinzufügen und diesen Server später als Sicherungsserver ausweisen.

Aus Gründen der Lesbarkeit stellen die Optionen in der folgenden Tabelle nicht den gesamten Befehl dar, der von Ihnen eingegeben werden muss. Es werden hier nur die Optionen angegeben, die sich auf eine bestimmte Aufgabe beziehen. Beispielsweise enthält die Tabelle eine Zeile mit den Optionen `--environment --list --enrollmentServers`. Der `vdmUtil`-Befehl, den Sie tatsächlich eingeben, verfügt aber auch über Optionen für die Authentifizierung und für die Angabe, dass True SSO konfiguriert wird:

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --
truesso --environment --list --enrollmentServers
```

Weitere Informationen zu den Authentifizierungsoptionen finden Sie unter [Befehlszeilenreferenz für die True SSO-Konfiguration](#).

Tabelle 5-2. vdmutil truesso-Befehlsoptionen zum Verwalten von Registrierungsservern

Befehl und Optionen	Beschreibung
<code>--environment --add --enrollmentServer enroll-server-fqdn</code>	Fügt der Umgebung den angegebenen Registrierungsserver hinzu, wobei <i>enroll-server-fqdn</i> für den FQDN des Registrierungservers steht. Wenn der Registrierungsserver bei der Ausführung dieses Befehls bereits hinzugefügt wurde, geschieht nichts.
<code>--environment --remove --enrollmentServer enroll-server-fqdn</code>	Entfernt den angegebenen Registrierungsserver aus der Umgebung, wobei <i>enroll-server-fqdn</i> für den FQDN des Registrierungservers steht. Wenn der Registrierungsserver bei der Ausführung dieses Befehls bereits entfernt wurde, geschieht nichts.
<code>--environment --list --enrollmentServers</code>	Listet die FQDNs aller Registrierungsserver in der Umgebung auf.
<code>--environment --list --enrollmentServer enroll-server-fqdn</code>	Listet die FQDNs der Domänen und Gesamtstrukturen auf, denen die Domänen und Gesamtstrukturen, denen der Registrierungsserver angehört, vertrauen, und gibt jeweils den Status des Registrierungszertifikats an. Dieser kann VALID oder INVALID lauten. VALID bedeutet, dass auf dem Registrierungsserver ein Registrierungs-Agent-Zertifikat installiert ist. Der Status kann aus verschiedenen Gründen INVALID lauten: <ul style="list-style-type: none"> ■ Es wurde kein Zertifikat installiert. ■ Das Zertifikat ist noch nicht gültig oder abgelaufen. ■ Das Zertifikat wurde von keiner vertrauenswürdigen Zertifizierungsstelle ausgestellt. ■ Der private Schlüssel ist nicht verfügbar. ■ Das Zertifikat ist beschädigt. Der Grund für den Status INVALID finden Sie in der Protokolldatei auf dem Registrierungsserver.
<code>--environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn</code>	Listet für den Registrierungsserver in der angegebenen Domäne die allgemeinen Namen (CNs) der verfügbaren Zertifizierungsstellen auf und stellt die folgenden Informationen zu den einzelnen Zertifikatvorlagen bereit, die für True SSO verwendet werden können: Name, Mindestschlüssellänge und Hashalgorithmus.

Befehle zum Verwalten von Connectors

Sie erstellen einen Connector pro Domäne. Der Connector definiert die Parameter, die für True SSO verwendet werden.

Aus Gründen der Lesbarkeit stellen die Optionen in der folgenden Tabelle nicht den gesamten Befehl dar, der von Ihnen eingegeben werden muss. Es werden hier nur die Optionen angegeben, die sich auf eine bestimmte Aufgabe beziehen. Beispielsweise enthält die Tabelle eine Zeile mit den Optionen `--list --connector`. Der `vdmUtil`-Befehl, den Sie tatsächlich eingeben, verfügt aber auch über Optionen für die Authentifizierung und für die Angabe, dass True SSO konfiguriert wird:

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truesso --list --connector
```

Weitere Informationen zu den Authentifizierungsoptionen finden Sie unter [Befehlszeilenreferenz für die True SSO-Konfiguration](#).

Tabelle 5-3. vdmutil truesso-Befehlsoptionen zum Verwalten von Connectors

Optionen	Beschreibung
<code>--create --connector --domain domain-fqdn</code> <code>--template template-name</code> <code>--primaryEnrollmentServer enroll-server1-fqdn</code> <code>[--secondaryEnrollmentServerenroll-server2-fqdn]</code> <code>--certificateServerCA-common-name--mode{enabled disabled}</code>	<p>Erstellt einen Connector für die angegebene Domäne und konfiguriert den Connector für die Verwendung der folgenden Einstellungen:</p> <ul style="list-style-type: none"> ■ <code>template-name</code> steht für den Namen der zu verwendenden Zertifikatvorlage. ■ <code>enroll-server1-fqdn</code> ist der FQDN des zu verwendenden primären Registrierungsservers. ■ <code>enroll-server2-fqdn</code> ist der FQDN des zu verwendenden sekundären Registrierungsservers. Diese Einstellung ist optional. ■ <code>CA-common-name</code> steht für den allgemeinen Namen der zu verwendenden Zertifizierungsstelle. Hier kann eine Liste mit kommagetrennten Zertifizierungsstellen angegeben werden. <p>Um zu ermitteln, welche Zertifikatvorlage und Zertifizierungsstelle für einen bestimmten Registrierungsserver verfügbar sind, können Sie den Befehl <code>vdmutil</code> mit den Optionen <code>--truesso --environment --list --enrollmentServerenroll-server-fqdn--domain domain-fqdn</code> ausführen.</p>
<code>--list --connector</code>	Listet die FQDNs der Domänen auf, für die bereits ein Connector erstellt wurde.
<code>--list --connector --verbose</code>	<p>Listet alle Domänen mit Connectors auf, und für jeden Connector werden die folgenden Informationen bereitgestellt:</p> <ul style="list-style-type: none"> ■ Primärer Registrierungsserver ■ Sekundärer Registrierungsserver, falls vorhanden ■ Name der Zertifikatvorlage ■ Ob der Connector aktiviert oder deaktiviert ist ■ Allgemeiner Name des/der Zertifizierungsstellenserver/s, wenn mehrere vorhanden sind

Tabelle 5-3. vdmutil truesso-Befehlsoptionen zum Verwalten von Connectors (Fortsetzung)

Optionen	Beschreibung
<code>--edit --connector <i>domain-fqdn</i></code> <code>[--template<i>template-name</i>]</code> <code>[--mode{enabled disabled}]</code> <code>[--primaryEnrollmentServer<i>enroll-server1-fqdn</i>]</code> <code>[--secondaryEnrollmentServer<i>enroll-server2-fqdn</i>]</code> <code>[--certificateServer<i>CA-common-name</i>]</code>	<p>Für den Connector, der für die durch <i>domain-fqdn</i> angegebene Domäne erstellt wurde, können Sie die folgenden Einstellungen ändern:</p> <ul style="list-style-type: none"> ■ <i>template-name</i> steht für den Namen der zu verwendenden Zertifikatvorlage. ■ Der Modus kann auf <code>enabled</code> oder <code>disabled</code> festgelegt werden. ■ <i>enroll-server1-fqdn</i> ist der FQDN des zu verwendenden primären Registrierungsservers. ■ <i>enroll-server2-fqdn</i> ist der FQDN des zu verwendenden sekundären Registrierungsservers. Diese Einstellung ist optional. ■ <i>CA-common-name</i> steht für den allgemeinen Namen der zu verwendenden Zertifizierungsstelle. Hier kann eine Liste mit kommagetrennten Zertifizierungsstellen angegeben werden.
<code>--delete --connector <i>domain-fqdn</i></code>	<p>Löscht den Connector, der für die durch <i>domain-fqdn</i> angegebene Domäne erstellt wurde.</p>

Befehle zum Verwalten von Authentifikatoren

Authentifikatoren werden erstellt, wenn Sie die SAML-Authentifizierung zwischen VMware Identity Manager Horizon 7 und einem Verbindungsserver konfigurieren. Die einzige Verwaltungsaufgabe besteht in der Aktivierung oder Deaktivierung von True SSO für den Authentifikator.

Aus Gründen der Lesbarkeit stellen die Optionen in der folgenden Tabelle nicht den gesamten Befehl dar, der von Ihnen eingegeben werden muss. Es werden hier nur die Optionen angegeben, die sich auf eine bestimmte Aufgabe beziehen. Beispielsweise enthält die Tabelle eine Zeile mit den Optionen `--list --authenticator`. Der `vdmUtil`-Befehl, den Sie tatsächlich eingeben, verfügt aber auch über Optionen für die Authentifizierung und für die Angabe, dass True SSO konfiguriert wird:

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truesso --list --authenticator
```

Weitere Informationen zu den Authentifizierungsoptionen finden Sie unter [Befehlszeilenreferenz für die True SSO-Konfiguration](#).

Tabelle 5-4. vdmutil truesso-Befehlsoptionen zum Verwalten von Authentifikatoren

Befehl und Optionen	Beschreibung
<code>--list --authenticator [--verbose]</code>	Listet die vollqualifizierten Domännennamen (FQDNs) aller SAML-Authentifikatoren auf, die in der Domäne gefunden wurden. Es wird jeweils angegeben, ob True SSO aktiviert ist. Bei Verwendung der Option <code>--verbose</code> werden auch die FQDNs der zugehörigen Verbindungsserver aufgelistet.
<code>--list --authenticator --name <i>label</i></code>	Gibt an, ob bei dem angegebenen Authentifikator True SSO aktiviert ist, und listet die FQDNs der zugehörigen Verbindungsserver auf. Verwenden Sie für <i>Bezeichnung</i> einen der Namen, die ausgegeben werden, wenn Sie die Option <code>--authenticator</code> ohne die Option <code>--name</code> verwenden.
<code>--edit --authenticator --name <i>label</i></code> <code>--truessoMode <i>mode-value</i></code>	<p>Legt den True SSO-Modus für den angegebenen Authentifikator auf den von Ihnen angegebenen Wert fest, wobei für <i>Moduswert</i> einer der folgenden Werte eingesetzt werden kann:</p> <ul style="list-style-type: none"> ■ ENABLED. True SSO wird nur verwendet, wenn die Active Directory-Anmeldeinformationen des Benutzers nicht verfügbar sind. ■ ALWAYS. True SSO wird immer verwendet, auch dann, wenn vIDM über die Active Directory-Anmeldeinformationen des Benutzers verfügt. ■ DISABLED. True SSO wird deaktiviert. <p>Verwenden Sie für <i>Bezeichnung</i> einen der Namen, die ausgegeben werden, wenn Sie die Option <code>--authenticator</code> ohne die Option <code>--name</code> verwenden.</p>

Erweiterte Konfigurationseinstellungen für True SSO

Die erweiterten True SSO-Einstellungen können mit der GPO-Vorlage auf dem Horizon Agent-Computer, mit den Registrierungseinstellungen auf dem Registrierungsserver und mit den LDAP-Einträgen auf dem Verbindungsserver verwaltet werden. Zu diesen Einstellungen gehören der Standardwert für die Zeitüberschreibung, die Konfiguration des Lastausgleichsdienstes, die Angabe der einzuschließenden Domänen und anderes mehr.

Konfigurationseinstellungen für Horizon Agent

Sie können die True SSO-Funktion in der GPO-Vorlage des Agent-Betriebssystems auf Poolebene deaktivieren oder die Standardwerte für die Zertifikateinstellungen ändern, beispielsweise die Schlüsselgröße und -anzahl sowie die Einstellungen für erneute Verbindungsversuche.

Hinweis Die folgende Tabelle enthält die Einstellungen für die Konfiguration des Agenten auf einzelnen virtuellen Maschinen. Alternativ können Sie auch die Vorlagendateien zur Horizon Agent-Konfiguration verwenden. Der Name der ADMX-Vorlagendatei lautet `vdm_agent.admx`. Wenden Sie mit den Vorlagendateien die Richtlinieneinstellungen auf alle virtuellen Maschinen in einem Desktop- oder Anwendungspool an. Wenn eine Richtlinie festgelegt ist, hat diese Vorrang gegenüber den Registrierungseinstellungen.

Die ADMX-Dateien stehen in `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` zur Verfügung. Diese Datei können Sie von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunterladen. Wählen Sie unter „Desktop & End-User Computing“ den VMware Horizon 7-Download, der die ZIP-Datei enthält.

Tabelle 5-5. Schlüssel für die Konfiguration von True SSO in Horizon Agent

Schlüssel	Min und Max	Beschreibung
Disable True SSO	–	Legen Sie für diesen Schlüssel true fest, um die Funktion im Agent zu deaktivieren. Verwenden Sie diese Einstellung in der Gruppenrichtlinie, um True SSO auf Poolebene zu deaktivieren. Die Standardeinstellung ist false .
Certificate wait timeout	10 - 120	Legt die Zeitüberschreitungsdauer der Zertifikate in Millisekunden fest. Innerhalb dieser Zeitspanne müssen die Zertifikate in Agent eintreffen. Die Standardeinstellung ist 40 .
Minimum key size	1024 - 8192	Zulässige Mindestgröße für einen Schlüssel. Die Standardeinstellung ist 1024 . Das heißt, ein Schlüssel kann nicht verwendet werden, wenn er kleiner als 1024 ist.
All key sizes	–	Es kann eine Liste kommagetrennter Schlüsselgrößen verwendet werden. Es lassen sich bis zu fünf Größen festlegen, z. B. 1024,2048,3072,4096 . Die Standardeinstellung ist 2048 .
Number of keys to pre-create	1 - 100	Anzahl der Schlüssel, die sich auf RDS-Servern, die Remote-Desktops und gehostete Windows-Anwendungen bereitstellen, vorab erstellen lassen. Die Standardeinstellung ist 5 .
Minimum validity period required for a certificate	–	Mindestgültigkeitsdauer in Minuten, die ein Zertifikat bei der Wiederverwendung zur erneuten Herstellung einer Verbindung zum Benutzer erfordert. Die Standardeinstellung ist 5 .

Registrierungsserver-Konfigurationseinstellungen

Sie können durch Konfiguration der Windows-Registrierungseinstellungen des Betriebssystems des Registrierungsservers festlegen, zu welchen Domänen eine Verbindung hergestellt wird. Ferner haben Sie die Möglichkeit, verschiedene Zeitüberschreitungsperioden, Abrufperioden und Wiederholungsperioden anzugeben. Außerdem können Sie festlegen, ob die Zertifizierungsstelle verwendet werden soll, die auf demselben lokalen Server installiert ist (empfohlen).

Sie ändern die erweiterten Konfigurationseinstellungen, indem Sie den Windows Registrierungs-Editor (regedit.exe) auf dem Computer öffnen, auf dem der Registrierungsserver installiert ist. Navigieren Sie dann zu folgenden Registrierungsschlüsseln:

```
HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service
```

Tabelle 5-6. Registrierungsschlüssel für die Konfiguration von True SSO auf dem Registrierungsserver

Registrierungsschlüssel	Min und Max	Typ	Beschreibung
ConnectToDomains	–	REG_MULTI_SZ	Liste der Domänen, mit denen der Registrierungsserver automatisch versucht, Verbindungen herzustellen. Bei diesem Registrierungstyp mit mehreren Zeichenfolgen muss jede Domäne mit ihrem vollqualifizierter DNS-Domännennamen (FQDN) in einer eigenen Zeile aufgelistet sein. Standardmäßig besteht zu allen Domänen ein Vertrauensverhältnis.
ExcludeDomains	–	REG_MULTI_SZ	Liste der Domänen, mit denen der Registrierungsserver nicht automatisch Verbindungen herstellt. Wenn ein Verbindungsserver eine Konfiguration mit einer oder mehreren dieser Domänen bereitstellt, wird der Registrierungsserver versuchen, eine Verbindung zu dieser Domäne bzw. zu diesen Domänen herzustellen. Bei diesem Registrierungstyp mit mehreren Zeichenfolgen muss jeder DNS-FQDN in einer eigenen Zeile aufgelistet sein. Standardmäßig wird keine Domäne ausgeschlossen.
ConnectToDomainsInForest	–	REG_SZ	Legt fest, ob eine Verbindung zu allen Domänen in der Gesamtstruktur hergestellt wird, in denen der Registrierungsserver Mitglied ist, bzw. ob diese benutzt werden sollen. Die Standardeinstellung ist TRUE. Wählen Sie einen der folgenden Werte aus: <ul style="list-style-type: none"> ■ 0 bedeutet FALSE. Es wird keine Verbindung zu den Domänen in der verwendeten Gesamtstruktur hergestellt. ■ !=0 bedeutet TRUE.
ConnectToTrustingDomains	–	REG_SZ	Legt fest, ob eine Verbindung zu explizit vertrauenswürdigen/ eingehenden Domänen hergestellt werden soll. Die Standardeinstellung ist TRUE. Wählen Sie einen der folgenden Werte aus: <ul style="list-style-type: none"> ■ 0 bedeutet FALSE. Es wird keine Verbindung zu explizit vertrauenswürdigen/ eingehenden Domänen hergestellt. ■ !=0 bedeutet TRUE.
PreferLocalCa	–	REG_SZ	Legt fest, ob die lokal installierte Zertifizierungsstelle (CA), sofern vorhanden, zur Verbesserung der Performance verwendet wird. Ist der Wert auf TRUE gesetzt, sendet der Registrierungsserver die Anforderungen an die lokale Zertifizierungsstelle. Wenn die Herstellung einer Verbindung zur lokalen Zertifizierungsstelle scheitert, sendet der Registrierungsserver die Zertifikatanforderungen an alternative Zertifizierungsstellen. Die Standardeinstellung ist FALSE. Wählen Sie einen der folgenden Werte aus: <ul style="list-style-type: none"> ■ 0 bedeutet FALSE. ■ !=0 bedeutet TRUE.

Tabelle 5-6. Registrierungsschlüssel für die Konfiguration von True SSO auf dem Registrierungsserver (Fortsetzung)

Registrierungsschlüssel	Min und Max	Typ	Beschreibung
MaxSubmitRetryTime	9500 - 59000	DWORD	Zeitraum in Millisekunden, bevor erneut versucht wird, einen Zertifikatanforderung zu versenden. Die Standardeinstellung ist 25000 .
SubmitLatencyWarningTime	500 - 5000	DWORD	<p>Warnzeit für die Sendelatenz in Millisekunden, wenn die Schnittstelle als „Heruntergestuft“ markiert ist. Die Standardeinstellung ist 1500.</p> <p>Der Registrierungsserver verwendet diese Einstellung, um zu bestimmen, ob eine Zertifizierungsstelle als „Heruntergestuft“ gilt. Wenn die letzten drei Zertifikatanforderungen mehr Millisekunden erfordert haben, als in dieser Einstellung festgelegt sind, gilt die Zertifizierungsstelle als „Heruntergestuft“. Dieser Status erscheint dann als Systemzustand im Horizon Administrator-Dashboard.</p> <p>Normalerweise stellt eine Zertifizierungsstelle ein Zertifikat innerhalb von 20 ms aus. Wenn sich aber die Zertifizierungsstelle einige Stunden im Leerlauf befindet, können die ersten Anforderungen einen längeren Zeitraum in Anspruch nehmen. Anhand dieser Einstellung hat ein Administrator die Möglichkeit, zu ermitteln, ob eine Zertifizierungsstelle langsam ist, ohne die Zertifizierungsstelle als langsam kennzeichnen zu müssen. Mit dieser Einstellung können Sie einen Schwellenwert für die Klassifizierung einer Zertifizierungsstelle als langsam konfigurieren.</p>
WarnForLonglivedCert	–	REG_SZ	<p>Deaktivieren Sie die Warnung für langlebiges True-SSO-Zertifikat (Vorlagen). Die Standardeinstellung ist True.</p> <p>Der Registrierungsserver zeigt den Warnungsstatus im Horizon Administrator-Systemzustand-Dashboard und meldet, dass True SSO-Vorlagen als fehlerhaft oder nicht in optimalem Zustand, wenn die Gültigkeitsdauer des Zertifikats auf mehr als 14 Tage festgelegt ist. Der Registrierungsserver verwendet diese Einstellung zum Deaktivieren der Warnung.</p> <p>Der Registrierungsserver muss neu gestartet werden, damit diese Einstellung wirksam wird.</p>

Konfigurationseinstellungen für den Verbindungsserver

Sie können View LDAP auf einem Verbindungsserver bearbeiten und dabei eine Zeitüberschreitung für das Generieren von Zertifikaten konfigurieren. Ferner haben Sie die Möglichkeit festzulegen, ob der Lastausgleichsdienst für Zertifikatanforderungen zwischen den Registrierungsservern aktiviert sein soll (empfohlen).

Zur Änderung der erweiterten Konfigurationseinstellungen benötigen Sie ADSI Edit auf einem Verbindungsserver-Host. Sie stellen die Verbindung her, indem Sie den definierten Namen **DC=vdi**, **DC=vmware**, **DC=int** als Verbindungspunkt sowie den Servernamen und -port für den Computer eingeben: **localhost:389**. Erweitern Sie **OU=Properties**, wählen Sie **OU=Global** aus und doppelklicken Sie im rechten Fensterbereich auf **CN=Common**.

Sie können nun das Attribut **pae-NameValuePair** bearbeiten und einen oder mehrere Werte aus der nachfolgend aufgeführten Tabelle hinzufügen. Beim Hinzufügen von Werten müssen Sie die Syntax *Name=Wert* beachten.

Tabelle 5-7. Erweiterte True SSO-Einstellungen für Verbindungsserver

Registrierungsschlüssel	Beschreibung
<code>cs-view-certss-enable-es-loadbalance=[true false]</code>	<p>Legt fest, ob der Lastausgleichsdienst für Zertifikatsignieranforderungen (CSR) zwischen den Registrierungsservern aktiviert ist. Die Standardeinstellung ist „False“.</p> <p>Beispiel: Fügen Sie <code>cs-view-certss-enable-es-loadbalance=true</code> hinzu, um den Lastausgleichsdienst zu aktivieren, sodass der Verbindungsserver beim Eingang von Zertifikatanforderungen alternative Registrierungsserver verwendet. Jeder Registrierungsserver kann die Anforderungen mithilfe der lokalen Zertifizierungsstelle verarbeiten, wenn sich Registrierungsserver und Zertifizierungsstelle auf demselben Host befinden.</p>
<code>cs-view-certss-certgen-timeout-sec=number</code>	<p>Legt die Wartezeit für das Generieren eines Zertifikats nach dem Empfang einer CSR-Anforderung in Sekunden fest. Die Standardeinstellung ist 35.</p>

Identifizieren eines AD-Benutzers ohne Active Directory-UPN

Sie können LDAP-URL-Filter für Verbindungsserver konfigurieren, um einen AD-Benutzer zu identifizieren, der über keine AD-UPN verfügt.

Sie müssen den ADAM ADSI-Editor auf einem Verbindungsserver-Host verwenden. Sie können durch Eingabe des definierten Namens **DC=vdi**, **DC=vmware**, **DC=int** eine Verbindung herstellen. Erweitern Sie **OU=Properties** und wählen Sie **OU=Authenticator** aus.

Sie können dann das **Pae-LDAPURLList**-Attribut bearbeiten, um einen LDAP-URL-Filter hinzuzufügen.

Fügen Sie z. B. den folgenden Filter hinzu:

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???(telephoneNumber=$NAMEID)
```

Der Verbindungsserver verwendet die folgenden standardmäßigen LDAP-URL-Filter:

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???(objectCategory=user)
(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///???(objectCategory=group)
(objectclass=group)(sAMAccountName=$NAMEID))
```

```
urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified=ldap:///???(objectCategory=user)
(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///???(objectCategory=group)
(objectclass=group)(sAMAccountName=$NAMEID))
```

Wenn Sie einen LDAP-URL-Filter konfigurieren, wird dieser vom Verbindungsserver zur Identifizierung des Benutzers verwendet und nicht der Standard-LDAP-URL-Filter.

Beispiele für Bezeichner, die Sie zur SAML-Authentifizierung für einen AD-Benutzer verwenden können, der über keinen Active Directory-UPN verfügt:

- "cn"
- "mail"
- "description"
- "givenName"
- "sn"
- "canonicalName"
- "SAMAccountName"
- "member"
- "memberOf"
- "distinguishedName"
- "telephoneNumber"
- "primaryGroupID"

Entsperren eines Desktops mit True SSO und Workspace ONE

Wenn Benutzer sich über True SSO bei einem Desktop angemeldet haben, können sie den Desktop nach der erneuten Authentifizierung im Workspace ONE-Portal mit denselben Anmeldeinformationen entsperren.

Voraussetzungen

- Stellen Sie sicher, dass Sie über Horizon 7 7.8 oder eine höhere Version verfügen.
- Stellen Sie sicher, dass Sie über Horizon Client für Windows 5.0 oder eine höhere Version verfügen.
- Stellen Sie sicher, dass Sie über VMware Identity Manager 19.03 oder eine höhere Version verfügen.

Verfahren

- 1 Aktivieren Sie Workspace ONE und konfigurieren Sie die Verwendung mit dem Verbindungsserver.

Weitere Informationen finden Sie in der Workspace ONE-Dokumentation auf der Webseite [Dokumentation zu Workspace ONE](#).

- 2 Konfigurieren Sie den Horizon-Verbindungsserver für True SSO.

Siehe [Konfigurieren des Horizon-Verbindungsservers für True SSO](#).

- 3 Um virtuelle oder veröffentlichte Desktops zu starten, müssen Sie im Workspace ONE-Modus eine Verbindung mit einem Verbindungsserver herstellen, auf dem True SSO konfiguriert ist. Weitere Informationen finden Sie in der Horizon Client-Dokumentation auf der Webseite [VMware Horizon Client-Dokumentation](#).

- 4 Starten Sie virtuelle oder veröffentlichte Desktops im Workspace ONE-Portal, damit Benutzer Single Sign-On mit True SSO verwenden können.
- 5 Sperren Sie den Desktop.
- 6 Wählen Sie zum Entsperren des Desktops **VMware True SSO-Benutzer** aus und klicken Sie auf **Übermitteln**.

Nächste Schritte

Sie können diese Funktion deaktivieren, indem Sie auf dem Computer, auf dem Horizon Agent installiert ist, einen Registrierungsschlüssel festlegen, der sich am folgenden Speicherort befindet:

HKLM\Software\VMware, Inc.\VMware VDM\Agent\CertSSO[DisableCertSSOUnlock=true]

Sie können diese Funktion auch deaktivieren, indem Sie den Registrierungsschlüssel DisabledFeatures=TrueSSOUnlock in Horizon Client für Windows an folgenden Speicherorten festlegen:

- Windows-32-Bit-Betriebssystem: [HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client] oder [HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client].
- Windows-64-Bit-Betriebssystem: [HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client] oder [HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client].

Wenn der Registrierungsschlüssel festgelegt ist, wird die Option **VMware True SSO-Benutzer** nicht angezeigt, wenn der Benutzer den Desktop entsperrt.

Verwenden des Systemzustand-Dashboards zur Behebung von Fehlern im Zusammenhang mit True SSO

Mithilfe des Systemzustand-Dashboards in Horizon Administrator können Sie rasch Probleme ermitteln, die sich auf die Funktionsweise der True SSO-Funktion auswirken können.

Wenn ein Endbenutzer versucht, sich beim Remote-Desktop oder bei einer Remoteanwendung anzumelden, und True SSO nicht mehr funktioniert, dann erhält der Benutzer die folgende Meldung: „Der Benutzername oder das Kennwort ist falsch“. Nachdem der Benutzer auf **OK** geklickt hat, wird der Anmeldebildschirm geöffnet. Der Windows-Anmeldebildschirm enthält eine zusätzliche Kachel mit dem Titel **VMware SSO-Benutzer**. Wenn der Benutzer die Active Directory-Anmeldeinformationen für einen berechtigten Benutzer besitzt, dann kann er sich mit den AD-Anmeldeinformationen anmelden.

Das Systemzustand-Dashboard im oberen linken Bereich der Horizon Administrator-Anzeige enthält einige Elemente, die sich auf True SSO beziehen.

Hinweis Die True SSO-Funktion übermittelt dem Dashboard nur einmal pro Minute Informationen. Klicken Sie auf das Symbol „Aktualisieren“ rechts oben, um die Informationen sofort zu aktualisieren.

- Sie können klicken, um **View-Komponenten > True SSO** zu erweitern und eine Liste der Domänen anzuzeigen, die True SSO verwenden.

Wenn Sie auf einen Domännennamen klicken, werden folgende Informationen angezeigt: eine Liste der für diese Domäne konfigurierten Registrierungsserver, der Name der verwendeten Zertifikatvorlage und der Status. Wenn ein Problem vorliegt, enthält das Statusfeld eine entsprechende Erläuterung.

Um die im Dialogfeld „Domänendetails für True SSO-Anmeldung“ angezeigten Konfigurationseinstellungen zu ändern, bearbeiten Sie den True SSO-Connector mithilfe der `vdmutl`-Befehlszeilenschnittstelle. Weitere Informationen finden Sie unter [Befehle zum Verwalten von Connectors](#).

- Klicken Sie, um **Andere Komponenten > SAML 2.0-Authentifikatoren** zu erweitern und eine Liste der SAML-Authentifikatoren anzuzeigen, die zum Delegieren der Authentifizierung bei VMware Identity Manager-Instanzen erstellt wurden. Sie können auf den Authentifikatorknamen klicken, um die Details und den Status zu überprüfen.

Hinweis Damit True SSO verwendet werden kann, muss die globale Einstellung für SSO aktiviert werden. Wählen Sie in Horizon Administrator **Konfiguration > Globale Einstellungen** aus und vergewissern Sie sich, dass **Einmalige Anmeldung (Single Sign-On)** auf **Aktiviert** festgelegt ist.

Tabelle 5-8. Verbindungsserver zum Status der Verbindung zum Registrierungsserver

Statustext	Beschreibung
Fehler beim Abrufen der True SSO-Zustandsinformationen.	Das Dashboard kann die Zustandsinformationen nicht von der Verbindungsserver-Instanz abrufen.
Mit dem <FQDN>-Registrierungsserver kann vom True SSO-Konfigurationsdienst kein Kontakt aufgenommen werden.	In einem Pod wird eine der Verbindungsserver-Instanzen zum Senden der Konfigurationsinformationen an alle vom Pod verwendeten Registrierungsserver ausgewählt. Diese Verbindungsserver-Instanz aktualisiert die Konfiguration des Registrierungsservers einmal pro Minute. Diese Meldung wird angezeigt, wenn der Registrierungsserver im Rahmen der Konfigurationsaufgabe nicht aktualisiert werden konnte. Weitere Informationen finden Sie in der Tabelle zu Registrierungsserververbindungen.
Mit dem <FQDN>-Registrierungsserver kann zur Verwaltung von Sitzungen auf diesem Verbindungsserver kein Kontakt aufgenommen werden.	Die aktuelle Verbindungsserver-Instanz kann keine Verbindung mit dem Registrierungsserver herstellen. Dieser Status wird nur für die Verbindungsserver-Instanz angezeigt, auf die Ihr Browser verweist. Wenn mehrere Verbindungsserver-Instanzen im Pod vorhanden sind, müssen Sie den Browser ändern, sodass er auf andere Verbindungsserver-Instanzen verweist, um deren Status überprüfen zu können. Weitere Informationen finden Sie in der Tabelle zu Registrierungsserververbindungen.

Tabelle 5-9. Registrierungsserververbindungen

Statustext	Beschreibung
Die Domäne <Domänenname> ist auf dem <FQDN>-Registrierungsserver nicht vorhanden.	Der True SSO-Konnektor wurde zur Verwendung dieses Registrierungsservers für diese Domäne konfiguriert, aber der Registrierungsserver wurde nicht zum Herstellen einer Verbindung mit dieser Domäne konfiguriert. Wenn der Status länger als eine Minute unverändert bleibt, müssen Sie den Status des Verbindungsservers überprüfen, der aktuell für die Aktualisierung der Registrierungskonfiguration verantwortlich ist.
Die Verbindung des <FQDN>-Registrierungsservers mit der Domäne <Domänenname> ist weiterhin eingerichtet.	Der Registrierungsserver konnte noch keine Verbindung mit einem Domänencontroller in dieser Domäne herstellen. Wenn der Status länger als eine Minute unverändert bleibt, sollten Sie überprüfen, ob die Namensauflösung zwischen Registrierungsserver und Domäne ordnungsgemäß erfolgt und ob eine Netzwerkverbindung zwischen dem Registrierungsserver und der Domäne besteht.
Die Verbindung des <FQDN>-Registrierungsservers mit der Domäne <Domänenname> wurde unterbrochen oder befindet sich in einem kritischen Status.	Der Registrierungsserver hat eine Verbindung mit einem Domänencontroller in der Domäne hergestellt, konnte aber die PKI-Informationen noch nicht vom Domänencontroller lesen. Ist dies der Fall, liegt das Problem wahrscheinlich beim Domänencontroller. Dieses Problem kann auch auftreten, wenn der DNS nicht ordnungsgemäß konfiguriert worden ist. Ermitteln Sie anhand der Protokolldatei auf dem Registrierungsserver, welchen Domänencontroller der Registrierungsserver zu verwenden versucht, und überprüfen Sie, ob dieser Domänencontroller einwandfrei funktioniert.
Der <FQDN>-Registrierungsserver hat die Registrierungseigenschaften noch nicht von einem Domänencontroller gelesen.	Dies ist ein Übergangszustand, der nur während des Startvorgangs des Registrierungsservers oder während des Hinzufügens einer neuen Domäne zur Umgebung angezeigt wird. Dieser Status ist in der Regel weniger als eine Minute gegeben. Wenn der Status länger als eine Minute unverändert bleibt, ist entweder das Netzwerk extrem langsam oder es liegt ein Problem vor, das Schwierigkeiten beim Zugriff auf den Domänencontroller verursacht.
Der <FQDN>-Registrierungsserver hat die Registrierungsinformationen mindestens einmal gelesen, konnte aber eine Zeit lang keinen Domänencontroller erreichen.	Solange der Registrierungsserver die PKI-Konfiguration von einem Domänencontroller liest, ruft er alle zwei Minuten Änderungen ab. Dieser Status wird aktiviert, wenn der Domänencontroller für eine kurze Zeit nicht erreichbar ist. In der Regel hat dieser fehlende Kontakt mit dem Domänencontroller zur Folge, dass der Registrierungsserver keine Änderungen in der PKI-Konfiguration erkennen kann. Solange die Zertifikatserver Zugriff auf einen Domänencontroller haben, können noch Zertifikate ausgestellt werden.
Der <FQDN>-Registrierungsserver hat die Registrierungsinformationen mindestens einmal gelesen, konnte aber entweder für eine längere Zeit keinen Domänencontroller erreichen oder es ist ein anderes Problem aufgetreten.	Wenn der Registrierungsserver den Domänencontroller über einen längeren Zeitraum nicht erreichen konnte, wird dieser Status angezeigt. Der Registrierungsserver versucht dann, einen alternativen Domänencontroller für diese Domäne zu finden. Wenn ein Zertifikatserver Zugriff auf einen Domänencontroller hat, können noch Zertifikate ausgestellt werden. Dauert dieser Status jedoch länger als eine Minute an, bedeutet dies, dass der Registrierungsserver auf keinen Domänencontroller der Domäne mehr zugreifen kann. Wahrscheinlich können dann auch keine Zertifikate mehr ausgestellt werden.

Tabelle 5-10. Status des Registrierungszertifikats

Statustext	Beschreibung
Für die Gesamtstruktur dieser Domäne <Domänenname> wurde kein gültiges Registrierungszertifikat auf dem <FQDN>-Registrierungsserver installiert oder es ist abgelaufen.	Es wurde kein Registrierungszertifikat für diese Domäne installiert, oder das Zertifikat ist ungültig oder abgelaufen. Das Registrierungszertifikat muss von einer Unternehmenszertifizierungsstelle ausgestellt werden, die in der Gesamtstruktur, der diese Domäne angehört, als vertrauenswürdig gilt. Überprüfen Sie, ob Sie die im Dokument <i>Horizon 7-Verwaltung</i> beschriebenen Schritte ausgeführt haben. In diesem Dokument wird erläutert, wie das Registrierungszertifikat auf dem Registrierungsserver installiert wird. Sie können auch im Zertifikat-Snap-In in der Microsoft Management Console (MMC) den Zertifikatspeicher des lokalen Computers öffnen. Öffnen Sie den Container „Eigene Zertifikate“ und überprüfen Sie, ob das Zertifikat installiert worden ist und ob es gültig ist. Sie können auch die Protokolldatei auf dem Registrierungsserver öffnen. Der Registrierungsserver protokolliert zusätzliche Informationen zum Status aller von ihm gefundenen Zertifikate.

Tabelle 5-11. Status der Zertifikatvorlage

Statustext	Beschreibung
Die Vorlage <Name> ist nicht in der <FQDN>-Registrierungsserverdomäne vorhanden.	Überprüfen Sie, ob Sie den richtigen Vorlagennamen angegeben haben.
Mit dieser Vorlage generierte Zertifikate können NICHT zum Anmelden bei Windows verwendet werden.	Für diese Vorlage ist die Smartcard-Anmeldung nicht aktiviert, jedoch die Datensignatur aktiviert. Überprüfen Sie, ob Sie den richtigen Vorlagennamen angegeben haben. Stellen Sie sicher, dass Sie die in Erstellen von Zertifikatvorlagen für die Verwendung mit True SSO beschriebenen Schritte ausgeführt haben.
Für die Vorlage <Name> wurde die Smartcard-Anmeldung aktiviert, diese kann aber nicht verwendet werden.	Bei dieser Vorlage wurde die Smartcard-Anmeldung aktiviert, aber die Vorlage kann nicht in Verbindung mit True SSO verwendet werden. Überprüfen Sie, ob Sie den richtigen Vorlagennamen angegeben haben, und überprüfen Sie, ob Sie alle in Erstellen von Zertifikatvorlagen für die Verwendung mit True SSO beschriebenen Schritte ausgeführt haben. Sie können auch die Protokolldatei des Registrierungservers überprüfen. Hier ist verzeichnet, welche Einstellung der Vorlage ihre Verwendung für True SSO verhindert.

Tabelle 5-12. Status der Zertifikatserverkonfiguration

Statustext	Beschreibung
Der Zertifikatserver <Allgemeiner Name der Zertifizierungsstelle> ist nicht in der Domäne vorhanden.	Überprüfen Sie, ob Sie den richtigen Namen für die Zertifizierungsstelle angegeben haben. Sie müssen den allgemeinen Namen (Common Name, CN) angeben.
Das Zertifikat ist nicht im NTAUTH-Speicher (Unternehmen) vorhanden.	Diese Zertifizierungsstelle ist keine Unternehmenszertifizierungsstelle oder ihr Zertifizierungsstellenzertifikat wurde nicht dem NTAUTH-Speicher hinzugefügt. Wenn diese Zertifizierungsstelle nicht Mitglied der Gesamtstruktur ist, müssen Sie das Zertifizierungsstellenzertifikat manuell dem NTAUTH-Speicher dieser Gesamtstruktur hinzufügen.

Tabelle 5-13. Status der Zertifikatserververbindung

Statustext	Beschreibung
Der <FQDN>-Registrierungsserver ist nicht mit dem Zertifikatsserver <Allgemeiner Name der Zertifizierungsstelle> verbunden.	Der Registrierungsserver ist nicht mit dem Zertifikatsserver verbunden. Dies kann ein Übergangszustand sein, wenn der Registrierungsserver gerade gestartet wurde oder wenn die Zertifizierungsstelle einem True SSO-Konnektor erst kürzlich hinzugefügt wurde. Wenn der Status länger als eine Minute unverändert bleibt, bedeutet dies, dass der Registrierungsserver keine Verbindung mit der Zertifizierungsstelle herstellen konnte. Überprüfen Sie, ob die Namensauflösung ordnungsgemäß funktioniert, ob eine Netzwerkverbindung mit der Zertifizierungsstelle besteht und ob das Systemkonto für den Registrierungsserver über eine Berechtigung zum Zugriff auf die Zertifizierungsstelle verfügt.
Der <FQDN>-Registrierungsserver hat eine Verbindung zum Zertifikatsserver <Allgemeiner Name der Zertifizierungsstelle> aufgenommen, der Zertifikatsserver befindet sich aber in einem herabgestuften Status.	Dieser Status wird angezeigt, wenn die Zertifizierungsstelle die Zertifikate langsam ausstellt. Wenn die Zertifizierungsstelle diesen Status beibehält, überprüfen Sie die Last der Zertifizierungsstelle oder die von der Zertifizierungsstelle verwendeten Domänencontroller. Hinweis Wenn die Zertifizierungsstelle als langsam markiert wurde, behält sie diesen Status so lange, bis mindestens eine Zertifikatanforderung erfolgreich abgeschlossen und das Zertifikat innerhalb eines normalen Zeitraums ausgestellt worden ist.
Der <FQDN>-Registrierungsserver kann eine Verbindung mit dem Zertifikatsserver <Allgemeiner Name der Zertifizierungsstelle> herstellen, der Dienst ist jedoch nicht verfügbar.	Dieser Status wird gemeldet, wenn der Registrierungsserver über eine aktive Verbindung mit der Zertifizierungsstelle verfügt, aber die Zertifizierungsstelle keine Zertifikate ausstellen kann. Hierbei handelt es sich in der Regel um einen Übergangszustand. Wenn die Zertifizierungsstelle nicht innerhalb kürzester Zeit verfügbar ist, wird der Status in „Verbindung getrennt“ geändert.

Konfigurieren der rollenbasierten Verwaltungsdelegierung

6

Eine wichtige Verwaltungsaufgabe in einer Horizon 7-Umgebung besteht darin, festzulegen, wer Horizon Administrator 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](#)
- [Verwendung von Zugriffsgruppen zur Delegation der Verwaltung von Pools und Farmen](#)
- [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 Administrator 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 Administrator 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 Administrator 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 Administrator 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. 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.

Verwendung von Zugriffsgruppen zur Delegierung der Verwaltung von Pools und Farmen

Standardmäßig werden automatisierte Desktop-Pools, manuelle Desktop-Pools und Farmen in der Stammzugriffsgruppe erstellt, die in Horizon Administrator 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 Administratorrolle 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 Administrator 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.

Hinweis Wenn Sie den Zugriff auf Ihre Desktops über VMware Identity Manager ermöglichen möchten, müssen Sie die Desktop- und Anwendungspools als Benutzer mit Administratorrolle für die Stammzugriffsgruppe in Horizon Administrator 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.

■ 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 6-1. Unterschiedliche Administratoren für unterschiedliche Zugriffsgruppen zeigt ein Beispiel für diese Art der Konfiguration.

Tabelle 6-1. 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 6-2. Unterschiedliche Administratoren für dieselbe Zugriffsgruppe zeigt ein Beispiel für diese Art der Konfiguration.

Tabelle 6-2. 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 Administrator 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 Administrator 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 Administrator angezeigt werden, wenn Sie einen Administratorbenutzer oder eine Administratorgruppe auswählen. Der Administratorbenutzer heißt „Admin 1“ und verfügt über zwei Berechtigungen.

Tabelle 6-3. 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 Administrator angezeigt werden, wenn Sie die Zugriffsgruppe MarketingDesktops auswählen.

Tabelle 6-4. Berechtigungen auf der Registerkarte „Ordner“ für „MarketingDesktops“

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

Die erste Berechtigung ist dieselbe wie die erste Berechtigung in [Tabelle 6-3. Berechtigungen auf der Registerkarte „Administratoren und Gruppen“ für Admin 1](#). Die zweite Berechtigung wird von der zweiten Berechtigung geerbt, wie in [Tabelle 6-3. 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 Administrator in [Tabelle 6-3. Berechtigungen auf der Registerkarte „Administratoren und Gruppen“ für Admin 1](#) angezeigt wird, wenn Sie die Rolle „Bestandslistenadministratoren“ auswählen.

Tabelle 6-5. Berechtigungen auf der Registerkarte „Rolle“ für Bestandslistenadministratoren

Administrator	Zugriffsgruppe
view-domain.com\Admin1	/MarketingDesktops

Verwalten von Administratoren

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

Die Administratorrolle ist die einflussreichste Rolle in Horizon Administrator. 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

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

■ Entfernen eines Administrators

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

Um einen Administrator zu erstellen, wählen Sie in Horizon Administrator einen Benutzer oder eine Gruppe aus den Active Directory-Benutzern und -Gruppen aus und weisen 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](#).
- 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 Wählen Sie in Horizon Administrator **View-Konfiguration > Administratoren** aus.
- 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.

- 5 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 .

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

Ergebnisse

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

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

- 1 Wählen Sie in View Administrator **View-Konfiguration > Administratoren** aus.
- 2 Wählen Sie auf der Registerkarte **Administratoren und Gruppen** den Administratorbenutzer oder die Administratorgruppe, klicken Sie auf **Benutzer oder Gruppe entfernen** und anschließend auf **OK**.

Ergebnisse

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

Verwalten und Überprüfen von Berechtigungen

Sie können mithilfe von Horizon Administrator Berechtigungen für spezifische Administratorbenutzer und -gruppen bzw. bestimmte Rollen und Zugriffsgruppen hinzufügen, löschen und überprüfen.

- **Hinzufügen einer Berechtigung**

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

- **Löschen einer Berechtigung**

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

- **Überprüfen von Berechtigungen**

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

Hinzufügen einer Berechtigung

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

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Administratoren** aus.

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 Rollen 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

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 Wählen Sie in Horizon Administrator **View-Konfiguration > Administratoren** aus.
- 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 löschen**.

Überprüfen von Berechtigungen

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

Verfahren

- 1 Wählen Sie **View-Konfiguration > 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 Rollen 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 Administrator Zugriffsgruppen hinzufügen und löschen und die Desktop-Pools und Maschinen in einer bestimmten Zugriffsgruppe überprüfen.

■ Hinzufügen einer Zugriffsgruppe

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

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

■ Entfernen einer Zugriffsgruppe

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

■ Überprüfen der Desktop-Pools, Anwendungspools oder Farmen in einer Zugriffsgruppe

Sie können in Horizon Administrator die Desktop-Pools, Anwendungspools oder Farmen in einer bestimmten Zugriffsgruppe anzeigen.

■ Überprüfen der vCenter-VMs in einer Zugriffsgruppe

Sie können die virtuellen vCenter-Maschinen in einer speziellen Zugriffsgruppe in Horizon Administrator anzeigen. Eine vCenter-VM erbt die Zugriffsgruppe von ihrem Pool.

Hinzufügen einer Zugriffsgruppe

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 Navigieren Sie in Horizon Administrator zum Dialogfeld „Zugriffsgruppe hinzufügen“.

Option	Aktion
Vom Katalog	<ul style="list-style-type: none"> ■ Wählen Sie Katalog > Desktop-Pools aus. ■ Wählen Sie aus dem Dropdown-Menü Zugriffsgruppe im obersten Fensterbereich Neue Zugriffsgruppe aus.
Von Ressourcen	<ul style="list-style-type: none"> ■ Wählen Sie Ressourcen > Farmen aus. ■ Wählen Sie aus dem Dropdown-Menü Zugriffsgruppe im obersten Fensterbereich Neue Zugriffsgruppe aus.
Von View-Konfiguration	<ul style="list-style-type: none"> ■ Wählen Sie View-Konfiguration > Administratoren aus. ■ Wählen Sie auf der Registerkarte Zugriffsgruppen die Option Zugriffsgruppe hinzufügen 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

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 Administrator **Katalog > Desktop-Pools** oder **Ressourcen > Farmen** aus.
- 2 Wählen Sie einen Pool oder eine Farm aus.
- 3 Wählen Sie im oberen Fensterbereich im Dropdown-Menü **Zugriffsgruppe** die Option **Zugriffsgruppe ändern**.
- 4 Wählen Sie die Zugriffsgruppe und klicken Sie auf **OK**.

Ergebnisse

Horizon Administrator verschiebt den Pool in die ausgewählte Zugriffsgruppe.

Entfernen einer Zugriffsgruppe

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](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Administratoren** aus.
- 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 Desktop-Pools, Anwendungspools oder Farmen in einer Zugriffsgruppe

Sie können in Horizon Administrator die Desktop-Pools, Anwendungspools oder Farmen in einer bestimmten Zugriffsgruppe anzeigen.

Verfahren

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

Objekt	Aktion
Desktop-Pools	Wählen Sie Katalog > Desktop-Pools aus.
Anwendungspools	Wählen Sie Katalog > Anwendungspools aus.
Farmen	Wählen Sie Ressourcen > Farmen 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 virtuellen vCenter-Maschinen in einer speziellen Zugriffsgruppe in Horizon Administrator anzeigen. Eine vCenter-VM erbt die Zugriffsgruppe von ihrem Pool.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Ressourcen > Maschinen** aus.
- 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 Administrator benutzerdefinierte Rollen hinzufügen, ändern und löschen.

■ [Hinzufügen einer benutzerdefinierten Rolle](#)

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

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

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

■ [Entfernen einer benutzerdefinierten Rolle](#)

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

Wenn die vordefinierten Administratorrollen nicht Ihren Anforderungen entsprechen, können Sie ausgewählte Berechtigungen kombinieren, um eigene Rollen in Horizon Administrator 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 Wählen Sie in Horizon Administrator **View-Konfiguration > Administratoren** aus.
- 2 Klicken Sie auf der Registerkarte **Rollen** 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

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 Wählen Sie in Horizon Administrator **View-Konfiguration > Administratoren** aus.
- 2 Wählen Sie auf der Registerkarte **Rollen** die gewünschte Rolle.
- 3 Klicken Sie auf **Berechtigungen**, um die Berechtigungen in der Rolle anzuzeigen, 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

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](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Administratoren** aus.
- 2 Wählen Sie auf der Registerkarte **Rollen** die gewünschte Rolle 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 Administrator 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 6-6. Vordefinierte Rollen in Horizon Administrator

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 Administrator. ■ Verwenden der Befehle <code>vdmin</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>vdmin</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 6-6. Vordefinierte Rollen in Horizon Administrator (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. ■ Anmeldung bei Horizon Administrator möglich. ■ 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. ■ Anmeldung bei Horizon Administrator möglich. 	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. <p>Wenn Administratoren über diese Rolle für eine Zugriffsgruppe verfügen, können sie nur diese Vorgänge für die Bestandsobjekte in dieser Zugriffsgruppe durchführen.</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 6-6. Vordefinierte Rollen in Horizon Administrator (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 6-7. Globale Berechtigungen

Berechtigung	Benutzerfähigkeiten	Vordefinierte Rollen
Konsoleninteraktion	Anmeldung an und Verwendung von Horizon Administrator.	Administratoren Administratoren (Nur Lesezugriff) Bestandslistenadministratoren Bestandslistenadministratoren (Nur Lesezugriff) Administratoren für globale Konfigurationen und Richtlinien Administratoren für globale Konfigurationen und Richtlinien (Nur Lesezugriff) Helpdesk-Administratoren Helpdesk-Administratoren (nur Lesezugriff) Lokale Administratoren Lokale Administratoren (Nur Lesezugriff)
Direkte Interaktion	Ausführen aller PowerShell-Befehle und Befehlszeilenprogramme mit Ausnahme von vdmadmin und vdmimport. Administratoren müssen über die Administratorrolle für die Stammzugriffsgruppe verfügen, um die Befehle vdmadmin, vdmimport und lmvutil verwenden zu können.	Administratoren Administratoren (Nur Lesezugriff)
Globale Konfiguration und globale Richtlinien verwalten	Anzeigen und Ändern globaler Richtlinien und Konfigurationseinstellungen, Administratorrollen und -berechtigungen ausgenommen.	Administratoren Administratoren für globale Konfigurationen und Richtlinien
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
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

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 6-8. Objektspezifische Berechtigungen

Berechtigung	Benutzerfähigkeiten	Objekt
Farmen 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
Composer-Desktop-Pool-Image verwalten	Neusynchronisieren, Aktualisieren und Neuverteilen von Linked-Clone-Pools sowie Ändern des standardmäßigen Pool-Images.	Desktop-Pool
Computer verwalten	Ausführen aller computer- und sitzungsbezogenen Vorgänge.	Computer
Persistente Festplatten verwalten	Durchführen aller View Composer-Vorgänge für persistente Festplatten, einschließlich Verknüpfen, Trennen und Importieren von persistenten Festplatten.	Persistente Festplatte
Farmen, 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
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 6-9. 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 Administrator verfügen.

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

Tabelle 6-10. Aufgaben und Berechtigungen für die Pool-Verwaltung

Aufgabe	Erforderliche Berechtigungen
Desktop-Pool aktivieren oder deaktivieren	Farmen und Desktop-Pools aktivieren
Zuweisen oder Entfernen von Benutzerberechtigungen für einen Pool	Berechtigung für Desktop- und Anwendungspools verleihen
Hinzufügen eines Pools	Farmen, Desktop- und Anwendungspools verwalten
Ändern oder Löschen eines Pools	Farmen, Desktop- und Anwendungspools verwalten
Hinzufügen oder Entfernen von Desktops zu bzw. aus einem Pool	Farmen, Desktop- und Anwendungspools verwalten
Aktualisieren, Neuzusammenstellen, Neuverteilen oder Ändern des standardmäßigen View Composer-Images	Composer-Desktop-Pool-Image verwalten
Zugriffsgruppen ändern	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 Administrator verfügen.

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

Tabelle 6-11. Aufgaben und Berechtigungen für die Verwaltung von Computern

Aufgabe	Erforderliche Berechtigungen
Entfernen einer virtuellen Maschine	Computer verwalten
Zurücksetzen einer virtuellen Maschine	Neustartvorgang verwalten
Neustarten eines virtuellen Desktops	Neustartvorgang verwalten
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 Administrator 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 „Persistent Disks“ (Persistente Festplatten) in Horizon Administrator ausgeführt.

Tabelle 6-12. Aufgaben und Berechtigungen für die Verwaltung persistenter Festplatten

Aufgabe	Erforderliche Berechtigungen
Trennen einer Festplatte	Persistente Festplatten verwalten für die Festplatte und Farmen, Desktop- und Anwendungspools verwalten für den Pool.
Verknüpfen einer Festplatte	Persistente Festplatten verwalten für die Festplatte und Farmen, Desktop- und Anwendungspools verwalten für die Maschine.
Bearbeiten einer Festplatte	Persistente Festplatten verwalten für die Festplatte und Farmen, Desktop- und Anwendungspools verwalten für den ausgewählten Pool.
Zugriffsgruppen ändern	Persistente Festplatten verwalten für die Quell- und Zielzugriffsgruppen.
Neuerstellen eines Desktops	Persistente Festplatten verwalten für die Festplatte und Farmen, Desktop- und Anwendungspools verwalten für den letzten Pool.
Importieren aus vCenter	Persistente Festplatten verwalten für den Ordner und Pool verwalten für den Pool.
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 Administrator 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 Administrator verwaltet. Administratoren werden in der globalen Administratorenansicht in Horizon Administrator verwaltet.

Tabelle 6-13. Aufgaben und Berechtigungen für die Verwaltung von Benutzern und Administratoren

Aufgabe	Erforderliche Berechtigungen
Aktualisieren allgemeiner Benutzerinformationen	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 Administrator 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 6-14. 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
Anmeldung bei Horizon Administrator möglich.	Konsoleninteraktion
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
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 6-15. 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 vdmadmin und vdmimport.	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.
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.

Konfigurieren von Richtlinien in Horizon Administrator und Active Directory

7

Sie können mithilfe von Horizon Administrator Richtlinien für Clientsitzungen festlegen. Sie können Active Directory-Gruppenrichtlinieneinstellungen konfigurieren, um das Verhalten des View-Verbindungsservers, des PCoIP-Anzeigeprotokolls und die Anmeldung sowie Leistungsalarme von Horizon 7 zu steuern.

Sie können Active Directory-Gruppenrichtlinieneinstellungen konfigurieren, um das Verhalten von Horizon Agent, Horizon Client für Windows, Horizon Persona Management und bestimmten Funktionen zu steuern. Weitere Informationen zur Konfiguration dieser Richtlinieneinstellungen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Dieses Kapitel enthält die folgenden Themen:

- [Festlegen von Richtlinien in Horizon Administrator](#)
- [Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien \(ADM\) für Horizon 7](#)

Festlegen von Richtlinien in Horizon Administrator

Sie können mithilfe von Horizon Administrator Richtlinien für Clientsitzungen konfigurieren.

Sie können diese Richtlinien so festlegen, dass sie auf bestimmte Benutzer, bestimmte Desktop-Pools oder auf alle Clientsitzungsbutzer 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.

- **Konfigurieren globaler Richtlinieneinstellungen**

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

- **Konfigurieren von Richtlinien für Desktop-Pools**

Sie können Richtlinien auf Desktop-Ebene konfigurieren, um diese auf spezifische Desktop-Pools anzuwenden. Eine Richtlinieneinstellung auf Desktop-Ebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung.

- **Konfigurieren von Richtlinien für Benutzer**

Sie können Richtlinien auf Benutzerebene konfigurieren, um diese auf spezifische Benutzer anzuwenden. Richtlinieneinstellungen auf Benutzerebene haben immer Vorrang vor äquivalenten globalen Richtlinieneinstellungen und Richtlinieneinstellungen auf Desktop-Pool-Ebene.

- **Horizon 7-Richtlinien**

Sie können Horizon 7-Richtlinien konfigurieren, die auf alle Clientsitzungen angewendet werden, Sie können die Richtlinien jedoch auch auf spezifische Desktop-Pools oder Benutzer anwenden.

Konfigurieren globaler Richtlinieneinstellungen

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

Voraussetzungen

Machen Sie sich mit den Richtlinienbeschreibungen vertraut. Siehe [Horizon 7-Richtlinien](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Richtlinien > Globale Richtlinien** aus.
- 2 Klicken Sie im Fensterbereich **View-Richtlinien** auf **Richtlinien bearbeiten**.
- 3 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfigurieren von Richtlinien für Desktop-Pools

Sie können Richtlinien auf Desktop-Ebene konfigurieren, um diese auf spezifische Desktop-Pools anzuwenden. Eine Richtlinieneinstellung auf Desktop-Ebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung.

Voraussetzungen

Machen Sie sich mit den Richtlinienbeschreibungen vertraut. Siehe [Horizon 7-Richtlinien](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > Desktop-Pools** aus.
- 2 Doppelklicken Sie auf die ID des Desktop-Pools und anschließend auf die Registerkarte **Richtlinien**.
Die Registerkarte **Richtlinien** zeigt die aktuellen Richtlinieneinstellungen. Wenn eine Einstellung von der äquivalenten globalen Richtlinie vererbt wird, wird in der Spalte **Desktop-Poolrichtlinie** der Wert **Vererben** angezeigt.
- 3 Klicken Sie im Fensterbereich **View-Richtlinien** auf **Richtlinien bearbeiten**.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Konfigurieren von Richtlinien für Benutzer

Sie können Richtlinien auf Benutzerebene konfigurieren, um diese auf spezifische Benutzer anzuwenden. Richtlinieneinstellungen auf Benutzerebene haben immer Vorrang vor äquivalenten globalen Richtlinieneinstellungen und Richtlinieneinstellungen auf Desktop-Pool-Ebene.

Voraussetzungen

Machen Sie sich mit den Richtlinienbeschreibungen vertraut. Siehe [Horizon 7-Richtlinien](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > Desktop-Pools** aus.
- 2 Doppelklicken Sie auf die ID des Desktop-Pools und anschließend auf die Registerkarte **Richtlinien**.
Die Registerkarte **Richtlinien** zeigt die aktuellen Richtlinieneinstellungen. Wenn eine Einstellung von der äquivalenten globalen Richtlinie vererbt wird, wird in der Spalte **Desktop-Poolrichtlinie** der Wert **Vererben** angezeigt.
- 3 Klicken Sie auf **Benutzeraußerkräftsetzung** und anschließend auf **Benutzer hinzufügen**.
- 4 Um einen Benutzer zu suchen, klicken Sie auf **Hinzufügen**, geben den Namen oder die Beschreibung des Benutzers ein und klicken anschließend auf **Suchen**.
- 5 Wählen Sie einen oder mehrere Benutzer aus der Liste aus, klicken Sie auf **OK** und anschließend auf **Weiter**.
Das Dialogfeld „Einzelne Richtlinie hinzufügen“ wird angezeigt.
- 6 Konfigurieren Sie die Horizon-Richtlinien und klicken Sie auf **Fertig stellen**, um Ihre Änderungen zu speichern.

Horizon 7-Richtlinien

Sie können Horizon 7-Richtlinien konfigurieren, die auf alle Clientsitzungen angewendet werden, Sie können die Richtlinien jedoch auch auf spezifische Desktop-Pools oder Benutzer anwenden.

Die folgende Tabelle beschreibt die einzelnen Horizon 7-Richtlinieneinstellungen.

Tabelle 7-1. 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>

Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien (ADM) für Horizon 7

Horizon 7 bietet verschiedene komponentenspezifische administrative ADMX-Vorlagendateien für Gruppenrichtlinien. Sie können Remote-Desktops und -anwendungen optimieren und schützen, indem Sie die Richtlinieneinstellungen in den ADMX-Vorlagendateien einem neuen oder vorhandenen Gruppenrichtlinienobjekt (Group Policy Object, GPO) in Active Directory hinzufügen.

Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, sind in der Datei VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip verfügbar, wobei x.x.x für die Version und yyyyyyy für die Build-Nummer steht. Sie können die Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunterladen. Wählen Sie unter „Desktop & End-User Computing“ den VMware Horizon 7-Download, der die ZIP-Datei enthält.

Die Horizon 7-ADMX-Vorlagendateien enthalten sowohl Gruppenrichtlinien für die Computerkonfiguration als auch Gruppenrichtlinien für die Benutzerkonfiguration.

- Die Richtlinien für die Computerkonfiguration gelten für alle Remote-Desktops, unabhängig davon, wer sich mit dem Desktop verbindet.

- Die Richtlinien für die Benutzerkonfiguration gelten für alle Benutzer, unabhängig davon, mit welchem Remote-Desktop oder mit welcher Remoteanwendung sie sich verbinden. Richtlinien für die Benutzerkonfiguration setzen gleichwertige Richtlinien für die Computerkonfiguration außer Kraft.

Microsoft Windows wendet Richtlinien beim Start eines Desktops und bei der Benutzeranmeldung an.

Horizon 7-ADMX-Vorlagendateien

Die ADMX-Vorlagendateien von Horizon 7 stellen Gruppenrichtlinieneinstellungen bereit, mit denen Sie Horizon 7-Komponenten steuern und optimieren können.

Die ADMX-Dateien stehen in VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip zur Verfügung. Diese Datei können Sie von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunterladen. Wählen Sie unter „Desktop & End-User Computing“ den VMware Horizon 7-Download, der die ZIP-Datei enthält.

Tabelle 7-2. Horizon-ADMX-Vorlagendateien

Name der Vorlage	Vorlagendatei	Beschreibung
VMware Blast	vdm_blast.admx	Enthält Richtlinieneinstellungen in Bezug auf das VMware Blast-Anzeigeprotokoll.
VMware View Agent-Konfiguration	vdm_agent.admx	Enthält Richtlinieneinstellungen in Bezug auf die Authentifizierung sowie Umgebungskomponenten von Horizon Agent. Siehe das Dokument <i>Konfigurieren von Remote-Desktop-Funktionen in Horizon 7</i> .
VMware Horizon Client-Konfiguration	vdm_client.admx	Enthält Richtlinieneinstellungen in Bezug auf Horizon Client für Windows. Für Clients, die von außerhalb der Verbindungsserver-Hostdomäne eine Verbindung herstellen, sind die auf Horizon Client angewendeten Richtlinien nicht gültig. Siehe das Dokument <i>VMware Horizon Client für Windows Installations- und Einrichtungshandbuch</i> .
VMware Horizon-URL-Umleitung	urlRedirection.admx	Enthält die Richtlinieneinstellungen für die URL-Inhaltsumleitungsfunktion. Wenn Sie diese Vorlage einem GPO für einen Remote-Desktop- oder Anwendungspool hinzufügen, können bestimmte URL-Links, die im Remote-Desktop oder in der Remoteanwendung angeklickt werden, zu einem Windows-basierten Client umgeleitet und in einem clientseitigen Browser geöffnet werden. Wenn Sie diese Vorlage einem clientseitigen GPO hinzufügen und ein Benutzer bestimmte URL-Links in einem Windows-basierten Clientsystem anklickt, kann die URL in einem Remote-Desktop oder in einer Remoteanwendung geöffnet werden. Siehe das Dokument <i>Konfigurieren von Remote-Desktop-Funktionen in Horizon 7</i> und das Dokument <i>VMware Horizon Client für Windows Installations- und Einrichtungshandbuch</i> .

Tabelle 7-2. Horizon-ADMX-Vorlagendateien (Fortsetzung)

Name der Vorlage	Vorlagendatei	Beschreibung
VMware View Server-Konfiguration	vdm_server.admx	Enthält Richtlinieneinstellungen in Bezug auf den Verbindungsserver.
Allgemeine VMware View-Konfiguration	vdm_common.admx	Enthält Richtlinieneinstellungen, die für alle Horizon-Komponenten gelten.
PCoIP-Sitzungsvariablen	pcoip.admx	Enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll. Siehe das Dokument <i>Konfigurieren von Remote-Desktop-Funktionen in Horizon 7</i> .
PCoIP-Client-Sitzungsvariablen	pcoip.client.admx	Enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll, das Auswirkungen auf Horizon Client für Windows hat. Siehe das Dokument <i>VMware Horizon Client für Windows Installations- und Einrichtungshandbuch</i> .
Persona-Verwaltung	ViewPM.admx	Enthält Richtlinieneinstellungen in Bezug auf Horizon Persona Management. Siehe das Dokument <i>Einrichten von virtuellen Desktops in Horizon 7</i> .
VMware Umleitung für virtuellen Druck	printerRedirection.admx	Enthält Richtlinieneinstellungen zur Deaktivierung des standortbasierten Druckens, zur Deaktivierung der dauerhaften Druckeinstellung und zur Auswahl des Druckertreibers für einen umgeleiteten Clientdrucker.
Standortbasiertes Drucken	LBP.xml	Vorlage zur Definition von Übersetzungsregeln für jeden standortbasierten Drucker für die virtuelle Druckfunktion von VMware.
View-RTAV-Konfiguration	vdm_agent_rtav.admx	Enthält Richtlinieneinstellungen in Bezug auf Webcams, die zusammen mit der Echtzeit-Audio/Video-Funktion verwendet werden. Siehe das Dokument <i>Konfigurieren von Remote-Desktop-Funktionen in Horizon 7</i> .
Scannerumleitung	vdm_agent_scanner.admx	Enthält Richtlinieneinstellungen für Scangeräte, die zur Verwendung mit veröffentlichten Remote-Desktops und Remoteanwendungen umgeleitet werden. Siehe das Dokument <i>Konfigurieren von Remote-Desktop-Funktionen in Horizon 7</i> .
Serieller COM-Port	vdm_agent_serialport.admx	Enthält Richtlinieneinstellungen für serielle Ports (COM-Ports), die zur Verwendung mit virtuellen Desktops umgeleitet werden. Siehe das Dokument <i>Konfigurieren von Remote-Desktop-Funktionen in Horizon 7</i> .
VMware Horizon-Druckerumleitung	vdm_agent_printing.admx	Enthält die Richtlinieneinstellungen in Bezug auf das Filtern von umgeleiteten Druckern. Siehe das Dokument <i>Konfigurieren von Remote-Desktop-Funktionen in Horizon 7</i> .

Tabelle 7-2. Horizon-ADMX-Vorlagendateien (Fortsetzung)

Name der Vorlage	Vorlagendatei	Beschreibung
View Agent Direct-Connection	view_agent_direct_connection.admx	Enthält Richtlinieneinstellungen in Bezug auf das View Agent Direct-Connection-Plug-In. Weitere Informationen finden Sie im Dokument <i>Verwaltung des Plug-Ins „View Agent Direct-Connection“</i> .
VMware Horizon Performance Tracker	perf_tracker.admx	Enthält Richtlinieneinstellungen in Bezug auf die VMware Horizon Performance Tracker-Funktion. Siehe Verwenden von VMware Horizon Performance Tracker .
VMware Horizon-Clientlaufwerkumleitung	vdm_agent_cdr.admx	Enthält die Richtlinieneinstellungen für die Clientlaufwerksumleitungsfunktion. Siehe das Dokument <i>Konfigurieren von Remote-Desktop-Funktionen in Horizon 7</i> .

Einstellungen für ADMX-Vorlagen für die Konfiguration des Horizon-Verbindungsservers

Die ADMX-Vorlagendateien (vdm_server.admx) für die View Server-Konfiguration enthalten Richtlinieneinstellungen für alle Horizon-Verbindungsserver.

Die folgende Tabelle beschreibt die in der ADMX-Vorlagendatei für die Verbindungsserver-Konfiguration enthaltenen Richtlinieneinstellungen. Die Vorlage enthält ausschließlich Einstellungen für die Computerkonfiguration. Alle Einstellungen befinden sich im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Server Configuration** im Gruppenrichtlinien-Editor.

Tabelle 7-3. Vorlageneinstellungen für die Horizon Server-Konfiguration

Einstellung	Eigenschaften
Enumerate Forest Trust Child Domains	<p>Legt fest, ob alle Domänen aufgelistet werden, die von der Serverdomäne als vertrauenswürdig eingestuft werden. Um eine vollständige Vertrauenskette zu erzielen, werden rekursiv auch die vertrauten Domänen aller vertrauten Domänen aufgelistet – so lange, bis alle vertrauenswürdigen Domänen ermittelt wurden. Diese Informationen werden an den Verbindungsserver weitergeleitet, um sicherzustellen, dass für die Clientanmeldung alle vertrauenswürdigen Domänen verfügbar sind.</p> <p>Diese Eigenschaft ist standardmäßig aktiviert. Ist diese Eigenschaft deaktiviert, werden nur Domänen mit einem direkten Vertrauensverhältnis aufgelistet, eine Verbindung mit Remote-Domänencontrollern findet nicht statt.</p> <p>Hinweis In Umgebungen mit komplexen Domänenbeziehungen – z. B. in Umgebungen mit mehreren Gesamtstrukturen, bei denen Vertrauensstellungen zwischen den Domänen der Gesamtstrukturen eingerichtet wurden – kann der Vorgang mehrere Minuten in Anspruch nehmen.</p>
Recursive Enumeration of Trusted Domains	<p>Legt fest, ob alle Domänen aufgelistet werden, die von der Serverdomäne als vertrauenswürdig eingestuft werden. Um eine vollständige Vertrauenskette zu erzielen, werden rekursiv auch die vertrauten Domänen aller vertrauten Domänen aufgelistet – so lange, bis alle vertrauten Domänen ermittelt wurden. Diese Informationen werden an View-Verbindungsserver weitergeleitet um sicherzustellen, dass für die Clientanmeldung alle vertrauten Domänen verfügbar sind.</p> <p>Diese Einstellung ist standardmäßig aktiviert. Ist diese Einstellung deaktiviert, werden nur Domänen mit einem direkten Vertrauensverhältnis aufgelistet, eine Verbindung mit Remote-Domänencontrollern findet nicht statt.</p> <p>In Umgebungen mit komplexen Domänenbeziehungen – z.B. in Umgebungen mit mehreren Gesamtstrukturen, bei denen Vertrauensstellungen zwischen den Domänen der Gesamtstrukturen eingerichtet wurden – kann dieser Vorgang mehrere Minuten in Anspruch nehmen.</p>
Windows Password Authentication Mode	<p>Wählen Sie den Windows-Kennwortauthentifizierungsmodus aus.</p> <ul style="list-style-type: none"> ■ KerberosOnly. Authentifizierung mithilfe von Kerberos. ■ KerberosWithFallbackToNTLM. Authentifizierung mithilfe von Kerberos, aber Verwendung von NTLM im Fehlerfall. ■ Legacy. Authentifizierung mithilfe von NTLM, aber Verwendung von Kerberos im Fehlerfall. Wird zur Unterstützung älterer NT-Domänencontroller verwendet. <p>Der Standardwert lautet KerberosOnly.</p>

Einstellungen für ADMX-Vorlagen für die allgemeine Horizon 7-Konfiguration

Die ADMX-Vorlagendateien (vdm_common.admx) für die allgemeine Horizon 7-Konfiguration enthalten Richtlinieneinstellungen, die für alle Horizon-Komponenten gelten. Diese Vorlagen beinhalten ausschließlich Einstellungen für die Computerkonfiguration.

Einstellungen für die Protokollkonfiguration

Die folgende Tabelle beschreibt die in den ADMX-Vorlagendateien für die allgemeine Horizon-Konfiguration enthaltenen Richtlinieneinstellungen für die Protokollkonfiguration. Alle Einstellungen befinden sich im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Common Configuration > Log Configuration** im Gruppenrichtlinien-Editor.

Tabelle 7-4. Allgemeine View-Konfigurationsvorlage: Einstellungen für die Protokollkonfiguration

Einstellung	Eigenschaften
Number of days to keep production logs	Gibt an, für wie lange (in Tagen) Protokolldateien auf dem System gespeichert werden. Wenn kein Wert festgelegt ist, gilt die Standardeinstellung, nach der Protokolldateien für 7 Tage beibehalten werden.
Maximum number of debug logs	Gibt an, wie viele Debug-Protokolldateien maximal auf dem System gespeichert werden. Wenn eine Protokolldatei ihre maximale Größe erreicht, werden keine weiteren Einträge hinzugefügt, und es wird eine neue Protokolldatei erstellt. Wenn die Anzahl der vorherigen Protokolldateien den hier angegebenen Wert erreicht, wird die älteste Protokolldatei gelöscht.
Maximum debug log size in Megabytes	Gibt die maximale Größe in Megabyte an, die eine Debug-Protokolldatei erreichen darf, bevor die Protokolldatei geschlossen und eine neue Protokolldatei erstellt wird.
Log Directory	Gibt den vollständigen Pfad zum Verzeichnis für Protokolldateien an. Wenn für den Speicherort kein Schreibzugriff möglich ist, wird der standardmäßige Speicherort verwendet. Für Clientprotokolldateien wird ein gesondertes Verzeichnis mit dem Namen des Clients erstellt.
Send logs to a Syslog server	<p>Damit können View Server-Protokolle an einen Syslog-Server wie beispielsweise VMware vCenter Log Insight gesendet werden. Protokolle werden von allen View Servern in der Organisationseinheit (OU) oder Domäne gesendet, in denen dieses Gruppenrichtlinienobjekt konfiguriert ist.</p> <p>Sie können Horizon Agent-Protokolle an einen Syslog-Server senden, indem Sie diese Einstellung in einem Gruppenrichtlinienobjekt aktivieren, das mit einer OU verknüpft ist, welche Ihre Desktops enthält.</p> <p>Um Protokolldaten an einen Syslog-Server zu senden, aktivieren Sie diese Einstellung und geben die Protokollebene und den voll qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Servers an. Sie können einen alternativen Port angeben, wenn Sie den Standardport 514 nicht verwenden möchten. Trennen Sie jedes Element in Ihrer Angabe mit einem senkrechten Strich (). Verwenden Sie die folgende Syntax:</p> <p>Protokollebene Server-FQDN oder IP [Portnummer(514 Standard)]</p> <p>Beispiel: Debug 192.0.2.2</p> <p>Wichtig Syslog-Daten werden ohne softwarebasierte Verschlüsselung über das Netzwerk gesendet. Da View Server-Protokolle möglicherweise vertrauliche Daten enthalten, vermeiden Sie das Senden von Syslog-Daten über ein unsicheres Netzwerk. Verwenden Sie nach Möglichkeit eine Sicherheitsmaßnahme auf Verbindungsebene (z. B. IPsec), um zu verhindern, dass diese Daten im Netzwerk überwacht werden können.</p>

Einstellungen für Leistungsalarme

Tabelle 7-5. Allgemeine View-Konfigurationsvorlage: Einstellungen für Leistungsalarme beschreibt die in den ADMX-Vorlagendateien für die allgemeine Horizon-Konfiguration enthaltenen Einstellungen für Leistungsalarme. Alle Einstellungen befinden sich im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Common Configuration > Performance Alarms** im Gruppenrichtlinien-Editor.

Tabelle 7-5. Allgemeine View-Konfigurationsvorlage: Einstellungen für Leistungsalarme

Einstellung	Eigenschaften
CPU and Memory Sampling Interval in Seconds	Gibt das Abrufintervall für CPU und Arbeitsspeicher an. Ein niedriges Samplingintervall kann zu einer großen Menge an Ausgabedaten im Protokoll führen.
Overall CPU usage percentage to issue log info	Gibt den Schwellenwert an, bei dem die CPU-Gesamtnutzung des Systems protokolliert wird. Wenn mehrere Prozessoren verfügbar sind, gibt der Prozentwert die kombinierte Nutzung an.
Overall memory usage percentage to issue log info	Gibt den Schwellenwert an, bei dem die Gesamtnutzung des zugesicherten Systemarbeitsspeichers protokolliert wird. Zugesicherter Systemarbeitsspeicher ist der Arbeitsspeicher, der von Prozessoren reserviert wurde und für den das Betriebssystem physischen Arbeitsspeicher oder Platz in der Auslagerungsdatei zugesichert hat.
Process CPU usage percentage to issue log info	Gibt den Schwellenwert an, bei dem die CPU-Nutzung einzelner Prozesse protokolliert wird.
Process memory usage percentage to issue log info	Gibt den Schwellenwert an, bei dem die Arbeitsspeichernutzung einzelner Prozesse protokolliert wird.
Process to check, comma separated name list allowing wild cards and exclusion	<p>Gibt eine kommasetrennte Liste mit Abfragen an, die dem Namen von einem oder mehreren Prozessen entsprechen, die untersucht werden sollen. Sie können die Liste filtern, indem Sie in der Abfrage Platzhalterzeichen verwenden.</p> <ul style="list-style-type: none"> ■ Ein Sternchen (*) entspricht keinem oder mehreren Zeichen. ■ Ein Fragezeichen (?) entspricht genau einem Zeichen. ■ Ein Ausrufezeichen (!) am Anfang einer Abfrage schließt alle Ergebnisse dieser Abfrage aus. <p>Beispielsweise werden mit der folgenden Abfrage alle Prozesse ausgewählt, die mit ws beginnen, gleichzeitig werden auf sys endende Prozesse ausgeschlossen:</p> <p>'!*sys,ws*'</p>

Hinweis Einstellungen für Leistungsalarme gelten nur für Horizon-Verbindungsserver- und Horizon Agent-Systeme. Einstellungen für Leistungsalarme gelten nicht für Horizon Client-Systeme.

Sicherheitseinstellungen

Tabelle 7-6. Allgemeine View-Konfigurationsvorlage: Sicherheitseinstellungen beschreibt die in den ADMX-Vorlagendateien für die allgemeine Horizon-Konfiguration enthaltenen Sicherheitseinstellungen. Alle Einstellungen befinden sich im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Common Configuration > Sicherheitseinstellungen** im Gruppenrichtlinien-Editor.

Tabelle 7-6. Allgemeine View-Konfigurationsvorlage: Sicherheitseinstellungen

Einstellung	Eigenschaften
Only use cached revocation URLs	Die Zertifikatsperrüberprüfung greift nur auf zwischengespeicherte URLs zu. Ist diese nicht konfiguriert, ist die Standardeinstellung „False“.
Revocation URL check timeout milliseconds	Die kumulative Zeitüberschreitung für alle Abrufe von Sperr-URLs in Millisekunden. Bei einem nicht konfigurierten Wert oder bei einem Wert von 0 wird die Microsoft-Standardbehandlung durchgeführt.
Type of certificate revocation check	Wählen Sie den gewünschten Typ der Zertifikatsperrüberprüfung aus: <ul style="list-style-type: none"> ■ Keine ■ EndCertificateOnly ■ WholeChain ■ WholeChain Die Standardeinstellung ist WholeChainButRoot.

Allgemeine Einstellungen

Tabelle 7-7. Allgemeine View-Konfigurationsvorlage: Allgemeine Einstellungen beschreibt die in den ADMX-Vorlagendateien für die allgemeine Horizon-Konfiguration enthaltenen allgemeinen Einstellungen. Alle Einstellungen befinden sich im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > VMware View Common Configuration** im Gruppenrichtlinien-Editor.

Tabelle 7-7. Allgemeine View-Konfigurationsvorlage: Allgemeine Einstellungen

Einstellung	Eigenschaften
Disk threshold for log and events in Megabytes	Gibt den Speicherplatz an, der in Bezug auf die Ereignisprotokollierung mindestens auf der Festplatte verfügbar bleiben muss. Wenn kein Wert angegeben ist, lautet die Standardeinstellung 200. Nach Erreichen dieses Werts wird die Ereignisprotokollierung gestoppt.
Enable extended logging	Legt fest, ob trace- und debug-Ereignisse in die Protokolldateien geschrieben werden.
Override the default View Windows event generation	Die folgenden Werte werden unterstützt: <ul style="list-style-type: none"> ■ 0 = Ereignisprotokolleinträge werden nur für View-Ereignisse erstellt (es werden keine Ereignisprotokolleinträge für Protokollmeldungen generiert). ■ 1 = Ereignisprotokolleinträge werden im Kompatibilitätsmodus von 4.5 (und früher) erstellt. Ereignisprotokolleinträge werden nicht für Standard-View-Ereignisse erstellt. Ereignisprotokolleinträge basieren ausschließlich auf dem Text von Protokolldateien. ■ 2 = Ereignisprotokolleinträge werden im Kompatibilitätsmodus von 4.5 (und früher) erstellt. Es werden auch View-Ereignisse berücksichtigt.

Warten von Horizon 7-Komponenten

8

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](#)
- [Überwachen von Horizon 7-Komponenten](#)
- [Überwachen des Computerstatus](#)
- [Grundlegendes zu Horizon 7-Diensten](#)
- [Ändern des Produktlizenzschlüssels](#)
- [Überwachen der Nutzung der Produktlizenz](#)
- [Aktualisieren allgemeiner Benutzerinformationen aus Active Directory](#)
- [Migrieren von View Composer auf eine andere Maschine](#)
- [Aktualisieren der Zertifikate auf einer Verbindungsserver-Instanz, einem Sicherheitsserver oder View Composer](#)
- [Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit](#)

Sichern und Wiederherstellen von Horizon 7-Konfigurationsdaten

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

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

Sichern von Horizon-Verbindungsserver- und View Composer-Daten

Nachdem Sie die anfängliche Konfiguration des Verbindungservers abgeschlossen haben, sollten Sie regelmäßige Sicherungen Ihrer Horizon 7- und View Composer-Konfigurationsdaten planen. Sie können Ihre Horizon 7- und View Composer-Daten mithilfe von Horizon Administrator sichern.

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

Hinweis Standardmäßig sichert Horizon 7 automatisch Verbindungsserver- und View Composer-Daten täglich um 12.00 Uhr.

Wenn Sie Sicherungen mithilfe von Horizon Administrator durchführen, sichert Horizon 7 die View LDAP-Konfigurationsdaten und die View Composer-Datenbank. Beide Sicherungsdateisätze werden am selben Speicherort gespeichert. Die View LDAP-Daten werden im verschlüsselten LDAP Data Interchange Format (LDIF) exportiert. Eine Beschreibung von View LDAP finden Sie unter [View LDAP-Verzeichnis](#).

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 Administrator.
- 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 View Composer-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 Composer-Diensten verwendet, sichert Horizon 7 alle mit sämtlichen vCenter Server-Instanzen verknüpften View 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 Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die zu sichernde Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 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 View Composer-Konfigurationsdaten in regelmäßigen Abständen sichern. In Horizon Administrator können Sie die Häufigkeit und andere Aspekte der Sicherungsvorgänge festlegen.

Hinweis Standardmäßig sichert Horizon 7 automatisch Verbindungsserver- und View Composer-Daten täglich um 12.00 Uhr.

Tabelle 8-1. 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>
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 View 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.

Ergebnisse

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 View Composer-Konfigurationsdaten](#).

Wiederherstellen von Horizon-Verbindungsserver- und View Composer-Konfigurationsdaten

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

Sie führen manuell verschiedene Dienstprogramme aus, um die Verbindungsserver- und View Composer-Konfigurationsdateien wiederherzustellen.

Bevor Sie Konfigurationsdaten wiederherstellen, sollten Sie sicherstellen, dass Sie die Konfigurationsdaten in Horizon Administrator gesichert haben. Siehe [Sichern von Horizon-Verbindungsserver- und View 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 View Composer-Daten aus den `.svi`-Sicherungsdateien in die View 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 Administrator 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 View 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 View Composer, indem Sie den Windows-Dienst „VMware Horizon View Composer“ auf den Servern anhalten, auf denen View Composer ausgeführt wird.
- 2 Stoppen Sie alle Sicherheitsserverinstanzen, indem Sie den Windows-Dienst „VMware Horizon Sicherheitsserver“ auf allen Sicherheitsservern stoppen.
- 3 Deinstallieren Sie alle Instanzen von Horizon-Verbindungsserver.
Deinstallieren Sie sowohl VMware Horizon-Verbindungsserver als auch die AD LDS-Instanz „VMwareVDMDS“.
- 4 Installieren Sie eine Instanz von Verbindungsserver.
- 5 Stoppen Sie die Verbindungsserver-Instanz, indem Sie den Windows-Dienst „VMware Horizon Verbindungsserver“ stoppen.
- 6 Klicken Sie auf **Start > Eingabeaufforderung**.
- 7 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:

```
vdmimport -d -p mypassword
-f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

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.

- 8 Importieren Sie die entschlüsselte LDIF-Datei, um die View LDAP-Konfiguration wiederherzustellen.
Geben Sie die Option `-f` mit der entschlüsselten LDIF-Datei an. Beispiel:

```
vdmimport -f MyDecryptedexport.LDF
```

- 9 Deinstallieren Sie den Verbindungsserver.
Deinstallieren Sie nur das Paket „VMware Horizon-Verbindungsserver“.
- 10 Installieren Sie den Verbindungsserver neu.
- 11 Melden Sie sich bei Horizon Administrator an und validieren Sie, dass die Konfiguration korrekt ist.
- 12 Starten Sie die View Composer-Instanzen.
- 13 Installieren Sie die Replikatserverinstanzen neu.
- 14 Starten Sie die Sicherheitsserverinstanzen.

Ergebnisse

Falls das Risiko besteht, dass die Sicherheitsserver eine inkonsistente Konfiguration haben, sollten sie ebenfalls deinstalliert werden, anstatt gestoppt und dann am Ende des Vorgangs neu installiert zu werden.

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 View Composer bekannt sind, falls letzter verwendet wird. Stellen Sie bei Bedarf die View Composer-Konfiguration von einer Sicherung wieder her. Siehe [Wiederherstellen einer View Composer-Datenbank](#). Nachdem Sie die View Composer-Konfiguration wiederherstellen, müssen Sie möglicherweise manuell Inkonsistenzen auflösen, falls sich die virtuellen Maschinen in vCenter Server seit der Sicherung der View Composer-Konfiguration geändert haben.

Wiederherstellen einer View Composer-Datenbank

Sie können die Sicherungsdateien für Ihre View Composer-Konfiguration in die View Composer-Datenbank importieren, die Linked-Clone-Informationen speichert.

Mithilfe des Befehls `SviConfig restoredata` können Sie die View Composer-Datenbank nach einem Systemausfall wiederherstellen oder die View Composer-Konfiguration in einen früheren Zustand zurückversetzen.

Wichtig Nur erfahrene View Composer-Administratoren sollten das Dienstprogramm `SviConfig` verwenden. Mit diesem Dienstprogramm lassen sich Fehler im Zusammenhang mit dem View Composer-Dienst behandeln.

Voraussetzungen

Ermitteln Sie den Speicherort der Sicherungsdateien für die View Composer-Datenbank. Standardmäßig speichert Horizon 7 die Sicherungsdateien auf Laufwerk C: des Verbindungsserver-Computers im Verzeichnis `C:\ProgramData\VMWare\VDM\backups`.

View 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 View 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 View Composer-Sicherungsdateien vom Verbindungsserver-Computer an einen Speicherort, auf den von dem Computer zugegriffen werden kann, auf dem der VMware Horizon View Composer-Dienst installiert ist.
- 2 Halten Sie auf dem Computer, auf dem View Composer installiert ist, den VMware Horizon View Composer-Dienst an.
- 3 Öffnen Sie eine Windows-Eingabeaufforderung und navigieren Sie zur ausführbaren SviConfig-Datei.

Die Datei befindet sich im Ordner der View 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 -dsname=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 View Composer-Dienst.

Nächste Schritte

Ergebniscodes zur Ausgabe des Befehls SviConfig restoredata finden Sie unter [Ergebniscodes für das Wiederherstellen der View Composer-Datenbank](#).

Ergebniscodes für das Wiederherstellen der View Composer-Datenbank

Wenn Sie eine View Composer-Datenbank wiederherstellen, zeigt der Befehl SviConfig restoredata einen Ergebniscode an.

Tabelle 8-2. Restoredata-Ergebniscode

Code	Beschreibung
0	Vorgang erfolgreich abgeschlossen.
1	Angegebener DSN wurde nicht gefunden.
2	Angegebene Anmeldeinformationen für Datenbankadministrator sind ungültig.
3	Treiber für die Datenbank wird nicht unterstützt.
4	Unerwartetes Problem ist aufgetreten und der Befehl konnte nicht abgeschlossen werden.
14	Der VMware Horizon View Composer-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 aus der View Composer-Datenbank

Sie können die Daten aus Ihrer View Composer-Datenbank in eine Datei exportieren.

Wichtig Das Dienstprogramm SviConfig sollte nur von erfahrenen View Composer-Administratoren verwendet werden.

Voraussetzungen

Standardmäßig speichert Horizon 7 die Sicherungsdateien auf Laufwerk C: des View-Verbindungsserver-Computers unter C:\Programme\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 Halten Sie auf dem Computer, auf dem View Composer installiert ist, den VMware Horizon View Composer-Dienst an.
- 2 Öffnen Sie eine Windows-Eingabeaufforderung und navigieren Sie zur ausführbaren SviConfig-Datei.

Die Datei befindet sich im Ordner der View Composer-Anwendung.

View-Composer-installation-directory\sviconfig.exe

3 Führen Sie den Befehl `SviConfig exportdata` aus.

```
sviconfig -operation=exportdata
          -DsnName=target_database_source_name_ (DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -OutputFilePath=path_to_View_Composer_output_file
```

Beispiel:

```
sviconfig -operation=exportdata -dsnname=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 das Exportieren der View Composer-Datenbank](#).

Ergebniscodes für das Exportieren der View Composer-Datenbank

Beim Export einer View Composer-Datenbank zeigt der `SviConfig exportdata` -Befehl einen Exitcode an.

Tabelle 8-3. 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	Die 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 Administrator-Dashboard überwachen.

Horizon Administrator zeigt Überwachungsinformationen zu Verbindungsserver-Instanzen, zur Ereignisdatenbank, zu Gateways, Sicherheitsservern, View Composer-Diensten, Datenspeichern, vCenter Server-Instanzen und Domänen an.

Hinweis Horizon 7 kann keine Statusinformationen zu Kerberos-Domänen sammeln. Horizon Administrator zeigt den Status von Kerberos-Domänen als unbekannt an, selbst wenn eine Domäne konfiguriert wurde und fehlerfrei arbeitet.

Verfahren

- 1 Klicken Sie in Horizon Administrator auf **Dashboard**.
- 2 Erweitern Sie im Fensterbereich „Systemzustand“ die Einträge **View-Komponenten**, **vSphere-Komponenten** oder **Andere Komponenten**.
 - Ein grüner, nach oben weisender Pfeil weist darauf hin, dass für eine Komponente keine Probleme vorliegen.
 - Ein roter, nach unten weisender Pfeil weist darauf hin, dass eine Komponente nicht verfügbar ist oder nicht funktioniert.
 - Ein gelber Doppelpfeil weist darauf hin, dass sich eine Komponente in einem Warnzustand befindet.
 - Ein Fragezeichen weist darauf hin, dass der Status einer Komponente unbekannt ist.
- 3 Klicken Sie auf einen Komponentennamen.

In einem Dialogfeld werden Name, Version, Status und weitere Informationen zur Komponente angezeigt.

Nächste Schritte

Verwenden Sie vCenter Server, um vSAN-Cluster und die an einem vSAN-Datenspeicher beteiligten Festplatten zu überwachen. Weitere Informationen zur Überwachung von vSAN in vSphere 5.5 Update 1 finden Sie im Dokument *vSphere Storage* und in der Dokumentation *Überwachung und Leistung von vSphere*. Weitere Informationen zur Überwachung von vSAN in vSphere 6 oder höher finden Sie im Dokument *Verwalten von VMware vSAN*.

Überwachen des Computerstatus

Sie können den Status von Computern in Ihrer Horizon 7-Bereitstellung problemlos über das Horizon Administrator-Dashboard überwachen. Beispielsweise können alle getrennten Computer oder alle Computer im Wartungsmodus angezeigt werden.

Voraussetzungen

Machen Sie sich mit den verschiedenen Statuswerten der virtuellen Maschine vertraut. Weitere Informationen zum Status virtueller Maschinen finden Sie unter „Status von vCenter Server-VMs“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Verfahren

- 1 Klicken Sie in Horizon Administrator auf **Dashboard**.

- 2 Erweitern Sie im Fenster „Computerstatus“ einen Statusordner.

Option	Beschreibung
Wird vorbereitet	Listet die Status auf, während der Computer bereitgestellt oder gelöscht wird bzw. sich im Wartungsmodus befindet.
Problematische Computer	Listet die Fehlerstatus auf.
Für die Verwendung vorbereitet	Listet die Status auf, wenn der Computer verwendet werden kann.

- 3 Ermitteln Sie den Computerstatus und klicken Sie auf die neben dem Status angezeigte Hyperlink-Nummer.

Ergebnisse

Auf der Seite **Computer** werden alle Computer mit dem ausgewählten Status angezeigt.

Nächste Schritte

Klicken Sie auf einen Computernamen, um Einzelheiten zu diesem Computer anzuzeigen, oder klicken Sie in Horizon Administrator auf „Zurück“, um erneut auf die Dashboard-Seite zu wechseln.

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 8-4. 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.

Tabelle 8-4. Horizon Verbindungsserver-Hostdienste (Fortsetzung)

Dienstname	Starttyp	Beschreibung
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 8-5. 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.
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

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 Administrator 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 Administrator 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 View 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 Administrator **View-Konfiguration > 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 **Lizenzierung** 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 **Lizenzierung** werden die aktualisierten Lizenzinformationen angezeigt.

- 4 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 **Lizenzierung** 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 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>.

- 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 Nutzung der Produktlizenz

In Horizon 7 Administrator können Sie die aktiven Benutzer überwachen, die derzeit mit Horizon verbunden sind. Auf der Seite **Produktlizenzierung und -verwendung** werden die aktuelle und die höchste historische Anzahl der Produktnutzung 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 bietet zwei Modelle für Nutzungslizenzen, eines für benannte und eines für gleichzeitige Benutzer. Horizon ermittelt die benannten und gleichzeitigen Benutzer in Ihrer Umgebung, unabhängig von Ihrer Produktlizenzedition oder Ihrer Nutzungsvereinbarung.

Für benannte Benutzer ermittelt Horizon die Anzahl eindeutiger Benutzer, die auf die Horizon-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** auf der Seite **Produktlizenzierung und -verwendung** die Anzahl der Benutzer seit der ersten Konfiguration Ihrer Horizon-Bereitstellung oder seit dem letzten Zurücksetzen von **Wert benannter Benutzer** angezeigt. Die Spalte **Höchste** gilt nicht für benannte Benutzer.

Für gleichzeitige Benutzer ermittelt Horizon 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** auf der Seite **Produktlizenzierung und -verwendung** die höchste Anzahl gleichzeitiger Benutzer von Desktop-Sitzungen sowie von veröffentlichten Desktops und veröffentlichten Anwendungen seit der ersten Konfiguration Ihrer Horizon-Bereitstellung oder seit dem letzten Zurücksetzen von **Höchster Wert** 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 werden, 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 Nutzung der Produktlizenz

Sie können in Horizon Administrator die historischen Nutzungsdaten 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 Nutzung der Produktlizenz](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > 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**.

Aktualisieren allgemeiner Benutzerinformationen aus Active Directory

Sie können Horizon 7 mit den aktuellen Benutzerinformationen aktualisieren, die in Active Directory gespeichert sind. Diese Funktion aktualisiert Name, Telefonnummer, E-Mail-Adresse, Benutzername und die standardmäßige Windows-Domäne der Horizon 7-Benutzer. Die vertrauenswürdigen externen Domänen werden ebenfalls aktualisiert.

Verwenden Sie diese Funktion, wenn Sie die Liste der vertrauenswürdigen externen Domänen in Active Directory ändern, insbesondere dann, wenn die geänderten Vertrauensbeziehungen zwischen Domänen sich auf Benutzerberechtigungen in Horizon 7 auswirken.

Diese Funktion überprüft Active Directory auf die neuesten Benutzerinformationen und aktualisiert die Horizon 7-Konfiguration.

Bei der Aktualisierung der allgemeinen Benutzerinformationen wird auch die Anzahl der benannten Benutzer auf 0 zurückgesetzt. Diese Zahl erscheint in Horizon Administrator auf der Seite

Produktlizenzierung und -verwendung. Siehe [Zurücksetzen der Daten zur Nutzung der Produktlizenz](#).

Sie können Benutzer- und Domäneninformationen auch über den Befehl `vdadmin` aktualisieren. Siehe [Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „F“](#).

Voraussetzungen

Vergewissern Sie sich, dass Sie sich bei Horizon Administrator als Administrator mit der Berechtigung **Globale Konfiguration und Richtlinien verwalten** anmelden können.

Verfahren

- 1 Klicken Sie in Horizon Administrator auf **Benutzer und Gruppen**.
- 2 Geben Sie an, ob die Informationen für alle Benutzer oder einen einzelnen Benutzer aktualisiert werden sollen.

Option	Aktion
Für alle Benutzer	Klicken Sie auf Allgemeine Benutzerinformationen aktualisieren . Das Aktualisieren aller Benutzer und Gruppen kann sehr viel Zeit beanspruchen.
Für einen einzelnen Benutzer	<ol style="list-style-type: none"> a Klicken Sie auf den Namen des Benutzers, für den Sie eine Aktualisierung durchführen möchten. b Klicken Sie auf Allgemeine Benutzerinformationen aktualisieren.

Migrieren von View Composer auf eine andere Maschine

In bestimmten Situationen kann es erforderlich sein, einen VMware Horizon View Composer-Dienst auf eine neue virtuelle Maschine oder einen neuen physischen Computer unter Windows Server zu migrieren. Möglicherweise migrieren Sie View Composer und vCenter Server z. B. auf einen neuen ESXi-Host oder -Cluster, um Ihre Horizon 7-Bereitstellung zu erweitern. Darüber hinaus müssen View Composer und vCenter Server nicht auf derselben Windows Server-Maschine installiert werden.

Sie können View Composer von der vCenter Server-Maschine auf einen eigenständigen oder von einer eigenständigen Maschine auf die vCenter Server-Maschine migrieren.

■ [Anleitungen für die Migration von View Composer](#)

Die für die Migration des VMware Horizon View Composer-Diensts durchzuführenden Schritte richten sich danach, ob Sie vorhandene virtuelle Linked-Clone-Maschinen beibehalten möchten.

- **Migrieren von View Composer mit einer vorhandenen Datenbank**

Wenn Sie View Composer auf einen anderen physischen Computer oder eine andere virtuelle Maschine migrieren und beabsichtigen, die aktuellen virtuellen Linked-Clone-Maschinen zu erhalten, muss der neue VMware Horizon View Composer-Dienst die vorhandene View Composer-Datenbank weiterverwenden.

- **Migrieren von View Composer ohne virtuelle Linked-Clone-Maschinen**

Wenn der aktuelle VMware Horizon View Composer-Dienst keine virtuellen Linked-Clone-Maschinen verwaltet, können Sie View Composer auf eine neue physische oder virtuelle Maschine migrieren, ohne die RSA-Schlüssel auf die neue Maschine zu migrieren. Der migrierte VMware Horizon View Composer-Dienst kann eine Verbindung zur ursprünglichen View Composer-Datenbank herstellen oder Sie können eine neue Datenbank für View Composer vorbereiten.

- **Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln**

Zur Verwendung einer vorhandenen View Composer-Datenbank müssen Sie den RSA-Schlüsselcontainer zwischen den Maschinen migrieren. Sie migrieren den RSA-Schlüsselcontainer mit dem Tool für die ASP.NET IIS-Registrierung, das zum Lieferumfang von Microsoft .NET Framework gehört.

- **Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst**

Zur Verwendung einer vorhandenen View Composer-Datenbank müssen Sie den RSA-Schlüsselcontainer von der physischen oder virtuellen Quellmaschine, auf der der vorhandene VMware Horizon View Composer-Dienst installiert ist, auf die Maschine migrieren, auf der Sie den neuen VMware Horizon View Composer-Dienst installieren möchten.

Anleitungen für die Migration von View Composer

Die für die Migration des VMware Horizon View Composer-Diensts durchzuführenden Schritte richten sich danach, ob Sie vorhandene virtuelle Linked-Clone-Maschinen beibehalten möchten.

Um die virtuellen Linked-Clone-Maschinen in Ihrer Bereitstellung beizubehalten, muss der VMware Horizon View Composer-Dienst, den Sie auf der neuen virtuellen Maschine oder dem neuen physischen Computer installieren, die vorhandene View Composer-Datenbank weiterhin verwenden. Die View Composer-Datenbank enthält Daten, die für die Erstellung, Bereitstellung, Wartung und Löschung von Linked-Clones erforderlich sind.

Wenn Sie den VMware Horizon View Composer-Dienst migrieren, können Sie auch die View Composer-Datenbank auf einen neuen Computer migrieren.

Unabhängig davon, ob Sie die View Composer-Datenbank migrieren, muss diese auf einem verfügbaren Computer in derselben Domäne wie der neue Computer, auf dem Sie den neuen VMware Horizon View Composer-Dienst installieren, oder in einer vertrauenswürdigen Domäne installiert werden.

View Composer erstellt RSA-Schlüsselpaare zum Ver- und Entschlüsseln der in der View Composer-Datenbank gespeicherten Authentifizierungsinformationen. Damit diese Datenquelle zur neuen Instanz des VMware Horizon View Composer-Dienstes kompatibel ist, müssen Sie zunächst den vom ursprünglichen VMware Horizon View Composer-Dienst erstellten RSA-Schlüsselcontainer migrieren. Importieren Sie den RSA-Schlüsselcontainer auf den Computer, auf dem Sie den neuen Dienst installieren.

Wenn der aktuelle VMware Horizon View Composer-Dienst keine virtuellen Linked-Clone-Maschinen verwaltet, können Sie den Dienst migrieren, ohne die vorhandene View Composer-Datenbank zu verwenden. Sie müssen die RSA-Schlüssel unabhängig davon, ob Sie die vorhandene Datenbank verwenden, nicht migrieren.

Hinweis Jede Instanz des VMware Horizon View Composer-Dienstes muss über eine eigene View Composer-Datenbank verfügen. Mehrere VMware Horizon View Composer-Dienste können eine View Composer-Datenbank nicht gemeinsam nutzen.

Migrieren von View Composer mit einer vorhandenen Datenbank

Wenn Sie View Composer auf einen anderen physischen Computer oder eine andere virtuelle Maschine migrieren und beabsichtigen, die aktuellen virtuellen Linked-Clone-Maschinen zu erhalten, muss der neue VMware Horizon View Composer-Dienst die vorhandene View Composer-Datenbank weiterverwenden.

Befolgen Sie die Schritte dieser Vorgehensweise, wenn Sie View Composer in eine der folgenden Richtungen migrieren:

- Von einem vCenter Server-Computer auf einen eigenständigen Computer
- Von einem eigenständigen Computer auf einen vCenter Server
- Von einem eigenständigen Computer auf einen anderen eigenständigen Computer
- Von einem vCenter Server-Computer auf einen anderen vCenter Server-Computer

Wenn Sie den VMware Horizon View Composer-Dienst migrieren, können Sie auch die View Composer-Datenbank auf einen neuen Speicherort migrieren. So müssen Sie beispielsweise die View Composer-Datenbank migrieren, wenn sich die aktuelle Datenbank auf einem vCenter Server-Computer befindet, den Sie ebenfalls migrieren.

Wenn Sie den VMware Horizon View Composer-Dienst auf dem neuen Computer installieren, müssen Sie den Dienst so konfigurieren, dass er eine Verbindung mit der View Composer-Datenbank herstellt.

Voraussetzungen

- Machen Sie sich mit den Migrationsanforderungen von View Composer vertraut. Siehe [Anleitungen für die Migration von View Composer](#).
- Machen Sie sich mit den Schritten zur Migration des RSA-Schlüsselcontainers auf den neuen VMware Horizon View Composer-Dienst vertraut. Siehe [Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln](#) und [Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst](#).

- Machen Sie sich im Dokument *Horizon 7-Installation* mit der Installation des VMware Horizon View Composer-Dienstes vertraut.
- Machen Sie sich im Dokument *Horizon 7-Installation* mit der Konfiguration eines TLS-Zertifikats für View Composer vertraut.
- Machen Sie sich mit der Konfiguration von View Composer in Horizon Administrator vertraut. Siehe [Konfigurieren von View Composer-Einstellungen](#) und [Konfigurieren von View Composer-Domänen](#).
- Als Best Practice empfiehlt es sich, dass Sie überprüfen, ob die Quell- und Zielmaschinen, die Sie für die Migration von View Composer verwenden, identisch sind und dieselben Administratoranmeldedaten verwenden. Wenn Sie View Composer von einem eigenständigen Computer auf eine vCenter Server-Maschine migrieren, auf der View Composer bereits installiert ist, schlägt die Konfiguration von View Composer möglicherweise fehl, wenn die auf den beiden Maschinen verwendeten Anmeldedaten unterschiedlich sind.

Verfahren

- 1 Deaktivieren Sie die Bereitstellung virtueller Maschinen auf der vCenter Server-Instanz, die mit dem VMware Horizon View Composer-Dienst verknüpft ist.
 - a Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
 - b Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz aus und klicken Sie auf **Bereitstellung deaktivieren**.
- 2 (Optional) Migrieren Sie die View Composer-Datenbank an einen neuen Ort.
Wenn Sie diesen Schritt ausführen müssen, fragen Sie den Datenbankadministrator nach Migrationsanweisungen.
- 3 Deinstallieren Sie den VMware Horizon View Composer-Dienst von der aktuellen Maschine.
- 4 Migrieren Sie den RSA-Schlüsselcontainer auf den neuen Computer.
- 5 Installieren Sie den VMware Horizon View Composer-Dienst auf der neuen Maschine.
Geben Sie während der Installation den DSN der Datenbank ein, die vom ursprünglichen VMware Horizon View Composer-Dienst verwendet wurde. Geben Sie auch den Benutzernamen und das Kennwort des Domänenadministrators an, die für die ODBC-Datenquelle für die Datenbank bereitgestellt wurden.
Wenn Sie die Datenbank migriert haben, müssen DSN und Datenquelleninformationen auf den neuen Speicherort der Datenbank verweisen. Unabhängig davon, ob Sie die Datenbank migriert haben, muss der neue VMware Horizon View Composer-Dienst Zugriff auf die ursprünglichen Datenbankinformationen über Linked Clones haben.
- 6 Konfigurieren Sie auf der neuen Maschine ein SSL-Serverzertifikat für View Composer.
Möglicherweise können Sie das Zertifikat kopieren, das auf der ursprünglichen Maschine für View Composer installiert war, oder Sie können ein neues Zertifikat installieren.

7 Konfigurieren Sie in Horizon Administrator die neuen View Composer-Einstellungen.

- a Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- b Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz aus, die mit diesem View Composer-Dienst verknüpft ist, und klicken Sie auf **Bearbeiten**.
- c Klicken Sie im Bereich „View Composer Server-Einstellungen“ auf **Bearbeiten** und geben Sie die neuen View Composer-Einstellungen an.

Wenn Sie View Composer mit vCenter Server auf der neuen Maschine installieren, wählen Sie **View Composer wurde zusammen mit vCenter Server installiert** aus.

Wenn Sie View Composer auf einer eigenständigen Maschine installieren, wählen Sie **Eigenständiger View Composer Server** aus und geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der View Composer-Maschine sowie den Benutzernamen und das Kennwort des View Composer-Benutzers an.

- d Klicken Sie im Bereich „Domänen“ auf **Serverinformationen bestätigen** und fügen Sie nach Bedarf View Composer-Domänen hinzu bzw. bearbeiten Sie diese.
- e Klicken Sie auf **OK**.

Migrieren von View Composer ohne virtuelle Linked-Clone-Maschinen

Wenn der aktuelle VMware Horizon View Composer-Dienst keine virtuellen Linked-Clone-Maschinen verwaltet, können Sie View Composer auf eine neue physische oder virtuelle Maschine migrieren, ohne die RSA-Schlüssel auf die neue Maschine zu migrieren. Der migrierte VMware Horizon View Composer-Dienst kann eine Verbindung zur ursprünglichen View Composer-Datenbank herstellen oder Sie können eine neue Datenbank für View Composer vorbereiten.

Voraussetzungen

- Machen Sie sich im Dokument *Horizon 7-Installation* mit der Installation des VMware Horizon View Composer-Dienstes vertraut.
- Machen Sie sich im Dokument *Horizon 7-Installation* mit der Konfiguration eines TLS-Zertifikats für View Composer vertraut.
- Machen Sie sich mit den Schritten zum Entfernen von View Composer aus Horizon Administrator vertraut. Siehe [Entfernen von View Composer aus Horizon 7](#).

Bevor Sie View Composer entfernen können, überprüfen Sie, dass es keine Linked-Clone-Desktops mehr verwaltet. Wenn Linked Clones verbleiben, müssen Sie diese löschen.

- Machen Sie sich mit der Konfiguration von View Composer in Horizon Administrator vertraut. Siehe [Konfigurieren von View Composer-Einstellungen](#) und [Konfigurieren von View Composer-Domänen](#).

Verfahren

- 1 Entfernen Sie View Composer in Horizon Administrator aus Horizon Administrator.
 - a Wählen Sie **View-Konfiguration > Server**.
 - b Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz aus, die mit dem View Composer-Dienst verknüpft ist, und klicken Sie auf **Bearbeiten**.
 - c Klicken Sie im Fensterbereich „View Composer Server-Einstellungen“ auf **Bearbeiten**.
 - d Wählen Sie **View Composer nicht verwenden** aus und klicken Sie auf **OK**.
- 2 Deinstallieren Sie den VMware Horizon View Composer-Dienst von der aktuellen Maschine.
- 3 Installieren Sie den VMware Horizon View Composer-Dienst auf der neuen Maschine.
 Konfigurieren Sie während der Installation View Composer, um eine Verbindung zum DSN der ursprünglichen oder neuen View Composer-Datenbank herzustellen.
- 4 Konfigurieren Sie auf der neuen Maschine ein TLS-Serverzertifikat für View Composer.
 Möglicherweise können Sie das Zertifikat kopieren, das auf der ursprünglichen Maschine für View Composer installiert war, oder Sie können ein neues Zertifikat installieren.
- 5 Konfigurieren Sie in Horizon Administrator die neuen View Composer-Einstellungen.
 - a Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
 - b Wählen Sie auf der Registerkarte **vCenter Server** die vCenter Server-Instanz aus, die mit diesem View Composer-Dienst verknüpft ist, und klicken Sie auf **Bearbeiten**.
 - c Klicken Sie im Fensterbereich „View Composer Server-Einstellungen,“ auf **Bearbeiten**.
 - d Geben Sie die neuen View Composer-Einstellungen an.
 Wenn Sie View Composer mit vCenter Server auf der neuen Maschine installieren, wählen Sie **View Composer wurde zusammen mit vCenter Server installiert** aus.
 Wenn Sie View Composer auf einer eigenständigen Maschine installieren, wählen Sie **Eigenständiger View Composer Server** aus und geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der View Composer-Maschine sowie den Benutzernamen und das Kennwort des View Composer-Benutzers an.
 - e Klicken Sie im Bereich „Domänen“ auf **Serverinformationen bestätigen** und fügen Sie nach Bedarf View Composer-Domänen hinzu bzw. bearbeiten Sie diese.
 - f Klicken Sie auf **OK**.

Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln

Zur Verwendung einer vorhandenen View Composer-Datenbank müssen Sie den RSA-Schlüsselcontainer zwischen den Maschinen migrieren. Sie migrieren den RSA-Schlüsselcontainer mit dem Tool für die ASP.NET IIS-Registrierung, das zum Lieferumfang von Microsoft .NET Framework gehört.

Voraussetzungen

Laden Sie .NET Framework herunter und lesen Sie die Informationen über das Tool für die ASP.NET IIS-Registrierung. Besuchen Sie <http://www.microsoft.com/net>.

Verfahren

- 1 Installieren Sie .NET Framework auf der physischen oder virtuellen Maschine, auf der der mit der vorhandenen Datenbank verknüpfte VMware Horizon View Composer-Dienst installiert ist.
- 2 Installieren Sie .NET Framework auf der Zielmaschine, auf der Sie den neuen VMware Horizon View Composer-Dienst installieren möchten.

Nächste Schritte

Migrieren Sie den RSA-Schlüsselcontainer auf die Zielmaschine. Siehe [Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst](#).

Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst

Zur Verwendung einer vorhandenen View Composer-Datenbank müssen Sie den RSA-Schlüsselcontainer von der physischen oder virtuellen Quellmaschine, auf der der vorhandene VMware Horizon View Composer-Dienst installiert ist, auf die Maschine migrieren, auf der Sie den neuen VMware Horizon View Composer-Dienst installieren möchten.

Sie müssen diese Schritte ausführen, bevor Sie den neuen VMware Horizon View Composer-Dienst installieren.

Voraussetzungen

Stellen Sie sicher, dass Microsoft .NET Framework und das Tool für die ASP.NET IIS-Registrierung auf den Quell- und Zielmaschinen installiert sind. Siehe [Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln](#).

Verfahren

- 1 Öffnen Sie auf der Quellmaschine mit dem vorhandenen VMware Horizon View Composer-Dienst eine Eingabeaufforderung und navigieren Sie zum Verzeichnis %windir%\Microsoft.NET\Framework\v2.0.xxxx.

- 2 Geben Sie den Befehl `aspnet_regiis` ein, um das RSA-Schlüsselpaar in einer lokalen Datei zu speichern.

```
aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
```

Das Tool für die ASP.NET IIS-Registrierung exportiert das RSA-Schlüsselpaar aus privatem und öffentlichem Schlüssel vom Container SviKeyContainer in die Datei `keys.xml` und speichert die Datei lokal.

- 3 Kopieren Sie die Datei `keys.xml` auf die Zielmaschine, auf der Sie den neuen VMware Horizon View Composer-Dienst installieren möchten.

- 4 Öffnen Sie auf der Zielfmaschine eine Eingabeaufforderung und navigieren Sie zum Verzeichnis %windir%\Microsoft.NET\Framework\v2.0xxxxx.
- 5 Geben Sie den Befehl `aspnet_regiis` ein, um die RSA-Schlüsselpaardaten zu migrieren.

`aspnet_regiis -pi "SviKeyContainer" "Pfad\keys.xml" -exp`

Hierbei steht *Pfad* für den Pfad zur exportierten Datei.

Die Option `-exp` erstellt ein exportierbares Schlüsselpaar. Wenn eine künftige Migration erforderlich ist, können die Schlüssel von dieser Maschine exportiert und auf eine andere Maschine importiert werden. Wenn Sie die Schlüssel zuvor auf diese Maschine migriert haben, ohne die Option `-exp` zu verwenden, können Sie die Schlüssel mit der Option `-exp` erneut importieren, sodass Sie sie künftig exportieren können.

Das Registrierungstool importiert das Schlüsselpaar in den lokalen Schlüsselcontainer.

Nächste Schritte

Installieren Sie den neuen VMware Horizon View Composer-Dienst auf der Zielfmaschine. Geben Sie die Quellinformationen für die DSN- und ODBC-Daten an, die es View Composer erlauben, eine Verbindung zu den selben Datenbankinformationen herzustellen, die vom ursprünglichen VMware Horizon View Composer-Dienst verwendet wurden. Installationsanleitungen finden Sie unter „Installation von View Composer“ im Dokument *Horizon 7-Installation*.

Führen Sie die Schritte zur Migration von View Composer auf eine neue Maschine aus und verwenden Sie dieselbe Datenbank. Siehe [Migrieren von View Composer mit einer vorhandenen Datenbank](#).

Aktualisieren der Zertifikate auf einer Verbindungsserver-Instanz, einem Sicherheitsserver oder View Composer

Wenn Sie aktualisierte Server-TLS-Zertifikate oder Zwischenzertifikate erhalten, importieren Sie die Zertifikate auf jedem Verbindungsserver, Sicherheitsserver oder View Composer-Host in die Zertifikatspeicher der lokalen Windows-Computer.

Üblicherweise verlieren Serverzertifikate nach 12 Monaten ihre Gültigkeit. Stamm- und Zwischenzertifikate laufen nach 5 oder 10 Jahren ab.

Weitere Informationen zum Importieren von Server- und Zwischenzertifikaten finden Sie unter „Konfigurieren von Horizon-Verbindungsserver, Sicherheitsserver oder View Composer für die Verwendung eines neuen TLS-Zertifikats“ im Dokument *Horizon 7-Installation*.

Voraussetzungen

- Fordern Sie aktualisierte Server- und Zwischenzertifikate von der Zertifizierungsstelle an, bevor die aktuellen Zertifikate ablaufen.
- Überprüfen Sie, dass das Zertifikat-Snap-in zur MMC auf dem Windows-Server hinzugefügt wurde, auf dem die Verbindungsserver-Instanz, der Sicherheitsserver oder der VMware Horizon View Composer-Dienst installiert wurde.

Verfahren

- 1 Importieren Sie das signierte TLS-Serverzertifikat in den Zertifikatspeicher des lokalen Windows-Computers auf dem Windows-Server-Host.
 - a Importieren Sie im Zertifikat-Snap-in das Serverzertifikat in den Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate**.
 - b Wählen Sie **Schlüssel als exportierbar markieren**.
 - c Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.
- 2 Löschen Sie für den Verbindungsserver oder den Sicherheitsserver das Zertifikat „Angezeigter Name“, **vdm**, aus dem alten Zertifikat, das für den Horizon 7-Server ausgestellt wurde.
 - a Klicken Sie mit der rechten Maustaste auf das alte Zertifikat und anschließend auf **Eigenschaften**.
 - b Löschen Sie auf der Registerkarte Allgemein den Text „Angezeigter Name“, **vdm**.
- 3 Fügen Sie für den Verbindungsserver oder den Sicherheitsserver das Zertifikat „Angezeigter Name“, **vdm**, zum neuen Zertifikat, das das vorherige Zertifikat ersetzt, hinzu.
 - a Klicken Sie mit der rechten Maustaste auf das neue Zertifikat und anschließend auf **Eigenschaften**.
 - b Geben Sie auf der Registerkarte Allgemein im Feld „Angezeigter Name“ **vdm** ein.
 - c Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
- 4 Führen Sie für ein Serverzertifikat, das für View Composer ausgestellt wurde, das Dienstprogramm SviConfig ReplaceCertificate aus, um das neue Zertifikat an den Port zu binden, der von View Composer verwendet wird.

Dieses Dienstprogramm ersetzt die alte Zertifikatsbindung durch die neue Zertifikatsbindung.

- a Halten Sie den VMware Horizon View Composer-Dienst an.
- b Öffnen Sie eine Windows-Eingabeaufforderung und navigieren Sie zur ausführbaren SviConfig-Datei.

Die Datei befindet sich im Ordner der View Composer-Anwendung. Der Standardpfad lautet C:\Programme (x86)\VMware\VMware View Composer\sviconfig.exe.

- c Geben Sie den Befehl SviConfig ReplaceCertificate ein. Beispiel:

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

Das Dienstprogramm zeigt eine nummerierte Liste mit TLS-Zertifikaten an, die im Windows-Zertifikatspeicher des lokalen Computers vorhanden sind.

- d Zum Auswählen eines Zertifikats geben Sie die Nummer des Zertifikats ein und drücken Sie die Eingabetaste.

- 5 Wenn für einen Verbindungsserver, Sicherheitsserver oder View Composer-Host Zwischenzertifikate ausgestellt werden, importieren Sie das neueste Update der Zwischenzertifikate in den Ordner **Zertifikate (Lokaler Computer) > Zwischenzertifizierungsstellen > Zertifikate** im Windows-Zertifikatspeicher.
- 6 Starten Sie den VMware Horizon View-Verbindungsserver-, den VMware Horizon View-Sicherheitsserver-Dienst oder den VMware Horizon View Composer-Dienst neu, damit die Änderungen wirksam werden.

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 Administrator **View-Konfiguration > Produktlizenzierung und -verwendung** aus.
- 2 Klicken Sie im Fensterbereich **Programm zur Verbesserung der Benutzerfreundlichkeit auf Einstellungen bearbeiten**.
- 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 Klicken Sie auf **OK**.

Verwalten von ThinApp-Anwendungen in Horizon Administrator

9

Sie können Horizon Administrator zum Verteilen und Verwalten von Anwendungen verwenden, die mit VMware ThinApp verpackt wurden. Die Verwaltung von ThinApp-Anwendungen in Horizon Administrator umfasst das Erfassen und Speichern von Anwendungspaketen, das Hinzufügen von ThinApp-Anwendungen zu Horizon Administrator und das Zuweisen von ThinApp-Anwendungen zu Computern und Desktop-Pools.

Zur Verwendung der ThinApp-Verwaltungsfunktion in Horizon Administrator benötigen Sie eine Lizenz.

Wichtig Wenn Sie ThinApps nicht verteilen, indem Sie sie Computern und Desktop-Pools, sondern stattdessen Active Directory-Benutzern und -Gruppen zuweisen, können Sie VMware Identity Manager verwenden.

Dieses Kapitel enthält die folgenden Themen:

- [Horizon 7-Anforderungen für ThinApp-Anwendungen](#)
- [Erfassen und Speichern von Anwendungspaketen](#)
- [Zuweisen von ThinApp-Anwendungen zu Maschinen und Desktop-Pools](#)
- [Verwalten von ThinApp-Anwendungen in Horizon Administrator](#)
- [Überwachen von und Fehlerbehebung bei ThinApp-Anwendungen in Horizon Administrator](#)
- [ThinApp-Konfigurationsbeispiel](#)

Horizon 7-Anforderungen für ThinApp-Anwendungen

Beim Erfassen und Speichern von ThinApp-Anwendungen zur Verteilung an Remote-Desktops in Horizon Administrator müssen bestimmte Anforderungen erfüllt werden.

- Sie müssen Ihre Anwendungen als MSI-Pakete (Microsoft Installation) paketieren.
- Zum Erstellen oder erneuten Paketieren der MSI-Pakete benötigen Sie ThinApp 4.6 oder höher.
- Sie müssen die MSI-Pakete auf einer Windows-Netzwerkfreigabe speichern, die sich in einer Active Directory-Domäne befindet, auf die Ihr Verbindungsserver-Host und Remote-Desktops zugreifen können. Der Dateiserver muss Authentifizierung und Dateiberechtigungen unterstützen, die auf Computerkonten basieren.

- Sie müssen die Datei- und Freigabeberechtigungen auf der Netzwerkfreigabe festlegen, auf der sich die MSI-Pakete befinden, um der integrierten Active Directory-Gruppe Domain Computers (Domänencomputer) Lesezugriff zu gewähren. Wenn Sie ThinApp-Anwendungen an Domänencontroller verteilen möchten, müssen Sie der integrierten Active Directory-Gruppe Domain Controllers (Domänencontroller) Lesezugriff gewähren.
- Wenn Sie das Streaming von ThinApp-Anwendungspaketen durch Benutzer zulassen möchten, müssen Sie die NTFS-Berechtigung der Netzwerkfreigabe, auf der die ThinApp-Pakete gehostet werden, auf Read&Execute (Lesen & Ausführen) festlegen.
- Stellen Sie sicher, dass ein nicht zusammenhängender Namespace Domänenmitgliedscomputer nicht daran hindert, auf die Netzwerkfreigabe zuzugreifen, auf der die MSI-Pakete gehostet werden. Ein nicht zusammenhängender Namespace liegt vor, wenn sich der Name einer Active Directory-Domäne vom DNS-Namespace unterscheidet, der von den Computern in dieser Domäne verwendet wird. Weitere Informationen finden Sie im VMware Knowledge Base-Artikel 1023309.
- Zur Ausführung gestreamter ThinApp-Anwendungen auf Remote-Desktops müssen Benutzer auf die Netzwerkfreigabe mit den MSI-Paketen zugreifen können.

Erfassen und Speichern von Anwendungspaketen

ThinApp ermöglicht die Anwendungsvirtualisierung, indem eine Anwendung von dem zugrunde liegenden Betriebssystem und dessen Bibliotheken und Framework entkoppelt und anschließend in eine ausführbare Datei gebündelt wird. Diese wird als Anwendungspaket bezeichnet.

Um ThinApp-Anwendungen in Horizon Administrator zu verwalten, muss der ThinApp **Setup Capture**-Assistent zum Erfassen und Erstellen von Anwendungspaketen im MSI-Format sowie zum Speichern der MSI-Pakete in einem Anwendungs-Repository verwendet werden.

Bei einem Anwendungs-Repository handelt es sich um eine Windows-Netzwerkfreigabe. Die Netzwerkfreigabe wird über Horizon Administrator als Anwendungs-Repository registriert. Sie können auch mehrere Anwendungs-Repositorys registrieren.

Hinweis Wenn Sie über mehrere Anwendungs-Repositorys verfügen, können Sie den Lastausgleich und die Verfügbarkeit mithilfe von Drittanbieterlösungen verwalten. Horizon 7 umfasst keine Lösungen für Lastausgleich oder Verfügbarkeit.

Vollständige Informationen zu ThinApp-Funktionen und zur Verwendung des ThinApp **Setup Capture**-Assistenten finden Sie in der *Einführung in VMware ThinApp* und im *ThinApp-Benutzerhandbuch*.

Verfahren

1 Paketieren von Anwendungen

Verwenden Sie den ThinApp **Setup Capture**-Assistenten, um Ihre Anwendungen zu paketieren.

2 Erstellen einer Windows-Netzwerkfreigabe

Zum Hosten der MSI-Pakete, die in Host an Remote-Desktops und -Pools verteilt werden, müssen Sie in Horizon Administrator eine Windows-Netzwerkfreigabe erstellen.

3 Registrieren eines Anwendungs-Repositorys

Sie müssen die Windows-Netzwerkfreigabe registrieren, die als Anwendungs-Repository für Ihre MSI-Pakete in Horizon Administrator verwendet wird.

4 Hinzufügen von ThinApp-Anwendungen zu Horizon Administrator

Sie fügen ThinApp-Anwendungen zu Horizon Administrator hinzu, indem Sie ein Anwendungs-Repository durchsuchen und ThinApp-Anwendungen auswählen. Nach dem Hinzufügen einer ThinApp-Anwendung zu Horizon Administrator kann die Anwendung Computern oder Desktop-Pools zugewiesen werden.

5 Erstellen einer ThinApp-Vorlage

Sie können in Horizon Administrator eine Vorlage erstellen, um eine Gruppe aus ThinApp-Anwendungen anzugeben. Mithilfe von Vorlagen können Sie Anwendungen nach Funktion, Anbieter oder einer beliebigen anderen logischen Gruppierung zusammenfassen, die in Ihrer Organisation sinnvoll ist.

Paketieren von Anwendungen

Verwenden Sie den ThinApp **Setup Capture**-Assistenten, um Ihre Anwendungen zu paketieren.

Voraussetzungen

- Laden Sie die ThinApp-Software von der Seite <http://www.vmware.com/products/thinapp> herunter und installieren Sie sie auf einem Computer, auf dem noch keine Version dieser Software vorhanden ist. View unterstützt ThinApp 4.6 und höher.
- Machen Sie sich mit den ThinApp-Softwareanforderungen und den Anweisungen zur Paketerstellung im *ThinApp-Benutzerhandbuch* vertraut.

Verfahren

- 1 Starten Sie den ThinApp **Setup Capture**-Assistenten und folgen Sie dessen Anweisungen.
- 2 Wenn Sie der ThinApp **Setup Capture**-Assistent auffordert, einen Projektspeicherort anzugeben, wählen Sie **MSI-Paket erstellen**.
- 3 Wenn Sie ein Streaming der Anwendung auf Remote-Desktops planen, legen Sie die MSIStreaming-Eigenschaft in der Datei `package.ini` auf den Wert 1 fest.

```
MSIStreaming=1
```

Ergebnisse

Der ThinApp **Setup Capture**-Assistent kapselt die Anwendung, alle zum Ausführen der Anwendung erforderlichen Komponenten und die Anwendung selbst in einem MSI-Paket.

Nächste Schritte

Erstellen Sie zum Speichern der MSI-Pakete eine Windows-Netzwerkfreigabe.

Erstellen einer Windows-Netzwerkfreigabe

Zum Hosten der MSI-Pakete, die in Host an Remote-Desktops und -Pools verteilt werden, müssen Sie in Horizon Administrator eine Windows-Netzwerkfreigabe erstellen.

Voraussetzungen

- Verwenden Sie den ThinApp **Setup Capture**-Assistenten, um die Anwendungen zu paketieren.
- Stellen Sie sicher, dass die Netzwerkfreigabe die Horizon 7-Anforderungen zum Speichern von ThinApp-Anwendungen erfüllt. Weitere Informationen finden Sie unter [Horizon 7-Anforderungen für ThinApp-Anwendungen](#).

Verfahren

- 1 Erstellen Sie eine Ordnerfreigabe auf einem Computer in einer Active Directory-Domäne, auf die Ihr Verbindungsserver-Host und Remote-Desktops zugreifen können.
- 2 Konfigurieren Sie die Datei- und Freigabeberechtigungen für die Ordnerfreigabe, um der integrierten Active Directory-Gruppe „Domain Computers“ (Domänencomputer) Lesezugriff zu gewähren.
- 3 Wenn Sie Domänencontrollern ThinApp-Anwendungen zuweisen möchten, müssen Sie der integrierten Active Directory-Gruppe Domain Controllers (Domänencontroller) Lesezugriff gewähren.
- 4 Wenn Sie das Streaming von ThinApp-Anwendungspaketen planen, legen Sie die NTFS-Berechtigung der Netzwerkfreigabe, auf der die ThinApp-Pakete gehostet werden, auf Read&Execute (Lesen & Ausführen) für die Benutzer fest.
- 5 Kopieren Sie die MSI-Pakete in den freigegebenen Ordner.

Nächste Schritte

Registrieren Sie die Windows-Netzwerkfreigabe als Anwendungs-Repository in Horizon Administrator.

Registrieren eines Anwendungs-Repositorys

Sie müssen die Windows-Netzwerkfreigabe registrieren, die als Anwendungs-Repository für Ihre MSI-Pakete in Horizon Administrator verwendet wird.

Sie können auch mehrere Anwendungs-Repositorys registrieren.

Voraussetzungen

Erstellen Sie eine Windows-Netzwerkfreigabe.

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > ThinApp-Konfiguration** und klicken Sie auf **Repository hinzufügen**.
- 2 Geben Sie in das Textfeld **Anzeigename** einen Anzeigenamen für das Anwendungs-Repository ein.

- 3 Geben Sie in das Textfeld **Freigabepfad** den Pfad zur Windows-Netzwerkfreigabe mit Ihren Anwendungspaketen ein.

Der Pfad zur Netzwerkfreigabe muss in der Form `\\Computername_des_Servers\Freigabename` angegeben werden, wobei `Computername_des_Servers` den DNS-Namen des Servercomputers angibt. Geben Sie keine IP-Adresse an.

Beispiel: `\\Server.Domaene.com\MSIPackages`

- 4 Klicken Sie auf **Speichern**, um das Anwendungs-Repository in Horizon Administrator zu registrieren.

Hinzufügen von ThinApp-Anwendungen zu Horizon Administrator

Sie fügen ThinApp-Anwendungen zu Horizon Administrator hinzu, indem Sie ein Anwendungs-Repository durchsuchen und ThinApp-Anwendungen auswählen. Nach dem Hinzufügen einer ThinApp-Anwendung zu Horizon Administrator kann die Anwendung Computern oder Desktop-Pools zugewiesen werden.

Voraussetzungen

Registrieren Sie ein Anwendungs-Repository mit Horizon Administrator.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** aus.
- 2 Klicken Sie auf der Registerkarte **Übersicht** auf **Neue ThinApps untersuchen**.
- 3 Wählen Sie ein Anwendungs-Repository und einen Ordner für die Suche aus und klicken Sie auf **Weiter**.

Wenn das Anwendungs-Repository Unterordner enthält, können Sie den Stammordner erweitern und einen Unterordner auswählen.
- 4 Wählen Sie die ThinApp-Anwendungen, die zu Horizon Administrator hinzugefügt werden sollen.

Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere ThinApp-Anwendungen auszuwählen.
- 5 Klicken Sie auf **Durchsuchen**, um die ausgewählten MSI-Pakete zu durchsuchen.

Wenn die Suche angehalten werden muss, klicken Sie auf **Suche beenden**.

Horizon Administrator zeigt den Status der einzelnen Suchvorgänge und die Anzahl an ThinApp-Anwendungen an, die zu Horizon Administrator hinzugefügt wurden. Bei Auswahl einer Anwendung, die sich bereits in Horizon Administrator befindet, wird diese nicht erneut hinzugefügt.
- 6 Klicken Sie auf **Fertigstellen**.

Die neuen ThinApp-Anwendungen werden auf der Registerkarte **Übersicht** angezeigt.

Nächste Schritte

(Optional) Erstellen Sie ThinApp-Vorlagen.

Erstellen einer ThinApp-Vorlage

Sie können in Horizon Administrator eine Vorlage erstellen, um eine Gruppe aus ThinApp-Anwendungen anzugeben. Mithilfe von Vorlagen können Sie Anwendungen nach Funktion, Anbieter oder einer beliebigen anderen logischen Gruppierung zusammenfassen, die in Ihrer Organisation sinnvoll ist.

Mit ThinApp-Vorlagen lässt sich die Verteilung mehrerer Anwendungen optimieren. Wenn Sie einem Computer oder Desktop-Pool eine ThinApp-Vorlage zuweisen, installiert Horizon Administrator alle gegenwärtig in der Vorlage enthaltenen Anwendungen.

Das Erstellen von ThinApp-Vorlagen ist optional.

Hinweis Wenn Sie eine Anwendung zu einer ThinApp-Vorlage hinzufügen, nachdem die Vorlage einem Computer oder Desktop-Pool zugewiesen wurde, weist Horizon Administrator die neue Anwendung nicht automatisch dem Computer oder Desktop-Pool zu. Beim Entfernen einer Anwendung aus einer ThinApp-Vorlage, die zuvor einem Computer oder Desktop-Pool zugewiesen wurde, wird die Zuweisung der Anwendung zum Computer oder Desktop-Pool beibehalten.

Voraussetzungen

Fügen Sie ausgewählte ThinApp-Anwendungen zu Horizon Administrator hinzu.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** aus und klicken Sie auf **Neue Vorlage**.
- 2 Geben Sie den Namen der Vorlage ein und klicken Sie auf **Hinzufügen**.
Alle verfügbaren ThinApp-Anwendungen werden in der Tabelle angezeigt.
- 3 Um nach einer bestimmten ThinApp-Anwendung zu suchen, geben Sie den Namen der Anwendung in das Textfeld **Suchen** ein und klicken Sie auf **Suchen**.
- 4 Wählen Sie die ThinApp-Anwendungen aus, die in die Vorlage aufgenommen werden sollen, und klicken Sie auf **Hinzufügen**.
Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere Anwendungen auszuwählen.
- 5 Klicken Sie auf **OK**, um die Vorlage zu speichern.

Zuweisen von ThinApp-Anwendungen zu Maschinen und Desktop-Pools

Um eine ThinApp-Anwendung auf einem Remote-Desktop zu installieren, weisen Sie die ThinApp-Anwendung über Horizon Administrator einer Maschine oder einem Desktop-Pool zu.

Wenn Sie einer Maschine eine ThinApp-Anwendung zuweisen, beginnt Horizon Administrator wenige Minuten später mit der Installation der Anwendung auf der virtuellen Maschine. Wenn Sie einem Desktop-Pool eine ThinApp-Anwendung zuweisen, beginnt Horizon Administrator mit der Installation der Anwendung, sobald sich ein Benutzer erstmalig bei einem Remote-Desktop im Pool anmeldet.

Streaming	Horizon Administrator installiert eine Verknüpfung mit der ThinApp-Anwendung auf dem Remote-Desktop. Die Verknüpfung weist auf die ThinApp-Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung gestreamter ThinApp-Anwendungen müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Vollständig	Horizon Administrator installiert die vollständige ThinApp-Anwendung auf dem lokalen Dateisystem.

Die Installationsdauer einer ThinApp-Anwendung hängt von der Größe der Anwendung ab.

Wichtig Sie können VM-basierten Desktops und automatisierten Desktop-Pools oder manuellen Pools, die vCenter Server-VMs enthalten, ThinApp-Anwendungen zuweisen. Sie können allerdings veröffentlichten Desktops oder herkömmlichen PCs keine ThinApp-Anwendungen zuweisen.

- [Empfohlene Vorgehensweisen für die Zuweisung von ThinApp-Anwendungen](#)
Befolgen Sie beim Zuweisen von ThinApp-Anwendungen zu Computern und Desktop-Pools die empfohlenen Vorgehensweisen.
- [Zuweisen einer ThinApp-Anwendung zu mehreren Computern](#)
Sie können einem oder mehreren Computern eine bestimmte ThinApp zuweisen.
- [Zuweisen mehrerer ThinApp-Anwendungen zu einem Computer](#)
Sie können einem bestimmten Computer eine oder mehrere ThinApp-Anwendungen zuweisen.
- [Zuweisen einer ThinApp-Anwendung zu mehreren Desktop-Pools](#)
Sie können einem oder mehreren Desktop-Pools eine bestimmte ThinApp-Anwendung zuweisen.
- [Zuweisen mehrerer ThinApp-Anwendungen zu einem Desktop-Pool](#)
Sie können einem bestimmten Desktop-Pool eine oder mehrere ThinApp-Anwendungen zuweisen.
- [Zuweisen einer ThinApp-Vorlage zu einer Maschine oder zu einem Desktop-Pool](#)
Um die Verteilung mehrerer ThinApp-Anwendungen zu optimieren, können Sie einer Maschine oder einem Desktop-Pool eine ThinApp-Vorlage zuweisen.
- [Anzeigen von ThinApp-Anwendungszuweisungen](#)
Sie können alle Maschinen und Desktop-Pools anzeigen, denen gegenwärtig eine bestimmte ThinApp-Anwendung zugewiesen ist. Sie können ebenso alle ThinApp-Anwendungen anzeigen, die einer bestimmten Maschine oder einem bestimmten Desktop-Pool zugewiesen sind.
- [Anzeigen von MSI-Paketinformationen](#)
Nach dem Hinzufügen einer ThinApp-Anwendung zu Horizon Administrator können Sie Informationen zu den MSI-Paketen anzeigen.

Empfohlene Vorgehensweisen für die Zuweisung von ThinApp-Anwendungen

Befolgen Sie beim Zuweisen von ThinApp-Anwendungen zu Computern und Desktop-Pools die empfohlenen Vorgehensweisen.

- Zur Installation einer ThinApp-Anwendung auf einem bestimmten Remote-Desktop weisen Sie die Anwendung der virtuellen Maschine zu, die den Desktop hostet. Wenn Sie eine allgemeine Benennungskonvention für Ihre Computer verwenden, können Sie Anwendungen mithilfe von Computer-Zuweisungen schnell auf alle Computer mit derselben Benennungskonvention verteilen.
- Um eine ThinApp-Anwendung auf allen Computern innerhalb eines Desktop-Pools zu installieren, weisen Sie die Anwendung dem Desktop-Pool zu. Wenn Sie Desktop-Pools nach Abteilung oder Benutzertyp organisieren, können Sie Anwendungen mithilfe von Pool-Zuweisungen schnell an bestimmte Abteilungen oder Benutzer verteilen. Wenn Sie beispielsweise über einen Desktop-Pool für Benutzer in der Buchhaltungsabteilung verfügen, können Sie dieselbe Anwendung an alle Benutzer in der Buchhaltungsabteilung verteilen, indem Sie dem Buchhaltungspool eine Anwendung zuweisen.
- Zum Optimieren der Verteilung mehrerer ThinApp-Anwendungen nehmen Sie die Anwendungen in eine ThinApp-Vorlage auf. Wenn Sie einem Computer oder Desktop-Pool eine ThinApp-Vorlage zuweisen, installiert Horizon Administrator alle gegenwärtig in der Vorlage enthaltenen Anwendungen.
- Weisen Sie einem Computer oder Desktop-Pool keine ThinApp-Vorlagen mit ThinApp-Anwendungen zu, die dem Computer oder Desktop-Pool bereits zugewiesen sind. Weisen Sie einem Computer oder Desktop-Pool eine ThinApp-Vorlage ferner nicht mehrfach mit unterschiedlichem Installationstyp zu. Horizon Administrator gibt in beiden Fällen ThinApp-Zuweisungsfehler zurück.

Zuweisen einer ThinApp-Anwendung zu mehreren Computern

Sie können einem oder mehreren Computern eine bestimmte ThinApp zuweisen.

Voraussetzungen

Prüfen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu Horizon Administrator hinzu. Siehe [Hinzufügen von ThinApp-Anwendungen zu Horizon Administrator](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** und anschließend die ThinApp-Anwendung aus.

- 2 Wählen Sie im Dropdown-Menü **Zuweisung hinzufügen** die Option **Computer zuweisen**.

Die Computer, denen die ThinApp-Anwendung noch nicht zugewiesen ist, werden in der Tabelle angezeigt.

Option	Aktion
Suchen nach einem bestimmten Computer	Geben Sie den Namen des Computers in das Textfeld Suchen ein und klicken Sie auf Suchen .
Suchen nach allen Computern mit derselben Benennungskonvention	Geben Sie einen Teil des Computer-Namens in das Textfeld Suchen ein und klicken Sie auf Suchen .

- 3 Wählen Sie die Computer aus, denen die ThinApp-Anwendung zugewiesen werden soll, und klicken Sie auf **Hinzufügen**.

Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere Computer auszuwählen.

- 4 Wählen Sie einen Installationstyp und klicken Sie auf **OK**.

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Computer. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Vollständig	Installiert die vollständige Anwendung auf dem lokalen Dateisystem des Computers.

Einige ThinApp-Anwendungen bieten keine Unterstützung für beide Installationstypen. Die Art und Weise, wie das Anwendungspaket erstellt wurde, bestimmt die verfügbaren Installationstypen.

Ergebnisse

Horizon Administrator beginnt wenige Minuten später mit der Installation der ThinApp-Anwendung. Nach der Installation steht die Anwendung allen Benutzern der Desktops zur Verfügung, die von den virtuellen Maschinen gehostet werden.

Zuweisen mehrerer ThinApp-Anwendungen zu einem Computer

Sie können einem bestimmten Computer eine oder mehrere ThinApp-Anwendungen zuweisen.

Voraussetzungen

Prüfen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu Horizon Administrator hinzu. Siehe [Hinzufügen von ThinApp-Anwendungen zu Horizon Administrator](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Ressourcen > Computer** aus und doppelklicken Sie in der Spalte „Computer“ auf den Namen des Computers.

- 2 Klicken Sie auf der Registerkarte **Übersicht** im ThinApps-Bereich auf **Zuweisung hinzufügen**.

Die ThinApp-Anwendungen, die dem Computer noch nicht zugewiesen sind, werden in der Tabelle angezeigt.

- 3 Um nach einer bestimmten Anwendung zu suchen, geben Sie den Namen der Anwendung in das Textfeld **Suchen** ein und klicken Sie auf **Suchen**.
- 4 Wählen Sie eine ThinApp-Anwendung aus, die dem Computer zugewiesen werden soll, und klicken Sie auf **Hinzufügen**.

Wiederholen Sie diesen Schritt, um mehrere Anwendungen hinzuzufügen.

- 5 Wählen Sie einen Installationstyp und klicken Sie auf **OK**.

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Computer. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Vollständig	Installiert die vollständige Anwendung auf dem lokalen Dateisystem des Computers.

Einige ThinApp-Anwendungen bieten keine Unterstützung für beide Installationstypen. Die Art und Weise, wie das Anwendungspaket erstellt wurde, bestimmt die verfügbaren Installationstypen.

Ergebnisse

Horizon Administrator beginnt wenige Minuten später mit der Installation der ThinApp-Anwendungen. Nach der Installation stehen die Anwendungen allen Benutzern des Desktops zur Verfügung, der von der virtuellen Maschine gehostet wird.

Zuweisen einer ThinApp-Anwendung zu mehreren Desktop-Pools

Sie können einem oder mehreren Desktop-Pools eine bestimmte ThinApp-Anwendung zuweisen.

Wenn Sie einem Linked-Clone-Pool eine ThinApp-Anwendung zuweisen und den Pool zu einem späteren Zeitpunkt aktualisieren, neu zusammenstellen oder neu verteilen, installiert Horizon Administrator die Anwendung erneut. Eine manuelle Neuinstallation der Anwendung ist nicht erforderlich.

Voraussetzungen

Prüfen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu Horizon Administrator hinzu. Siehe [Hinzufügen von ThinApp-Anwendungen zu Horizon Administrator](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** und anschließend die ThinApp-Anwendung aus.

- Wählen Sie die Option **Desktop-Pools zuweisen** aus dem Dropdown-Menü **Zuweisung hinzufügen** aus.

Die Desktop-Pools, denen die ThinApp-Anwendung noch nicht zugewiesen ist, werden in der Tabelle angezeigt.

Option	Aktion
Suchen nach einem bestimmten Desktop-Pool	Geben Sie den Namen des Desktop-Pools in das Textfeld Suchen ein und klicken Sie auf Suchen .
Suchen nach allen Desktop-Pools mit derselben Benennungskonvention	Geben Sie einen Teil des Desktop-Pool-Namens in das Textfeld Suchen ein und klicken Sie auf Suchen .

- Wählen Sie die Desktop-Pools aus, denen die ThinApp-Anwendung zugewiesen werden soll, und klicken Sie auf **Hinzufügen**.

Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere Desktop-Pools auszuwählen.

- Wählen Sie einen Installationstyp und klicken Sie auf **OK**.

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Computer. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Vollständig	Installiert die vollständige Anwendung auf dem lokalen Dateisystem des Computers.

Einige ThinApp-Anwendungen bieten keine Unterstützung für beide Installationstypen. Die Art und Weise, wie das Anwendungspaket erstellt wurde, bestimmt die verfügbaren Installationstypen.

Ergebnisse

Horizon Administrator beginnt mit der Installation der ThinApp-Anwendung, sobald sich ein Benutzer erstmalig an einem Desktop im Pool anmeldet. Nach der Installation steht die Anwendung allen Benutzern des Desktop-Pools zur Verfügung.

Zuweisen mehrerer ThinApp-Anwendungen zu einem Desktop-Pool

Sie können einem bestimmten Desktop-Pool eine oder mehrere ThinApp-Anwendungen zuweisen.

Wenn Sie einem Linked-Clone-Pool eine ThinApp-Anwendung zuweisen und den Pool zu einem späteren Zeitpunkt aktualisieren, neu zusammenstellen oder neu verteilen, installiert Horizon Administrator die Anwendung erneut. Eine manuelle Neuinstallation der Anwendung ist nicht erforderlich.

Voraussetzungen

Prüfen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu Horizon Administrator hinzu. Siehe [Hinzufügen von ThinApp-Anwendungen zu Horizon Administrator](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > Desktop-Pools** und doppelklicken Sie auf die Pool-ID.

- 2 Klicken Sie auf der Registerkarte **Bestandsliste** auf **ThinApps** und anschließend auf **Zuweisung hinzufügen**.

Die ThinApp-Anwendungen, die dem Pool noch nicht zugewiesen sind, werden in der Tabelle angezeigt.

- 3 Um nach einer bestimmten Anwendung zu suchen, geben Sie den Namen der ThinApp-Anwendung in das Textfeld **Suchen** ein und klicken Sie auf **Suchen**.

- 4 Wählen Sie eine ThinApp-Anwendung aus, die dem Pool zugewiesen werden soll, und klicken Sie auf **Hinzufügen**.

Wiederholen Sie diesen Schritt, um mehrere Anwendungen auszuwählen.

- 5 Wählen Sie einen Installationstyp und klicken Sie auf **OK**.

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Computer. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Vollständig	Installiert die vollständige Anwendung auf dem lokalen Dateisystem des Computers.

Einige ThinApp-Anwendungen bieten keine Unterstützung für beide Installationstypen. Die Art und Weise, wie das Anwendungspaket erstellt wurde, bestimmt die verfügbaren Installationstypen.

Ergebnisse

Horizon Administrator beginnt mit der Installation der ThinApp-Anwendungen, sobald sich ein Benutzer erstmalig an einem Desktop im Pool anmeldet. Nach der Installation stehen die Anwendungen allen Benutzern des Desktop-Pools zur Verfügung.

Zuweisen einer ThinApp-Vorlage zu einer Maschine oder zu einem Desktop-Pool

Um die Verteilung mehrerer ThinApp-Anwendungen zu optimieren, können Sie einer Maschine oder einem Desktop-Pool eine ThinApp-Vorlage zuweisen.

Wenn Sie einer Maschine oder einem Desktop-Pool eine ThinApp-Vorlage zuweisen, installiert Horizon Administrator die gegenwärtig in der Vorlage enthaltenen ThinApp-Anwendungen.

Voraussetzungen

Erstellen Sie eine ThinApp-Vorlage. Siehe [Erstellen einer ThinApp-Vorlage](#).

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** aus.
- 2 Wählen Sie die ThinApp-Vorlage.
- 3 Wählen Sie die Option **Computer zuweisen** oder **Desktop-Pools zuweisen** aus dem Dropdown-Menü **Zuweisung hinzufügen** aus.

Sämtliche Maschinen oder Desktop-Pools werden in der Tabelle angezeigt.

Option	Aktion
Suchen nach einer bestimmten Maschine oder einem bestimmten Desktop-Pool	Geben Sie den Namen der Maschine oder des Desktop-Pools in das Textfeld Suchen ein und klicken Sie auf Suchen .
Suchen nach allen Maschinen oder Desktop-Pools mit derselben Benennungskonvention	Geben Sie einen Teil des Maschinen- oder Desktop-Pool-Namens in das Textfeld Suchen ein und klicken Sie auf Suchen .

- 4 Wählen Sie die Maschinen oder Desktop-Pools aus, denen die ThinApp-Vorlage zugewiesen werden soll, und klicken Sie auf **Hinzufügen**.

Wiederholen Sie diesen Schritt, um mehrere Maschinen oder Desktop-Pools auszuwählen.

- 5 Wählen Sie einen Installationstyp und klicken Sie auf **OK**.

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Computer. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Vollständig	Installiert die vollständige Anwendung auf dem lokalen Dateisystem des Computers.

Einige ThinApp-Anwendungen bieten keine Unterstützung für beide Installationstypen. Die Art und Weise, wie das Anwendungspaket erstellt wurde, bestimmt die verfügbaren Installationstypen.

Ergebnisse

Wenn Sie einer Maschine eine ThinApp-Vorlage zuweisen, beginnt Horizon Administrator wenige Minuten später mit der Installation der in der Vorlage enthaltenen Anwendungen. Wenn Sie einem Desktop-Pool eine ThinApp-Vorlage zuweisen, beginnt Horizon Administrator mit der Installation der in der Vorlage enthaltenen Anwendungen, sobald sich ein Benutzer erstmalig bei einem Remote-Desktop im Desktop-Pool anmeldet. Nach der Installation stehen die Anwendungen allen Benutzern der Maschine bzw. des Desktop-Pools zur Verfügung.

Wenn eine ThinApp-Vorlage eine Anwendung enthält, die der Maschine oder dem Desktop-Pool bereits zugewiesen ist, gibt Horizon Administrator einen Zuweisungsfehler für die Anwendung zurück.

Anzeigen von ThinApp-Anwendungszuweisungen

Sie können alle Maschinen und Desktop-Pools anzeigen, denen gegenwärtig eine bestimmte ThinApp-Anwendung zugewiesen ist. Sie können ebenso alle ThinApp-Anwendungen anzeigen, die einer bestimmten Maschine oder einem bestimmten Desktop-Pool zugewiesen sind.

Voraussetzungen

Machen Sie sich mit den verschiedenen ThinApp-Installationsstatuswerten unter [Installationsstatuswerte für ThinApp-Anwendungen](#) vertraut.

Verfahren

- ◆ Wählen Sie die ThinApp-Anwendungszuweisungen, die Sie anzeigen möchten.

Option	Aktion
Anzeigen aller Maschinen und Desktop-Pools, denen gegenwärtig eine bestimmte ThinApp-Anwendung zugewiesen ist	<p>Wählen Sie Katalog > ThinApps aus und doppelklicken Sie auf den Namen der ThinApp-Anwendung.</p> <p>Auf der Registerkarte Zuweisungen werden die Maschinen und Desktop-Pools angezeigt, denen die Anwendung gegenwärtig zugewiesen ist (einschließlich Installationstyp).</p> <p>Die Registerkarte Maschinen zeigt die Maschinen, die gegenwärtig mit der Anwendung verknüpft sind (einschließlich Installationsstatus).</p> <p>Hinweis Wenn Sie einem Pool eine ThinApp-Anwendung zuweisen, werden die Maschinen im Pool auf der Registerkarte Maschinen erst angezeigt, nachdem die Anwendung installiert ist.</p>
Anzeigen aller ThinApp-Anwendungen, die einer bestimmten Maschine zugewiesen sind	<p>Wählen Sie Ressourcen > Computer und doppelklicken Sie auf den Namen des Computers in der Spalte „Computer“.</p> <p>Im ThinApps-Bereich auf der Registerkarte Übersicht werden die einzelnen Anwendungen (einschließlich Installationsstatus) angezeigt, die der Maschine gegenwärtig zugewiesen sind.</p>
Anzeigen aller ThinApp-Anwendungen, die einem bestimmten Desktop-Pool zugewiesen sind	<p>Wählen Sie Katalog > Desktop-Pools aus, doppelklicken Sie auf die Pool-ID, wählen Sie die Registerkarte Bestand aus und klicken Sie auf ThinApps.</p> <p>Im Fensterbereich mit den ThinApp-Zuweisungen werden die einzelnen Anwendungen angezeigt, die dem Desktop-Pool gegenwärtig zugewiesen sind.</p>

Installationsstatuswerte für ThinApp-Anwendungen

Nachdem Sie einem Computer oder Pool eine ThinApp-Anwendung zugewiesen haben, zeigt Horizon Administrator den Status der Installation an.

Die folgende Tabelle zeigt eine Beschreibung der einzelnen Statuswerte.

Tabelle 9-1. Installationsstatus für ThinApp-Anwendungen

Status	Beschreibung
Zugewiesen	Die ThinApp-Anwendung wurde dem Computer zugewiesen.
Fehler bei der Installation	Als Horizon Administrator versucht hat, die ThinApp-Anwendung zu installieren, ist ein Fehler aufgetreten.

Tabelle 9-1. Installationsstatus für ThinApp-Anwendungen (Fortsetzung)

Status	Beschreibung
Fehler bei der Deinstallation	Als Horizon Administrator versucht hat, die ThinApp-Anwendung zu deinstallieren, ist ein Fehler aufgetreten.
Installiert	Die ThinApp-Anwendung wurde installiert.
Ausstehende Installation	Horizon Administrator versucht, die ThinApp-Anwendung zu installieren. Die Zuweisung einer Anwendung mit diesem Status kann nicht aufgehoben werden. Hinweis Für Computer in Desktop-Pools wird dieser Wert nicht angezeigt.
Ausstehende Deinstallation	Horizon Administrator versucht, die ThinApp-Anwendung zu deinstallieren.

Anzeigen von MSI-Paketinformationen

Nach dem Hinzufügen einer ThinApp-Anwendung zu Horizon Administrator können Sie Informationen zu den MSI-Paketen anzeigen.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** aus.
Auf der Registerkarte **Übersicht** werden die gegenwärtig verfügbaren Anwendungen sowie die Anzahl an vollständigen Zuweisungen und Streaming-Zuweisungen angezeigt.
- 2 Doppelklicken Sie in der Spalte „ThinApp“ auf den Namen der Anwendung.
- 3 Wählen Sie die Registerkarte **Übersicht**, um allgemeine Informationen zum MSI-Paket anzuzeigen.
- 4 Um detaillierte Informationen zum MSI-Paket anzuzeigen, klicken Sie auf **Paketinfo**.

Verwalten von ThinApp-Anwendungen in Horizon Administrator

Das Verwalten von ThinApp-Anwendungen in Horizon Administrator umfasst Aufgaben wie das Entfernen von ThinApp-Anwendungszuweisungen, ThinApp-Anwendungen und Anwendungs-Repositorys sowie das Ändern und Löschen von ThinApp-Vorlagen.

Hinweis Zum Aktualisieren einer ThinApp-Anwendung müssen Sie die ältere Version der Anwendung entfernen und eine neuere Version hinzufügen und zuweisen.

- **Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Computern**
Die Zuweisung zu einer bestimmten ThinApp-Anwendung kann aus einem oder mehreren Computern entfernt werden.
- **Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einer Maschine**
Sie können Zuweisungen zu einer oder mehreren ThinApp-Anwendungen aus einer bestimmten Maschine entfernen.

- [Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Desktop-Pools](#)

Sie können eine Zuweisung zu einer bestimmten ThinApp-Anwendung von einem oder mehreren Desktop-Pools entfernen.

- [Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einem Desktop-Pool](#)

Sie können eine oder mehrere ThinApp-Anwendungszuweisungen aus einem bestimmten Desktop-Pool entfernen.

- [Entfernen einer ThinApp-Anwendung aus Horizon Administrator](#)

Wenn Sie eine ThinApp-Anwendung aus Horizon Administrator entfernen, können Sie die Anwendung nicht länger Computern und Desktop-Pools zuweisen.

- [Ändern oder Löschen einer ThinApp-Vorlage](#)

Sie können Anwendungen zu einer ThinApp-Vorlage hinzufügen oder aus dieser entfernen. Eine ThinApp-Vorlage kann zudem gelöscht werden.

- [Entfernen eines Anwendungs-Repository](#)

Sie können ein Anwendungs-Repository aus Horizon Administrator entfernen.

Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Computern

Die Zuweisung zu einer bestimmten ThinApp-Anwendung kann aus einem oder mehreren Computern entfernt werden.

Voraussetzungen

Benachrichtigen Sie die Benutzer der Remote-Desktops, die von den betreffenden Computern gehostet werden, über die bevorstehende Entfernung der Anwendung.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** aus und doppelklicken Sie auf den Namen der ThinApp-Anwendung.
- 2 Wählen Sie auf der Registerkarte **Zuweisungen** einen Computer und klicken Sie auf **Zuweisung entfernen**.

Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere Computer auszuwählen.

Ergebnisse

Horizon Administrator beginnt wenige Minuten später mit der Deinstallation der ThinApp-Anwendung.

Wichtig Wenn ein Endbenutzer die ThinApp-Anwendung verwendet, während Horizon Administrator versucht, die Anwendung zu deinstallieren, schlägt die Deinstallation fehl und der Anwendungsstatus ändert sich in „Fehler bei der Deinstallation“. Wenn dieser Fehler auftritt, müssen Sie die ThinApp-Anwendungsdateien zunächst manuell auf dem Computer deinstallieren und anschließend in Horizon Administrator auf **App-Status für Desktop entfernen** klicken.

Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einer Maschine

Sie können Zuweisungen zu einer oder mehreren ThinApp-Anwendungen aus einer bestimmten Maschine entfernen.

Voraussetzungen

Benachrichtigen Sie die Benutzer des Remote-Desktops, der von der Maschine gehostet wird, dass Sie beabsichtigen, die Anwendungen zu entfernen.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Ressourcen > Computer** aus und doppelklicken Sie in der Spalte „Computer“ auf den Namen des Computers.
- 2 Wählen Sie auf der Registerkarte **Übersicht** die ThinApp-Anwendung aus und klicken Sie im ThinApps-Fensterbereich auf **Zuweisung entfernen**.

Wiederholen Sie diesen Schritt, um eine weitere Anwendungszuweisung zu entfernen.

Ergebnisse

Horizon Administrator beginnt wenige Minuten später mit der Deinstallation der ThinApp-Anwendung.

Wichtig Wenn ein Endbenutzer die ThinApp-Anwendung verwendet, während Horizon Administrator versucht, die Anwendung zu deinstallieren, schlägt die Deinstallation fehl und der Anwendungsstatus ändert sich in „Fehler bei der Deinstallation“. Wenn dieser Fehler auftritt, müssen Sie die ThinApp-Anwendungsdateien zunächst manuell auf dem Computer deinstallieren und anschließend in Horizon Administrator auf **App-Status für Desktop entfernen** klicken.

Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Desktop-Pools

Sie können eine Zuweisung zu einer bestimmten ThinApp-Anwendung von einem oder mehreren Desktop-Pools entfernen.

Voraussetzungen

Benachrichtigen Sie die Benutzer der Remote-Desktops innerhalb der Pools darüber, dass die Anwendung entfernt werden soll.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** aus und doppelklicken Sie auf den Namen der ThinApp-Anwendung.
- 2 Wählen Sie auf der Registerkarte **Zuweisungen** einen Desktop-Pool und klicken Sie auf **Zuweisung entfernen**.

Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere Desktop-Pools auszuwählen.

Ergebnisse

Horizon Administrator deinstalliert die ThinApp-Anwendung, wenn ein Benutzer sich das erste Mal bei einem Remote-Desktop im Pool anmeldet.

Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einem Desktop-Pool

Sie können eine oder mehrere ThinApp-Anwendungszuweisungen aus einem bestimmten Desktop-Pool entfernen.

Voraussetzungen

Benachrichtigen Sie die Benutzer der Remote-Desktops im Pool darüber, dass die Anwendungen entfernt werden sollen.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > Desktop-Pools** und doppelklicken Sie auf die Pool-ID.
- 2 Klicken Sie auf der Registerkarte **Bestandsliste** auf **ThinApps**, wählen Sie die ThinApp-Anwendung und klicken Sie auf **Zuweisung entfernen**.

Wiederholen Sie diesen Schritt, um mehrere Anwendungen zu entfernen.

Ergebnisse

Horizon Administrator deinstalliert die ThinApp-Anwendungen, wenn ein Benutzer sich das erste Mal bei einem Remote-Desktop im Pool anmeldet.

Entfernen einer ThinApp-Anwendung aus Horizon Administrator

Wenn Sie eine ThinApp-Anwendung aus Horizon Administrator entfernen, können Sie die Anwendung nicht länger Computern und Desktop-Pools zuweisen.

Es kann erforderlich sein, eine ThinApp-Anwendung zu entfernen, wenn Ihre Organisation diese durch eine Anwendung eines anderen Anbieters ersetzen möchte.

Hinweis Das Entfernen einer ThinApp-Anwendung ist nicht möglich, wenn die Anwendung bereits einem Computer oder Desktop-Pool zugewiesen ist oder den Status „Ausstehende Deinstallation“ aufweist.

Voraussetzungen

Wenn eine ThinApp-Anwendung gegenwärtig einem Computer oder Desktop-Pool zugewiesen ist, entfernen Sie die Zuweisung aus dem betreffenden Computer oder Desktop-Pool.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** und anschließend die ThinApp-Anwendung aus.

2 Klicken Sie auf **ThinApp entfernen**.

3 Klicken Sie auf **OK**.

Ändern oder Löschen einer ThinApp-Vorlage

Sie können Anwendungen zu einer ThinApp-Vorlage hinzufügen oder aus dieser entfernen. Eine ThinApp-Vorlage kann zudem gelöscht werden.

Wenn Sie eine Anwendung zu einer ThinApp-Vorlage hinzufügen, nachdem die Vorlage einem Computer oder Desktop-Pool zugewiesen wurde, weist Horizon Administrator die neue Anwendung nicht automatisch dem Computer oder Desktop-Pool zu. Beim Entfernen einer Anwendung aus einer ThinApp-Vorlage, die zuvor einem Computer oder Desktop-Pool zugewiesen wurde, wird die Zuweisung der Anwendung zum Computer oder Desktop-Pool beibehalten.

Verfahren

- ◆ Wählen Sie in Horizon Administrator **Katalog > ThinApps** und anschließend die ThinApp-Vorlage aus.

Option	Aktion
Hinzufügen oder Entfernen von ThinApp-Anwendungen aus einer Vorlage	Klicken Sie auf Vorlage bearbeiten .
Löschen der Vorlage	Klicken Sie auf Vorlage entfernen .

Entfernen eines Anwendungs-Repository

Sie können ein Anwendungs-Repository aus Horizon Administrator entfernen.

Möglicherweise ist es erforderlich, dass Sie ein Anwendungs-Repository entfernen, wenn Sie die darin enthaltenen MSI-Pakete nicht mehr benötigen oder Sie die MSI-Pakete auf eine andere Netzwerkfreigabe verschieben müssen. Der Freigabepfad eines Anwendungs-Repositorys in Horizon Administrator kann nicht geändert werden.

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > ThinApp-Konfiguration** und wählen Sie das Anwendungs-Repository aus.
- 2 Klicken Sie auf **Repository entfernen**.

Überwachen von und Fehlerbehebung bei ThinApp-Anwendungen in Horizon Administrator

Horizon Administrator protokolliert mit der ThinApp-Anwendungsverwaltung verbundene Ereignisse in der Datenbank für Ereignisse und Berichterstellung. Diese Ereignisse werden in Horizon Administrator auf der Seite **Ereignisse** angezeigt.

Auf der Seite **Ereignisse** wird in folgenden Fällen ein Ereignis angezeigt:

- Eine ThinApp-Anwendung wird zugewiesen oder eine Anwendungszuweisung wird entfernt
- Eine ThinApp-Anwendung wird auf einem Computer installiert oder deinstalliert
- Eine ThinApp-Anwendung kann nicht installiert oder deinstalliert werden
- Ein ThinApp-Anwendungs-Repository wird registriert, geändert oder aus Horizon Administrator entfernt
- Eine ThinApp-Anwendung wird zu Horizon Administrator hinzugefügt

Für häufige Probleme bei der ThinApp-Anwendungsverwaltung sind Tipps zur Fehlerbehebung verfügbar.

Keine Registrierung eines Anwendungs-Repositorys möglich

Sie können ein Anwendungs-Repository nicht in Horizon Administrator registrieren.

Problem

Beim Versuch, ein Anwendungs-Repository in Horizon Administrator zu registrieren, wird eine Fehlermeldung ausgegeben.

Ursache

Der Verbindungsserver-Host kann nicht auf die Netzwerkfreigabe zugreifen, auf der sich das Anwendungs-Repository befindet. Der im Textfeld **Freigabepfad** eingegebene Pfad zur Netzwerkfreigabe ist möglicherweise falsch, die Netzwerkfreigabe mit dem Anwendungs-Repository befindet sich in einer Domäne, auf die nicht vom Verbindungsserver-Host aus zugegriffen werden kann, oder die Berechtigungen für die Netzwerkfreigabe wurden nicht ordnungsgemäß eingerichtet.

Lösung

- Wenn der Pfad zur Netzwerkfreigabe falsch ist, geben Sie den richtigen Pfad zur Netzwerkfreigabe ein. Pfade zu Netzwerkfreigaben, die IP-Adressen enthalten, werden nicht unterstützt.
- Gehört die Netzwerkfreigabe nicht zu einer Domäne, auf die zugegriffen werden kann, kopieren Sie Ihre Anwendungspakete auf eine Netzwerkfreigabe in einer Domäne, auf die der Verbindungsserver-Host zugreifen kann.
- Überprüfen Sie die Datei- und Freigabeberechtigungen für die Ordnerfreigabe, um der integrierten Active Directory-Gruppe „Domänencomputer“ Lesezugriff zu gewähren. Wenn Sie ThinApps zu Domänencontrollern zuweisen möchten, stellen Sie sicher, dass die Datei- und Freigabeberechtigungen auch der integrierten Active Directory-Gruppe „Domänencomputer“ Lesezugriff gewähren. Nachdem Sie Berechtigungen festgelegt oder geändert haben, kann es bis zu 20 Minuten dauern, bis die Netzwerkfreigabe verfügbar ist.

Kein Hinzufügen von ThinApp-Anwendungen zu Horizon Administrator möglich

Horizon Administrator kann keine ThinApp-Anwendungen zu Horizon Administrator zuweisen.

Problem

Beim Klicken auf **Neue ThinApps untersuchen** in Horizon Administrator sind keine MSI-Pakete verfügbar.

Ursache

Die Anwendungspakete liegen entweder nicht im MSI-Format vor oder der Verbindungsserver-Host kann nicht auf die Verzeichnisse auf der Netzwerkfreigabe zugreifen.

Lösung

- Stellen Sie sicher, dass die Anwendungspakete im Anwendungs-Repository im MSI-Format vorliegen.
- Stellen Sie sicher, dass die Netzwerkfreigabe die Horizon 7-Anforderungen für ThinApp-Anwendungen erfüllt. Weitere Informationen finden Sie unter [Horizon 7-Anforderungen für ThinApp-Anwendungen](#).
- Stellen Sie sicher, dass für die Verzeichnisse auf der Netzwerkfreigabe die richtigen Berechtigungen festgelegt wurden. Weitere Informationen finden Sie unter [Keine Registrierung eines Anwendungs-Repositorys möglich](#).

Während ein Anwendungs-Repository durchsucht wird, werden Meldungen in der Debug-Protokolldatei vom Verbindungsserver aufgeführt. Verbindungsserver-Protokolldateien befinden sich auf dem Verbindungsserver-Host im Verzeichnis `Laufwerk:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs`.

Kein Zuweisen einer ThinApp-Vorlage möglich

Eine ThinApp-Vorlage kann keinem Computer oder Desktop-Pool zugewiesen werden.

Problem

Horizon Administrator gibt beim Versuch, eine ThinApp-Vorlage einem Computer oder Desktop-Pool zuzuweisen, einen Zuweisungsfehler zurück.

Ursache

Die ThinApp-Vorlage enthält entweder eine Anwendung, die dem Computer oder Desktop-Pool bereits zugewiesen wurde, oder die ThinApp-Vorlage wurde dem Computer oder Desktop-Pool bereits mit einem anderen Installationstyp zugewiesen.

Lösung

Wenn die Vorlage eine ThinApp-Anwendung enthält, die dem Computer oder Desktop-Pool bereits zugewiesen wurde, erstellen Sie eine neue Vorlage ohne diese Anwendung oder entfernen Sie die Anwendung aus der vorhandenen Vorlage. Weisen Sie die neue oder geänderte Vorlage dem Computer oder Desktop-Pool zu.

Um den Installationstyp einer ThinApp-Anwendung zu ändern, muss die vorhandene Anwendungszuweisung aus dem Computer oder Desktop-Pool entfernt werden. Nach der Deinstallation der ThinApp-Anwendung können Sie diese dem Computer oder Desktop-Pool mit einem anderen Installationstyp zuweisen.

ThinApp-Anwendung wird nicht installiert

Horizon Administrator kann eine ThinApp-Anwendung nicht installieren.

Problem

Der Installationsstatus einer ThinApp-Anwendung weist entweder auf eine ausstehende Installation oder auf einen Fehler bei der Installation hin.

Ursache

Folgendes sind häufige Ursachen für dieses Problem:

- Es war nicht genügend Speicherplatz vorhanden, um die ThinApp-Anwendung auf dem Computer zu installieren.
- Die Netzwerkverbindung zwischen Verbindungsserver-Host und Computer bzw. zwischen Verbindungsserver-Host und Anwendungs-Repository wurde getrennt.
- Ein Zugriff auf die ThinApp-Anwendung auf der Netzwerkfreigabe war nicht möglich.
- Die ThinApp-Anwendung wurde bereits installiert oder das Verzeichnis bzw. die Datei ist bereits auf dem Computer vorhanden.

In den Horizon Agent- und Verbindungsserver-Protokolldateien finden Sie weitere Informationen zur Ursache des Problems.

Horizon Agent-Protokolldateien befinden sich auf dem Computer im Verzeichnis
Laufwerk: \ProgramData\VMware\VDM\logs.

Verbindungsserver-Protokolldateien befinden sich auf dem Verbindungsserver-Host im Verzeichnis
Laufwerk: \Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs.

Lösung

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** aus.
- 2 Klicken Sie auf den Namen der ThinApp-Anwendung.
- 3 Wählen Sie auf der Registerkarte **Computer** den Computer aus und klicken Sie auf **Installation erneut versuchen**, um die ThinApp-Anwendung erneut zu installieren.

ThinApp-Anwendung wird nicht deinstalliert

Horizon Administrator kann eine ThinApp-Anwendung nicht deinstallieren.

Problem

Der Installationsstatus einer ThinApp-Anwendung weist auf einen Fehler bei der Deinstallation hin.

Ursache

Folgendes sind häufige Ursachen für diesen Fehler:

- Die ThinApp-Anwendung wurde verwendet, als Horizon Administrator versucht hat, sie zu deinstallieren.
- Die Netzwerkverbindung zwischen Verbindungsserver-Host und Computer wurde getrennt.

In den Horizon Agent- und Verbindungsserver-Protokolldateien finden Sie weitere Informationen zur Ursache des Problems.

Horizon Agent-Protokolldateien befinden sich auf dem Computer im Verzeichnis *Laufwerk:* \Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs (auf Windows XP-Systemen) und im Verzeichnis *Laufwerk:* \Programme\VMware\VDM\logs (auf Windows 7-Systemen).

Verbindungsserver-Protokolldateien befinden sich auf dem Verbindungsserver-Host im Verzeichnis *Laufwerk:* \Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs.

Lösung

- 1 Wählen Sie in Horizon Administrator **Katalog > ThinApps** aus.
- 2 Klicken Sie auf den Namen der ThinApp-Anwendung.
- 3 Klicken Sie auf die Registerkarte **Computer**, wählen Sie den Computer aus und klicken Sie auf **Deinstallation erneut versuchen**, um den Deinstallationsvorgang erneut auszuführen.
- 4 Schlägt die Deinstallation erneut fehl, entfernen Sie die ThinApp-Anwendung manuell aus dem Computer und klicken Sie anschließend auf **App-Status für Desktop entfernen**.

Über diesen Befehl wird die ThinApp-Anwendungszuweisung in Horizon Administrator gelöscht. Dateien oder Einstellungen im Computer werden nicht entfernt.

Wichtig Verwenden Sie diesen Befehl nur nach dem manuellen Entfernen der ThinApp-Anwendung aus dem Computer.

MSI-Paket ist ungültig

Horizon Administrator meldet ein ungültiges MSI-Paket in einem Anwendungs-Repository.

Problem

Horizon Administrator meldet während eines Vorgangs zum Durchsuchen ein ungültiges MSI-Paket.

Ursache

Folgendes sind häufige Ursachen für dieses Problem:

- Die MSI-Datei ist beschädigt.
- Die MSI-Datei wurde nicht mit ThinApp erstellt.
- Die MSI-Datei wurde mit einer nicht unterstützten Version von ThinApp erstellt oder erneut paketierrt. Sie müssen ThinApp Version 4.6 oder höher verwenden.

Lösung

Weitere Informationen zum Beheben von Problemen mit MSI-Paketen finden Sie im *ThinApp-Benutzerhandbuch*.

ThinApp-Konfigurationsbeispiel

In diesem ThinApp-Konfigurationsbeispiel werden alle Schritte einer typischen ThinApp-Konfiguration beschrieben, angefangen beim Erstellen von Anwendungspaketen bis hin zum Überprüfen des Status einer Installation.

Voraussetzungen

Vollständige Informationen zum Ausführen der Schritte in diesem Beispiel finden Sie in den folgenden Themen.

- [Erfassen und Speichern von Anwendungspaketen](#)
- [Zuweisen von ThinApp-Anwendungen zu Maschinen und Desktop-Pools](#)

Verfahren

Verfahren

- 1 Laden Sie die ThinApp-Software von der Seite <http://www.vmware.com/products/thinapp> herunter und installieren Sie sie auf einem Computer, auf dem noch keine Version dieser Software vorhanden ist.

Horizon 7 unterstützt ThinApp 4.6 und höher.

- 2 Verwenden Sie den ThinApp **Setup Capture**-Assistenten zum Erstellen von Anwendungspaketen im MSI-Format.
- 3 Erstellen Sie eine Ordnerfreigabe auf einem Computer in einer Active Directory-Domäne, auf die der Verbindungsserver-Host und Ihre Remote-Desktops zugreifen können, und konfigurieren Sie die Datei- und Freigabeberechtigungen für die Ordnerfreigabe, um der integrierten Active Directory-Gruppe „Domänencomputer“ Lesezugriff zu gewähren.

Wenn Sie Domänencontrollern ThinApp-Anwendungen zuweisen möchten, müssen Sie der integrierten Active Directory-Gruppe Domain Controllers (Domänencontroller) Lesezugriff gewähren.

- 4 Kopieren Sie die MSI-Pakete in den freigegebenen Ordner.
- 5 Registrieren Sie den freigegebenen Ordner als Anwendungs-Repository in Horizon Administrator.
- 6 Durchsuchen Sie die MSI-Pakete im Anwendungs-Repository in Horizon Administrator und fügen Sie ausgewählte ThinApp-Anwendungen zu Horizon Administrator hinzu.

- 7 Legen Sie fest, ob die ThinApp-Anwendungen Computern oder Desktop-Pools zugewiesen werden sollen.

Wenn Sie eine allgemeine Benennungskonvention für Ihre Computer verwenden, können Sie Anwendungen mithilfe von Computer-Zuweisungen schnell auf alle Computer mit derselben Benennungskonvention verteilen. Wenn Sie Desktop-Pools nach Abteilung oder Benutzertyp organisieren, können Sie Anwendungen mithilfe von Desktop-Pool-Zuweisungen schnell an bestimmte Abteilungen oder Benutzer verteilen.

- 8 Wählen Sie in Horizon Administrator die ThinApp-Anwendungen aus, die Ihren Computern oder Desktop-Pools zugewiesen werden sollen, und geben Sie die Installationsmethode an.

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Computer. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Vollständig	Installiert die vollständige Anwendung auf dem lokalen Dateisystem des Computers.

- 9 Überprüfen Sie in Horizon Administrator den Installationsstatus der ThinApp-Anwendungen.

Einrichten von Clients im Kiosk-Modus

10

Sie können unbeaufsichtigte Clients einrichten, die über Horizon 7 auf ihre Desktops zugreifen können.

Ein Client im Kiosk-Modus ist ein Thin Client oder ein PC mit eingeschränkten Funktionen, auf dem Horizon Client ausgeführt wird, um die Verbindung mit einer Verbindungsserver-Instanz herzustellen und eine Sitzung zu starten. Endbenutzer müssen sich typischerweise nicht für den Zugriff auf das Clientgerät anmelden. Der veröffentlichte Desktop fordert für einige Anwendungen jedoch möglicherweise Authentifizierungsinformationen an. Beispiele sind Arbeitsstationen zur Eingabe medizinischer Daten, Check-in-Schalter, Selbstbedienungsstationen und Informationsterminals mit öffentlichem Zugriff.

Sie sollten sicherstellen, dass die Desktop-Anwendung Authentifizierungsmechanismen für sichere Transaktionen implementiert, das physische Netzwerk gegen das Manipulieren und Ausspähen von Daten geschützt ist und alle mit dem Netzwerk verbundenen Geräte als vertrauenswürdig eingestuft werden.

Clients im Kiosk-Modus unterstützen die eigenständigen Funktionen für den Remote-Zugriff, z.B. die automatische Umleitung von USB-Geräten an die Remote-Sitzung und die standortbasierte Druckfunktion.

Horizon 7 verwendet die Funktion zur flexiblen Authentifizierung in Horizon 7 4.5 und höher, um anstelle des Endbenutzers ein Client-Gerät im Kiosk-Modus zu authentifizieren. Eine Verbindungsserver-Instanz kann für die Authentifizierung von Clients konfiguriert werden, die über ihre MAC-Adresse oder einen Benutzernamen identifiziert werden, der mit der Zeichenfolge „custom-“ oder einer anderen Präfixzeichenfolge beginnt, die Sie in ADAM definiert haben. Wenn für einen Client das automatische Generieren eines Kennworts konfiguriert ist, kann Horizon Client auf dem Gerät ohne Angabe eines Kennworts ausgeführt werden. Bei Konfiguration eines expliziten Kennworts muss dieses Kennwort für Horizon Client angegeben werden. Da Horizon Client normalerweise über ein Skript ausgeführt und das Kennwort als Klartext angezeigt würde, sollten Sie sicherstellen, dass das Skript nicht von Benutzern ohne entsprechende Berechtigung gelesen werden kann.

Nur Verbindungsserver-Instanzen, die für die Authentifizierung von Clients im Kiosk-Modus aktiviert wurden, können Verbindungen von Konten akzeptieren, deren Namen mit den Zeichen „cm-“ (gefolgt von einer MAC-Adresse) oder mit den Zeichen „Custom-“ oder einer alternativen Zeichenfolge beginnen, die Sie definiert haben. Die manuelle Eingabe von Benutzernamen mit diesen Formaten ist bei Horizon Client in Horizon 7 4.5 und höher nicht zulässig.

Es hat sich bewährt, dedizierte Verbindungsserver-Instanzen für die Verwaltung von Clients im Kiosk-Modus einzusetzen und dedizierte Organisationseinheiten und Gruppen in Active Directory für die Konten dieser Clients zu erstellen. Bei dieser Vorgehensweise werden die Systeme nicht nur partitioniert und gegen unberechtigten Zugriff geschützt, sondern gleichzeitig wird die Konfiguration und Verwaltung der Clients vereinfacht.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren von Clients im Kiosk-Modus](#)

Konfigurieren von Clients im Kiosk-Modus

Zur Konfiguration von Active Directory und Horizon 7 für die Unterstützung von Clients im Kiosk-Modus müssen mehrere Aufgaben mit einer bestimmten Reihenfolge ausgeführt werden.

Voraussetzungen

Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Ausführen der Konfigurationsaufgaben verfügen.

- **Domänen-Admins** oder **Konten-Operatoren** – die Anmeldeinformationen dieser Rollen sind erforderlich, um in Active Directory Änderungen an Konten von Benutzern und Gruppen in einer Domäne vorzunehmen.
- **Administratoren**, **Bestandslistenadministratoren** oder eine äquivalente Rolle – diese Rollen sind erforderlich, um Horizon Administrator zum Berechtigen von Benutzern oder Gruppen für Desktops zu verwenden.
- **Administratoren** oder eine äquivalente Rolle – diese Rollen sind erforderlich, um den Befehl `vdmadmin` ausführen zu können.

Verfahren

1 [Vorbereiten von Active Directory und Horizon 7 für Clients im Kiosk-Modus](#)

Active Directory muss für das Akzeptieren der Konten konfiguriert werden, die zur Authentifizierung von Clientgeräten erstellt werden. Beim Erstellen einer Gruppe muss die Gruppe zudem für den Desktop-Pool berechtigt werden, auf den ein Client zugreift. Der von den Clients verwendete Desktop-Pool kann ebenfalls vorbereitet werden.

2 [Festlegen von Standardwerten für Clients im Kiosk-Modus](#)

Mithilfe des Befehls `vdmadmin` können Sie die Standardwerte für eine Organisationseinheit, die Ablaufzeit von Kennwörtern sowie Gruppenmitgliedschaften in Active Directory für Clients im Kiosk-Modus festlegen.

3 [Anzeigen der MAC-Adressen von Clientgeräten](#)

Wenn Sie basierend auf der MAC-Adresse ein Konto für einen Client erstellen möchten, können Sie die MAC-Adresse des Clientgeräts mit Horizon Client ermitteln.

4 Hinzufügen von Konten für Clients im Kiosk-Modus

Mithilfe des Befehls `vdadmin` können Clientkonten zur Konfiguration einer Verbindungsserver-Gruppe hinzugefügt werden. Nach dem Hinzufügen eines Clients kann dieser mit einer Verbindungsserver-Instanz verwendet werden, auf der die Authentifizierung von Clients aktiviert ist. Zudem können Sie die Konfiguration von Clients aktualisieren oder die Clientkonten aus dem System entfernen.

5 Authentifizierung von Clients im Kiosk-Modus aktivieren

Mithilfe des Befehls `vdadmin` kann die Authentifizierung von Clients aktiviert werden, die versuchen, über eine Verbindungsserver-Instanz eine Verbindung mit ihren Remote-Desktops herzustellen.

6 Überprüfen der Konfiguration von Clients im Kiosk-Modus

Mithilfe des Befehls `vdadmin` können Informationen zu Clients im Kiosk-Modus und zu Verbindungsserver-Instanzen angezeigt werden, die zur Authentifizierung dieser Clients konfiguriert sind.

7 Verbinden mit Remote-Desktops über Clients im Kiosk-Modus

Sie können den Client über die Befehlszeile ausführen oder ein Skript verwenden, um einen Client mit einer Remote-Sitzung zu verbinden.

Vorbereiten von Active Directory und Horizon 7 für Clients im Kiosk-Modus

Active Directory muss für das Akzeptieren der Konten konfiguriert werden, die zur Authentifizierung von Clientgeräten erstellt werden. Beim Erstellen einer Gruppe muss die Gruppe zudem für den Desktop-Pool berechtigt werden, auf den ein Client zugreift. Der von den Clients verwendete Desktop-Pool kann ebenfalls vorbereitet werden.

Die empfohlene Vorgehensweise sieht das Erstellen einer separaten Organisationseinheit und Gruppe vor, um den Verwaltungsaufwand für Clients im Kiosk-Modus zu minimieren. Sie können einzelne Konten für Clients hinzufügen, die keiner Gruppe angehören, bei Konfiguration einer größeren Anzahl an Clients führt dies jedoch zu einem erheblichen Verwaltungsaufwand.

Verfahren

- 1 Erstellen Sie in Active Directory eine separate Organisationseinheit und Gruppe für Clients im Kiosk-Modus.

Für die Gruppe muss ein Prä-Windows 2000-Name angegeben werden. Dieser Name wird zur Identifizierung der Gruppe gegenüber dem Befehl `vdadmin` verwendet.

- 2 Erstellen Sie das Image oder die Vorlage für die virtuelle Gastmaschine.

Sie können eine virtuelle Maschine, die von vCenter Server verwaltet wird, als Vorlage für einen automatisierten Pool, als übergeordnetes Element für einen Linked-Clone-Pool oder als virtuelle Maschine in einem manuellen Desktop-Pool verwenden. Zudem können Sie Anwendungen auf dem Gastbetriebssystem installieren und konfigurieren.

- 3 Konfigurieren Sie das Gastbetriebssystem so, dass die Clients bei unbeaufsichtigtem Betrieb nicht gesperrt werden.

Horizon 7 unterdrückt die Prä-Anmeldenachricht für Clients, die eine Verbindung im Kiosk-Modus herstellen. Wenn es erforderlich ist, dass ein Ereignis den Bildschirm entsperrt und eine Meldung anzeigt, können Sie eine geeignete Anwendung auf dem Gastbetriebssystem konfigurieren.

- 4 Erstellen Sie in Horizon Administrator den von den Clients verwendeten Desktop-Pool und berechtigen Sie die Gruppe für diesen Pool.

Möglicherweise entscheiden Sie sich zur Erstellung eines Linked-Clone-Desktop-Pools mit dynamischer Zuweisung, da diese Art von Pool sich am besten für die Anforderungen Ihrer Clientanwendung eignet. Sie können zudem eine oder mehrere ThinApp-Anwendungen mit dem Desktop-Pool verknüpfen.

Wichtig Berechtigen Sie einen Client oder eine Gruppe nicht für mehrere Desktop-Pools. Anderenfalls weist Horizon 7 nach dem Zufallsprinzip einen Remote-Desktop aus den Pools zu, für die ein Client berechtigt ist, und es wird eine Warnung generiert.

- 5 Wenn für die Clients der standortbasierte Druck eingerichtet werden soll, konfigurieren Sie die Active Directory-Gruppenrichtlinieneinstellung AutoConnect Location-based Printing for VMware View, die sich im Gruppenrichtlinienobjekt-Editor von Microsoft im Ordner Softwareeinstellungen unterhalb von Computerkonfiguration befindet.
- 6 Konfigurieren Sie andere erforderliche Richtlinien, um die Remote-Desktops der Clients zu optimieren und zu schützen.

Beispielsweise kann es sinnvoll sein, die Richtlinien zum Verbinden lokaler USB-Geräte mit dem Remote-Desktop außer Kraft zu setzen, wenn der Desktop gestartet wird oder die Geräte verbunden werden. Horizon Client für Windows aktiviert diese Richtlinien standardmäßig für Clients im Kiosk-Modus.

Beispiel: Vorbereiten von Active Directory für Clients im Kiosk-Modus

Ein Unternehmensintranet verfügt über eine Domäne MYORG und eine Organisationseinheit mit dem Distinguished Name OU=myorg-ou,DC=myorg,DC=com. Erstellen Sie in Active Directory die Organisationseinheit kiosk-ou mit dem Distinguished Name OU=kiosk-ou,DC=myorg,DC=com und die Gruppe kc-grp zur Verwendung mit Clients im Kiosk-Modus.

Nächste Schritte

Legen Sie Standardwerte für die Clients fest.

Festlegen von Standardwerten für Clients im Kiosk-Modus

Mithilfe des Befehls `vdadmin` können Sie die Standardwerte für eine Organisationseinheit, die Ablaufzeit von Kennwörtern sowie Gruppenmitgliedschaften in Active Directory für Clients im Kiosk-Modus festlegen.

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 veröffentlichten 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.

Verfahren

- ◆ Legen Sie die Standardwerte für Clients fest.

```
vdmadmin
-Q
-clientauth
-setdefaults [-b Authentifizierungsargumente] [-ouDN] [ -expirepassword |
-noexpirepassword ] [-groupGruppenname | -nogroup]
```

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>-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>-noexpirepassword</code>	Gibt an, dass Kennwörter für Clientkonten nicht ablaufen.
<code>-nogroup</code>	Löscht die Einstellung für die Standardgruppe.
<code>-ou <i>DN</i></code>	Gibt den Distinguished Name der standardmäßigen Organisationseinheit an, zu der Clientkonten hinzugefügt werden. Beispiel: OU=kiosk-ou,DC=myorg,DC=com Hinweis Die Konfiguration einer Organisationseinheit kann nicht über diesen Befehl geändert werden.

Der Befehl aktualisiert die Standardwerte für Clients in der Verbindungsserver-Gruppe.

Beispiel: Festlegen von Standardwerten für Clients im Kiosk-Modus

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
```

Nächste Schritte

Ermitteln Sie die MAC-Adressen von Clientgeräten, die sich über ihre MAC-Adresse authentifizieren.

Anzeigen der MAC-Adressen von Clientgeräten

Wenn Sie basierend auf der MAC-Adresse ein Konto für einen Client erstellen möchten, können Sie die MAC-Adresse des Clientgeräts mit Horizon Client ermitteln.

Voraussetzungen

Melden Sie sich an der Clientkonsole an.

Verfahren

- ◆ Zum Anzeigen der MAC-Adresse geben Sie den geeigneten Befehl für Ihre Plattform ein.

Option	Aktion
Windows	<p>Geben Sie</p> <p>C:\Programme (x86)\VMware\VMware Horizon View Client\vmware-view.exe -printEnvironmentInfo ein.</p> <p>Der Client verwendet die konfigurierte standardmäßige Verbindungsserver-Instanz. Wenn Sie keinen Standardwert konfiguriert haben, werden Sie vom Client zur Angabe des Werts aufgefordert.</p> <p>Der Befehl zeigt die IP-Adresse, die MAC-Adresse und den Maschinennamen des Clientgeräts an.</p>
Linux	<p>Geben Sie vmware-view --printEnvironmentInfo -s <i>Verbindungsserver</i> ein.</p> <p>Sie müssen die IP-Adresse oder den FQDN der Verbindungsserver-Instanz angeben, die der Client zur Herstellung einer Verbindung mit dem Desktop verwendet.</p> <p>Der Befehl zeigt die IP-Adresse, die MAC-Adresse, den Maschinennamen, die Domäne, den Namen und die Domäne angemeldeter Benutzer sowie die Zeitzone des Clientgeräts an.</p>

Nächste Schritte

Fügen Sie Konten für die Clients hinzu.

Hinzufügen von Konten für Clients im Kiosk-Modus

Mithilfe des Befehls `vdmadmin` können Clientkonten zur Konfiguration einer Verbindungsserver-Gruppe hinzugefügt werden. Nach dem Hinzufügen eines Clients kann dieser mit einer Verbindungsserver-Instanz verwendet werden, auf der die Authentifizierung von Clients aktiviert ist. Zudem können Sie die Konfiguration von Clients aktualisieren oder die Clientkonten aus dem System entfernen.

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 veröffentlichten Desktops verwenden.

Beim Hinzufügen von Clients im Kiosk-Modus erstellt Horizon 7 ein Benutzerkonto für den Client in Active Directory. Wenn Sie für einen Client einen Namen angeben, muss dieser Name mit einer erkannten Präfixzeichenfolge, z.B. „custom-“, oder einer alternativen, von Ihnen in ADAM definierten Präfixzeichenfolge beginnen und darf maximal 20 Zeichen umfassen. 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.

Wichtig Verwenden Sie einen angegebenen Namen nicht für mehrere Clientgeräte. Diese Konfiguration wird in zukünftigen Releases möglicherweise nicht unterstützt.

Verfahren

- ◆ Führen Sie den Befehl `vdmadmin` mit den Optionen `-domain` und `-clientid` aus, um die Domäne und den Namen oder die MAC-Adresse des Clients anzugeben.

```
vdmadmin
-Q
-clientauth
-add [-bAuthentifizierungsargumente] -domainDomänenname-clientidClient-ID [-password
"Kennwort" | -genpassword] [-ouDN] [-expirepassword | -noexpirepassword] [-groupGruppenname | -nogroup]
[-description "Beschreibungstext"]
```

Option	Beschreibung
<code>-clientid Client-ID</code>	Gibt den Namen oder die MAC-Adresse des Clients an.
<code>-description "description_text"</code>	Erstellt eine Beschreibung des Kontos für das Clientgerät in Active Directory.
<code>-domain Domänenname</code>	Gibt die Domäne für den Client an.
<code>-expirepassword</code>	Gibt an, dass die Ablaufzeit für das Kennwort des Clientkontos mit der Ablaufzeit für die Verbindungsserver-Gruppe übereinstimmt. Wenn für die Gruppe keine Ablaufzeit definiert ist, läuft das Kennwort nicht ab.
<code>-genpassword</code>	Generiert ein Kennwort für das Clientkonto. Dies ist das Standardverhalten, wenn weder <code>-password</code> noch <code>-genpassword</code> angegeben wird. Ein 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, geben Sie das Kennwort über die Option <code>-password</code> an.
<code>-group Gruppenname</code>	Gibt den Namen der Gruppe an, zu der das Clientkonto hinzugefügt wird. Der Name der Gruppe muss als der Prä-Windows 2000-Gruppenname aus Active Directory angegeben werden. Wenn zuvor eine Standardgruppe festgelegt wurde, wird das Clientkonto zu dieser Gruppe hinzugefügt.
<code>-noexpirepassword</code>	Gibt an, dass das Kennwort für das Clientkonto nicht abläuft.
<code>-nogroup</code>	Gibt an, dass das Clientkonto nicht zur Standardgruppe hinzugefügt wird.
<code>-ou DN</code>	Gibt den Distinguished Name der Organisationseinheit an, zu der das Clientkonto hinzugefügt wird. Beispiel: OU=kiosk-ou,DC=myorg,DC=com
<code>-password "Kennwort"</code>	Gibt ein explizites Kennwort für das Clientkonto an.

Der Befehl erstellt in Active Directory ein Benutzerkonto für den Client in der angegebenen Domäne und Gruppe (sofern vorhanden).

Beispiel: Hinzufügen von Konten für Clients

Fügen Sie ein Konto für einen Client, der über die MAC-Adresse angegeben wird, zur Domäne MYORG hinzu, indem Sie die Standardeinstellungen für die Gruppe „kc-grp“ verwenden.

```
vdadmin -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.

```
vdadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword
```

Fügen Sie ein Konto für einen benannten Client hinzu und geben Sie ein Kennwort zur Verwendung mit dem Client an.

```
vdadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Fügen Sie ein Konto für einen benannten Client hinzu, der ein automatisch generiertes Kennwort verwendet.

```
vdadmin -Q -clientauth -add -domain MYORG -clientid custom-Kiosk11 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Kiosk 11"
```

Nächste Schritte

Aktivieren Sie die Authentifizierung der Clients.

Authentifizierung von Clients im Kiosk-Modus aktivieren

Mithilfe des Befehls `vdadmin` kann die Authentifizierung von Clients aktiviert werden, die versuchen, über eine Verbindungsserver-Instanz eine Verbindung mit ihren Remote-Desktops herzustellen.

Der Befehl `vdadmin` 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.

Wenngleich die Authentifizierung für eine einzelne Verbindungsserver-Instanz aktiviert wird, gelten die anderen Einstellungen für die Clientauthentifizierung für alle Verbindungsserver-Instanzen innerhalb einer Gruppe. Das Konto für einen Client muss nur einmal hinzugefügt werden. Alle aktivierten Verbindungsserver-Instanzen innerhalb einer Verbindungsserver-Gruppe können den Client authentifizieren.

Wenn Sie den Kiosk-Modus zusammen mit einem sitzungsbasierten Desktop auf einem RDS-Host verwenden, müssen Sie auch das Benutzerkonto zur Gruppe der Remote-Desktop-Benutzer hinzufügen.

Verfahren

- 1 Aktivieren Sie die Authentifizierung von Clients für eine Verbindungsserver-Instanz.

```
vdmadmin
-Q
-enable [-bauthentication_arguments] -s connection_server [-requirepassword]
```

Option	Beschreibung
-requirepassword	Gibt an, dass Clients Kennwörter angeben müssen. Wichtig Bei Angabe dieser Option 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.
-s <i>Verbindungsserver</i>	Gibt den NetBIOS-Namen der Verbindungsserver-Instanz an, für welche die Authentifizierung von Clients aktiviert werden soll.

Der Befehl aktiviert die angegebene Verbindungsserver-Instanz für die Authentifizierung von Clients.

- 2 Wenn der veröffentlichte Desktop von einem Microsoft RDS-Host bereitgestellt wird, melden Sie sich an dem RDS-Host an und fügen Sie das Benutzerkonto zur Gruppe der Remote-Desktop-Benutzer hinzu.

Angenommen, Sie erteilen auf dem Horizon 7-Server dem Benutzerkonto custom-11 die Berechtigung für einen sitzungsbasierten Desktop auf einem RDS-Host. Sie müssen sich dann an dem RDS-Host anmelden und den Benutzer custom-11 zur Gruppe der Remote-Desktop-Benutzer hinzufügen, indem Sie zu **Systemsteuerung > System und Sicherheit > System > Remoteeinstellungen > Benutzer auswählen > Hinzufügen** navigieren.

Beispiel: Aktivieren der Authentifizierung von Clients im Kiosk-Modus

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
```

Nächste Schritte

Überprüfen Sie die Konfiguration der Verbindungsserver-Instanzen und Clients.

Überprüfen der Konfiguration von Clients im Kiosk-Modus

Mithilfe des Befehls `vdmadmin` können Informationen zu Clients im Kiosk-Modus und zu Verbindungsserver-Instanzen angezeigt werden, die zur Authentifizierung dieser Clients konfiguriert sind.

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.

Verfahren

- ◆ Zeigen Sie Informationen zu Clients im Kiosk-Modus und zur Clientauthentifizierung an.

```
vdmadmin
-Q
-clientauth
-list [-b Authentifizierungsargumente] [-xml]
```

Der Befehl zeigt Informationen zu Clients im Kiosk-Modus und zu den Verbindungsserver-Instanzen an, auf denen die Clientauthentifizierung aktiviert ist.

Beispiel: Anzeigen von Informationen für Clients im Kiosk-Modus

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
```

Nächste Schritte

Stellen Sie sicher, dass sich die Clients mit ihren Remote-Desktops verbinden können.

Verbinden mit Remote-Desktops über Clients im Kiosk-Modus

Sie können den Client über die Befehlszeile ausführen oder ein Skript verwenden, um einen Client mit einer Remote-Sitzung zu verbinden.

Normalerweise würden Sie Horizon Client unter Verwendung eines Befehlsskripts auf einem bereitgestellten Clientgerät ausführen.

Hinweis Auf einem Windows- oder Mac-Client werden USB-Geräte auf dem Client standardmäßig nicht automatisch weitergeleitet, wenn sie beim Start der Remote-Desktop-Sitzung von einer anderen Anwendung oder einem anderen Dienst verwendet werden. Auf alle Clients werden Eingabegeräte (Human Interface Devices, HIDs) und Smartcard-Leser standardmäßig nicht weitergeleitet.

Verfahren

- ◆ Zum Herstellen einer Verbindung mit einer Remote-Sitzung geben Sie den geeigneten Befehl für Ihre Plattform ein.

Option	Beschreibung
Windows	<p>Geben Sie C:\Programme (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended [-serverURL <i>connection_server</i>] [-userName <i>Benutzername</i>] [-password <i>Kennwort</i>] ein.</p> <p>-password<i>Kennwort</i> Gibt das Kennwort für das Clientkonto an. Wenn ein Kennwort für das Konto definiert wurde, muss dieses Kennwort angegeben werden.</p> <p>-serverURL<i>Verbindungs</i>server Gibt die IP-Adresse oder den FQDN der Verbindungsserver-Instanz an, die Horizon Client zur Herstellung einer Verbindung mit einem Remote-Desktop verwendet. Wenn Sie die IP-Adresse oder den FQDN der Verbindungsserver-Instanz, die der Client zum Herstellen einer Verbindung mit einem Remote-Desktop verwendet, nicht angeben, verwendet der Client die von Ihnen dafür konfigurierte, standardmäßige Verbindungsserver-Instanz.</p> <p>-userName<i>Benutzer</i>name Gibt den Namen des Clientkontos an. Wenn sich ein Client nicht über die MAC-Adresse, sondern unter Verwendung eines Kontonamens authentifizieren soll, der mit der erkannten Präfixzeichenfolge, z. B. „custom-“ beginnt, muss dieser Name angegeben werden.</p>
Linux	<p>Geben Sie vmware-view --unattended -s <i>Verbindungs</i>server [--once] [-u <i>Benutzername</i>] [-p <i>Kennwort</i>] ein.</p> <p>--once Gibt an, dass Horizon Client bei einem Fehler nicht erneut versuchen soll, eine Verbindung herzustellen.</p> <p>Wichtig Sie sollten diese Option normalerweise angeben und den Fehler anhand des Exitcodes behandeln. Andernfalls kann es schwierig sein, den vmware-view-Prozess remote zu beenden.</p> <p>-p<i>Kennwort</i> Gibt das Kennwort für das Clientkonto an. Wenn ein Kennwort für das Konto definiert wurde, muss dieses Kennwort angegeben werden.</p>

Option	Beschreibung
<i>-sVerbindungsserver</i>	Gibt die IP-Adresse oder den FQDN der Verbindungsserver-Instanz an, die der Client zur Herstellung einer Verbindung mit einem Desktop verwendet.
<i>-uBenutzername</i>	Gibt den Namen des Clientkontos an. Wenn sich ein Client nicht über die MAC-Adresse, sondern unter Verwendung eines Kontonamens authentifizieren soll, der mit der erkannten Präfixzeichenfolge, z. B. „custom-“ beginnt, muss dieser Name angegeben werden.

Wenn der Server den Kiosk-Client authentifiziert und ein Remote-Desktop verfügbar ist, startet der Befehl die Remote-Sitzung.

Beispiel: Ausführen von Horizon Client auf Clients im Kiosk-Modus

Führen Sie Horizon Client auf einem Windows-Client aus, dessen Kontoname auf der MAC-Adresse basiert und der über ein automatisch generiertes Kennwort verfügt.

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended -serverURL consvr2.myorg.com
```

Führen Sie Horizon Client auf einem Linux-Client aus, der einen zugewiesenen Namen und ein zugewiesenes Kennwort verwendet.

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

Fehlerbehebung für Horizon 7

11

Zur Diagnose und Behandlung von Problemen bei der Verwendung von Horizon 7 können Sie zwischen verschiedenen Vorgehensweisen wählen. Sie können zur Fehlerbehebung Horizon Help Desk Tool verwenden oder mit anderen Verfahren zur Fehlerbehebung Probleme untersuchen und beheben oder sich an den technischen Support von VMware wenden.

Informationen zur Fehlerbehebung bei Desktop- und Anwendungspools finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden von Horizon Help Desk Tool](#)
- [Verwenden der VMware-Anmeldeüberwachung](#)
- [Verwenden von VMware Horizon Performance Tracker](#)
- [Überwachen des Systemzustands](#)
- [Überwachen von Ereignissen in Horizon 7](#)
- [Sammeln von Diagnoseinformationen für Horizon 7](#)
- [Integration des Horizon-Verbindungsservers mit Skyline Collector-Appliance](#)
- [Aktualisieren von Supportanfragen](#)
- [Fehlerbehebung einer nicht erfolgreichen Sicherheitsserverkopplung mit Horizon-Verbindungsserver](#)
- [Fehlerbehebung der Horizon 7 Server-Zertifikatsperrüberprüfung](#)
- [Fehlerbehebung bei der Smartcard-Zertifikatsperrüberprüfung](#)
- [Weitere Informationen zur Fehlerbehebung](#)

Verwenden von Horizon Help Desk Tool

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 darüber, ob Sie über die richtige Lizenz verfügen, finden Sie unter [Prüfen der Horizon Help Desk Tool-Lizenz](#).
- Eine Ereignisdatenbank zum Speichern von Informationen zu Horizon 7-Komponenten. Weitere Informationen zur Konfiguration einer Ereignisdatenbank finden Sie im Dokument *Horizon 7-Installation*.
- Die Rolle „Helpdesk-Administrator“ oder „Helpdesk-Administrator (Nur Lesezugriff)“ zum Anmelden bei Horizon Help Desk Tool. Weitere Informationen zu diesen Rollen finden Sie unter [Konfigurieren des rollenbasierten Zugriffs für Horizon Help Desk Tool](#)
- 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}
```

Prüfen der Horizon Help Desk Tool-Lizenz

Wenn Sie über keinen gültigen Produktlizenzschlüssel verfügen, können Sie sich nicht bei Horizon Help Desk Tool anmelden. Sie können den Produktlizenzschlüssel in Horizon Administrator prüfen und gegebenenfalls eine gültige Lizenz angeben.

Voraussetzungen

- Besorgen Sie sich einen gültigen Produktlizenzschlüssel für die Horizon Enterprise Edition-Lizenz oder für die Horizon Apps Advanced Edition-Lizenz.

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Produktlizenzierung und -verwendung** aus.

Im Bereich **Lizenzierung** werden die ersten und die letzten fünf Zeichen des aktuellen Lizenzschlüssels dargestellt.

2 Prüfen Sie den Lizenzstatus im Feld **Helpdesk-Lizenz**.

Option	Beschreibung
Deaktiviert	Der Produktlizenzschlüssel ist ungültig. Sie können sich nicht bei Horizon Help Desk Tool anmelden.
Aktiviert	Der Produktlizenzschlüssel ist gültig. Sie können sich bei Horizon Help Desk Tool anmelden.

- 3 (Optional) Wenn der Produktlizenzschlüssel ungültig ist, klicken Sie auf **Lizenz bearbeiten**, geben Sie die gültige Lizenzseriennummer ein, klicken Sie auf **OK** und aktualisieren Sie die Horizon-Administrator-URL.

Im Fenster **Produktlizenzierung** werden die aktualisierten Lizenzinformationen angezeigt.

Nächste Schritte

Melden Sie sich bei Horizon Help Desk Tool an.

Konfigurieren des rollenbasierten Zugriffs für Horizon Help Desk Tool

Sie können Horizon Help Desk Tool-Administratoren vordefinierte Administratorrollen zuweisen, um die Aufgaben zur Fehlerbehebung an verschiedene Administratorbenutzer zu delegieren. Sie haben auch die Möglichkeit, benutzerdefinierte Rollen zu erstellen und Berechtigungen basierend auf den vordefinierten Administratorrollen hinzuzufügen.

Sie können Horizon Help Desk Tool-Administratoren die folgenden vordefinierten Administratorrollen zuweisen:

- Helpdesk-Administrator
- Helpdesk-Administrator (Nur Lesezugriff)

Bei der Erstellung einer benutzerdefinierten Rolle für einen Horizon Help Desk Tool-Administrator müssen Sie die Berechtigung „Helpdesk verwalten (Nur Lesezugriff)“ zusammen mit anderen Berechtigungen auf der Basis der Rolle „Helpdesk-Administrator“ oder „Helpdesk-Administrator (Nur Lesezugriff)“ zuweisen.

Voraussetzungen

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

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Administratoren** aus und klicken Sie auf die Registerkarte **Rollen**.

- 2 Klicken Sie auf der Registerkarte **Rollen** auf **Rolle hinzufügen**, wählen Sie die Rolle „Helpdesk-Administrator“ oder „Helpdesk-Administrator (Nur Lesezugriff)“ aus und klicken Sie auf **OK**.
 - a (Optional) Um eine benutzerdefinierte Rolle hinzuzufügen, klicken Sie auf der Registerkarte **Rollen** auf **Rolle hinzufügen**. Anschließend wählen Sie die Berechtigung „Helpdesk verwalten (Nur Lesezugriff)“ oder beliebige Berechtigungen basierend auf der Rolle „Helpdesk-Administrator“ oder „Helpdesk-Administrator (Nur Lesezugriff)“ aus und klicken Sie auf **OK**.

Anmelden bei Horizon Help Desk Tool

Das Horizon Help Desk Tool ist in der Horizon Console enthalten. Ab Horizon 7 Version 7.5 können Sie die Horizon Help Desk Tool-URL nicht mehr verwenden, um sich bei Horizon Help Desk Tool anzumelden.

Verfahren

- 1 Um sich bei Horizon Help Desk Tool von Horizon Administrator aus anzumelden, klicken Sie rechts oben auf **Horizon Console**. Dies ist eine Single-Sign-On-Anmeldung bei der Horizon Console-Webschnittstelle.
- 2 Geben Sie an der Horizon Console einen Benutzernamen im Feld „Benutzersuche“ ein.
An der Horizon Console wird eine Liste der Benutzer in den Suchergebnissen angezeigt. Die Suche kann bis zu 100 übereinstimmende Ergebnisse zurückgeben.
- 3 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“.

Sie können durch Klicken auf die Telefonnummer eine Skype for Business-Sitzung öffnen, um den Benutzer für eine Kontaktaufnahme zur Fehlerbehebung anzurufen.

Durch Klicken auf die E-Mail-Adresse können Sie dem Benutzer eine E-Mail senden.

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 11-1. 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. ■ G, wenn die Sitzung in einem anderen Pod im Pod-Verbund 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. Siehe Sitzungsdetails für das Horizon Help Desk Tool. ■ Die Registerkarte Prozesse zeigt Informationen zu den Prozessen an, die CPU und Arbeitsspeicher betreffen. Siehe Sitzungsprozesse für das Horizon Help Desk Tool. ■ Die Registerkarte Anwendungen zeigt die Details zu den ausgeführten Anwendungen an. Siehe Anwendungsstatus für das Horizon Help Desk Tool.
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.

Desktop-Berechtigungen

Die Registerkarte **Desktop-Berechtigungen** zeigt Informationen zu den veröffentlichten oder virtuellen Desktops an, für die der Benutzer über Berechtigungen verfügt.

Tabelle 11-2. Desktop-Berechtigungen

Option	Beschreibung
Status	<p>Zeigt Informationen zum Status der 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.

Tabelle 11-2. Desktop-Berechtigungen (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. ■ „Global“ für eine globale 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>

Anwendungsberechtigungen

Die Registerkarte **Anwendungsberechtigungen** enthält Informationen zu den veröffentlichten Anwendungen, für die der Benutzer über Berechtigungen verfügt.

Tabelle 11-3. Anwendungsberechtigungen

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. ■ „Global“ für eine globale 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 Administraturname 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 CPA-Umgebung angezeigt.

Tabelle 11-4. Aktivitäten

Option	Beschreibung
Uhrzeit	Ermöglicht die Auswahl eines Zeitraums. Standardmäßig sind die letzten 12 Stunden ausgewählt. <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 für einen Benutzer werden auf der Registerkarte **Details** angezeigt, wenn Sie auf in der Option **Computername** auf der Registerkarte **Sitzungen** 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 11-5. VM-Details

Option	Beschreibung
Computername	Name der Desktop- oder Anwendungssitzung.
Agent-Version	Version von Horizon Agent.
Sitzungsstatus	Status der Desktop- oder Anwendungssitzung.
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.
Sitzungsdauer	Der Zeitraum, in dem die Sitzung mit dem Verbindungsserver verbunden war.
Verbindungsserver	Der Verbindungsserver, mit dem die Sitzung verbunden ist.
Unified Access Gateway-Name	Der Name der Unified Access Gateway-Appliance. Diese Informationen werden 30 bis 60 Sekunden nach dem Herstellen einer Verbindung mit der Sitzung angezeigt.
Unified Access Gateway-IP	Die IP-Adresse der Unified Access Gateway-Appliance. Diese Informationen werden 30 bis 60 Sekunden nach dem Herstellen einer Verbindung mit der Sitzung angezeigt.
Pool	Der Name des Desktop- oder Anwendungspools.
Farm	Die Farm von RDS-Hosts für die veröffentlichte Desktop- oder Anwendungssitzung.
vCenter	Die IP-Adresse von vCenter Server.

Blast-Metriken anzeigen

Zeigt Leistungsdetails für eine virtuelle oder veröffentlichte Desktop-Sitzung an, die das VMware Blast-Anzeigeprotokoll verwendet. Um diese Leistungsdetails anzuzeigen, klicken Sie auf **Blast-Metriken anzeigen**.

Tabelle 11-6. Blast-Anzeigeprotokolldetails

Option	Beschreibung
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 11-6. 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, Arbeitsspeicher und Latenz

Zeigt Diagramme für die Auslastung von CPU und Arbeitsspeicher des virtuellen oder veröffentlichten Desktops oder der Anwendung sowie die Latenz für das PCoIP- oder Blast-Anzeigeprotokoll an.

Tabelle 11-7. CPU-, Arbeitsspeicher- und Latenzdetails

Option	Beschreibung
Sitzungs-CPU	CPU-Auslastung der aktuellen Sitzung.
Host-CPU	CPU-Auslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.
Sitzungsarbeitsspeicher	Arbeitsspeicherauslastung der aktuellen Sitzung.
Hostarbeitsspeicher	Arbeitsspeicherauslastung der virtuellen Maschine, der die Sitzung zugewiesen ist.
Sitzungslatenz	<p>Zeigt ein Diagramm der Latenz für das PCoIP- oder Blast-Anzeigeprotokoll 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>

Segmente der Sitzungsanmeldung

Zeigt die Segmente für die Anmeldungsdauer und -nutzung an, die während der Anmeldung erstellt werden.

Tabelle 11-8. 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. ■ 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. Der Zeitraum des Anmeldesegments ist für **GPO laden** 0, wenn keine globale Richtlinie konfiguriert ist.
- 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** müssen für neue Sitzungen angezeigt werden. Wenn diese Anmeldesegmente für neue Sitzungen nicht eingeblendet werden, müssen Sie den RDS-Host neu starten.

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.

Tabelle 11-9. 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.
Prozesse	Anzahl der Prozesse in der virtuellen Maschine
Aktualisieren	Mit dem Symbol „Aktualisieren“ wird die Liste der Prozesse aktualisiert.
Prozess beenden	Beendet einen aktuell ausgeführten Prozess. Hinweis Um einen Prozess beenden zu können, müssen Sie über die Rolle „Helpdesk-Administrator“ verfügen. Um einen Prozess zu beenden, wählen Sie diesen aus und klicken Sie auf die Schaltfläche Prozess beenden .

Anwendungsstatus für das 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.

Anwendungen

Für jede Anwendung können Sie den aktuellen Status und weitere Details anzeigen.

Tabelle 11-10. 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.
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>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 der VMware-Anmeldeüberwachung

Bei der VMware-Anmeldeüberwachung werden Windows-Benutzeranmeldungen überwacht und Leistungsmetriken bereitgestellt, anhand derer Administratoren, Supportmitarbeiter und Entwickler Probleme mit einer schlechten Anmeldeleistung beheben können.

Die Metriken enthalten den Zeitpunkt der Anmeldung, den Zeitpunkt des Anmeldeskripts, die CPU-/Arbeitsspeicherauslastung und die Geschwindigkeit der Netzwerkverbindung. Die Anmeldeüberwachung kann außerdem Metriken von anderen VMware-Produkten empfangen, um weitere Informationen zum Anmeldevorgang bereitzustellen.

Unterstützte Plattformen

Die Anmeldeüberwachung unterstützt dieselben Windows-Plattformen wie Horizon Agent.

Wichtige Funktionen

Die Anmeldeüberwachung bietet folgende Funktionen:

- Als Bestandteil von Horizon Agent installiert. Informationen zum Starten des Dienstes finden Sie in [KB 57051](#).
- Kann in das Horizon Help Desk Tool „Zeitprofiler“ integriert werden. Anmeldebezogene Metriken werden zusammengefasst an die Ereignisdatenbank von Horizon Agent gesendet.
- Kunden können Protokolldateien auf einen Dateiserver hochladen, um den Zugriff zu vereinfachen.
- Kann in andere VMware-Produkte, wie Horizon Persona Management, App Volumes, UEM und Horizon Agent integriert werden, die Ereignisse im Zusammenhang mit der Anmeldung an die Anmeldeüberwachung senden. Die Anmeldeüberwachung protokolliert Ereignisse, sobald sie auftreten, und zeigt die Ereignisse im Verlauf der Anmeldung sowie deren Dauer an.
- Überwacht gleichzeitige Anmeldungen auf demselben Computer.

Protokolle

Die Anmeldeüberwachung erstellt Protokolldateien für Servicestatusmeldungen sowie für Benutzersitzungen. Standardmäßig werden alle Protokolldateien unter `C:\ProgramData\VMware\VMware Logon Monitor\Logs` gespeichert.

- Hauptprotokoll: Die Hauptprotokolldatei `vm\lm.txt` enthält alle Statusmeldungen für den Dienst „vmlm“ sowie die Sitzungsereignisse, die vor und nach der Überwachung der Anmeldung eingeht. Prüfen Sie dieses Protokoll, um festzustellen, ob die Anmeldeüberwachung ordnungsgemäß ausgeführt wird.
- Sitzungsprotokoll: Das Sitzungsprotokoll enthält alle Ereignisse im Zusammenhang mit einer Benutzeranmeldungssitzung. Ereignisse beginnen in diesem Protokoll mit dem Start der Anmeldung und gelten nur für eine einzelne Benutzersitzung. Eine Zusammenfassung am Ende des Protokolls bietet eine Übersicht der wichtigsten Metriken. Prüfen Sie dieses Protokoll, um Probleme mit langsamen Anmeldungen zu beheben. Sobald die Anmeldung abgeschlossen ist, werden keine weiteren Ereignisse in das Sitzungsprotokoll geschrieben.

Metriken der Anmeldeüberwachung

Die Anmeldeüberwachung berechnet Metriken im Zusammenhang mit der Anmeldung, der Gruppenrichtlinie, dem Benutzerprofil und der Leistung. Diese Metriken bieten Administratoren detaillierte Einblicke in die Endbenutzersysteme zum Zeitpunkt der Anmeldung, anhand derer sie die Hauptursachen für Leistungsengpässe ermitteln können.

Tabelle 11-11. Metriken der Anmeldeüberwachung

Metrik	Parameter	Beschreibung
Anmeldezeitpunkt	<ul style="list-style-type: none"> ■ Start ■ Ende ■ Gesamtzeit 	Zu den Metriken gehören der Zeitpunkt des Starts der Anmeldung beim Gastbetriebssystem, der Zeitpunkt des Abschlusses der Anmeldung, der Zeitpunkt des Ladens des Profils und der Zeitpunkt der Anzeige des Desktops sowie die insgesamt für die Verarbeitung der Anmeldung auf dem Gastbetriebssystem aufgewendete Zeit. Außerhalb des Gastbetriebssystems angefallene Zeiten werden nicht berücksichtigt.
Sitzungsstart bis Start der Anmeldung	Gesamtzeit	Von dem Zeitpunkt, ab dem Windows eine Benutzersitzung erstellt, bis zum Beginn der Anmeldung.
Dauer der Profilsynchronisierung	Gesamtzeit	Die Zeit, die Windows bei der Anmeldung benötigt, um das Benutzerprofil abzustimmen.
Laden der Shell	<ul style="list-style-type: none"> ■ Start ■ Ende ■ Gesamtzeit 	Windows liefert die Startzeit des Ladens der Benutzer-Shell. Der Vorgang endet, sobald das Explorer-Fenster erstellt wird.
Anmeldung bis Laden der Struktur	Gesamtzeit	Diese Metrik gibt die Gesamtzeit vom Beginn der Anmeldung bis zum Laden der Registrierungsstruktur des Benutzers an.
Windows-Ordnerumleitung	<ul style="list-style-type: none"> ■ Start ■ Ende ■ Gesamtzeit 	Metriken für den Start der Windows-Ordnerumleitung bis zur vollständigen Anwendung sowie die insgesamt für die Aktivierung der Windows-Ordnerumleitung benötigte Zeit. Dieser Zeitraum kann lang sein, falls die erste Ordnerumleitung angewendet wurde oder wenn neue Dateien in die umgeleitete Freigabe hochgeladen wurden.
Zeit für die Gruppenrichtlinie	<ul style="list-style-type: none"> ■ Zeit für die Anwendung der Gruppenrichtlinie des Benutzers ■ Zeit für die Anwendung der Gruppenrichtlinie des Computers 	Die Metriken für die Anwendung der Gruppenrichtlinie auf das Gastbetriebssystem geben die Zeit an, die für die Anwendung der Gruppenrichtlinie für den Benutzer und der Gruppenrichtlinie für den Computer angefallen ist.

Tabelle 11-11. Metriken der Anmeldeüberwachung (Fortsetzung)

Metrik	Parameter	Beschreibung
Profilmetriken	<ul style="list-style-type: none"> ■ Profiltyp: lokal, servergespeichert und temporär ■ Profilgröße: Anzahl der Dateien, Anzahl der Ordner, Megabyte insgesamt 	<p>Metriken für das Benutzerprofil geben den Typ des Benutzerprofils an und ob es auf dem lokalen Computer oder in einem zentralen Profilspeicher gespeichert ist oder nach der Abmeldung gelöscht wird.</p> <p>Die Profilgröße enthält Metriken zur Anzahl der Dateien, der Gesamtzahl der Ordner und der Gesamtgröße des Benutzerprofils in MB.</p>
Profilgrößenverteilung	<ul style="list-style-type: none"> ■ Anzahl der Dateien zwischen 0 MB und 1 MB ■ Anzahl der Dateien zwischen 1 MB und 10 MB ■ Anzahl der Dateien zwischen 10 MB und 100 MB ■ Anzahl der Dateien zwischen 100 MB und 1 GB ■ Anzahl der Dateien zwischen 1 GB und 10 GB 	Die Anzahl der im Benutzerprofil in den verschiedenen Größenbereichen enthaltenen Dateien.
Während der Anmeldung gestartete Prozesse	<ul style="list-style-type: none"> ■ Name ■ Prozess-ID ■ Übergeordnete Prozess-ID ■ Sitzungs-ID 	Diese Werte werden für alle Prozesse protokolliert, die ab dem Start der Anmeldung bis zum Abschluss der Anmeldung gestartet wurden.
Zeit für Anmeldeskript der Gruppenrichtlinie	Gesamtzeit	Die Metrik für die Ausführung der Anmeldeskripts der Gruppenrichtlinie gibt die insgesamt für die Ausführung der Anmeldeskripts der Gruppenrichtlinie benötigte Zeit an.
Zeit für Power Shell-Skript der Gruppenrichtlinie	Gesamtzeit	Die Metrik für die Ausführung der Power Shell-Skripts der Gruppenrichtlinie gibt die insgesamt für die Ausführung der Power Shell-Skripts der Gruppenrichtlinie benötigte Zeit an.
Speicherauslastung	<ul style="list-style-type: none"> ■ Verfügbare Byte: Min., Max., Durchschnitt ■ Zugesicherte Byte: Min., Max., Durchschnitt ■ Ausgelagerter Pool: Min., Max., Durchschnitt 	WMI-Metriken für die Speicherauslastung bei der Anmeldung. Die Daten werden bis zum Abschluss der Anmeldung ermittelt. Standardmäßig deaktiviert.
CPU-Auslastung	<ul style="list-style-type: none"> ■ CPU im Leerlauf: Min., Max., Durchschnitt ■ Benutzer-CPU: Min., Max., Durchschnitt ■ Kernel-CPU: Min., Max., Durchschnitt 	WMI-Metriken für die CPU-Auslastung bei der Anmeldung. Die Daten werden bis zum Abschluss der Anmeldung ermittelt. Standardmäßig deaktiviert.

Tabelle 11-11. Metriken der Anmeldeüberwachung (Fortsetzung)

Metrik	Parameter	Beschreibung
Anmeldeskripts synchron?		Gibt an, ob die Anmeldeskripts der Gruppenrichtlinie bei der Anmeldung synchron oder asynchron ausgeführt wurden.
Netzwerkverbindungsstatus	<ul style="list-style-type: none"> ■ Getrennt ■ Wiederhergestellt 	Gibt an, ob die Netzwerkverbindung aktiv oder getrennt war.
Softwareinstallation der Gruppenrichtlinie	<ul style="list-style-type: none"> ■ Asynchron: Wahr/Falsch ■ Fehlercode ■ Gesamtzeit 	Metriken für die Softwareinstallation der Gruppenrichtlinie, die angeben, ob die Installation synchron oder asynchron zur Anmeldung verlaufen ist, ob die Installationen erfolgreich war oder fehlgeschlagen ist und wie viel Zeit insgesamt für die Installation von Software mithilfe der Gruppenrichtlinie benötigt wurde.
Festplattennutzung für Volume des Profils	<ul style="list-style-type: none"> ■ Für Benutzer verfügbarer Festplattenspeicher ■ Freier Festplattenspeicher ■ Festplattenspeicher insgesamt 	Metriken zur Festplattennutzung auf dem Volume, auf dem das Benutzerprofil gespeichert ist.
Domänencontroller-Ermittlung	<ul style="list-style-type: none"> ■ Fehlercode ■ Gesamtzeit 	Metriken zum Domänencontroller. Der Fehlercode gibt an, ob beim Erreichen des Domänencontrollers ein Fehler aufgetreten ist.
Geschätzte Netzwerkbandbreite	Bandbreite	Aus Ereignis-ID 5327 erfasster Wert.
Netzwerkverbindungsdetails	<ul style="list-style-type: none"> ■ Bandbreite ■ Schwellenwert für langsame Verbindung ■ Langsame Verbindung erkannt: Wahr/Falsch 	Aus Ereignis-ID 5314 erfasste Werte.

Tabelle 11-11. Metriken der Anmeldeüberwachung (Fortsetzung)

Metrik	Parameter	Beschreibung
Einstellungen, die sich auf die Anmeldezeit auswirken können	■ Computer\Administrative Vorlagen \Anmeldung\Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten	
	■ Computer\Administrative Vorlagen \Anmeldung\Diese Programme bei der Benutzeranmeldung ausführen	
	■ Computer\Administrative Vorlagen \Benutzerprofile\Auf servergespeichertes Benutzerprofil warten	
	■ Computer\Administrative Vorlagen \Benutzerprofile\Maximale Wartezeit für das Netzwerk festlegen, wenn ein Benutzer über ein servergespeichertes Benutzerprofil oder ein Remotestammverzeichnis verfügt	
	■ Computer\Administrative Vorlagen \Gruppenrichtlinie \Anmeldeskriptverzögerung konfigurieren	
	■ Benutzer\Administrative Vorlagen \System\Anmeldung\Diese Programme bei der Benutzeranmeldung ausführen	
	■ Benutzer\Administrative Vorlagen \System\Benutzerprofile\Nur bei der An-/Abmeldung zu synchronisierende Netzwerkverzeichnisse angeben	
Metriken von Horizon Agent, Persona Management, App Volumes		VMware-Produkte, die mit der Anmeldeüberwachung interagieren, übergeben benutzerdefinierte Metriken an die Protokolle der Anmeldeüberwachung. Mithilfe dieser Metriken kann ermittelt werden, ob sich eines der Produkte negativ auf die für die Anmeldung benötigte Zeit auswirkt.

Konfigurationseinstellungen der Anmeldeüberwachung

Sie können die Einstellungen für die Anmeldeüberwachung über Windows-Registrierungswerte konfigurieren.

Registrierungseinstellungen

Navigieren Sie zum Ändern der Konfigurationseinstellungen zum Registrierungsschlüssel HKLM \Software\VMware, Inc.\VMware Logon Monitor.

Tabelle 11-12. Konfigurationswerte für die Anmeldeüberwachung

Registrierungsschlüssel	Typ	Beschreibung
RemoteLogPath	REG_SZ	<p>Pfad zur Remotefreigabe für das Hochladen von Protokollen. Wenn Protokolle in eine Remoteprotokollfreigabe kopiert werden, werden sie in den im Registrierungsschlüssel „RemoteLogPath“ angegebenen Ordnern gespeichert. Beispiel: \\server\share\%username%.%userdomain%. Die Anmeldeüberwachung erstellt die Ordner gegebenenfalls. Standardmäßig deaktiviert.</p> <ul style="list-style-type: none"> ■ UNC-Pfad zum Remoteprotokollordner ■ Optional; wenn nicht konfiguriert, wird das Protokoll nicht hochgeladen. ■ Optionale lokale Umgebungsvariablen werden unterstützt.
Flags	REG_DWORD	<p>Dieser Wert ist eine Bitmaske, die das Verhalten der Anmeldeüberwachung beeinflusst.</p> <ul style="list-style-type: none"> ■ Indem Sie den Wert „0x4“ festlegen oder entfernen, aktivieren bzw. deaktivieren Sie die Metriken für die CPU und den Arbeitsspeicher. Standardmäßig deaktiviert. ■ Indem Sie den Wert „0x8“ festlegen oder entfernen, aktivieren bzw. deaktivieren Sie die Metriken für Verarbeitungsereignisse und Anmeldeskripts. Standardmäßig deaktiviert. ■ Mit dem Wert „0x2“ aktivieren bzw. deaktivieren Sie die Integration in Horizon 7. Standardmäßig aktiviert. ■ Mit dem Wert „0x1“ deaktivieren Sie Absturzabbilder. Absturzabbilder werden unter C:\ProgramData\VMware\VMware Logon Monitor\Data gespeichert. Standardmäßig deaktiviert. ■ Zum Erstellen von Ordnern pro Benutzer in Remote-Pfaden muss der Wert 0x10 festgelegt werden. Standardmäßig deaktiviert.
LogMaxSizeMB	REG_DWORD	Maximale Größe des Hauptprotokolls in MB. Standardmäßig sind dies 100 MB.
LogKeepDays	REG_DWORD	Anzahl der Tage, die maximal im Hauptprotokoll vorhanden sind, bevor rolliert wird. Standardmäßig sind dies 7 Tage.

Zeitprofilereinstellungen

Die Anmeldeüberwachung ist in den Zeitprofiler für den Horizon-Helpdesk integriert. Der Zeitprofiler ist standardmäßig deaktiviert.

- Führen Sie `vdadmin -I -timingProfiler -enable` aus, damit die Anmeldeüberwachung den Zeitprofiler verwendet, um Ereignisse in die Ereignisdatenbank zu schreiben.
- Führen Sie `vdadmin -I -timingProfiler -disable` aus, um die Verwendung des Zeitprofilers durch die Anmeldeüberwachung zu deaktivieren.

Verwenden von VMware Horizon Performance Tracker

Der VMware Horizon Performance Tracker ist ein Dienstprogramm, das auf einem Remote-Desktop ausgeführt wird und die Leistung des Anzeigeprotokolls und die Systemressourcennutzung überwacht. Sie können auch einen Anwendungspool erstellen und den Horizon Performance Tracker als eine veröffentlichte Anwendung ausführen.

Konfigurieren von VMware Horizon Performance Tracker

Sie können den Horizon Performance Tracker in einem Remote-Desktop ausführen. Sie können den Horizon Performance Tracker auch als veröffentlichte Anwendung ausführen.

Funktionen von Horizon Performance Tracker

Der Horizon Performance Tracker zeigt kritische Daten für folgende Funktionen an:

Tabelle 11-13. Funktionen von Horizon Performance Tracker

Leistungsüberwachung	Details
Protokollieren bestimmter Daten	<ul style="list-style-type: none"> ■ Encoder-Name: Der Name des im Anzeigeprotokoll verwendeten Encoders ■ Verwendete Bandbreite: Die gesamte Bandbreite der durchschnittlichen eingehenden und ausgehenden Bandbreite für Anzeigeprotokoll, PCoIP oder Blast im Abfragezeitraum ■ Frame-Rate pro Sekunde: Anzahl der Bildverarbeitungs-Frames, die in einem Abfragezeitraum von einer Sekunde codiert wurden ■ Audio ein: Gibt an, ob die Audiofunktion eingeschaltet ist ■ Audio gestartet: gibt an, ob die Audiofunktion gestartet wurde ■ CPU-Auslastung: <ul style="list-style-type: none"> ■ Encoder-CPU: CPU-Auslastung durch den Anzeigeprotokoll-Encoder in der aktuellen Benutzersitzung ■ System-CPU: Gesamte CPU-Auslastung des Systems
Transporttyp	<ul style="list-style-type: none"> ■ Client an Remotesitzung: Das vom Client zum Remote-Peer verwendete UDP- oder TCP-Transportpaket ■ Remotesitzung an Client: Das vom Remote-Peer zum Client verwendete UDP- oder TCP-Transportpaket ■ Horizon Connection Server: Das zum Herstellen einer Verbindung zu einer Verbindungsserver-Instanz verwendete UDP- oder TCP-Transportpaket
Systemzustand	<ul style="list-style-type: none"> ■ Geschätzte Bandbreite: geschätzte verfügbare Bandbreite insgesamt zwischen Horizon Client und Horizon Agent ■ Roundtrip: Roundtrip-Latenz in Millisekunden zwischen Horizon Agent und Horizon Client
Sitzungskontext	<ul style="list-style-type: none"> ■ Serverdetails, wie DNS-Name, Domänenname, ob getunnelt, URL, Remote-IP-Adresse ■ Details zum Clientcomputer, Anzahl Bildschirme, IP-Adresse, Tastatur und Maus-Layout, Sprache, Zeitzone
Protokollwechsel in Echtzeit	

Hinweis Der Horizon Performance Tracker erfasst und zeigt nur Daten an, wenn Horizon Agent in einer virtuellen Desktop-Sitzung ausgeführt wird.

Systemanforderungen für Horizon Performance Tracker

Der Horizon Performance Tracker unterstützt die folgenden Konfigurationen.

Tabelle 11-14. Systemanforderungen für Horizon Performance Tracker

System	Anforderungen
Betriebssysteme für virtuelle Desktops	Alle Betriebssysteme, die Horizon Agent unterstützen, außer Linux-Agenten.
Betriebssysteme für Clientcomputer:	Alle Horizon Client-Versionen werden unterstützt. Horizon Client für Linux und Horizon Client für Windows 10 UWP werden jedoch nicht als veröffentlichte Anwendungen unterstützt.
Anzeigeprotokolle	VMware Blast und PCoIP
.NET Framework	Für Horizon Performance Tracker ist .NET Framework Version 4.0 oder höher erforderlich.

Installieren von Horizon Performance Tracker

Horizon Performance Tracker ist eine benutzerdefinierte Setup-Option im Horizon Agent-Installationsprogramm. Sie müssen die Option auswählen, da sie standardmäßig nicht aktiviert ist. Der Horizon Performance Tracker ist sowohl für IPv4 als auch für IPv6 verfügbar.

Sie können den Horizon Performance Tracker auf einem virtuellen Desktop oder auf einem RDS-Host installieren. Wenn Sie den Horizon Performance Tracker auf einem RDS-Host installieren, können Sie ihn als veröffentlichte Anwendung veröffentlichen und die veröffentlichte Anwendung über Horizon Client ausführen. Weitere Informationen finden Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Bei der Installation wird eine Verknüpfung auf dem Desktop erstellt.

Konfigurieren von Gruppenrichtlinieneinstellungen für Horizon Performance Tracker

Sie können Gruppenrichtlinieneinstellungen konfigurieren, um die Standardeinstellungen zu ändern. Siehe [Konfigurieren der Gruppenrichtlinieneinstellungen für den Horizon Performance Tracker](#).

Konfigurieren der Gruppenrichtlinieneinstellungen für den Horizon Performance Tracker

Um den Horizon Performance Tracker zu konfigurieren, installieren Sie die ADMX-Vorlagendatei für den Horizon Performance Tracker (`perf_tracker.admx`) auf dem Agent-Computer und verwenden Sie den lokalen Gruppenrichtlinien-Editor, um die Richtlinieneinstellungen zu konfigurieren.

Alle ADMX-Dateien, die Gruppenrichtlinieneinstellungen für Horizon 7 bereitstellen, sind in der Datei `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` verfügbar, wobei `x.x.x` für die Version und `yyyyyy` für die Build-Nummer steht. Sie können die Datei von der VMware-Download-Site unter <https://my.vmware.com/web/vmware/downloads> herunterladen. Wählen Sie unter „Desktop & End-User Computing“ den VMware Horizon 7-Download, der die ZIP-Datei enthält.

Verfahren

- 1 Extrahieren Sie die Datei `perf_tracker.admx` aus der Datei `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` und kopieren Sie sie in den Ordner `%systemroot%\PolicyDefinitions` auf dem Agent-Computer.
- 2 Extrahieren Sie die Datei `perf_tracker.adml` aus der Datei `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` und kopieren Sie sie in den Unterordner der entsprechenden Sprache `%systemroot%\PolicyDefinitions\` auf dem Agent-Computer.

Kopieren Sie beispielsweise die Version `de_de` der Datei `perf_tracker.adml` in den Unterordner `%systemroot%\PolicyDefinitions\de_de`.

- 3 Starten Sie den lokalen Gruppenrichtlinien-Editor (`gpedit.msc`) und navigieren Sie zu **Computerkonfiguration > Administrative Vorlagen > VMware Horizon Performance Tracker**.
- 4 Bearbeiten Sie die Gruppenrichtlinieneinstellungen.

Einstellung	Beschreibung
Grundeinstellung für Horizon Performance Tracker	Wenn aktiviert, können Sie die Häufigkeit in Sekunden festlegen, in der der Horizon Performance Tracker Daten erfasst.
Automatischen Start von Horizon Performance Tracker in Remote-Desktop-Verbindung aktivieren	Wenn aktiviert, wird der Horizon Performance Tracker automatisch gestartet, wenn sich ein Benutzer bei einer Remote-Desktop-Verbindung anmeldet. Wählen Sie Deaktivieren aus, um diese GPO-Einstellung zu löschen.
Automatischen Start von Horizon Performance Tracker in Remoteanwendungsverbindung aktivieren	Wenn aktiviert, wird der Horizon Performance Tracker automatisch gestartet, wenn sich ein Benutzer bei einer Remoteanwendungsverbindung anmeldet. Wählen Sie Deaktivieren aus, um diese GPO-Einstellung zu löschen.

- 5 Damit die Änderungen wirksam werden, starten Sie den Horizon Performance Tracker auf dem Agent-Computer neu.

Ausführen von Horizon Performance Tracker

Mit Horizon Client können Sie den Horizon Performance Tracker in einem Remote-Desktop oder als veröffentlichte Anwendung ausführen.

Wenn die verwendete Horizon Client-Plattform mehrere Sitzungen unterstützt, können Sie mehrere veröffentlichte Horizon Performance Tracker-Anwendungen aus verschiedenen Farmen ausführen. Auf Windows- und Mac-Clients, die mehrere Sitzungen unterstützen, gibt der Computernamen im Übersichtsfenster die Farm an, aus der die veröffentlichte Anwendung stammt. Auf IOS- und Android-Clients und in HTML Access wird jeweils nur eine Sitzung unterstützt. Wenn Sie eine zweite Sitzung aus einer anderen Farm öffnen, wird die erste Sitzung geschlossen.

Voraussetzungen

- Installieren und konfigurieren Sie den Horizon Performance Tracker. Siehe [Konfigurieren von VMware Horizon Performance Tracker](#).

- Konfigurieren Sie die Gruppenrichtlinieneinstellungen für den Horizon Performance Tracker. Siehe [Konfigurieren der Gruppenrichtlinieneinstellungen für den Horizon Performance Tracker](#).

Verfahren

- ◆ Um den Horizon Performance Tracker in einem Remote-Desktop auszuführen, verwenden Sie Horizon Client oder HTML Access, um eine Verbindung mit dem Server herzustellen und den Remote-Desktop zu starten.

Wenn der Horizon Performance Tracker beim Öffnen des Remote-Desktops nicht automatisch gestartet wird, können Sie auf dem Windows-Desktop auf die Verknüpfung von **VMware Horizon Performance Tracker** doppelklicken oder den Horizon Performance Tracker wie andere Windows-Anwendungen starten.

Klicken Sie auf der Taskleiste des Remote-Desktops mit der rechten Maustaste auf das Symbol für den VMware Horizon Performance Tracker, um Optionen zum Anzeigen des Übersichtsfensters oder der flexiblen Leiste auszuwählen oder um die Anwendung zu beenden.

- ◆ Um den Horizon Performance Tracker als veröffentlichte Anwendung auszuführen, verwenden Sie Horizon Client oder HTML Access, um eine Verbindung mit dem Server herzustellen, und starten Sie die veröffentlichte Horizon Performance Tracker-Anwendung.

Wie Sie die veröffentlichte Horizon Performance Tracker-Anwendung verwenden, hängt vom Typ des von Ihnen verwendeten Clients ab. Mit Horizon Client für Linux oder Horizon Client für Windows 10 UWP können Sie den Horizon Performance Tracker nicht als veröffentlichte Anwendung ausführen.

- Mit Horizon Client für Windows wird das VMware Horizon Performance Tracker-Symbol in der Taskleiste des Windows-Clientsystems angezeigt. Doppelklicken Sie auf dieses Symbol, um den Horizon Performance Tracker auf dem Windows-Client zu öffnen. Sie können mit der rechten Maustaste auf dieses Symbol klicken, um Optionen auszuwählen, wie die Anzeige des Übersichtsfensters oder der flexiblen Leiste, oder um die Anwendung zu beenden.
- Mit Horizon Client für Mac wird das VMware Horizon Performance Tracker-Symbol in der Menüleiste des Mac-Clientsystems angezeigt. Doppelklicken Sie auf dieses Symbol, um den Horizon Performance Tracker auf dem Mac-Client zu öffnen. Sie können auch mit der rechten Maustaste auf dieses Symbol klicken, um Optionen auszuwählen, wie die Anzeige des Übersichtsfensters oder der flexiblen Leiste, oder um die Anwendung zu beenden.
- Mit Horizon Client für Android oder Horizon Client für iOS wird das VMware Horizon Performance Tracker-Symbol in Horizon Client auf der Unity Touch-Randleiste angezeigt. Sie können dieses Symbol berühren und halten, um Optionen zum Anzeigen des Übersichtsfensters oder der flexiblen Leiste auszuwählen oder um die Anwendung zu beenden.
- Mit HTML Access wird das VMware Horizon Performance Tracker-Symbol in der Randleiste von HTML Access angezeigt. Sie können mit der rechten Maustaste auf dieses Symbol klicken, um Optionen auszuwählen, wie die Anzeige des Übersichtsfensters oder der flexiblen Leiste, oder um die Anwendung zu beenden.

Nächste Schritte

Weitere Informationen zu den vom Horizon Performance Tracker angezeigten Daten finden Sie unter [Konfigurieren von VMware Horizon Performance Tracker](#).

Überwachen des Systemzustands

Mithilfe des Dashboards zum Systemzustand in Horizon Administrator können Sie rasch Probleme ermitteln, die sich auf die Ausführung von Horizon 7 oder auf den Benutzerzugriff auf Remote-Desktops auswirken können.

Das Dashboard zum Systemzustand befindet sich oben links in der Horizon Administrator-Anzeige und bietet verschiedene Links, um Berichte zur Ausführung von Horizon 7 anzuzeigen:

Sitzungen	Bietet einen Link zum Bildschirm „Globale Remote-Sitzungen“, in dem Informationen zum Status von Remote-Desktop- und Anwendungssitzungen angezeigt werden.
Problematische vCenter-VMs	Bietet einen Link zum Bildschirm „Computer“, in dem Informationen zu virtuellen vCenter-Maschinen, RDS-Hosts oder anderen Computern angezeigt werden, die von Horizon 7 als problematisch gekennzeichnet wurden.
Problematische RDS-Hosts	Bietet auf dem Bildschirm „Computer“ einen Link zur Registerkarte RDS-Hosts , in dem Informationen zu RDS-Hosts angezeigt werden, die von Horizon 7 als problematisch gekennzeichnet wurden.
Ereignisse	Bietet Links zum Bildschirm Events (Ereignisse), der nach Ereignissen und Warnungsereignissen gefiltert ist.
Systemzustand	Bietet Links zum Bildschirm „Dashboard“, in dem Übersichten über den Status der Horizon 7-Komponenten, registrierte Details zu Unified Access Gateway Version 3.4 oder höher, vSphere-Komponenten, Domänen, Desktops und Datenspeichernutzung angezeigt werden.

Das Dashboard zum Systemzustand zeigt für jedes Element einen nummerierten Link an. Dieser Wert gibt die Anzahl an Elementen an, zu denen der verknüpfte Bericht Details enthält.

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 Administrator auftreten. Sie

werden im Dashboard über die Anzahl der Ereignisse benachrichtigt. Im Ereignisbildschirm können Sie die Ereignisse im Detail untersuchen.

Hinweis Ereignisse werden in der Horizon Administrator-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 Administrator-Benutzeroberfläche anzeigen zu können.

Neben der Überwachung von Ereignissen in Horizon Administrator können Sie Horizon 7-Ereignisse im Syslog-Format generieren, damit die Analysesoftware auf die Ereignisdaten zugreifen kann. Weitere Informationen finden Sie unter [Generieren von Horizon 7-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-l“](#) und „Konfigurieren der Ereignisprotokollierung für Syslog-Server“ im Dokument *Horizon 7-Installation*.

Voraussetzungen

Erstellen und konfigurieren Sie die Ereignisdatenbank. Die erforderlichen Schritte sind im Dokument *Horizon 7-Installation* beschrieben.

Verfahren

- 1 Wählen Sie in Horizon Administrator **Überwachung > Ereignisse** aus.
- 2 (Optional) Im Ereignisfenster können Sie den Zeitraum der Ereignisse auswählen, die Ereignisse filtern und die aufgelisteten Ereignisse nach einer oder mehreren Spalten sortieren.

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 11-15. 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.

Tabelle 11-15. Von Horizon 7 angezeigte Ereignistypen (Fortsetzung)

Ereignistyp	Beschreibung
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.

Sammeln von Diagnoseinformationen für Horizon 7

Sie können Diagnoseinformationen sammeln, um den technischen Support von VMware bei der Diagnose und Behandlung von Problemen mit Horizon 7 zu unterstützen.

Sie können Diagnoseinformationen für verschiedene Horizon 7-Komponenten sammeln. Wie diese Informationen gesammelt werden, ist je nach Horizon 7-Komponente unterschiedlich.

- [Erstellen eines Data Collection Tool-Pakets für Horizon Agent](#)

Um den technischen Support von VMware bei der Fehlerbehebung für Horizon Agent zu unterstützen, müssen Sie möglicherweise den Befehl `vdmadmin` zum Erstellen eines DCT-Pakets (Data Collection Tool) verwenden. Sie können das DCT-Paket auch manuell abrufen, ohne `vdmadmin` zu verwenden.

- [Speichern von Diagnoseinformationen für Horizon Client für Windows](#)

Wenn bei der Verwendung von Horizon Client für Windows Probleme auftreten, die sich nicht mit den allgemeinen Verfahren zur Behandlung von Netzwerkproblemen lösen lassen, können Sie eine Kopie der Protokolldateien und der Informationen zur Konfiguration speichern.

- [Sammeln von Diagnoseinformationen für View Composer mithilfe des Supportskripts](#)

Mithilfe des View Composer-Supportskripts können Sie Konfigurationsdaten sammeln und Protokolldateien für View Composer generieren. Diese Informationen erleichtern den Mitarbeitern des Kundensupports von VMware die Diagnose von Problemen im Zusammenhang mit View Composer.

- [Sammeln von Diagnoseinformationen für Horizon-Verbindungsserver](#)

Mithilfe des Supporttools können Sie Protokollierungsebenen festlegen und Protokolldateien für Horizon-Verbindungsserver generieren.

- [Sammeln von Diagnoseinformationen für Horizon Agent, Horizon Client oder den Horizon-Verbindungsserver von der Konsole aus](#)

Wenn Sie über einen direkten Zugriff auf die Konsole verfügen, können Sie mit Supportskripts Protokolldateien für den Verbindungsserver, für Horizon Client oder für Remote-Desktops generieren, auf denen Horizon Agent ausgeführt wird. Diese Informationen erleichtern den Mitarbeitern des technischen Supports von VMware die Diagnose von Problemen im Zusammenhang mit diesen Komponenten.

Erstellen eines Data Collection Tool-Pakets für Horizon Agent

Um den technischen Support von VMware bei der Fehlerbehebung für Horizon Agent zu unterstützen, müssen Sie möglicherweise den Befehl `vdmadmin` zum Erstellen eines DCT-Pakets (Data Collection Tool) verwenden. Sie können das DCT-Paket auch manuell abrufen, ohne `vdmadmin` zu verwenden.

Sie können den Befehl `vdmadmin` in einer Verbindungsserver-Instanz verwenden, um ein DCT-Paket von einem Remote-Desktop anzufordern. Das Paket wird an den Verbindungsserver gesendet.

Alternativ können Sie sich bei einem bestimmten Remote-Desktop anmelden und den Befehl `support` ausführen, der das DCT-Paket auf dem Desktop erstellt. Wenn die Benutzerkontensteuerung (UAC, User Account Control) aktiviert ist, müssen Sie das DCT-Paket auf diese Weise erhalten.

Verfahren

- 1 Melden Sie sich als Benutzer mit entsprechenden Rechten an.

Option	Aktion
Auf View-Verbindungsserver mit „ <code>vdmadmin</code> “	Melden Sie sich bei einer Standard- oder Replikatinstanz des Verbindungsservers als Benutzer mit der Rolle Administratoren an.
Auf dem Remote-Desktop	Melden Sie sich auf dem Remote-Desktop als Benutzer mit Administratorrechten an.

- 2 Öffnen Sie eine Eingabeaufforderung und führen Sie den Befehl zum Generieren des DCT-Pakets aus.

Option	Aktion
Auf View-Verbindungsserver mit „ <code>vdmadmin</code> “	Um den Namen der Ausgabepaketdatei, des Desktop-Pools und der Maschine anzugeben, verwenden Sie die Optionen <code>-outfile</code> , <code>-d</code> und <code>-m</code> mit dem Befehl <code>vdmadmin</code> . <pre>vdmadmin-A [-bAuthentifizierungsargumente] -getDCT-outfile <i>lokale_Datei</i>-d<i>Desktop</i>-m<i>Maschine</i></pre>
Auf dem Remote-Desktop	Wechseln Sie in das Verzeichnis <code>c:\Programme\VMware\VMware View\Agent\DCT</code> und führen Sie folgenden Befehl aus: <pre>support</pre>

Ergebnisse

Der Befehl schreibt das Paket in die angegebene Ausgabedatei.

Beispiel: Verwenden von `vdmadmin` zum Erstellen einer Paketdatei für Horizon Agent

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
```

Nächste Schritte

Wenn bereits eine Supportanfrage geöffnet wurde, können Sie sie aktualisieren, indem Sie die DCT-Paketdatei anfügen.

Speichern von Diagnoseinformationen für Horizon Client für Windows

Wenn bei der Verwendung von Horizon Client für Windows Probleme auftreten, die sich nicht mit den allgemeinen Verfahren zur Behandlung von Netzwerkproblemen lösen lassen, können Sie eine Kopie der Protokolldateien und der Informationen zur Konfiguration speichern.

Sie können versuchen, Verbindungsprobleme mit Horizon Client für Windows zu lösen, bevor Sie die Diagnoseinformationen speichern und sich an den technischen Support von VMware wenden. Weitere Informationen finden Sie unter „Verbindungsprobleme zwischen Horizon Client und Horizon-Verbindungsserver“ im Dokument *Einrichten von virtuellen Desktops in Horizon 7*.

Informationen zum Erfassen von Supportdaten für andere Horizon Client-Plattformen finden Sie im Installations- und Einrichtungshandbuch für die jeweilige Plattform. Für Horizon Client für Mac z. B. in *VMware Horizon Client für Mac Installations- und Einrichtungshandbuch*.

Verfahren

- 1 Klicken Sie in Horizon Client auf **Supportinformationen** oder wählen Sie im Remote-Desktop-Menü **Optionen > Supportinformationen** aus.
- 2 Klicken Sie im Fenster **Supportinformationen** auf **Supportdaten sammeln** und klicken Sie bei Aufforderung auf **Ja**.

Ein Befehlsfenster zeigt den Fortschritt beim Sammeln der Informationen. Dieser Vorgang kann einige Minuten dauern.
- 3 Geben Sie im Befehlsfenster bei Aufforderung die URLs der Horizon-Verbindungsserver-Instanzen ein, für die Sie die Konfiguration von Horizon Client testen möchten. Aktivieren Sie gegebenenfalls die Option zum Generieren von Diagnose-Dumps der Horizon 7-Prozesse.

Die Informationen werden in eine ZIP-Datei in einen Ordner auf dem Desktop des Clientcomputers geschrieben.
- 4 Senden Sie über die Support-Seite der VMware-Website eine Support-Anfrage und fügen Sie die ZIP-Ausgabedatei an.

Sammeln von Diagnoseinformationen für View Composer mithilfe des Supportskripts

Mithilfe des View Composer-Supportskripts können Sie Konfigurationsdaten sammeln und Protokolldateien für View Composer generieren. Diese Informationen erleichtern den Mitarbeitern des Kundensupports von VMware die Diagnose von Problemen im Zusammenhang mit View Composer.

Voraussetzungen

Melden Sie sich am Computer an, auf dem View Composer installiert ist.

Da Sie zum Ausführen des Supportskripts das Windows Script Host-Dienstprogramm (cscript) verwenden müssen, machen Sie sich mit dem Befehl cscript vertraut. Siehe <http://technet.microsoft.com/library/bb490887.aspx>.

Verfahren

- 1 Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das Verzeichnis C:\Programme\VMware\VMware View Composer.

Wenn Sie die Software nicht in den Standardverzeichnissen installiert haben, ersetzen Sie den entsprechenden Laufwerksbuchstaben und Pfad.

- 2 Geben Sie den Befehl zur Ausführung des svi-support-Skripts ein.

```
cscript ".\svi-support.wsf" /zip
```

Über die Option /? können Sie Informationen zu anderen Befehlsoptionen anzeigen, die mit dem Skript verwendet werden können.

Nach Ausführung des Skripts werden Sie über den Namen und Speicherort der Ausgabedatei informiert.

- 3 Senden Sie über die Supportseite der VMware-Website eine Supportanfrage und fügen Sie die Ausgabedatei an.

Sammeln von Diagnoseinformationen für Horizon-Verbindungsserver

Mithilfe des Supporttools können Sie Protokollierungsebenen festlegen und Protokolldateien für Horizon-Verbindungsserver generieren.

Das Supporttool sammelt Protokollierungsdaten für den Verbindungsserver. Diese Informationen erleichtern den Mitarbeitern des technischen Supports von VMware die Diagnose von Problemen im Zusammenhang mit dem Verbindungsserver. Das Supporttool ist nicht geeignet, um Diagnoseinformationen für Horizon Client oder Horizon Agent zu sammeln. Für diese Komponenten muss stattdessen das Supportskript verwendet werden. Siehe [Sammeln von Diagnoseinformationen für Horizon Agent, Horizon Client oder den Horizon-Verbindungsserver von der Konsole aus](#).

Voraussetzungen

Melden Sie sich an einer Standard- oder Replikatinstanz des Verbindungservers als Benutzer mit der Rolle **Administratoren** an.

Verfahren

- 1 Wählen Sie **Start > Alle Programme > VMware > Protokollebenen für View-Verbindungsserver festlegen** aus.

- 2 Geben Sie im Textfeld **Auswahl** einen numerischen Wert zur Festlegung der Protokollierungsebene ein und drücken Sie die Eingabetaste.

Option	Beschreibung
0	Setzt die Protokollierungsebene auf den Standardwert zurück.
1	Legt die normale Protokollierungsebene fest.
2	Legt die Debug-Protokollierungsebene (Standardeinstellung) fest.
3	Legt die vollständige Protokollierung fest.

Das System beginnt unter Verwendung der ausgewählten Protokollierungsebene mit der Aufzeichnung von Protokollinformationen.

- 3 Wenn Sie genügend Informationen zum Verhalten des Verbindungsservers gesammelt haben, wählen Sie **Start > Alle Programme > VMware > View-Verbindungsserver-Protokollpaket generieren** aus.

Das Supporttool schreibt die Protokolldateien in den Ordner vdm-sdct auf dem Desktop der Verbindungsserver-Instanz.

- 4 Senden Sie über die Supportseite der VMware-Website eine Supportanfrage und fügen Sie die Ausgabedateien an.

Sammeln von Diagnoseinformationen für Horizon Agent, Horizon Client oder den Horizon-Verbindungsserver von der Konsole aus

Wenn Sie über einen direkten Zugriff auf die Konsole verfügen, können Sie mit Supportskripts Protokolldateien für den Verbindungsserver, für Horizon Client oder für Remote-Desktops generieren, auf denen Horizon Agent ausgeführt wird. Diese Informationen erleichtern den Mitarbeitern des technischen Supports von VMware die Diagnose von Problemen im Zusammenhang mit diesen Komponenten.

Voraussetzungen

Melden Sie sich an dem System an, für das Sie Informationen sammeln möchten. Sie müssen sich als Benutzer mit Administratorberechtigungen anmelden.

- Für Horizon Agent melden Sie sich bei der virtuellen Maschine an, auf der Horizon Agent installiert ist.
- Melden Sie sich für Horizon Client beim System mit installiertem Horizon Client an.
- Für den Verbindungsserver melden Sie sich beim Verbindungsserver-Host an.

Verfahren

- 1 Öffnen Sie ein Eingabeaufforderungsfenster und wechseln Sie in das entsprechende Verzeichnis der Horizon 7-Komponente, für die Diagnoseinformationen gesammelt werden sollen.

Option	Beschreibung
Horizon Agent	Wechseln Sie in das Verzeichnis C:\Programme\VMware View\Agent\DCT.
Horizon Client	Wechseln Sie in das Verzeichnis C:\Programme\VMware View\Client\DCT.
View-Verbindungsserver	Wechseln Sie in das Verzeichnis C:\Programme\VMware View\Server\DCT.

Wenn Sie die Software nicht in den Standardverzeichnissen installiert haben, ersetzen Sie den entsprechenden Laufwerksbuchstaben und Pfad.

- 2 Geben Sie den Befehl zur Ausführung des Supportskripts ein.

```
.\support.bat [loglevels]
```

Wenn Sie die erweiterte Protokollierung aktivieren möchten, verwenden Sie die Option `loglevels` und geben bei Aufforderung den numerischen Wert für die Protokollierungsebene ein.

Option	Beschreibung
0	Setzt die Protokollierungsebene auf den Standardwert zurück.
1	Legt die normale Protokollierungsebene fest.
2	Legt die Debug-Protokollierungsebene (Standardeinstellung) fest.
3	Legt die vollständige Protokollierung fest.
4	Legt die Protokollierung von Informationen für PCoIP fest (nur bei Horizon Agent und Horizon Client).
5	Legt die Debug-Protokollierung für PCoIP fest (nur bei Horizon Agent und Horizon Client).
6	Legt die Protokollierung von Informationen für virtuelle Kanäle fest (nur bei Horizon Agent und Horizon Client).
7	Legt die Debug-Protokollierung für virtuelle Kanäle fest (nur bei Horizon Agent und Horizon Client).
8	Legt die Ablaufprotokollierung für virtuelle Kanäle fest (nur bei Horizon Agent und Horizon Client).

Das Skript schreibt die komprimierten Protokolldateien in den Ordner `vdm-sdct` auf dem Desktop.

- 3 Die View Composer Guest Agent-Protokolle werden im Verzeichnis C:\Programme\Gemeinsame Dateien\VMware\View Composer Guest Agent `svi-ga-support` gespeichert.
- 4 Senden Sie über die Supportseite der VMware-Website eine Supportanfrage und fügen Sie die Ausgabedatei an.

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 Administrator eine benutzerdefinierte Rolle mit dem Namen „Protokollerfassende Administratoren“ mit der Berechtigung zum Erfassen von Betriebsprotokollen. Weitere Informationen finden Sie unter [Hinzufügen einer benutzerdefinierten Rolle](#).
- 2 Fügen Sie eine Beschreibung für die benutzerdefinierte Rolle hinzu.
- 3 Fügen Sie einen neuen Benutzer mit Administratorberechtigungen hinzu und wählen Sie die Berechtigung „Bestandslistenadministrator (schreibgeschützt)“ und die Rolle „Protokollerfassender Administrator“ für den Benutzer.

Ergebnisse

Die Skyline Collector-Appliance kann die Verbindungsserver-Protokolle für diesen Benutzer mit Administratorrechten abrufen, um Horizon 7-Probleme zu diagnostizieren und zu beheben.

Aktualisieren von Supportanfragen

Sie können eine vorhandene Supportanfrage auf der Support-Website aktualisieren.

Nachdem Sie eine Supportanfrage gesendet haben, erhalten Sie möglicherweise eine E-Mail vom technischen Support von VMware, in der Sie zur Bereitstellung der Ausgabedateien des Skripts `support` oder `svi-support` aufgefordert werden. Bei der Ausführung der Skripts werden Sie über den Namen und Speicherort der Ausgabedatei informiert. Antworten Sie auf diese E-Mail und hängen Sie die Ausgabedatei an Ihre Antwort an.

Wenn die Ausgabedatei für eine E-Mail-Anlage zu groß ist (10 MB oder mehr), wenden Sie sich unter Angabe der Supportanfragennummer an den technischen Support von VMware und bitten Sie um Anweisungen für einen FTP-Upload. Alternativ können Sie die Datei auf der Support-Website an Ihre vorhandene Supportanfrage anfügen.

Verfahren

- 1 Wechseln Sie zur Supportseite der VMware-Website und melden Sie sich an.
- 2 Klicken Sie auf **Supportanfrageverlauf** und suchen Sie nach der gewünschten Supportanfragenummer.
- 3 Aktualisieren Sie Ihre Supportanfrage und hängen Sie die Ausgabedatei des Skripts `support` oder `svi-support` an.

Fehlerbehebung einer nicht erfolgreichen Sicherheitsserverkopplung mit Horizon-Verbindungsserver

Ein Sicherheitsserver funktioniert womöglich nicht, wenn keine erfolgreiche Kopplung mit einer Verbindungsserver-Instanz erfolgte.

Problem

Es können die folgenden Sicherheitsserverprobleme auftreten, wenn ein Sicherheitsserver keine Kopplung mit dem Verbindungsserver herstellen konnte:

- Wenn Sie versuchen, den Sicherheitsserver ein zweites Mal zu installieren, kann sich der Sicherheitsserver nicht mit dem Verbindungsserver verbinden.
- Horizon Client kann sich nicht mit Horizon 7 verbinden. Die folgende Fehlermeldung wird angezeigt: Die Authentifizierung von View-Verbindungsserver ist fehlgeschlagen. Für die Ermöglichung einer sicheren Verbindung zu einem Desktop ist kein Gateway verfügbar. Wenden Sie sich an Ihren Netzwerkadministrator.
- Der Sicherheitsserver wird im Horizon Administrator-Dashboard als Ausgefallen angezeigt.

Ursache

Dieses Problem kann auftreten, wenn Sie begonnen haben, einen Sicherheitsserver zu installieren, und der Versuch absichtlich oder unabsichtlich abgebrochen wurde, nachdem Sie ein Kennwort für die Kopplung mit dem Sicherheitsserver eingegeben haben.

Lösung

Wenn Sie beabsichtigen, den Sicherheitsserver in Ihrer Horizon 7-Umgebung zu behalten, führen Sie folgende Schritte aus:

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Sicherheitsserver** einen Sicherheitsserver aus, wählen Sie **Auf Aktualisierung oder Neuinstallation vorbereiten** aus dem Dropdown-Menü **Weitere Befehle** aus und klicken Sie auf **OK**.
- 3 Wählen Sie auf der Registerkarte **Verbindungsserver** die Verbindungsserver-Instanz aus, die Sie mit dem Sicherheitsserver koppeln möchten, wählen Sie **Kennwort für die Kombination des Sicherheitsservers angeben** aus dem Dropdown-Menü **Weitere Befehle** aus, geben Sie das Kennwort ein und klicken Sie auf **OK**.
- 4 Installieren Sie den Sicherheitsserver erneut.

Wenn Sie vorhaben, den Sicherheitsservereintrag aus Ihrer Horizon 7-Umgebung zu entfernen, führen Sie den Befehl `vdmadmin -S` aus.

Beispiel: `vdmadmin -S -r -s security_server_name`

Fehlerbehebung der Horizon 7 Server-Zertifikatsperrüberprüfung

Ein Sicherheitsserver oder eine Verbindungsserver-Instanz, die für sichere Horizon Client-Verbindungen verwendet wird, kann in View Administrator rot angezeigt werden, wenn eine Zertifikatsperrüberprüfung beim TLS-Zertifikat des Servers nicht durchgeführt werden kann.

Problem

Ein Sicherheitsserver- oder Verbindungsserver-Symbol ist im Horizon Administrator-Dashboard rot. Mit dem Status der Horizon 7-Server wird folgende Meldung angezeigt: Das Serverzertifikat kann nicht geprüft werden.

Ursache

Die Zertifikatsperrüberprüfung kann fehlschlagen, wenn Ihre Organisation für den Internetzugriff einen Proxy-Server verwendet oder wenn eine Verbindungsserver-Instanz die Server, die die Sperrüberprüfung durchführen, aufgrund von Firewalls oder anderen Kontrollen nicht erreichen kann.

Eine Verbindungsserver-Instanz führt eine Zertifikatsperrüberprüfung für ihre eigenen Zertifikate und für die Zertifikate auf dem Sicherheitsserver durch, mit dem der Verbindungsserver kombiniert ist. Der VMware Horizon View Connection Server-Dienst wird standardmäßig mit dem Konto LocalSystem gestartet. Wenn sie unter LocalSystem ausgeführt wird, kann eine Verbindungsserver-Instanz die Proxy-Einstellungen, die im Internet Explorer konfiguriert sind, nicht für den Zugriff auf die CRL DP URL oder den OCSP-Antwortdienst verwenden, um den Widerrufstatus des Zertifikats zu ermitteln.

Sie können die Microsoft Netshell-Befehle verwenden, um die Proxy-Einstellungen in die Verbindungsserver-Instanz zu importieren, sodass der Server auf die Websites für die Zertifikatsperrüberprüfung im Internet zugreifen kann.

Lösung

- 1 Öffnen Sie auf dem Verbindungsserver-Computer ein Befehlszeilenfenster mit der Einstellung **Als Administrator ausführen**.

Klicken Sie beispielsweise auf **Start**, geben Sie **cmd** ein, klicken Sie mit der rechten Maustaste auf das Symbol **cmd.exe** und wählen Sie **Als Administrator ausführen** aus.

- 2 Geben Sie **netsh** ein und drücken Sie die Eingabetaste.
- 3 Geben Sie **winhttp** ein und drücken Sie die Eingabetaste.
- 4 Geben Sie **show proxy** ein und drücken Sie die Eingabetaste.

Netshell zeigt an, dass der Proxy auf DIREKT-Verbindung eingestellt war. Bei dieser Einstellung kann der Verbindungsserver-Computer keine Verbindung zum Internet herstellen, wenn Ihre Organisation einen Proxy verwendet.

5 Konfigurieren Sie die Proxy-Einstellungen.

Geben Sie z. B. an der Eingabeaufforderung `netsh winhttp>` die Zeichenfolge **`import proxy source=ie`** ein.

Die Proxy-Einstellungen werden auf den Verbindungsserver-Computer importiert.

6 Überprüfen Sie die Proxy-Einstellungen durch Eingabe von **`show proxy`**.

7 Starten Sie den VMware Horizon View Connection Server-Dienst neu.

8 Überprüfen Sie im Horizon Administrator-Dashboard, dass das Sicherheitsserver- oder Verbindungsserver-Symbol grün ist.

Fehlerbehebung bei der Smartcard-Zertifikatsperrüberprüfung

Die Verbindungsserver-Instanz oder der Sicherheitsserver, mit der bzw. dem die Smartcard verbunden ist, kann die Zertifikatsperrüberprüfung für das TLS-Zertifikat des Servers nur dann durchführen, wenn Sie die Smartcard-Zertifikatsperrüberprüfung konfiguriert haben.

Problem

Die Zertifikatsperrüberprüfung kann fehlschlagen, wenn Ihre Organisation für den Internetzugriff einen Proxy-Server verwendet oder wenn eine Verbindungsserver-Instanz oder ein Sicherheitsserver die Server, die die Sperrüberprüfung durchführen, aufgrund von Firewalls oder anderen Kontrollen nicht erreichen kann.

Wichtig Stellen Sie sicher, dass die Zertifikatsperrlistendatei auf dem neuesten Stand ist.

Ursache

Horizon 7 unterstützt die Zertifikatsperrüberprüfung mit Zertifikatsperrlisten und dem Online Certificate Status Protocol (OCSP). Eine Zertifikatsperrliste 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. Der Zugriff auf die Zertifizierungsstelle muss über den Verbindungsserver- oder Sicherheitsserverhost möglich sein. Dieses Problem kann nur auftreten, wenn Sie die Zertifikatsperrüberprüfung für Smartcard-Zertifikate konfiguriert haben. Siehe [Verwenden der Smartcard-Zertifikatsperrüberprüfung](#).

Lösung

- 1 Erstellen Sie eine eigene (manuelle) Vorgehensweise für das Herunterladen einer aktuellen Zertifikatsperrliste von der Website der Zertifizierungsstelle in ein Verzeichnis auf Ihrem Horizon 7 Server.
- 2 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`

- 3 Fügen Sie die Eigenschaften `enableRevocationChecking` und `crlLocation` in der Datei `locked.properties` zum lokalen Verzeichnis hinzu, in dem die Zertifikatsperrliste gespeichert ist.
- 4 Starten Sie den Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Weitere Informationen zur Fehlerbehebung

Weitere Informationen zur Fehlerbehebung finden Sie in VMware Knowledge Base-Artikeln.

Die VMware Knowledge Base (KB) wird kontinuierlich mit neuen Informationen zur Fehlerbehebung für VMware-Produkte aktualisiert.

Weitere Informationen zur Fehlerbehebung für Horizon 7 finden Sie in den KB-Artikeln auf der VMware KB-Website:

<http://kb.vmware.com/selfservice/microsites/microsite.do>

Verwenden des Befehls „vdmadmin“

12

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 `vdmadmin` 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 `vdmadmin` 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 `vdmadmin` 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 `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.

- **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.

- **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 berechnigte 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 berechnigt sind.

- **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.

- **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.

- **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 [Kapitel 6 Konfigurieren der rollenbasierten Verwaltungsdelegierung](#).

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 12-1. 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 12-2. 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“ .
-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“ .
-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“ .

Tabelle 12-2. Optionen des Befehls „vdmadmin“ (Fortsetzung)

Option	Beschreibung
-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 12-3. 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 12-3. 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.

```
vdmadmin -A -d dtpool2 -m machine1 -getloglevel
```

Legen Sie die Protokollierungsebene von Horizon Agent für die Maschine „machine1“ im Desktop-Pool „dtpool2“ fest.

```
vdmadmin -A -d dtpool2 -m machine1 -setloglevel debug
```

Zeigen Sie die Liste der Horizon Agent-Protokolldateien für die Maschine „machine1“ im Desktop-Pool „dtpool2“ an.

```
vdmadmin -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`.

```
vdmadmin -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 12-4. 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 12-5. 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 12-6. 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.

```
vdadmin -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 `vdadmin` mit der Option `-I` verwenden, um die verfügbaren Berichte zum Horizon 7-Betrieb aufzulisten und die Ergebnisse beim Ausführen eines dieser Berichte anzuzeigen.

Syntax

```
vdadmin
-I [-b Authentifizierungsargumente] -list [-xml] [-w | -n]
```

```
vdadmin
-I [-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 `vdadmin` auch mit der Option `-I` 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 12-7. 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 12-8. 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 12-9. 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 `vdmadmin` mit der Option `-M` verwenden, um Informationen zur Konfiguration virtueller Maschinen oder physischer Computer anzuzeigen.

Syntax

```
vdmadmin
-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 Maschinenstatus 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 12-10. 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 [Zulassen, dass vSphere Speicherplatz auf virtuellen Linked-Clone-Maschinen freigibt](#).
- 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 12-11. 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 12-12. 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 12-12. 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 12-13. 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 12-14. 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 12-14. 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 12-15. 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 12-15. 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 12-16. 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 12-16. 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

```
vdmadmin
-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 `vdmadmin` 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 `vdmadmin` 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`.

```
vdmadmin -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 12-17. 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 12-18. 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 12-18. 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 12-19. 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 12-20. 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
```