

Administration von View

VMware Horizon 6 6.0



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 © 2009–2014 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Verwaltung von View 11

1 Verwenden von View Administrator 12

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

2 View-Verbindungsserver wird konfiguriert 17

- Konfigurieren von vCenter Server und View Composer 17
 - Erstellen eines Benutzerkontos für View Composer-AD-Vorgänge 17
 - Hinzufügen von vCenter Server-Instanzen zu View 19
 - Konfigurieren von View Composer-Einstellungen 21
 - Konfigurieren von View Composer-Domänen 22
 - Zulassen, dass vSphere Speicherplatz auf virtuellen Maschinen mit verknüpften Klonen freigibt 23
 - Konfigurieren der View-Speicherbeschleunigung für vCenter Server 25
 - Grenzwerte für parallele Vorgänge für vCenter Server und View Composer 27
 - Einstellen der Anzahl paralleler Vorgänge zum Ändern des Betriebszustands, um Remote-Desktop-Anmeldungsüberlastungen zu unterstützen 28
 - Akzeptieren des Fingerabdrucks eines standardmäßigen SSL-Zertifikats 29
 - Entfernen einer vCenter Server-Instanz aus View 31
 - Entfernen von View Composer aus View 31
 - Konflikte bei eindeutigen IDs für vCenter Server 32
- Sichern von View-Verbindungsserver 33
- Konfigurieren der Einstellungen für Clientsitzungen 33
 - Festlegen von Optionen für Clientsitzungen und -verbindungen 33
 - Ändern des Kennworts für die Datenwiederherstellung 34
 - Globale Einstellungen für Clientsitzungen 35
 - Globale Sicherheitseinstellungen für Clientsitzungen und -verbindungen 37
 - Sicherheitsmodus für Nachrichten für View-Komponenten 38
 - Konfigurieren des sicheren Tunnels und des PCoIP Secure Gateway 40
 - Konfigurieren des sicheren HTML-Zugriff 41
 - Verschieben von SSL-Verbindungen auf Zwischenserver 42
- Deaktivieren oder Aktivieren von View-Verbindungsserver 45
- Bearbeiten der externen URLs 46
- Beitreten oder Verlassen des Programms zur Verbesserung der Benutzerfreundlichkeit 47
- View LDAP-Verzeichnis 48

3 Einrichten der Authentifizierung 49

- Verwenden der zweistufigen Authentifizierung 49
 - Anmeldung unter Verwendung der zweistufigen Authentifizierung 50
 - Aktivieren der zweistufigen Authentifizierung in View Administrator 51
 - Fehlerbehebung bei Verweigerung des Zugriffs auf RSA SecurID 54
 - Fehlerbehebung bei Verweigerung des Zugriffs auf RADIUS 54
- Verwenden der Smartcard-Authentifizierung 55
 - Anmelden über eine Smartcard 55
 - Konfigurieren der Smartcard-Authentifizierung 56
 - Vorbereiten von Active Directory für die Smartcard-Authentifizierung 62
 - Überprüfen der Smartcard-Authentifizierungskonfiguration 66
- Verwenden der SAML-Authentifizierung zur Workspace-Integration 68
 - Konfigurieren der SAML-Authentifikatoren in View Administrator 69
- Verwenden der Smartcard-Zertifikatssperrüberprüfung 71
 - Anmelden bei Verwendung der Überprüfung von Zertifikatssperrlisten 72
 - Anmelden bei Verwendung der OCSP-Zertifikatssperrüberprüfung 72
 - Konfigurieren der Überprüfung von Zertifikatssperrlisten 72
 - Konfigurieren der OCSP-Zertifikatssperrüberprüfung 73
 - Eigenschaften der Smartcard-Zertifikatssperrüberprüfung 74
- Verwenden der Funktion „Als aktueller Benutzer anmelden“, die mit Windows-basierten Horizon Client-Instanzen verfügbar ist 75
- Zulassen, dass Benutzer Anmeldeinformationen speichern 77

4 Konfigurieren der rollenbasierten Verwaltungsdelegierung 78

- Grundlegendes zu Rollen und Berechtigungen 78
- Verwendung von Zugriffsgruppen zur Delegierung der Verwaltung von Pools und Farmen 79
 - Unterschiedliche Administratoren für unterschiedliche Zugriffsgruppen 80
 - Unterschiedliche Administratoren für dieselbe Zugriffsgruppe 80
- Grundlegendes zu Berechtigungen 81
- Verwalten von Administratoren 82
 - Erstellen eines Administrators 83
 - Entfernen eines Administrators 84
- Verwalten und Überprüfen von Berechtigungen 84
 - Hinzufügen einer Berechtigung 85
 - Löschen einer Berechtigung 86
 - Überprüfen von Berechtigungen 87
- Verwalten und Prüfen von Zugriffsgruppen 88
 - Hinzufügen einer Zugriffsgruppe 88
 - Verschieben eines Desktop-Pools oder einer Farm in eine andere Zugriffsgruppe 89
 - Entfernen einer Zugriffsgruppe 89
 - Überprüfen der Desktop-Pools, Anwendungspools oder Farmen in einer Zugriffsgruppe 89

Überprüfen der vCenter-VMs in einer Zugriffsgruppe	90
Verwalten von benutzerdefinierten Rollen	90
Hinzufügen einer benutzerdefinierten Rolle	91
Ändern der Berechtigungen in einer benutzerdefinierten Rolle	91
Entfernen einer benutzerdefinierten Rolle	91
Vordefinierte Rollen und Berechtigungen	92
Vordefinierte Administratorrollen	92
Globale Berechtigungen	94
Objektspezifische Berechtigungen	95
Interne Berechtigungen	96
Erforderliche Berechtigungen für häufige Aufgaben	97
Berechtigungen für die Pool-Verwaltung	97
Berechtigungen für die Verwaltung von Computern	97
Berechtigungen für die Verwaltung persistenter Festplatten	98
Berechtigungen für die Verwaltung von Benutzern und Administratoren	98
Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle	99
Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen	100
5 Konfigurieren von Richtlinien in View Administrator und Active Directory	101
Festlegen von Richtlinien in View Administrator	101
Konfigurieren globaler Richtlinieneinstellungen	102
Konfigurieren von Richtlinien für Desktop-Pools	102
Konfigurieren von Richtlinien für Benutzer	103
View-Richtlinien	103
Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien (ADM) für View	104
ADM- und ADMX-Vorlagendateien für View	105
ADM-Vorlageneinstellungen für die View Server-Konfiguration	106
ADM-Vorlageneinstellungen für die allgemeine View-Konfiguration	107
6 Warten von View-Komponenten	110
Sichern und Wiederherstellen von View-Konfigurationsdaten	110
Sichern von View-Verbindungsserver- und View Composer-Daten	110
Wiederherstellen von View-Verbindungsserver- und View Composer-Konfigurationsdaten	114
Exportieren von Daten aus der View Composer-Datenbank	119
Überwachen von View-Komponenten	120
Überwachen des Computerstatus	121
Grundlegendes zu View-Diensten	122
Beenden und Starten der View-Dienste	122
Dienste auf einem View-Verbindungsserver-Host	123
Dienste auf einem Sicherheitsserver	124
Ändern des Produktlizenzschlüssels	124

Überwachen gleichzeitiger Verbindungen zu View und Zurücksetzen historischer Nutzungsdaten	125
Aktualisieren allgemeiner Benutzerinformationen aus Active Directory	126
Migrieren von View Composer auf eine andere Maschine	126
Anleitungen für die Migration von View Composer	127
Migrieren von View Composer mit einer vorhandenen Datenbank	128
Migrieren von View Composer ohne virtuelle Linked-Clone-Maschinen	130
Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln	131
Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst	132
Aktualisieren der Zertifikate auf einer View-Verbindungsserver-Instanz, einem Sicherheitsserver oder View Composer	133
Vom Programm zur Verbesserung der Benutzerfreundlichkeit erfasste Daten	135
Wie VMware Ihre Daten schützt	136
Vorschau von vom Programm zur Verbesserung der Benutzerfreundlichkeit erfassten Daten	136
Zusätzliche Informationen über das Programm zur Verbesserung der Benutzerfreundlichkeit	137
Von VMware erfasste globale View-Daten	138
Von VMware erfasste View-Verbindungsserver-Daten	139
Von VMware erfasste Sicherheitsserverdaten	142
Von VMware erfasste Desktop-Pool-Daten	142
Von VMware erfasste Computerdaten	146
Von VMware erfasste vCenter Server-Daten	147
Von VMware erfasste ThinApp-Daten	148
Von VMware erfasste Cloud Pod Architecture-Daten	149
Durch VMware gesammelte Horizon Client-Daten	150
Von VMware erfasste Daten	152

7 Verwalten von virtuellen Linked-Clone-Maschinen 154

Reduzieren der Größe von verknüpften Klonen durch eine Maschinenaktualisierung	154
Computer-Aktualisierungen	156
Aktualisieren von Linked-Clone-Desktops	157
Vorbereiten einer übergeordneten virtuellen Maschine für die Neuzusammenstellung von verknüpften Klonen	158
Neuzusammenstellung von virtuellen Linked-Clone-Maschinen	158
Aktualisieren verknüpfter Klone bei der Neuzusammenstellung	161
Korrigieren einer nicht erfolgreichen Neuzusammenstellung	162
Neuverteilen von virtuellen Linked-Clone-Maschinen	163
Neuverteilung verknüpfter Klone auf logische Laufwerke	164
Migrieren von virtuellen Maschinen mit verknüpften Klonen auf einen anderen Datenspeicher	166
Dateinamen von Linked-Clone-Festplatten nach einer Neuverteilung	167
Verwalten persistenter View Composer-Festplatten	167
Persistente View Composer-Festplatten	167
Trennen einer persistenten View Composer-Festplatte	168
Verbinden einer persistenten View Composer-Festplatte mit einem anderen verknüpften Klon	169

Bearbeiten des Pools oder Benutzers einer persistenten View Composer-Festplatte	170
Neuerstellung eines verknüpften Klons mit einer getrennten persistenten Festplatte	171
Wiederherstellen eines verknüpften Klons durch den Import einer persistenten Festplatte aus vSphere	172
Löschen einer getrennten persistenten View Composer-Festplatte	173

8 Verwalten von Desktop-Pools, Maschinen und Sitzungen 174

Verwalten von Desktop-Pools	174
Bearbeiten eines Desktop-Pools	174
Ändern der Einstellungen in einem vorhandenen Desktop-Pool	175
Feste Einstellungen in einem vorhandenen Desktop-Pool	177
Ändern der Größe eines automatisierten Pools, der über ein Benennungsmuster bereitgestellt wurde	177
Hinzufügen von Computern zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde	178
Deaktivieren oder Aktivieren eines Desktop-Pools	179
Deaktivieren oder Aktivieren der Bereitstellung in einem automatisierten Desktop-Pool	180
Konfigurieren der Adobe Flash-Qualität und -Drosselung	181
Adobe Flash-Qualität und -Drosselung	181
Löschen eines Desktop-Pools	182
Verwalten von VM-basierten Desktops	183
Zuweisen einer Maschine zu einem Benutzer	184
Aufheben der Benutzerzuweisung für eine dedizierte Maschine	184
Anpassen von vorhandenen Computern im Wartungsmodus	185
Überwachen des Status von VM-Desktops	185
Status von vCenter Server-VMs	186
Löschen von VM-Desktops	188
Verwalten von nicht verwalteten Computern	190
Hinzufügen eines nicht verwalteten Computers zu einem manuellen Pool	190
Entfernen eines nicht verwalteten Computers aus einem manuellen Desktop-Pool	191
Entfernen von registrierten Maschinen aus View	191
Status nicht verwalteter Computer	192
Verwalten der Remote-Desktop- und Anwendungssitzungen	193
Exportieren von View-Informationen in externe Dateien	194

9 Verwalten von Anwendungspools, Farmen und RDS-Hosts 196

Verwalten von Anwendungspools	196
Bearbeiten eines Anwendungspools	196
Löschen eines Anwendungspools	197
Verwalten von Farmen	197
Bearbeiten einer Farm	197
Löschen einer Farm	198

Aktivieren oder Deaktivieren einer Farm	198
Verwalten von RDS-Hosts	198
Bearbeiten eines RDS-Hosts	199
Entfernen eines RDS-Hosts von einer Farm	199
Entfernen eines RDS-Hosts aus View	199
Deaktivieren oder Aktivieren eines RDS-Hosts	200
Überwachen von RDS-Hosts	200
Status von RDS-Hosts	201
Konfigurieren der Adobe Flash-Drosselung in Internet Explorer für RDS-Desktops	202

10 Verwalten von ThinApp-Anwendungen in View Administrator 203

View-Anforderungen für ThinApp-Anwendungen	203
Erfassen und Speichern von Anwendungspaketen	204
Paketieren von Anwendungen	205
Erstellen einer Windows-Netzwerkfreigabe	206
Registrieren eines Anwendungs-Repositorys	206
Hinzufügen von ThinApp-Anwendungen zu View Administrator	207
Erstellen einer ThinApp-Vorlage	208
Zuweisen von ThinApp-Anwendungen zu Maschinen und Desktop-Pools	208
Empfohlene Vorgehensweisen für die Zuweisung von ThinApp-Anwendungen	210
Zuweisen einer ThinApp-Anwendung zu mehreren Computern	210
Zuweisen mehrerer ThinApp-Anwendungen zu einem Computer	211
Zuweisen einer ThinApp-Anwendung zu mehreren Desktop-Pools	212
Zuweisen mehrerer ThinApp-Anwendungen zu einem Desktop-Pool	213
Zuweisen einer ThinApp-Vorlage zu einer Maschine oder zu einem Desktop-Pool	214
Anzeigen von ThinApp-Anwendungszuweisungen	215
Anzeigen von MSI-Paketinformationen	217
Warten von ThinApp-Anwendungen in View Administrator	217
Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Computern	218
Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einer Maschine	218
Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Desktop-Pools	219
Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einem Desktop-Pool	219
Entfernen einer ThinApp-Anwendung aus View Administrator	220
Ändern oder Löschen einer ThinApp-Vorlage	220
Entfernen eines Anwendungs-Repositorys	221
Überwachen von und Fehlerbehebung bei ThinApp-Anwendungen in View Administrator	221
Keine Registrierung eines Anwendungs-Repositorys möglich	221
Kein Hinzufügen von ThinApp-Anwendungen zu View Administrator möglich	222
Kein Zuweisen einer ThinApp-Vorlage möglich	223
ThinApp-Anwendung wird nicht installiert	223
ThinApp-Anwendung wird nicht deinstalliert	224

MSI-Paket ist ungültig	225
ThinApp-Konfigurationsbeispiel	225
11 Einrichten von Clients im Kiosk-Modus	227
Konfigurieren von Clients im Kiosk-Modus	228
Vorbereiten von Active Directory und View für Clients im Kiosk-Modus	229
Festlegen von Standardwerten für Clients im Kiosk-Modus	230
Anzeigen der MAC-Adressen von Clientgeräten	232
Hinzufügen von Konten für Clients im Kiosk-Modus	232
Authentifizierung von Clients im Kiosk-Modus aktivieren	234
Überprüfen der Konfiguration von Clients im Kiosk-Modus	236
Verbinden mit Remote-Desktops über Clients im Kiosk-Modus	237
12 Fehlerbehebung bei View	240
Überwachen des Systemzustands	240
Überwachen von Ereignissen in View	241
View-Ereignismeldungen	242
Sammeln von Diagnoseinformationen für View	242
Erstellen eines Data Collection Tool-Pakets für View Agent	243
Speichern von Diagnoseinformationen für Horizon Client	244
Sammeln von Diagnoseinformationen für View Composer mithilfe des Supportskripts	245
Sammeln von Diagnoseinformationen für View-Verbindungsserver mithilfe des Supporttools	245
Sammeln von Diagnoseinformationen für View Agent, Horizon Client oder View-Verbindungsserver von der Konsole	246
Aktualisieren von Supportanfragen	248
Fehlerbehebung einer nicht erfolgreichen Sicherheitsserver-Kombination mit View-Verbindungsserver	248
Fehlerbehebung der View Server-Zertifikatssperrüberprüfung	249
Fehlerbehebung bei der Smartcard-Zertifikatssperrüberprüfung	251
Weitere Informationen zur Fehlerbehebung	251
13 Verwenden des Befehls „vdmadmin“	253
Verwendung des Befehls „vdmadmin“	255
Authentifizierung für den Befehl „vdmadmin“	256
Ausgabeformat des Befehls „vdmadmin“	256
Optionen des Befehls „vdmadmin“	257
Konfigurieren der Protokollierung in View Agent unter Verwendung der Option „-A“	258
Außerkräftsetzen von IP-Adressen unter Verwendung der Option „-A“	261
Festlegen des Namens einer View-Verbindungsserver-Gruppe unter Verwendung der Option „-C“	262
Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F“	263
Auflisten und Anzeigen von Systemüberwachungen unter Verwendung der Option „-H“	264
Auflisten und Anzeigen von Berichten zum View-Betrieb unter Verwendung der Option „-I“	266

Generieren von View-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-I“	267
Zuweisen von dedizierten Computern unter Verwendung der Option „-L“	269
Anzeigen von Informationen zu Maschinen unter Verwendung der Option „-M“	271
Rückgewinnung von Datenträgerplatz auf virtuellen Maschinen mit der Option „-M“	272
Konfigurieren von Domänenfiltern unter Verwendung der Option „-N“	273
Konfigurieren von Domänenfiltern	276
Beispiel für die Filterung zum Einschließen von Domänen	278
Beispiel für die Filterung zum Ausschließen von Domänen	279
Anzeigen der Maschinen und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“	281
Konfigurieren von Clients im Kiosk-Modus unter Verwendung der Option „-Q“	283
Anzeigen des ersten Benutzers einer Maschine unter Verwendung der Option „-R“	288
Entfernen des Eintrags für eine View-Verbindungsserver-Instanz oder einen Sicherheitsserver mit der Option „-S“	289
Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U“	290
Entsperren oder Sperren von virtuellen Maschinen unter Verwendung der Option „-V“	291
Ermitteln und Lösen von Konflikten bei LDAP-Einträgen mit der Option „-X“	292

Verwaltung von View

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

Zielgruppe

Diese Informationen sind für alle Benutzer gedacht, die View 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 View Administrator

1

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

Einen Vergleich der Vorgänge, die Sie mit View Administrator, View-Cmdlets und `vdadmin` durchführen können, finden Sie im Dokument *Integration von View*.

Dieses Kapitel enthält die folgenden Themen:

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

View Administrator und View-Verbindungsserver

View Administrator bietet eine Verwaltungsschnittstelle für View.

Abhängig von Ihrer View-Bereitstellung können Sie eine oder mehrere View Administrator-Schnittstellen verwenden.

- Verwenden Sie eine View Administrator-Schnittstelle zum Verwalten der View-Komponenten, die mit einer einzelnen, eigenständigen View-Verbindungsserver-Instanz oder einer Gruppe replizierter View-Verbindungsserver-Instanzen verknüpft sind.

Sie können den Hostnamen oder die IP-Adresse einer beliebigen replizierten Instanz verwenden, um sich bei View Administrator anzumelden.

- Sie müssen eine separate View Administrator-Schnittstelle zum Verwalten der View-Komponenten für jede einzelne, eigenständige View-Verbindungsserver-Instanz und jede Gruppe replizierter View-Verbindungsserver-Instanzen verwenden.

Sie können mithilfe von View Administrator auch Sicherheitsserver verwalten, die mit View-Verbindungsservern verknüpft sind. Jeder Sicherheitsserver ist mit einer View-Verbindungsserver-Instanz verknüpft.

Anmelden an View Administrator

Zum Ausführen anfänglicher Konfigurationsaufgaben müssen Sie sich an View Administrator anmelden. Sie können unter Verwendung einer sicheren Verbindung (SSL) auf View Administrator zugreifen.

Voraussetzungen

- Stellen Sie sicher, dass View-Verbindungsserver auf einem dedizierten Computer installiert ist.
- Vergewissern Sie sich, dass Sie einen von View Administrator unterstützten Webbrowser verwenden. Informationen zu den View Administrator-Anforderungen finden Sie im Dokument *Installation von View*.

Verfahren

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

`https://Server/admin`

Hinweis Um auf eine View-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 SSL-Zertifikat, das für die View-Verbindungsserver-Instanz konfiguriert ist. Dies führt dazu, dass der Zugriff blockiert wird oder weniger sicher ist.

Ihr Zugriff auf View Administrator hängt von der Art Zertifikat ab, die auf dem View-Verbindungsserver-Computer konfiguriert ist.

Wenn Sie den Webbrowser auf dem View-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 View-Verbindungsserver signiert ist.	Wenn Sie zum ersten Mal eine Verbindung herstellen, zeigt Ihr Webbrowser View Administrator an.
Das standardmäßige selbst signierte Zertifikat, das mit View-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 SSL-Zertifikats fortzufahren.

- 2 Melden Sie sich als Benutzer mit Anmeldeinformationen an, um auf das View Administrators-Konto zuzugreifen.

Sie geben ein View Administrators-Konto an, wenn Sie eine eigenständige View-Verbindungsserver-Instanz oder die erste View-Verbindungsserver-Instanz in einer replizierten Gruppe installieren. Das View Administrators-Konto kann die lokale Administratorengruppe (BUILTIN\Administrators) auf dem View-Verbindungsserver-Computer oder ein Domänenbenutzer- oder Gruppenkonto sein.

Nachdem Sie sich bei View Administrator angemeldet haben, können Sie **View-Konfiguration > Administratoren** auswählen, um die Liste der Benutzer und Gruppen zu ändern, die die Administratorrolle für View haben.

Tipps zur Verwendung der View Administrator-Oberfläche

Sie können mithilfe der View Administrator-Benutzeroberflächenfunktionen in View-Seiten navigieren, nach View-Objekten suchen sowie View-Objekte filtern und sortieren.

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

In [Tabelle 1-1. View Administrator-Navigations- und Anzeigefunktionen](#) werden einige weitere Funktionen beschrieben, die die Verwendung von View Administrator unterstützen.

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

View Administrator-Funktion	Beschreibung
In View Administrator-Seiten rückwärts und vorwärts navigieren	<p>Klicken Sie die Schaltfläche Zurück in Ihrem Browser, um zur vorher angezeigten View Administrator-Seite zurückzukehren. Klicken Sie auf die Schaltfläche Weiter, um zur aktuellen Seite zurückzukehren.</p> <p>Falls Sie auf die Schaltfläche Zurück des Browsers klicken, während Sie einen Assistenten oder ein Dialogfeld von View Administrator verwenden, kehren Sie zur Hauptseite von View Administrator zurück. Die im Assistenten oder Dialogfeld eingegebenen Informationen gehen dann verloren.</p> <p>In View-Versionen vor View 5.1 konnten Sie die Schaltflächen Zurück und Weiter nicht verwenden, um innerhalb von View Administrator zu navigieren. Es waren getrennte Schaltflächen Zurück und Weiter im View Administrator-Fenster zur Navigation vorgesehen. Diese Schaltflächen wurden in Version 5.1 von View entfernt.</p>
Erstellen von Lesezeichen von View Administrator-Seiten	Sie können in Ihrem Browser Lesezeichen von View Administrator-Seiten erstellen.

View Administrator-Funktion	Beschreibung
Mehrspaltige Sortierung	<p>Sie können View-Objekte mithilfe der mehrspaltigen Sortierung auf unterschiedliche Art und Weise sortieren.</p> <p>Klicken Sie auf eine Überschrift in der obersten Zeile einer View Administrator-Tabelle, um die View-Objekte alphabetisch anhand dieser Überschrift zu sortieren. Beispielsweise können Sie auf der Seite Ressourcen > Maschinen 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 View-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>
Anpassen der Tabellenspalten	<p>Sie können die Anzeige von View 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.

View Administrator-Funktion	Beschreibung
Auswählen von View-Objekten und Anzeigen von View-Objektdetails	<p>Sie können in View Administrator-Tabellen, die View-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 der 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 View 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 View-Objekte	<p>Sie können mit der rechten Maustaste auf View-Objekte in View Administrator-Tabellen klicken, um Kontextmenüs anzuzeigen. Ein Kontextmenü ermöglicht Ihnen den Zugriff auf die Befehle, die für das ausgewählte View-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 View Administrator

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

Problem

Der Text in der View Administrator-Oberfläche ist unleserlich. Es treten beispielsweise Leerzeichen in Wörtern auf.

Ursache

Für View Administrator sind Microsoft-spezifische Schriftarten erforderlich.

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.

View-Verbindungsserver wird konfiguriert

2

Nachdem Sie View-Verbindungsserver installiert und die Erstkonfiguration durchgeführt haben, können Sie vCenter Server-Instanzen und View Composer-Dienste zu Ihrer View-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 View-Verbindungsserver](#)
- [Konfigurieren der Einstellungen für Clientsitzungen](#)
- [Deaktivieren oder Aktivieren von View-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 View Administrator konfigurieren.

Sie können auch Speichereinstellungen für View 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 View-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 View Administrator an, wenn Sie View Composer-Domänen im Assistenten zum Hinzufügen von vCenter Server konfigurieren und Linked-Clone-Desktop-Pools konfigurieren und bereitstellen.

Hinzufügen von vCenter Server-Instanzen zu View

Sie müssen View zur Herstellung von Verbindungen mit den vCenter Server-Instanzen in Ihrer View-Bereitstellung konfigurieren. vCenter Server erstellt und verwaltet die virtuellen Maschinen, die View in Desktop-Pools verwendet.

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

View stellt über eine sichere Verbindung (SSL) eine Verbindung mit der vCenter Server-Instanz her.

Voraussetzungen

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

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

- Überprüfen Sie, dass auf dem vCenter Server-Host ein SSL-Serverzertifikat installiert ist. Installieren Sie in einer Produktionsumgebung ein gültiges SSL-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 View zu vCenter Server hinzufügen.

- Überprüfen Sie, dass alle Instanzen von View-Verbindungsserver 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 Zertifikatsspeichern der lokalen Windows-Computer auf den View-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 *Installation von View*.

- 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 View 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.
- 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 View Administrator **View-Konfiguration > Server**.
- 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 View kein DNS-Lookup durch, um zu überprüfen, ob ein Administrator View diesen Server zuvor unter Verwendung seiner IP-Adresse hinzugefügt hatte. Es entsteht ein Konflikt, wenn eine vCenter Server-Instanz sowohl mit dem DNS-Namen als auch mit der IP-Adresse angegeben wird.

- 4 Geben Sie den Namen des vCenter Server-Benutzers ein.
Beispiel: **domain\user** oder **user@domain.com**
- 5 Geben Sie das Kennwort für den vCenter Server-Benutzer ein.
- 6 (Optional) Geben Sie eine Beschreibung für diese vCenter Server-Instanz ein.
- 7 Geben Sie die TCP-Portnummer ein.
Der Standardport lautet 443.
- 8 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 View-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 SSL-Zertifikats](#).

Wenn View 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 View 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 View-Bereitstellung können Sie den VMware Horizon View Composer-Dienst auf einen neuen Host migrieren, um eine wachsende oder sich ändernde View-Bereitstellung zu unterstützen. Sie können die ursprünglichen View Composer-Einstellungen in View 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 verknüpften Klone enthält. Siehe [Erstellen eines Benutzerkontos für View Composer-AD-Vorgänge](#).
- Vergewissern Sie sich, dass View 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 View](#).
- 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 View 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 Domänennamen (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 SSL-Zertifikat konfiguriert ist und View-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 SSL-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 die anfänglichen vCenter Server- und View Composer-Einstellungen zu View hinzugefügt haben, können Sie weitere View Composer-Domänen hinzufügen, indem Sie die vCenter Server-Instanz in View Administrator bearbeiten.

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 (verknüpften Klone) enthält. Zum Verwalten der Konten der Linked-Clone-Maschinen in Active Directory muss der Domänenbenutzer die Berechtigungen **Computerobjekte erstellen**, **Computerobjekte löschen** und **Alle Eigenschaften schreiben** besitzen.

Siehe [Erstellen eines Benutzerkontos für View Composer-AD-Vorgänge](#).

- Überprüfen Sie in View Administrator, ob die Seiten mit den vCenter Server-Informationen und den View Composer-Einstellungen im Assistenten zum Hinzufügen von vCenter Server-Instanzen 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 Domänennamen der Active Directory-Domäne ein.
Beispiel: **domain.com**
- 3 Geben Sie den Domänenbenutzernamen (einschließlich des Domänennamens) 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 View.

Zulassen, dass vSphere Speicherplatz auf virtuellen Maschinen mit verknüpften Klonen freigibt

In vSphere 5.1 und höher können Sie die Funktion zur Rückgewinnung von Datenträgerplatz für View aktivieren. Mit Einführung von vSphere 5.1 erstellt View virtuelle Linked-Clone-Maschinen in einem effizienten Festplattenformat, welches es ESXi-Hosts erlaubt, nicht genutzten Festplattenspeicherplatz in den verknüpften Klonen zurückzugewinnen. Dadurch kann der insgesamt erforderliche Speicherplatz für verlinkte Klone 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 verknüpften Klone 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 View verknüpfte Klone 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 View verknüpfte Klone 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 Datenträgerplatz müssen Sie View Administrator verwenden, um die Rückgewinnung von Datenträgerplatz 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 verknüpften Klonen.
- 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.
- Sie funktioniert nur auf Windows XP- und Windows 7-Desktops. Sie funktioniert nicht auf Windows 8-Desktops.

Die systemeigene NFS-Snapshot-Technologie (VAAI) wird nicht in Pools unterstützt, die virtuelle Maschinen mit platzsparenden Festplatten enthalten. VAAI wird auf verknüpften Klonen mit der virtuellen Hardwareversion 9 oder höher nicht unterstützt, da diese Betriebssystemfestplatten immer speicherplatzsparend sind, sogar wenn Sie den Vorgang zur Rückgewinnung von Speicherplatz deaktivieren.

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 View 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** aus.
 - 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 View 5.2 oder höher durchführen. Sie müssen **Zurückgewinnung von Datenträgerplatz aktivieren** auswählen, wenn Sie ein Upgrade auf View 5.2 oder höher von View 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 View abzuschließen, richten Sie die Rückgewinnung von Datenträgerplatz für Desktop-Pools ein.

Konfigurieren der View-Speicherbeschleunigung für vCenter Server

In vSphere 5.0 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 View 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 View-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 View Administrator wie in dieser Vorgehensweise beschrieben aus.

Stellen Sie sicher, dass die View-Speicherbeschleunigung auch für einzelne Desktop-Pools konfiguriert ist. Die View-Speicherbeschleunigung ist standardmäßig für Desktop-Pools aktiviert. Die Funktion kann beim Erstellen oder Bearbeiten eines Desktop-Pools jedoch deaktiviert oder aktiviert werden. 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.

Sie können die View-Speicherbeschleunigung für Desktop-Pools aktivieren, die verknüpfte Klone enthalten, und auch für Pools, die vollständige virtuelle Maschinen enthalten.

Die View-Speicherbeschleunigung kann nun in Konfigurationen eingesetzt werden, in denen eine mehrstufige Speicherung von View-Replikaten verwendet wird und Replikate in einem anderen Datenspeicher gespeichert werden als verknüpfte Klone. Wenngleich bei der Verwendung der View-Speicherbeschleunigung mit der mehrstufigen Speicherung von View-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.

Voraussetzungen

- Stellen Sie sicher, dass Ihr vCenter Server und Ihre ESXi-Hosts in der Version 5.0 oder höher vorliegen.

Überprüfen Sie in einem ESXi-Cluster, ob alle Hosts mindestens in der Version 5.0 ausgeführt werden.

- Stellen Sie sicher, dass dem vCenter Server-Benutzer die Berechtigung **Global > Agieren als vCenter Server** in vCenter Server zugewiesen wurde.

Lesen Sie dazu die Themen im Dokument *Installation von View*, in denen die View- und View Composer-Rechte beschrieben werden, die der vCenter Server-Benutzer benötigt.

Verfahren

- 1 Führen Sie in View 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 Cachegröße muss zwischen 100 MB und 2.048 MB betragen.

- 4 Um für einen einzelnen ESXi-Host eine andere Cachegröße anzugeben, wählen Sie einen ESXi-Host aus, und klicken Sie auf **Cachegröße bearbeiten**.
 - a Aktivieren Sie im Dialogfeld „Host-Cache“ das Kontrollkästchen **Standard-Hostzwischenspeichergröße 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 View 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 View 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 Desktop- und Anwendungspools in View*.

Grenzwerte für parallele Vorgänge für vCenter Server und View Composer

Wenn Sie vCenter Server zu View 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 View-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 View-Verbindungsserver verwaltet werden.</p> <p>Der Standardwert lautet 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 verknüpfte Klone.</p>

Einstellung	Beschreibung
Maximale parallele View Composer-Wartungsvorgänge	<p>Legt die maximale Anzahl an parallelen View Composer-Vorgängen zur Aktualisierung, Neuzusammenstellung und Neuverteilung fest, die auf den verknüpften Klonen ausgeführt werden können, die von dieser View Composer-Instanz verwaltet werden.</p> <p>Der Standardwert lautet 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 verknüpfte Klone.</p>
Maximale parallele View Composer-Bereitstellungsvorgänge	<p>Legt die maximale Anzahl an parallelen Erstellungs- und Löschvorgängen fest, die auf verknüpften Klonen ausgeführt werden können, die von dieser View Composer-Instanz verwaltet werden.</p> <p>Der Standardwert lautet 8.</p> <p>Diese Einstellung gilt nur für verknüpfte Klone.</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 View-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 Einschalttrate während Spitzenzeiten ist. Bei einer vorsichtigen Herangehensweise unterstützt die Standardeinstellung 50 eine Einschalttrate während Spitzenzeiten von 10 Desktops pro Minute.

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

Akzeptieren des Fingerabdrucks eines standardmäßigen SSL-Zertifikats

Wenn Sie vCenter Server und View Composer-Instanzen zu View hinzufügen, müssen Sie sicherstellen, dass die SSL-Zertifikate, die für vCenter Server und View Composer-Instanzen verwendet werden, gültig sind und vom View-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 ein vCenter Server oder eine View Composer-Instanz mit einem Zertifikat konfiguriert ist, das von einer Zertifizierungsstelle (CA) signiert ist, und das Stammzertifikat vom View-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 View-Verbindungsserver das Stammzertifikat jedoch nicht als vertrauenswürdig einstuft, müssen Sie festlegen, ob der Zertifikatsfingerabdruck 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 SSL-Zertifikat verwenden, aber Sie müssen das Zertifikat separat für jede Komponente konfigurieren.

Einzelheiten zur Konfiguration von SSL-Zertifikaten finden Sie unter „Konfigurieren von SSL-Zertifikaten für View Server“ im Dokument *Installation von View*.

Zunächst fügen Sie vCenter Server und View Composer in View Administrator hinzu; verwenden Sie dazu den Assistenten zum Hinzufügen von vCenter Server. 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 Zertifikatsfingerabdruck 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 View 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 auf Überprüfen** und führen Sie die hier beschriebenen Schritte aus.

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

Verfahren

- 1 **Klicken Sie auf** Zertifikat anzeigen, wenn View Administrator ein Dialogfeld Ungültiges Zertifikat ermittelt anzeigt.
- 2 Überprüfen Sie den Zertifikatsfingerabdruck 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 Zertifikatsfingerabdruck anzuzeigen.

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

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

Überprüfen Sie ebenfalls, ob die Fingerabdrücke für einen SAML-Authentifikator übereinstimmen.

5 Geben Sie an, ob der Zertifikatsfingerabdruck 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 View

Sie können die Verbindung zwischen View und einer vCenter Server-Instanz entfernen. Dann werden in View 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. Siehe [Löschen eines Desktop-Pools](#).

Verfahren

- 1 Klicken Sie 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 View über keinen Zugriff auf die virtuellen Maschinen mehr verfügt, die von dieser vCenter Server-Instanz verwaltet werden.

- 4 Klicken Sie auf **OK**.

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

Entfernen von View Composer aus View

Sie können die Verbindung zwischen View 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 Maschinen mit verknüpftem Klon, die über View Composer erstellt wurden, aus View entfernen. View verhindert, dass Sie View Composer entfernen, wenn noch verknüpfte Klone vorhanden sind. Nachdem die Verbindung zu View Composer deaktiviert wurde, kann View neue verknüpfte Klone weder bereitstellen noch verwalten.

Verfahren

1 Entfernen Sie die Desktop-Pools mit verknüpften Klonen, die von View Composer erstellt wurden.

a Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.

b Wählen Sie einen Desktop-Pool mit verknüpften Klonen aus und klicken Sie auf **Löschen**.

Sie werden über ein Dialogfeld gewarnt, dass Sie den Desktop-Pool mit verknüpften Klonen endgültig aus View löschen. Falls die virtuellen Maschinen mit verknüpften Klonen 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 verknüpftem Klon, 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**.

In dieser vCenter Server-Instanz können Sie keine Desktop-Pools mit verknüpften Klonen 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 View 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 View 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 View-Verbindungsserver

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

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

Konfigurieren der Einstellungen für Clientsitzungen

Sie können globale Einstellungen für die Clientsitzungen und -verbindungen konfigurieren, die von einer View-Verbindungsserver-Instanz oder replizierten Gruppe verwaltet werden. Sie können die Dauer bis zur Zeitüberschreitung festlegen, Prä-Anmelde- 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 View-Verbindungsserver-Instanz zugeordnet. Sie wirken sich auf alle Clientsitzungen aus, die von einer eigenständigen View-Verbindungsserver-Instanz oder einer Gruppe von replizierten Instanzen verwaltet werden.

Sie können View-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 View 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 View-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 View-Verbindungsserver sichern, wird die View LDAP-Konfiguration in Form verschlüsselter LDIF-Daten exportiert. Um die verschlüsselte View-Sicherungskonfiguration wiederherzustellen, müssen Sie das Kennwort für die Datenwiederherstellung bereitstellen.

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 View 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.

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

Nächste Schritte

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

Globale Einstellungen für Clientsitzungen

Allgemeine globale Einstellungen bestimmen die Dauer bis zur Zeitüberschreitung, SSO-Aktivierung und Zeitüberschreitungslimits sowie Statusaktualisierungen in View Administrator. Sie bestimmen außerdem, ob Prä-Anmeldenachrichten und Warnmeldungen angezeigt werden und ob Windows Server 2008 R2 von View Administrator als unterstütztes Betriebssystem für Remote-Desktops behandelt wird.

Änderungen an sämtlichen Einstellungen in der unten angegebenen Tabelle werden sofort wirksam. Der View-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 View Administrator-Sitzung im Leerlauf bleibt, bevor die Sitzung abläuft.</p> <p>Wichtig Wenn Sie den Zeitüberschreitungswert für die View Administrator-Sitzung auf eine hohe Minutenzahl einstellen, steigt das Risiko, dass View Administrator unautorisiert genutzt werden könnte. Seien Sie vorsichtig, wenn Sie zulassen, dass eine Sitzung lange Zeit im Leerlauf bleibt.</p> <p>Standardmäßig beträgt die Zeitüberschreitung für die View 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 View alle Desktops und Anwendungen. Alle Desktops und Anwendungen werden gleichzeitig getrennt, unabhängig davon, wann der Benutzer sie geöffnet hat.</p> <p>Für Clients, die die Remote-Ausführung von Anwendungen nicht unterstützen, gilt für das maximale Zeitlimit ein Wert von 1200 Minuten, wenn der Wert dieser Einstellung auf Nie gesetzt wurde oder 1200 Minuten übersteigt.</p> <p>Die Standardeinstellung ist Nach 600 Minuten.</p>
Einmalige Anmeldung (Single Sign-On, SSO):	<p>Bei aktivierter SSO werden die Anmeldeinformationen eines Benutzers von View 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>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 View Agent 6.0 oder höher ausgeführt wird, werden die SSO-Anmeldedaten des Benutzers vom View-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 View-Verbindungsserver trennen oder Horizon Client beenden und eine erneute Verbindung zum View-Verbindungsserver herstellen. Wenn ein Desktop jedoch über Workspace gestartet wird und dieser Desktop gesperrt ist, werden die SSO-Anmeldedaten nicht verworfen.</p>

Einstellung	Beschreibung
<p>Für Clients, die Anwendungen unterstützen.</p> <p>Verbindungen zu Anwendungen trennen und SSO-Anmeldeinformationen verwerfen, sobald der Benutzer nicht mehr mit Tastatur und Maus arbeitet:</p>	<p>Schützt Anwendungssitzungen, wenn auf dem Client-Gerät keine Tastatur- oder Mausaktivitäten stattfinden. Bei Festlegung auf Nach ... Minuten trennt View 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>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 View in keinem Fall Anwendungen oder verwirft SSO-Anmeldeinformationen aufgrund von Benutzerinaktivität.</p> <p>Die Standardeinstellung ist Nie.</p>
<p>Andere Clients.</p> <p>SSO-Anmeldeinformationen verwerfen:</p>	<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 View 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 View die SSO-Anmeldedaten, bis der Benutzer Horizon Client schließt oder bis das für Trennung der Benutzer erzwingen angegebene Zeitlimit erreicht ist, je nachdem, welcher Fall zuerst eintritt.</p> <p>Die Standardeinstellung ist Nach 15 Minuten.</p>
<p>Automatische Status-Updates aktivieren</p>	<p>Legt fest, ob Statusaktualisierungen in der globalen Statusanzeige im oberen linken Bereich von View Administrator mit einem Intervall von wenigen Minuten aktualisiert werden. Die Dashboard-Seite von View Administrator wird ebenfalls mit einem Intervall von wenigen Minuten aktualisiert.</p> <p>Diese Einstellung ist standardmäßig nicht aktiviert.</p>
<p>Display a pre-login message (Meldung vor der Anmeldung anzeigen)</p>	<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>
<p>Display a warning before forced logoff (Vor erzwungener Abmeldung eine Warnung anzeigen)</p>	<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 Desktop wurde eine wichtige Aktualisierung geplant. Ihr Desktop wird in 5 Minuten heruntergefahren. Speichern Sie jetzt alle noch nicht gespeicherten Arbeiten.</p> </div>

Einstellung	Beschreibung
Windows Server 2008 R2-Desktops aktivieren	<p>Legt fest, ob verfügbare Windows Server 2008 R2-Computer zur Verwendung als Desktops ausgewählt werden können. Wenn diese Einstellung aktiviert ist, werden in View Administrator alle verfügbaren Windows Server 2008 R2-Computer angezeigt, einschließlich der Computer, auf denen View-Serverkomponenten installiert sind.</p> <p>Hinweis Die View-Software darf nicht auf derselben virtuellen Maschine oder demselben physischen Computer wie eine andere View-Server-Softwarekomponente installiert sein, Sicherheitsserver, View-Verbindungsserver oder View Composer eingeschlossen.</p>
Mirage-Serverkonfiguration	<p>Ermöglicht Ihnen, die URL eines Mirage-Servers anzugeben, und zwar in dem 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 View 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 View Administrator unterstützt wird, lesen Sie die Mirage-Dokumentation unter https://www.vmware.com/support/pubs/mirage_pubs.html.</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 View Administrator-Verbindungen mit View ist SSL erforderlich. Wenn Ihre View-Bereitstellung Lastausgleichsmodule oder andere Zwischenserver mit Client-Verbindung verwendet, können Sie SSL darauf verlagern und dann Nicht-SSL-Verbindungen auf einzelnen View-Verbindungsserver-Instanzen und Sicherheitsservern konfigurieren. Siehe [Verschieben von SSL-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>Legt fest, ob zwischen den View-Komponenten übermittelte JMS-Nachrichten signiert und überprüft werden. Weitere Informationen finden Sie unter Sicherheitsmodus für Nachrichten für View-Komponenten.</p> <p>Der Sicherheitsmodus für Nachrichten ist standardmäßig aktiviert.</p>
IPSec für Sicherheitsserver-Verbindungen verwenden	<p>Bestimmt, ob Internet Protocol Security (IPSec) für Verbindungen zwischen Sicherheitsservern und View-Verbindungsserver-Instanzen verwendet wird.</p> <p>Standardmäßig sind sichere Verbindungen (über IPSec) für Sicherheitsserver-Verbindungen aktiviert.</p>

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

Sicherheitsmodus für Nachrichten für View-Komponenten

Sie können einen Sicherheitsmodus für Nachrichten für View-Komponenten einrichten. Diese Einstellung legt fest, wie Absendersignaturen in JMS-Nachrichten behandelt werden. JMS-Nachrichten werden abgelehnt, wenn die Signatur fehlt oder ungültig ist oder wenn eine Nachricht nach dem Signieren verändert wurde.

Wenn eine der Komponenten in Ihrer View-Umgebung zum Zeitpunkt der Einrichtung des Sicherheitsmodus für Nachrichten eine Version vor View 3.0 verwendet, können Sie den Modus dahingehend ändern, dass bei Auftreten einer der genannten Bedingungen eine Warnung protokolliert wird, oder dass keinerlei Prüfung von Signaturen erfolgt. Diese Optionen sind allerdings nicht zu empfehlen; ältere Komponenten sollten aktualisiert werden.

Einige JMS-Nachrichten sind verschlüsselt, da sie vertrauliche Daten wie z. B. Benutzeranmeldeinformationen enthalten. Ziehen Sie die Verwendung von IPSec zur Verschlüsselung aller JMS-Nachrichten zwischen View-Verbindungsserver-Instanzen sowie zwischen View-Verbindungsserver-Instanzen und Sicherheitsservern in Betracht.

Tabelle 2-4. Optionen für den Sicherheitsmodus für Nachrichten 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. Sie können diesen Modus verwenden, um Komponenten in Ihrer View-Umgebung zu ermitteln, die eine Version vor View 3.0 verwenden. Die von View-Verbindungsserver generierten Protokolldateien enthalten Verweise auf diese Komponenten.
Aktiviert	Der Sicherheitsmodus für Nachrichten ist aktiviert. Nicht signierte Nachrichten werden von View-Komponenten abgelehnt. Der Sicherheitsmodus für Nachrichten ist standardmäßig aktiviert. Hinweis View-Komponenten, die eine Version vor View 3.0 verwenden, dürfen mit anderen View-Komponenten nicht kommunizieren.

Wenn Sie View erstmalig auf einem System installieren, wird der Sicherheitsmodus für Nachrichten auf **Aktiviert** gesetzt. Wenn Sie ein Upgrade für View durchführen, bleibt der Sicherheitsmodus für Nachrichten unverändert auf der aktuellen Einstellung.

Der Sicherheitsmodus für Nachrichten wird in View 3.0 und höher unterstützt. Wenn Sie den Sicherheitsmodus für Nachrichten von **Deaktiviert** oder **Gemischt** auf **Aktiviert** setzen, können Sie keinen Remote-Desktop starten, der über einen View Agent aus der Virtual Desktop Manager-Version 2.1 oder früher verfügt. Wenn Sie den Sicherheitsmodus für Nachrichten dann von **Aktiviert** auf **Gemischt** oder **Deaktiviert** ändern, kann der Desktop immer noch nicht gestartet werden. Um einen Desktop nach dem Ändern des Sicherheitsmodus für Nachrichten von **Aktiviert** in **Gemischt** oder **Deaktiviert** zu starten, müssen Sie den Remote-Desktop neu starten.

Wenn Sie vorhaben, eine aktive View-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 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 View-Verbindungsserver- oder Sicherheitsserverhost auf.

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 View-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 View Administrator zum Aktivieren oder Deaktivieren des sicheren Tunnels und des PCoIP Secure Gateway auf einem Sicherheitsserver verwenden möchten, müssen Sie die View-Verbindungsserver-Instanz bearbeiten, die mit dem Sicherheitsserver kombiniert ist.

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

Voraussetzungen

- Wenn Sie beabsichtigen, das PCoIP Secure Gateway zu aktivieren, stellen Sie sicher, dass die View-Verbindungsserver-Instanz und der kombinierte Sicherheitsserver in der Version View 4.6 oder höher vorliegen.
- Wenn Sie einen Sicherheitsserver mit einer View-Verbindungsserver-Instanz kombinieren, auf der Sie das PCoIP Secure Gateway bereits aktiviert haben, stellen Sie sicher, dass der Sicherheitsserver in der Version View 4.6 oder höher vorliegt.

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die View-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 sicheren HTML-Zugriff

Sie können in View Administrator die Verwendung des Blast Secure Gateways konfigurieren, um sicheren HTML-Zugriff für Remote-Desktops bereitzustellen.

Sie können sichere Verbindungen für externe Benutzer bereitstellen, die über HTML Access eine Verbindung mit Remote-Desktops herstellen. Das Blast Secure Gateway, das auf View-Verbindungsserver- und Sicherheitsserverhosts standardmäßig aktiviert ist, stellt sicher, dass nur authentifizierte Benutzer mit Remote-Desktops kommunizieren können. Mit HTML Access muss keine Clientsoftware auf Endgeräten der Benutzer installiert werden.

Wenn das Blast Secure Gateway nicht aktiviert ist, verwenden Client-Webbrowser HTML Access, um direkte Verbindungen mit den virtuellen Remote-Desktop-Maschinen herzustellen, und umgehen somit das Blast Secure Gateway.

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

Voraussetzungen

- Wenn Benutzer Remote-Desktops über das Workspace App Portal auswählen, müssen Sie überprüfen, ob Workspace installiert und für die Verwendung mit dem View-Verbindungsserver konfiguriert ist. Außerdem muss der View-Verbindungsserver mit einem SAML 2.0-Authentifizierungsserver kombiniert sein.

- Stellen Sie sicher, dass der sichere Tunnel aktiviert ist. Wenn der sichere Tunnel gesperrt ist, kann das Blast Secure Gateway nicht aktiviert werden.

Verfahren

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

Option	Beschreibung
Aktivieren des Blast Secure Gateway	Wählen Sie Verwenden Sie Blast Secure Gateway für den HTML Access auf den Computer aus.
Deaktivieren des Blast Secure Gateway	Deaktivieren Sie Verwenden Sie Blast Secure Gateway für den HTML Access auf den Computer .

Das Blast Secure Gateway ist standardmäßig aktiviert.

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

Öffnen des Ports, der von HTML Access auf Sicherheitsservern verwendet wird

Wenn Sie die HTML Access-Komponente während einer View-Verbindungsserver-Installation installieren, erstellt das Installationsprogramm eine Windows-Firewallregel und aktiviert diese, um den Port zu öffnen, der von HTML Access für Client-Verbindungen verwendet wird. Auf Sicherheitsservern müssen Sie die Regel in der Windows-Firewall allerdings manuell aktivieren, um die Kommunikation über diesen Port zu ermöglichen.

Standardmäßig benutzt HTML Access den TCP-Port 8443 für Client-Verbindungen zum Blast Secure Gateway.

Verfahren

- ◆ Um den von HTML Access genutzten Port auf einem View-Verbindungsserver-Computer zu öffnen, installieren Sie HTML Access mit View-Verbindungsserver auf diesem Computer.

Das Installationsprogramm aktiviert die **VMware View-Verbindungsserver (Blast-In)**-Regel in der Windows-Firewall.

- ◆ Um den Port für HTML Access auf einem Sicherheitsserver zu öffnen, aktivieren Sie die **VMware View-Verbindungsserver (Blast-In)**-Regel in der Windows-Firewall manuell.

Verschieben von SSL-Verbindungen auf Zwischenserver

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

Importieren von SSL-Zertifikaten verschiebender Server auf View-Server

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

Wenn Sie Sicherheitsserver bereitstellen, muss sich sowohl auf dem Zwischenserver als auch auf den Sicherheitsservern, die eine Verbindung zum Zwischenserver herstellen, dasselbe SSL-Zertifikat befinden. Es ist nicht erforderlich, dasselbe SSL-Zertifikat auf View-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 View-Verbindungsserver-Instanzen mit externen Verbindungen handelt, muss sich sowohl auf dem Zwischenserver als auch auf den View-Verbindungsserver-Instanzen, die eine Verbindung zum Zwischenserver herstellen, dasselbe SSL-Zertifikat befinden.

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

Verwechseln Sie nicht Lastausgleich mit SSL-Verschieben. Das zuvor genannte Erfordernis gilt für alle Geräte, die konfiguriert wurden, SSL-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 View-Server finden Sie unter „Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher“ im Dokument *Installation von View*.

Einstellen externer URLs von View Server, sodass sie Clients auf verschiebende SSL-Server verweisen

Wenn SSL auf einen Zwischenserver verschoben wird und Horizon Client-Geräte den sicheren Tunnel nutzen, um sich mit View 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 View-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 View-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 View-Verbindungsserver-Instanzen verfügen, sind externe URLs für alle View-Verbindungsserver-Instanzen notwendig, die eine Verbindung mit dem Zwischenserver herstellen.

Hinweis Sie können SSL-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 SSL-Verbindungen zwischen dem Zwischenserver und dem View Server herzustellen.

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

Zulassen der HTTP-Verbindungen von Zwischenservern

Wenn SSL auf einen Zwischenserver verschoben wird, können Sie View-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 View-Servern und Zwischengeräten zuzulassen, müssen Sie die Datei `locked.properties` auf jeder View-Verbindungsserver-Instanz und jedem Sicherheitsserver konfigurieren, auf denen HTTP-Verbindungen zugelassen sind.

Auch wenn HTTP-Verbindungen zwischen View-Servern und Zwischengeräten zugelassen sind, können Sie SSL in View nicht deaktivieren. Die View-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 View-Verbindungsserver bzw. zum Sicherheitsserver herstellen. Die Smartcard-Authentifizierung unterstützt das Verschieben von SSL nicht.

Verfahren

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf dem View-Verbindungsserver- oder dem Sicherheitsserverhost.

Beispiel: `Installationsverzeichnis\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- 2 Um das View-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 View-Server zu konfigurieren.
 - Um den HTTP-Überwachungsport von 80 zu ändern, legen Sie für `serverPortNonSSL` eine andere Portnummer fest, zu der das Zwischengerät per Konfiguration eine Verbindung herstellen soll.
 - Wenn der View-Server über mehr als eine Netzwerkschnittstelle verfügt, der Server aber HTTP-Verbindungen nur an einer Schnittstelle überwachen soll, geben Sie für `serverHostNonSSL` die IP-Adresse dieser Netzwerkschnittstelle an.
- 4 Speichern Sie die Datei `locked.properties`.
- 5 Starten Sie den View-Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Beispiel: `locked.properties`, Datei

Diese Datei lässt Nicht-SSL-HTTP-Verbindungen zu einem View-Server zu. Die IP-Adresse der Netzwerkschnittstelle mit Client-Verbindung des View-Servers lautet 10.20.30.40. Der Server verwendet den Standardport 80 zur Überwachung von HTTP-Verbindungen. Der Wert `http` muss in Kleinbuchstaben eingegeben werden.

```
serverProtocol=http
serverHostNonSSL=10.20.30.40
```

Deaktivieren oder Aktivieren von View-Verbindungsserver

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

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

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

- Wenn es sich um eine einzelne, eigenständige View-Verbindungsserver-Instanz handelt, können sich Benutzer bei ihren Remote-Desktops oder -Anwendungen nicht anmelden. Sie können keine Verbindung mit View-Verbindungsserver herstellen.
- Wenn es sich um eine replizierte View-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 Remote-Desktops und -Anwendungen anmelden.

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die View-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 View-Verbindungsserver-Instanzen und Sicherheitsservern View Administrator verwenden.

Ein View-Verbindungsserver- oder Sicherheitsserverhost können 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 View-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 View-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 View-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 über einen Webbrowser eine sichere Verbindung 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 Für einen Sicherheitsserver, der nicht auf View-Verbindungsserver 4.5 oder höher aktualisiert wurde, können Sie die externen URLs nicht bearbeiten.

Verfahren

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

Option	Aktion
View-Verbindungsserver-Instanz	Wählen Sie die View-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 View-Verbindungsserver-Instanz oder auf einen Sicherheitsserver zugreifen können, wenn deren bzw. dessen Hostname nicht aufgelöst werden kann. Der Host, den Sie kontaktieren, passt jedoch nicht zu dem SSL-Zertifikat, das für die View-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 View-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.

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

Beitreten oder Verlassen des Programms zur Verbesserung der Benutzerfreundlichkeit

Wenn Sie den View-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 View 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 [Vom Programm zur Verbesserung der Benutzerfreundlichkeit erfasste Daten](#).

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration > Produktlizenzierung und -verwendung**.
- 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 View-Konfigurationsinformationen. View LDAP ist ein eingebettetes LDAP-Verzeichnis (Lightweight Directory Access Protocol), das mit der View-Verbindungsserver-Installation bereitgestellt wird.

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

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

View LDAP enthält Verzeichniseinträge, die View-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.
- View-Komponenteneinträge, die Konfigurationseinstellungen speichern

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

Hinweis Sicherheitsserverinstanzen haben kein View LDAP-Verzeichnis.

Einrichten der Authentifizierung

View nutzt die vorhandene Active Directory-Infrastruktur für die Benutzer- und Administratorauthentifizierung und -verwaltung. Zur Optimierung der Sicherheit können Sie View mit Smartcard-Authentifizierung integrieren. Sie können auch Zwei-Faktor-Authentifizierungslösungen wie RSA SecurID und RADIUS zur Authentifizierung von Benutzern verwenden, die Remote-Desktops und -anwendungen nutzen.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden der zweistufigen Authentifizierung](#)
- [Verwenden der Smartcard-Authentifizierung](#)
- [Verwenden der SAML-Authentifizierung zur Workspace-Integration](#)
- [Verwenden der Smartcard-Zertifikatssperrüberprüfung](#)
- [Verwenden der Funktion „Als aktueller Benutzer anmelden“, die mit Windows-basierten Horizon Client-Instanzen verfügbar ist](#)
- [Zulassen, dass Benutzer Anmeldeinformationen speichern](#)

Verwenden der zweistufigen Authentifizierung

Sie können eine View-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.
- View bietet auch eine offene Standarderweiterungsschnittstelle, die es Drittanbietern ermöglicht, fortschrittliche Authentifizierungserweiterungen in View 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 View-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 View-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.

View 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 an einer View-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 View Administrator**

Sie aktivieren eine View-Verbindungsserver-Instanz für die RSA SecurID- oder RADIUS-Authentifizierung, indem Sie die View-Verbindungsserver-Einstellungen in View 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 an einer View-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 View 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 View Administrator

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

Verfahren

- 1 Wählen Sie in View 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-AuthentifizierungRSA 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 View-Verbindungsserver-Dienst muss nicht neu gestartet werden. Die erforderlichen Konfigurationsdateien werden automatisch verteilt und die Konfigurationseinstellungen werden umgehend angewendet.

Wenn Benutzer Horizon Client öffnen und sich beim View-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 View-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 View Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** den View-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 **Knotenkennwort erstellt**.

Die Option **Knotenkennwort erstellt** wird bei jeder Bearbeitung standardmäßig aktiviert.

- 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 View auftritt.

Die folgenden allgemeinen Konfigurationsfehler führen am häufigsten zu dieser Situation:

- Der RADIUS-Server wurde nicht konfiguriert, um die View-Verbindungsserver-Instanz als RADIUS-Client zu akzeptieren. Jede View-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 View-Verbindungsserver-Instanz und dem RADIUS-Server stimmen nicht überein.

Verwenden der Smartcard-Authentifizierung

Sie können eine View-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 *Installation von View*. 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://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

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. 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 View-Verbindungsserver-Instanz oder einem Sicherheitsserver herstellt, die bzw. der für die Smartcard-Authentifizierung konfiguriert ist, sendet die View-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 View-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.

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 Smartcard-Authentifizierung

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

Verfahren

1 [Anfordern des Stammzertifikats von der Zertifizierungsstelle](#)

Sie müssen das Stammzertifikat von der Zertifizierungsstelle anfordern, welche die Zertifikate auf den von Ihren Benutzern und Administratoren verwendeten Smartcards signiert hat.

2 [Anfordern des Stammzertifikats 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.

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

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

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

Zur Aktivierung der Smartcard-Authentifizierung müssen auf dem View-Verbindungsserver- oder Sicherheitsserverhost View-Verbindungsserver-Konfigurationseigenschaften geändert werden.

5 Konfigurieren von Smartcard-Einstellungen in View Administrator

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

Anfordern des Stammzertifikats von der Zertifizierungsstelle

Sie müssen das Stammzertifikat von der Zertifizierungsstelle anfordern, welche die Zertifikate auf den von Ihren Benutzern und Administratoren verwendeten Smartcards signiert hat.

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

Verfahren

- ◆ Fordern Sie das Stammzertifikat aus einer der folgenden Quellen an.
 - Microsoft IIS-Server, auf dem die Microsoft-Zertifikatsdienste 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 zu einer Server-Vertrauensspeicherdatei hinzu. Siehe [Hinzufügen des Stammzertifikats zu einer Server-Vertrauensspeicherdatei](#).

Anfordern des Stammzertifikats 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.

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](#) 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.

- 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 Stammzertifikat zu einer Server-Vertrauensspeicherdatei hinzu.

Hinzufügen des Stammzertifikats zu einer Server-Vertrauensspeicherdatei

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

Voraussetzungen

- Fordern Sie die Stammzertifikate an, die zur Signierung der Zertifikate auf den von Ihren Benutzern oder Administratoren verwendeten Smartcards verwendet wurden. Siehe [Anfordern des Stammzertifikats von der Zertifizierungsstelle](#) und [Anfordern des Stammzertifikats von Windows](#).
- Stellen Sie sicher, dass das Dienstprogramm `keytool` dem Systempfad auf Ihrem View-Verbindungsserver- oder Sicherheitsserverhost hinzugefügt wurde. Weitere Informationen finden Sie im Dokument *Installation von View*.

Verfahren

- 1 Verwenden Sie das Dienstprogramm `keytool` auf Ihren View-Verbindungsserver- oder Sicherheitsserverhost, um das Stammzertifikat in die Server-Vertrauensspeicherdatei zu importieren.

Beispiel:

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

In diesem Befehl steht *Alias* für einen eindeutigen Namen eines neuen Eintrags in der Vertrauensspeicherdatei (Groß-/Kleinschreibung wird beachtet), *Stammzertifikat* gibt das Stammzertifikat 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 das SSL-Gateway-Konfigurationsverzeichnis auf dem View-Verbindungsserver- oder Sicherheitsserverhost.

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

Nächste Schritte

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

Ändern von View-Verbindungsserver-Konfigurationseigenschaften

Zur Aktivierung der Smartcard-Authentifizierung müssen auf dem View-Verbindungsserver- oder Sicherheitsserverhost View-Verbindungsserver-Konfigurationseigenschaften geändert werden.

Voraussetzungen

Fügen Sie die Stammzertifikate für alle vertrauenswürdigen Benutzer zu einer Server-Vertrauensspeicherdatei hinzu.

Verfahren

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf dem View-Verbindungsserver- oder dem Sicherheitsserverhost.

Beispiel: `Installationsverzeichnis\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 View-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 View-Verbindungsserver-Instanz konfiguriert haben, konfigurieren Sie die Smartcard-Authentifizierungseinstellungen in View Administrator. Sie müssen die Einstellungen für die Smartcard-Authentifizierung für einen Sicherheitsserver nicht konfigurieren. Einstellungen, die auf einer View-Verbindungsserver-Instanz konfiguriert werden, gelten auch für einen gekoppelten Sicherheitsserver.

Konfigurieren von Smartcard-Einstellungen in View Administrator

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

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

Voraussetzungen

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

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die View-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 View-Verbindungsserver-Instanz deaktiviert.
Optional	Benutzer können für die Verbindung mit der View-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 View-Verbindungsserver-Instanz die Smartcard-Authentifizierung verwenden. Wenn die Smartcard-Authentifizierung erforderlich ist, schlägt die Authentifizierung von Benutzern fehl, die das Kontrollkästchen Anmelden als aktueller Benutzer zur Herstellung einer Verbindung mit der View-Verbindungsserver-Instanz aktivieren. Diese Benutzer müssen sich bei der Anmeldung an View-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 View-Verbindungsserver-Instanz verbunden sind, für die das Kontrollkästchen **Anmelden als aktueller Benutzer** aktiviert ist, selbst wenn sie sich an ihrem Clientsystem mit einer Smartcard anmelden.

- 4 Um die Smartcard-Authentifizierung für Administratoren zu konfigurieren, die sich bei View 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 View-Verbindungsserver-Instanz deaktiviert.
Optional	Administratoren können die Authentifizierung per Smartcard oder Kennwort verwenden, um sich bei View Administrator anzumelden. Wenn die Smartcard-Authentifizierung fehlschlägt, muss der Administrator ein Kennwort angeben.
Erforderlich	Administratoren müssen die Smartcard-Authentifizierung verwenden, wenn sie sich bei View Administrator anmelden.

- 5 Klicken Sie auf **OK**.
- 6 Starten Sie den View-Verbindungsserver-Dienst neu.

Mit einer Ausnahme müssen Sie den View-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 View-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](#).

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 View 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 View per Smartcard authentifizieren, über einen gültigen UPN verfügen.

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

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

Voraussetzungen

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

Verfahren

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

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

Hinzufügen des Stammzertifikats zum Enterprise NTAAuth-Speicher

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

Verfahren

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

Beispiel:

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

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

Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen

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

Verfahren

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

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

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

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

Nächste Schritte

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

Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen

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

Verfahren

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

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

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

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

Überprüfen der Smartcard-Authentifizierungskonfiguration

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 Clientsystem **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 View-Verbindungsserver- oder Sicherheitsserverhost, 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 View-Verbindungsserver-Instanz konfiguriert haben, überprüfen Sie die Smartcard-Authentifizierungseinstellung im View Administrator.
 - a Wählen Sie **View-Konfiguration > Server** aus.
 - b Wählen Sie auf der Registerkarte **Verbindungsserver** die View-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 View-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 für die Verbindung mit Remote-Desktops das PCoIP-Anzeigeprotokoll verwenden, stellen Sie sicher, dass die Unterfunktion „View Agent PCoIP-Smartcard“ installiert ist. Die Unterfunktion PCoIP Smartcard (PCoIP-Smartcard) ermöglicht Benutzern die Authentifizierung per Smartcard, wenn sie das PCoIP-Anzeigeprotokoll verwenden.

Hinweis Die PCoIP-Smartcard-Unterfunktion wird auf Windows Vista nicht unterstützt.

- ◆ Überprüfen Sie auf dem View-Verbindungsserver- oder Sicherheitsserverhost die Protokolldateien unter *Laufwerk:* \Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM \Logs auf Meldungen, die die Aktivierung der Smartcard-Authentifizierung angeben.

Verwenden der SAML-Authentifizierung zur Workspace-Integration

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.

Die Workspace- und View-Integrationsimplementierung 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 Workspace mit Active Directory-Anmeldedaten anmelden, Remote-Desktops und -Anwendungen starten, ohne einen zweiten Anmeldevorgang zu durchlaufen.

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

Workspace Manager sendet das SAML-Artefakt über Workspace Gateway an den Horizon-Client, der seinerseits das Artefakt an die View-Verbindungsserver-Instanz sendet. Die View-Verbindungsserver-Instanz verwendet das SAML-Artefakt, um die SAML-Zusicherung von Workspace Manager über Workspace Gateway abzurufen.

Nachdem eine View-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 Workspace und die View-Integration erfordert auch die Konfiguration von Workspace mit View-Informationen und die Konfiguration von View zur Delegierung der Verantwortlichkeit zur Authentifizierung an Workspace.

Zur Delegierung der Verantwortlichkeit zur Authentifizierung an Workspace müssen Sie einen SAML-Authentifikator in View erstellen. Ein SAML-Authentifikator enthält den Vertrauens- und Metadaten austausch zwischen View und Workspace. Sie verknüpfen einen SAML-Authentifikator mit einer View-Verbindungsserver-Instanz.

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

Konfigurieren der SAML-Authentifikatoren in View Administrator

Um Remote-Desktops und -Anwendungen von Workspace aus zu starten, müssen Sie einen SAML-Authentifikator in View Administrator erstellen. Ein SAML-Authentifikator enthält den Vertrauens- und Metadaten austausch zwischen View und Workspace.

You associate a SAML authenticator with a View-Verbindungsserver instance. Wenn Ihre Bereitstellung mehr als eine View-Verbindungsserver-Instanz beinhaltet, müssen Sie den SAML-Authentifikator mit jeder Instanz verknüpfen.

Voraussetzungen

- Stellen Sie sicher, dass Workspace installiert und konfiguriert ist. Information dazu finden Sie im *VMware Workspace Portal-Installations- und Konfigurationshandbuch*.
- Stellen Sie sicher, dass das Stammzertifikat für die signierende Zertifizierungsstelle für das SAML-Server-Zertifikat auf dem View-Verbindungsserver-Host installiert ist. VMware empfiehlt nicht, SAML-Authentifikatoren zur Verwendung selbstsignierter Zertifikate zu konfigurieren. Informationen zur Zertifikatsauthentifizierung finden Sie im Dokument *Installation von View*.
- Notieren Sie sich den FQDN oder die IP-Adresse des Workspace Gateway-Servers oder des externen Lastausgleichsdiensts.
- Notieren Sie sich die URL der Workspace Connector-Webschnittstelle.

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration>Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** eine View-Verbindungsserver-Instanz aus, um sie mit dem SAML-Authentifikator zu verknüpfen, 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 aus Horizon Client als auch Workspace heraus starten.
Erforderlich	Die SAML-Authentifizierung ist aktiviert. Sie können Remote-Desktops und -Anwendungen nur aus Workspace heraus starten. Sie können Desktops oder Anwendungen nicht manuell aus Horizon Client heraus starten.

Sie können jede View-Verbindungsserver-Instanz in Ihrer Bereitstellung so konfigurieren, dass sie abhängig von Ihren Anforderungen unterschiedliche SAML-Authentifizierungseinstellungen haben.

- 4 Wählen Sie aus dem Dropdown-Menü **SAML-Authentifikator** die Option **Neuen Authentifikator erstellen** aus oder klicken Sie, falls ein SAML-Authentifikator bereits hinzugefügt wurde, auf **Authentifikatoren verwalten** und danach auf **Hinzufügen**.
- 5 Konfigurieren Sie den SAML-Authentifikator im Dialogfeld zum Hinzufügen von SAML 2.0-Authentifikatoren.

Option	Beschreibung
Bezeichnung	Eindeutiger Name, der den SAML-Authentifikator identifiziert.
Beschreibung	Kurzbeschreibung des SAML-Authentifikators. Dieser Wert ist optional.
Metadaten-URL	URL zum Abrufen aller Informationen, die für den Austausch von SAML-Informationen zwischen dem SAML-Identitätsanbieter und der View-Verbindungsserver-Instanz erforderlich sind. Klicken Sie auf <IHR HORIZON-SERVERNAME> und ersetzen Sie ihn durch den FQDN oder die IP-Adresse des Workspace Gateway-Servers oder des externen Lastausgleichsdiensts.
Verwaltungs-URL	URL für den Zugriff auf die Administrationskonsole des SAML-Identitätsanbieters. Diese URL sollte auf die Workspace Connector-Webschnittstelle verweisen. Dieser Wert ist optional.

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

Sofern Sie gültige Informationen angegeben haben, müssen Sie entweder das selbstsignierte Zertifikat akzeptieren (nicht empfohlen) oder ein vertrauenswürdigen Zertifikat für View und Workspace 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 View Administrator-Dashboard **Andere Komponenten > SAML 2.0-Authentifikatoren** aus, wählen Sie den SAML-Authentifikator aus, den Sie hinzugefügt haben, und prüfen Sie die Details.

Falls die Konfiguration erfolgreich ist, steht der Systemzustand des Authentifikators auf grün. Der Systemzustand eines Authentifikators kann nach rot wechseln, wenn das Zertifikat nicht vertrauenswürdig ist, wenn Workspace Gateway nicht verfügbar ist oder wenn der 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.

Verwenden der Smartcard-Zertifikatssperrüberprüfung

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

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

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

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

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

Wenn Sie die Überprüfung von Zertifikatssperrlisten konfigurieren, erstellt und liest View eine Zertifikatssperrliste, um den Sperrstatus eines Benutzerzertifikats zu ermitteln.

- **Anmelden bei Verwendung der OCSP-Zertifikatssperrüberprüfung**

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

- **Konfigurieren der Überprüfung von Zertifikatssperrlisten**

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

- [Konfigurieren der OCSP-Zertifikatssperrüberprüfung](#)

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

- [Eigenschaften der Smartcard-Zertifikatssperrüberprüfung](#)

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

Anmelden bei Verwendung der Überprüfung von Zertifikatssperrlisten

Wenn Sie die Überprüfung von Zertifikatssperrlisten konfigurieren, erstellt und liest View eine Zertifikatssperrliste, um den Sperrstatus eines Benutzerzertifikats zu ermitteln.

Wenn ein Zertifikat gesperrt wird und die Smartcard-Authentifizierung optional ist, wird der Benutzer über das Dialogfeld **Geben Sie Benutzernamen und 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 View die Zertifikatssperrliste nicht lesen kann.

Anmelden bei Verwendung der OCSP-Zertifikatssperrüberprüfung

Wenn Sie die OCSP-Zertifikatssperrüberprüfung konfigurieren, sendet View eine Anforderung an einen OCSP-Antwortdienst, um den Sperrstatus eines bestimmten Benutzerzertifikats zu ermitteln. View 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 **Enter your user name and password (Geben Sie Benutzernamen und 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 View 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 View 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 SSL-Gateway-Konfigurationsordner auf dem View-Verbindungsserver- oder dem Sicherheitsserverhost.

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 View-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-Zertifikatssperrüberprüfung

Wenn Sie die OCSP-Zertifikatssperrüberprüfung konfigurieren, sendet View 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 SSL-Gateway-Konfigurationsordner auf dem View-Verbindungsserver- oder dem Sicherheitsserverhost.

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 View-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-Zertifikatssperrüberprüfung

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

[Tabelle 3-1. Eigenschaften für die Smartcard-Zertifikatssperrüberprüfung](#) listet die Eigenschaften der Datei `locked.properties` für die Zertifikatssperrüberprüfung auf.

Tabelle 3-1. Eigenschaften für die Smartcard-Zertifikatssperrüberprüfung

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

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

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

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

- Auf der View-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 View LDAP oder in einer Datei auf der Festplatte gespeichert.
- 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.

Administratoren können mit Gruppenrichtlinieneinstellungen von Horizon Client die Verfügbarkeit des Kontrollkästchens **Als aktueller Benutzer anmelden** steuern und seine Standardeinstellung festlegen. Außerdem können Administratoren mithilfe einer Gruppenrichtlinie festlegen, welche View-Verbindungsserver-Instanzen die Benutzeridentitäts- und Anmeldedaten akzeptieren, die übergeben werden, wenn das Kontrollkästchen **Als aktueller Benutzer anmelden** in Horizon Client aktiviert ist.

Für die Funktion „Anmelden als aktueller Benutzer“ gelten folgende Einschränkungen und Anforderungen:

- Wenn die Smartcard-Authentifizierung auf einer View-Verbindungsserver-Instanz erforderlich ist, schlägt die Authentifizierung bei Benutzern fehl, die das Kontrollkästchen **Anmelden als aktueller Benutzer** aktiviert haben, wenn sie eine Verbindung zur View-Verbindungsserver-Instanz herstellen. Diese Benutzer müssen sich bei der Anmeldung an View-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 View-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 View-Verbindungsserver-Instanz herzustellen, ohne zunächst eine VPN-Verbindung herzustellen, wird der Benutzer aufgefordert, Anmeldedaten anzugeben, und die Funktion „Als aktueller Benutzer anmelden“ funktioniert nicht.

Zulassen, dass Benutzer Anmeldeinformationen speichern

Administratoren können View-Verbindungsserver so konfigurieren, dass sich mobile Horizon Client-Endgeräte den Benutzernamen, das Kennwort und die Domäneninformationen eines Benutzers merken können. Wenn Benutzer ihre Anmeldedaten speichern dürfen, werden diese Daten bei den nächsten Verbindungen zu den Anmeldefeldern in Horizon Client hinzugefügt.

Auf Windows-basierten Horizon-Clients entfällt durch die Funktion zur Anmeldung als aktueller Benutzer die Notwendigkeit von Benutzern, Anmeldedaten mehrmals eingeben zu müssen. Mit Horizon Client für mobile Endgeräte wie beispielsweise Android und iPad können Sie eine Funktion konfigurieren, durch die das Kontrollkästchen **Kennwort speichern** auf den Dialogfeldern zur Anmeldung angezeigt wird.

Durch Setzen eines Werts in View LDAP konfigurieren Sie ein Zeitlimit, das angibt, wie lange die Anmeldedaten gespeichert bleiben sollen. Das Zeitüberschreitungslimit wird in Minuten festgelegt. Wenn Sie View LDAP auf einer View-Verbindungsserver-Instanz ändern, werden diese Änderungen auf alle replizierten View-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 View-Verbindungsserver-Host.
- 2 Wählen Sie im Dialogfeld „Verbindungseinstellungen“ **DC=vdi,DC=vmware,DC=int** aus oder verbinden Sie sich damit.
- 3 Wählen Sie im Fensterbereich „Computer“ **localhost:389** oder den voll qualifizierten Domännennamen (FQDN) des View-Verbindungsserver-Hosts gefolgt von Port 389 aus bzw. geben Sie diese Daten ein.

Beispiel: **localhost:389** oder **mycomputer.mydomain.com:389**

- 4 Setzen Sie für das Objekt **CN=Common, OU=Global, OU=Properties** das Attribut **pae-ClientCredentialCacheTimeout**.

Wenn dieses Attribut nicht gesetzt oder auf **0** eingestellt 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.

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

Konfigurieren der rollenbasierten Verwaltungsdelegierung

4

Eine wichtige Verwaltungsaufgabe in einer View-Umgebung besteht darin festzustellen, wer View 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 Delegierung 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 View 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 View 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 an View 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. View 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 Delegation der Verwaltung von Pools und Farmen

Standardmäßig werden automatisierte Desktop-Pools, manuelle Desktop-Pools und Farmen in der Stammzugriffsgruppe erstellt, die in View Administrator als / oder Root(/) angezeigt wird. RDS-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 RDS-Desktop-Zugriffspools oder eines Anwendungspools nicht direkt ändern. Sie müssen die Zugriffsgruppe der Farm ändern, zu der der RDS-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 View 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 Workspace ermöglichen möchten, müssen Sie die Desktop- und Anwendungspools als Benutzer mit Administratorrolle für die Stammzugriffsgruppe in View Administrator erstellen. Wenn Sie dem Benutzer die Administratorrolle für eine andere Zugriffsgruppe als die Stammzugriffsgruppe gewähren, erkennt Workspace den in View konfigurierten SAML-Authentifikator nicht, und Sie können den Pool nicht in Workspace 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 4-1. Unterschiedliche Administratoren für unterschiedliche Zugriffsgruppen zeigt ein Beispiel für diese Art der Konfiguration.

Tabelle 4-1. 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 4-2. Unterschiedliche Administratoren für dieselbe Zugriffsgruppe](#) zeigt ein Beispiel für diese Art der Konfiguration.

Tabelle 4-2. 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

View 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 View Administrator unterschiedlich angezeigt, abhängig davon, ob Sie einen Administratorbenutzer oder eine Administratorgruppe, eine Zugriffsgruppe oder eine Rolle auswählen.

[Tabelle 4-3. Berechtigungen auf der Registerkarte „Administratoren und Gruppen“ für Admin 1](#) zeigt, wie Berechtigungen in View Administrator angezeigt werden, wenn Sie einen Administratorbenutzer oder eine Administratorgruppe auswählen. Der Administratorbenutzer heißt „Admin 1“ und verfügt über zwei Berechtigungen.

Tabelle 4-3. Berechtigungen auf der Registerkarte „Administratoren und Gruppen“ für Admin 1

Rolle	Zugriffsgruppe
Bestandslistenadministratoren	MarketingDesktops
Administratoren (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.

[Tabelle 4-4. Berechtigungen auf der Registerkarte „Ordner“ für „MarketingDesktops“](#) zeigt, wie dieselben Berechtigungen in View Administrator angezeigt werden, wenn Sie die Zugriffsgruppe MarketingDesktops auswählen.

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

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

Die erste Berechtigung ist dieselbe wie die erste Berechtigung in [Tabelle 4-3. Berechtigungen auf der Registerkarte „Administratoren und Gruppen“ für Admin 1](#). Die zweite Berechtigung wird von der zweiten Berechtigung geerbt, wie in [Tabelle 4-3. 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“.

[Tabelle 4-5. Berechtigungen auf der Registerkarte „Rolle“ für Bestandslistenadministratoren](#) zeigt, wie die erste Berechtigung in View Administrator in [Tabelle 4-3. Berechtigungen auf der Registerkarte „Administratoren und Gruppen“ für Admin 1](#) angezeigt wird, wenn Sie die Rolle „Bestandslistenadministratoren“ auswählen.

Tabelle 4-5. Berechtigungen auf der Registerkarte „Rolle“ für Bestandslistenadministratoren

Administrator	Zugriffsgruppe
view-domain.com\Admin1	/MarketingDesktops

Verwalten von Administratoren

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

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

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

■ Erstellen eines Administrators

Um einen Administrator zu erstellen, wählen Sie in View 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 View 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 View 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.

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

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

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

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

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

Entfernen eines Administrators

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

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

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

Verwalten und Überprüfen von Berechtigungen

Sie können mithilfe von View 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 View 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 gelöscht. Da mindestens ein Administrator über die Administratorrolle für die Stammzugriffsgruppe verfügen muss, können Sie keine Berechtigung löschen, die zum Entfernen des Administrators führen würde. Eine vererbte Berechtigung kann nicht gelöscht werden.

Verfahren

- 1 Wählen Sie in View 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 View 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 View Administrator die Desktop-Pools, Anwendungspools oder Farmen in einer bestimmten Zugriffsgruppe anzeigen.

■ Überprüfen der vCenter-VMs in einer Zugriffsgruppe

Sie können die vCenter-VMs in einer speziellen Zugriffsgruppe in View 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 View 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. ■ 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 View 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**.

View 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 View 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 View Administrator die Desktop-Pools, Anwendungspools oder Farmen in einer bestimmten Zugriffsgruppe anzeigen.

Verfahren

- 1 Navigieren Sie in View 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 vCenter-VMs in einer speziellen Zugriffsgruppe in View Administrator anzeigen. Eine vCenter-VM erbt die Zugriffsgruppe von ihrem Pool.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Computer** 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 View 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 View 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 View Administrator zu erstellen.

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 View 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 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 View 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 View 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

View 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.

Tabelle 4-6. Vordefinierte Rollen in View Administrator beschreibt die vordefinierten Rollen und gibt an, ob eine Rolle auf eine Zugriffsgruppe angewendet werden kann.

Tabelle 4-6. Vordefinierte Rollen in View Administrator

Rolle	Benutzerfähigkeiten	Gilt für eine Zugriffsgruppe
Administratoren	<p>Durchführen aller Administratortaufgaben 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 View-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 View 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

Rolle	Benutzerfähigkeiten	Gilt für eine Zugriffsgruppe
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
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>	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>	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.

Tabelle 4-7. Globale Berechtigungen zeigt die globalen Berechtigungen sowie die vordefinierten Rollen, die diese Berechtigungen enthalten.

Tabelle 4-7. Globale Berechtigungen

Berechtigung	Benutzerfähigkeiten	Vordefinierte Rollen
Konsoleninteraktion	Anmeldung an und Verwendung von View Administrator.	Administratoren Administratoren (Nur Lesezugriff) Bestandslistenadministratoren Bestandslistenadministratoren (Nur Lesezugriff) Administratoren für globale Konfigurationen und Richtlinien Administratoren für globale Konfigurationen und Richtlinien (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 von View Agent auf nicht verwalteten Computern, z. B. auf physischen Systemen, eigenständigen virtuellen Maschinen und RDS-Hosts. Während der View Agent-Installation müssen Sie Ihre Administratoranmeldeinformationen angeben, um den nicht verwalteten Computer bei der View-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.

[Tabelle 4-8. Objektspezifische Berechtigungen](#) beschreibt die objektspezifischen Berechtigungen. Die vordefinierten Rollen Administrators (Administratoren) und Inventory Administrators (Bestandslistenadministratoren) umfassen all diese Berechtigungen.

Tabelle 4-8. 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 von Computern.	Computer

Interne Berechtigungen

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

[Tabelle 4-9. Interne Berechtigungen](#) zeigt die internen Berechtigungen sowie die vordefinierten Rollen, die diese Berechtigungen enthalten.

Tabelle 4-9. Interne Berechtigungen

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

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 View Administrator verfügen.

[Tabelle 4-10. Aufgaben und Berechtigungen für die Pool-Verwaltung](#) listet gängige Pool-Verwaltungsaufgaben sowie die erforderlichen Berechtigungen zur Ausführung der einzelnen Aufgaben auf.

Tabelle 4-10. 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 Computern

Administratoren müssen über bestimmte Berechtigungen für die Verwaltung von Computern in View Administrator verfügen.

[Tabelle 4-11. Aufgaben und Berechtigungen für die Verwaltung von Computern](#) listet gängige Verwaltungsaufgaben für Computer sowie die erforderlichen Berechtigungen zur Ausführung der einzelnen Aufgaben auf.

Tabelle 4-11. Aufgaben und Berechtigungen für die Verwaltung von Computern

Aufgabe	Erforderliche Berechtigungen
Entfernen einer virtuellen Maschine	Computer verwalten
Zurücksetzen einer virtuellen Maschine	Neustartvorgang verwalten
Zuweisen oder Entfernen von Besitzrechten	Computer verwalten

Aufgabe	Erforderliche Berechtigungen
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 View Administrator verfügen.

[Tabelle 4-12. Aufgaben und Berechtigungen für die Verwaltung persistenter Festplatten](#) 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 View Administrator ausgeführt.

Tabelle 4-12. 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 View Administrator verfügen.

[Tabelle 4-13. Aufgaben und Berechtigungen für die Verwaltung von Benutzern und Administratoren](#) 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 View Administrator verwaltet. Administratoren werden in der globalen Administratorenansicht in View Administrator verwaltet.

Tabelle 4-13. 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 allgemeine Verwaltungsaufgaben und -befehle

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

[Tabelle 4-14. Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle](#) zeigt die erforderlichen Berechtigungen, um allgemeine Verwaltungsaufgaben und Befehlszeilenprogramme auszuführen.

Tabelle 4-14. Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle

Aufgabe	Erforderliche Berechtigungen
Hinzufügen oder Löschen einer Zugriffsgruppe	Administratorenrolle für die Stammzugriffsgruppe.
Verwalten von ThinApp-Anwendungen und -Einstellungen in View Administrator	Administratorenrolle für die Stammzugriffsgruppe.
Installieren von View 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 View Administrator	Globale Konfiguration und Globale Richtlinien verwalten
Ausführen aller PowerShell-Befehle und Befehlszeilenprogramme mit Ausnahme von vdmadmin und vdmimport.	Direkte Interaktion
Verwenden der Befehle vdmadmin und vdmimport	Administratorenrolle für die Stammzugriffsgruppe.
Verwenden des vdmexport-Befehls	Administratorenrolle (Lese- und Schreibzugriff oder nur Lesezugriff) für die Stammzugriffsgruppe.

Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen

Um die Sicherheit und Verwaltbarkeit Ihrer View-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 View-Administrationsrollen zu. Vermeiden Sie es, in Windows integrierte Gruppen oder andere vorhandene Gruppen zu verwenden, die möglicherweise Benutzer enthalten, die keine View-Berechtigung benötigen oder haben sollten.
- Halten Sie die Anzahl an Benutzern mit View-Administrationsrichtlinien auf ein Minimum begrenzt.
- Da die Administratorenrolle jede Berechtigung besitzt, sollte sie nicht für die alltägliche Verwaltung verwendet werden.
- Wählen Sie zum Zuweisen der Administratorrolle einen lokalen Windows-Benutzer oder eine lokale Windows-Gruppe.
- 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 View-Konfigurationseinstellungen ändern können.

Konfigurieren von Richtlinien in View Administrator und Active Directory

5

Sie können mithilfe von View 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 View zu steuern.

Sie können Active Directory-Gruppenrichtlinieneinstellungen konfigurieren, um das Verhalten von View Agent, Horizon Client for Windows, View Persona Management und bestimmte Funktionen zu steuern. Weitere Informationen zu diesen Richtlinieneinstellungen finden Sie im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Dieses Kapitel enthält die folgenden Themen:

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

Festlegen von Richtlinien in View Administrator

Sie können mithilfe von View Administrator Richtlinien für Clientsitzungen konfigurieren.

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

- **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.

- **View-Richtlinien**

Sie können View-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 [View-Richtlinien](#).

Verfahren

- 1 Wählen Sie in View 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 [View-Richtlinien](#).

Verfahren

- 1 Wählen Sie in View 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 [View-Richtlinien](#).

Verfahren

- 1 Wählen Sie in View 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 View-Richtlinien und klicken Sie auf **Fertig stellen**, um Ihre Änderungen zu speichern.

View-Richtlinien

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

[Tabelle 5-1. View-Richtlinien](#) beschreibt alle View-Richtlinieneinstellungen.

Tabelle 5-1. View-Richtlinien

Richtlinie	Beschreibung
Multimedia-Umleitung (MMR)	<p>Legt fest, ob MMR für Clientsysteme aktiviert ist.</p> <p>MMR ist ein Microsoft DirectShow-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 arbeitet nicht ordnungsgemäß, wenn die Hardware zur Videoanzeige auf dem Clientsystem keine Overlay-Unterstützung bietet.</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 View

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

Alle ADM- und ADMX-Dateien, die Gruppenrichtlinieneinstellungen für View bereitstellen, stehen in einer mitgelieferten .zip-Datei namens VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip zur Verfügung, wobei x.x.x die Version und yyyyyyy die Build-Nummer ist. Sie können die Datei von der Download-Site VMware Horizon (mit View) unter <http://www.vmware.com/go/downloadview> herunterladen.

Die ADM- und ADMX-Vorlagendateien von View 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.

ADM- und ADMX-Vorlagendateien für View

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

Tabelle 5-2. ADM- und ADMX-Vorlagendateien für View

Name der Vorlage	Vorlagendatei	Beschreibung
View Agent-Konfiguration	vdm_agent.adm	Enthält Richtlinieneinstellungen in Bezug auf die Authentifizierung sowie Umgebungskomponenten von View Agent. Weitere Informationen finden Sie im Dokument <i>Einrichten von Desktop- und Anwendungspools in View</i> .
Horizon Client-Konfiguration	vdm_client.adm	Enthält Richtlinieneinstellungen in Bezug auf Horizon Client für Windows. Auf Clients, die von außerhalb der View-Verbindungsserver-Hostdomäne eine Verbindung herstellen, wirken sich die auf Horizon Client angewendeten Richtlinien nicht aus. Weitere Informationen finden Sie im Dokument <i>Verwendung von VMware Horizon Client für Windows</i> .
View Server-Konfiguration	vdm_server.adm	Enthält Richtlinieneinstellungen in Bezug auf View-Verbindungsserver. Siehe ADM-Vorlageneinstellungen für die View Server-Konfiguration .
View-Konfiguration, allgemeine	vdm_common.adm	Enthält Richtlinieneinstellungen, die für alle View-Komponenten gelten. Siehe ADM-Vorlageneinstellungen für die allgemeine View-Konfiguration .
View-PCoIP-Sitzungsvariablen	pcoip.adm	Enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll. Weitere Informationen finden Sie im Dokument <i>Einrichten von Desktop- und Anwendungspools in View</i> .

Name der Vorlage	Vorlagendatei	Beschreibung
View-PCoIP-Client-Sitzungsvariablen	pcoip.client.adm	Enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll, das Auswirkungen auf Horizon Client für Windows hat. Weitere Informationen finden Sie im Dokument <i>Verwendung von VMware Horizon Client für Windows</i> .
View Persona Management-Konfiguration	ViewPM.adm	Enthält Richtlinieneinstellungen in Bezug auf View Persona Management. Weitere Informationen finden Sie im Dokument <i>Einrichten von Desktop- und Anwendungspools in View</i> .
View-Remote-Desktop-Dienste	vmware_rdsh.admx vmware_rdsh_server.admx	Enthält Richtlinieneinstellungen in Bezug auf Remote-Desktop-Dienste. Weitere Informationen finden Sie im Dokument <i>Einrichten von Desktop- und Anwendungspools in View</i> .

ADM-Vorlageneinstellungen für die View Server-Konfiguration

Die ADM-Vorlagendatei (vdm_server.adm) für die View Server-Konfiguration enthält Richtlinieneinstellungen in Bezug auf alle View-Verbindungsserver-Instanzen.

[Tabelle 5-3. Vorlageneinstellungen für die View Server-Konfiguration](#) beschreibt die in der ADM-Vorlagendatei für die View Server-Konfiguration enthaltenen Richtlinieneinstellungen. Die Vorlage enthält ausschließlich Einstellungen für die Computerkonfiguration.

Tabelle 5-3. Vorlageneinstellungen für die View Server-Konfiguration

Einstellung	Eigenschaften
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>

ADM-Vorlageneinstellungen für die allgemeine View-Konfiguration

Die ADM-Vorlagendatei (`vdm_common.adm`) für die allgemeine View Server-Konfiguration enthält Richtlinieneinstellungen, die für alle View-Komponenten gelten. Diese Vorlage enthält ausschließlich Einstellungen für die Computerkonfiguration.

Einstellungen für die Protokollkonfiguration

[Tabelle 5-4. Allgemeine View-Konfigurationsvorlage: Einstellungen für die Protokollkonfiguration](#)

beschreibt die in der ADM-Vorlagendatei für die allgemeine View-Konfiguration enthaltenen Richtlinieneinstellungen für die Protokollkonfiguration.

Tabelle 5-4. 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.

Einstellung	Eigenschaften
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 View 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>Log Level Server FQDN or IP [Port number(514 default)]</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 5-5. Allgemeine View-Konfigurationsvorlage: Einstellungen für Leistungsalarme beschreibt die in der ADM-Vorlagendatei für die allgemeine View-Konfiguration enthaltenen Einstellungen für Leistungsalarme.

Tabelle 5-5. 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.

Einstellung	Eigenschaften
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 View-Verbindungs- und View Agent-Systeme. Einstellungen für Leistungsalarme gelten nicht für Horizon Client-Systeme.

Allgemeine Einstellungen

[Tabelle 5-6. Allgemeine View-Konfigurationsvorlage: Allgemeine Einstellungen](#) beschreibt die in der ADM-Vorlagendatei für die allgemeine View-Konfiguration enthaltenen allgemeinen Einstellungen.

Tabelle 5-6. 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.

Warten von View-Komponenten

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

Dieses Kapitel enthält die folgenden Themen:

- [Sichern und Wiederherstellen von View-Konfigurationsdaten](#)
- [Überwachen von View-Komponenten](#)
- [Überwachen des Computerstatus](#)
- [Grundlegendes zu View-Diensten](#)
- [Ändern des Produktlizenzschlüssels](#)
- [Überwachen gleichzeitiger Verbindungen zu View und Zurücksetzen historischer Nutzungsdaten](#)
- [Aktualisieren allgemeiner Benutzerinformationen aus Active Directory](#)
- [Migrieren von View Composer auf eine andere Maschine](#)
- [Aktualisieren der Zertifikate auf einer View-Verbindungsserver-Instanz, einem Sicherheitsserver oder View Composer](#)
- [Vom Programm zur Verbesserung der Benutzerfreundlichkeit erfasste Daten](#)

Sichern und Wiederherstellen von View-Konfigurationsdaten

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

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

Sichern von View-Verbindungsserver- und View Composer-Daten

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

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

Wenn Sie Sicherungen mithilfe von View Administrator durchführen, sichert View die View LDAP-Konfigurationsdaten und die View Composer-Datenbank. Beide Sicherungsdateisätze werden am selben Speicherort abgelegt. 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 View-Funktion für die Konfigurationssicherung.
- Wenn Sie sofort eine Sicherung durchführen möchten, verwenden Sie die Funktion **Jetzt sichern** in View Administrator.
- Sie können mit dem Dienstprogramm `vdmexport` einen manuellen Export der View LDAP-Daten durchführen. Dieses Dienstprogramm wird mit jeder Instanz von View-Verbindungsserver 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 View-Verbindungsserver](#).

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

- View kann Konfigurationsdaten aus einer beliebigen View-Verbindungsserver-Instanz exportieren.
- Wenn mehrere View-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 View-Verbindungsserver als Sicherungsmechanismus fungieren. Wenn View Daten in replizierten Instanzen des View-Verbindungservers synchronisiert, werden die auf einer Instanz verlorenen Daten bei der Datenharmonisierung von allen Mitgliedern der Gruppe entfernt.
- Wenn der View-Verbindungsserver mehrere vCenter Server-Instanzen mit mehreren View Composer-Diensten verwendet, sichert View alle mit sämtlichen vCenter Server-Instanzen verknüpften View Composer-Datenbanken.

Planen von View-Konfigurationssicherungen

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

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

Voraussetzungen

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

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie auf der Registerkarte **Verbindungsserver** die zu sichernde View-Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 3 Geben Sie auf der Registerkarte **Sicherung** die Einstellungen für die View-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 Kennwörterinnerung ein.
 - d Klicken Sie auf **OK**.
- 5 Klicken Sie auf **OK**.

Sicherungseinstellungen zur View-Konfiguration

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

Tabelle 6-1. Sicherungseinstellungen zur View-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 Uhr 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 View-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 View 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 View-Verbindungsserver aufgeführt wird: C:\Programdata\VMware\VDM\backups</p> <p>Bei Verwendung der Option Jetzt sichern legt View die Sicherungsdateien ebenfalls an diesem Speicherort ab.</p>

Exportieren von Konfigurationsdaten aus View-Verbindungsserver

Sie können die Konfigurationsdaten einer View-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 View-Verbindungsserver-Instanz ausführen. Wenn mehrere View-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 View-Verbindungsserver installiert wird.

C:\Program Files\VMware\VMware View\Server\tools\bin

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

Verfahren

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

```
vdmexport > Myexport.LDF
```

Die exportierten Daten sind standardmäßig verschlüsselt.

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

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

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

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

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

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

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

Weitere Informationen zum Befehl `vdmexport` finden Sie im Dokument *Integration von View*.

Nächste Schritte

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

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

Wiederherstellen von View-Verbindungsserver- und View Composer-Konfigurationsdaten

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

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

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

Verwenden Sie das Dienstprogramm `vdmimport`, um die View-Verbindungsserver-Daten aus den LDIF-Sicherungsdateien in das View LDAP-Repository der View-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 View-Verbindungsserver-Instanz installieren und die vorhandene View-Konfiguration wiederherstellen, indem Sie die View-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 View-Konfiguration einzurichten, oder aus anderen Gründen erforderlich sein. Weitere Informationen finden Sie unter „Neuinstallieren von View-Verbindungsserver mit einer Konfigurationssicherung“ im Dokument *Installation von View*.

Importieren von Konfigurationsdaten in View-Verbindungsserver

Sie können die Konfigurationsdaten einer View-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 View-Verbindungsserver-Instanz zu importieren.

Wenn Sie Ihre View LDAP-Konfiguration mit View 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 View-Verbindungsserver- und View Composer-Daten](#).

Voraussetzungen

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

`C:\Program Files\VMware\VMware View\Server\tools\bin`

- Melden Sie sich bei einer View-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 Stoppen 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 View-Verbindungsserver.

Deinstallieren Sie sowohl VMware Horizon View-Verbindungsserver als auch die AD LDS-Instanz „VMwareVDMDS“ .
- 4 Installieren Sie eine Instanz von View-Verbindungsserver.
- 5 Stoppen Sie die View-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 View-Verbindungsserver.

Deinstallieren Sie nur das Paket „VMware Horizon View-Verbindungsserver“.
- 10 Installieren Sie den View-Verbindungsserver neu.
- 11 Melden Sie sich bei View 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.

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 View-Verbindungsserver mit den Konfigurationsdaten aus der LDIF-Datei. Weitere Informationen zum Befehl `vdmimport` finden Sie im Dokument *Integration von View*.

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 View die Sicherungsdateien auf Laufwerk C: des View-Verbindungsserver-Computers im Verzeichnis `C:\Programdata\VMWare\VDM\backups`.

View Composer-Sicherungsdateien folgen einer Namenskonvention mit Datumstempel und `.svi`-Suffix.

`Backup-YearMonthDayCount-vCenter Server Name_Domain Name.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 View-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 6-2. Restoredata-Ergebniscodes

Code	Beschreibung
0	Vorgang erfolgreich abgeschlossen.
1	Angegebener DSN wurde nicht gefunden.

Code	Beschreibung
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 View 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 -dsname=LinkedClone
          -username=Admin -password=Pass
          -outputfilepath="C:\Program Files\VMware\VMware View
          Composer\Export-20090304000010-foobar_test_org.SVI"
```

Nächste Schritte

Exportergebniscodes des Befehls `SviConfig exportdata` finden Sie unter [Ergebniscodes für 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 6-3. 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 View-Komponenten

Sie können den Status der View- und vSphere-Komponenten in Ihrer View-Bereitstellung problemlos über das View Administrator-Dashboard überwachen.

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

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

Verfahren

- 1 Klicken Sie in View 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 beliebige Virtual SAN-Cluster und die an einem Virtual SAN-Datenspeicher beteiligten Festplatten zu überwachen. Weitere Informationen finden Sie im Dokument *Speicher von vSphere* und im Handbuch *Überwachung und Leistung von vSphere*.

Überwachen des Computerstatus

Sie können den Status von Computern in Ihrer View-Bereitstellung problemlos über das View 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. Siehe [Status von vCenter Server-VMs](#).

Verfahren

- 1 Klicken Sie in View 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.

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 View Administrator auf „Zurück“, um erneut auf die Dashboard-Seite zu wechseln.

Grundlegendes zu View-Diensten

Der Betrieb von View-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 View-Diensten. Wenn Sie die View-Dienste auf einem View-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 View-Funktionalität eingeschränkt ist.

Beenden und Starten der View-Dienste

Der Betrieb von View-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 View manuell stoppen und starten müssen.

Wenn Sie View-Dienste stoppen, können Endbenutzer keine Verbindung mehr zu ihren Remote-Desktops und Anwendungen 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 View-Verbindungsserver-Dienst auf einem View-Verbindungsserver-Host oder den VMware View-Sicherheitsserver-Dienst auf einem Sicherheitsserver. Beenden Sie keine anderen Komponentendienste.

Voraussetzungen

Machen Sie sich mit den Diensten vertraut, die auf View-Verbindungsserver-Hosts und Sicherheitsservern ausgeführt werden, wie unter [Dienste auf einem View-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 View-Verbindungsserver-Dienst auf einem View-Verbindungsserver-Host oder den VMware 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 View-Verbindungsserver-Host

Der Betrieb von View hängt von verschiedenen Diensten ab, die auf einem View-Verbindungsserver-Host ausgeführt werden.

Tabelle 6-4. View-Verbindungsserver-Hostdienste

Dienstname	Starttyp	Beschreibung
VMware Horizon View Blast Secure Gateway	Automatisch	Stellt sichere HTML Access-Dienste bereit. Dieser Dienst muss ausgeführt werden, wenn Clients die Verbindung zu View-Verbindungsserver über den HTML Access 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 View-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 zu View-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 Security Gateway-Komponente	Manuell	Stellt gängige Gateway-Dienste bereit. Dieser Dienst muss immer ausgeführt werden.

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 View stellt dieser Dienst sicher, dass vorhandene Daten korrekt migriert werden.

Dienste auf einem Sicherheitsserver

Der Betrieb von View hängt von verschiedenen Diensten ab, die auf einem Sicherheitsserver ausgeführt werden.

Tabelle 6-5. Dienste auf einem Sicherheitsserver

Dienstname	Starttyp	Beschreibung
VMware Horizon View Blast Secure Gateway	Automatisch	Stellt sichere HTML Access-Dienste bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu diesem Sicherheitsserver über ein HTML Access 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 View-Funktionen zugreifen möchten, die derzeit nicht lizenziert sind, können Sie mithilfe von View Administrator den Produktlizenzschlüssel ändern.

Sie können eine Lizenz zu View hinzufügen, während View 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 View und Add-On-Funktionen, wie beispielsweise View Composer und Remoteanwendungen, müssen Sie einen gültigen Produktlizenzschlüssel erwerben.

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration > Produktlizenzierung und -verwendung** aus.
- 2 Klicken Sie im Bereich **Lizenzierung** auf **Lizenz bearbeiten**.
- 3 Geben Sie die Seriennummer der Lizenz ein und klicken Sie auf **OK**.

Im Fenster **Produktlizenzierung** werden die aktualisierten Lizenzinformationen angezeigt.

- 4 Überprüfen Sie das Ablaufdatum der Lizenz.
- 5 Überprüfen Sie, ob die Lizenzen für Desktops, die Remote-Ausführung von Anwendungen sowie View Composer aktiviert oder deaktiviert sind, je nach der VMware Horizon-Edition, zu deren Verwendung Ihre Produktlizenz Sie berechtigt.

Nicht alle Funktionen und Merkmale von VMware Horizon mit View stehen in allen Editionen zur Verfügung. Einen Funktionsvergleich der einzelnen Editionen finden Sie unter <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

Überwachen gleichzeitiger Verbindungen zu View und Zurücksetzen historischer Nutzungsdaten

In View Administrator können Sie die aktiven Desktop-Sitzungen und Anwendungsbenutzer überwachen, die derzeit mit View verbunden sind. Auf der Seite **Produktlizenzierung und -verwendung** werden die aktuelle und die höchste Anzahl historischer gleichzeitiger Verbindungen 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.

Remote-Desktop-Verbindungen werden pro Sitzung gezählt. Wenn ein Benutzer mehrere Remote-Desktops ausführt, wird jede verbundene Desktop-Sitzung separat gezählt.

Remoteanwendungsverbindungen werden pro Benutzer gezählt. Wenn ein Benutzer mehrere Remoteanwendungen ausführt, wird der Benutzer nur einmal gezählt, auch wenn verschiedene Anwendungen auf verschiedenen RDS-Hosts gehostet werden.

In der Spalte **Höchster Wert** auf der Seite **Produktlizenzierung und -verwendung** wird die höchste Anzahl an gleichzeitigen Desktop-Sitzungen und Remoteanwendungsbenutzern seit der ersten Konfiguration Ihrer View-Bereitstellung oder seit der Auswahl der Einstellung **Höchsten Wert zurücksetzen** angezeigt.

Ein Administrator mit der Berechtigung **Globale Konfiguration und Richtlinien verwalten** kann die Einstellung **Höchsten Wert zurücksetzen** auswählen. Erteilen Sie diese Berechtigung nur bestimmten Administratoren, um den Zugriff auf die Einstellung **Höchsten Wert zurücksetzen** zu beschränken.

Verfahren

- 1 Wählen Sie in View 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.

Aktualisieren allgemeiner Benutzerinformationen aus Active Directory

Sie können View 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 View-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 View auswirken.

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

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 View Administrator als Administrator mit der Berechtigung **Globale Konfiguration und Richtlinien verwalten** anmelden können.

Verfahren

- 1 Klicken Sie in View 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 View-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 eine eigenständige 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 mit der Installation des VMware Horizon View Composer-Diensts vertraut. Weitere Informationen finden Sie unter „Installation von View Composer“ im Dokument *Installation von View*.
- Machen Sie sich mit der Konfiguration eines SSL-Zertifikats für View Composer vertraut. Lesen Sie den Abschnitt „Konfigurieren von SSL-Zertifikaten für View Server“ im Dokument *Installation von View*.
- Machen Sie sich mit der Konfiguration von View Composer in View Administrator vertraut. Siehe [Konfigurieren von View Composer-Einstellungen](#) und [Konfigurieren von View Composer-Domänen](#).

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 View Administrator **View-Konfiguration > Server**.
 - 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 (Optional) 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 View Administrator die neuen View Composer-Einstellungen.

- a Wählen Sie in View Administrator **View-Konfiguration > Server**.
- 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 Domännennamen (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 mit der Installation des VMware Horizon View Composer-Diensts vertraut. Weitere Informationen finden Sie unter „Installation von View Composer“ im Dokument *Installation von View*.
- Machen Sie sich mit der Konfiguration eines SSL-Zertifikats für View Composer vertraut. Lesen Sie den Abschnitt „Konfigurieren von SSL-Zertifikaten für View Server“ im Dokument *Installation von View*.

- Machen Sie sich mit den Schritten zum Entfernen von View Composer aus View Administrator vertraut. Siehe [Entfernen von View Composer aus View](#).

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 View Administrator vertraut. Siehe [Konfigurieren von View Composer-Einstellungen](#) und [Konfigurieren von View Composer-Domänen](#).

Verfahren

- 1 Entfernen Sie in View Administrator die View Composer-Komponente aus View 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 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.
- 5 Konfigurieren Sie in View Administrator die neuen View Composer-Einstellungen.
 - a Wählen Sie in View Administrator **View-Konfiguration > Server**.
 - 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 Zielformaschine, auf der Sie den neuen VMware Horizon View Composer-Dienst installieren möchten.

Nächste Schritte

Migrieren Sie den RSA-Schlüsselcontainer auf die Zielformaschine. 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 Zielformaschinen 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.xxxxx.

- 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 Zielformaschine, auf der Sie den neuen VMware Horizon View Composer-Dienst installieren möchten.

- 4 Öffnen Sie auf der Zielformaschine eine Eingabeaufforderung und navigieren Sie zum Verzeichnis %windir%\Microsoft.NET\Framework\v2.0xxxxx.
- 5 Geben Sie den Befehl `aspnet_regiis` ein, um die RSA-Schlüsselpaaraten 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 Zielformaschine. 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 *Installation von View*.

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 View-Verbindungsserver-Instanz, einem Sicherheitsserver oder View Composer

Wenn Sie aktualisierte Server-SSL-Zertifikate oder Zwischenzertifikate erhalten, importieren Sie die Zertifikate auf jedem View-Verbindungsserver, Sicherheitsserver oder View Composer-Host in die Zertifikatsspeicher 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 View-Verbindungsserver, Sicherheitsserver oder View Composer für die Verwendung eines neuen SSL-Zertifikats“ im Dokument *Installation von View*.

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 View-Verbindungsserver-Instanz, der Sicherheitsserver oder der VMware Horizon View Composer-Dienst installiert wurde.

Verfahren

- 1 Importieren Sie das signierte SSL-Serverzertifikat in den Zertifikatsspeicher 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 View-Verbindungsserver oder den Sicherheitsserver das Zertifikat „Angezeigter Name“, **vdm**, aus dem alten Zertifikat, das für den View 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 View-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 SSL-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 View-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.

Vom Programm zur Verbesserung der Benutzerfreundlichkeit erfasste Daten

Sie können an einem Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen. Wenn Sie am Programm teilnehmen, erfasst VMware anonyme Daten zu Ihrer Bereitstellung, um die Reaktionen von VMware auf Benutzeranforderungen zu verbessern. VMware verwendet diese Informationen, um die Qualität, Zuverlässigkeit und Leistung unserer Produkte zu verbessern. Es werden jedoch keine Daten gesammelt, die Aufschluss über Ihr Unternehmen geben könnten.

Die Teilnahme an dem Programm ist optional. Sie können auswählen, ob Sie teilnehmen möchten, indem Sie die Option deaktivieren, wenn Sie den View-Verbindungsserver mit einer neuen Konfiguration installieren. Wenn Sie nach Abschluss der Installation Ihre Meinung hinsichtlich der Teilnahme zu irgendeiner Zeit ändern, können Sie dem Programm beitreten bzw. es verlassen, indem Sie die Seite „Produktlizenzierung und -verwendung“ in View Administrator bearbeiten.

Bevor Sie Daten erfassen, anonymisiert VMware alle Felder, die Ihre unternehmensspezifischen Informationen enthalten. Die bereinigten Felder identifizieren Computer, Datenspeicher, Netzwerkfunktionen, Anwendungen und Benutzer. Beispiel: Die IP-Adressen und Anpassungsspezifikationen der virtuellen Maschine werden anonymisiert.

VMware bereinigt ein Feld, indem ein Hash des aktuellen Werts generiert wird. Wenn ein Hash-Wert erfasst wurde, kann VMware den aktuellen Wert nicht identifizieren, jedoch die Änderungen am Wert ermitteln, wenn Sie Ihre Umgebung ändern.

Um zu entscheiden, ob Sie an dem Programm teilnehmen, können Sie die Felder überprüfen, über die VMware Daten erfasst. Zudem können Sie alle bereinigten Felder überprüfen. Die Felder werden nach der View-Komponente organisiert. Weitere Informationen finden Sie unter [Von VMware erfasste globale View-Daten](#) sowie in den folgenden verwandten Themen.

Wie VMware Ihre Daten schützt

VMware verpflichtet sich zur Wahrung der Vertraulichkeit Ihrer Daten und unternimmt verschiedene Schritte, um sicherzustellen, dass die im Rahmen des Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP) erhobenen Daten keinerlei vertrauliche Informationen enthalten, anhand deren ein bestimmter Kunde oder Benutzer eindeutig identifiziert werden könnte. Das Programm erhebt keinerlei Daten, die dazu verwendet werden können, Sie zu kontaktieren oder zu identifizieren. Es werden keine Daten gesammelt, die Aufschluss über Ihr Unternehmen oder Ihre Benutzer geben könnten.

Wenn die CEIP-Funktion aktiviert ist, sammelt der View-Verbindungsserver Daten aus Ihrer Bereitstellung und führt auf Basis dieser Daten folgende Aktionen aus:

- 1 Daten wie z. B. Benutzer, Servernamen, IP-Adressen und Netzwerk-Serverpfade, anhand deren Ihre Bereitstellung eindeutig identifiziert werden könnte, werden anonymisiert, indem auf Basis dieser Daten eine unidirektionale Hash-Funktion ausgeführt wird. Auf diese Weise kann VMware nützliche Information darüber sammeln, wie viele einzelne Server, Computer und Benutzer Ihre Bereitstellung umfasst, ohne spezifische Servernamen, Benutzernamen oder Adressen zu erfassen.
- 2 Sämtliche Daten werden mithilfe eines öffentlichen Schlüssels verschlüsselt. Der private Schlüssel, der für die Entschlüsselung des Datensatzes erforderlich ist, steht nur VMware zur Verfügung.
- 3 Die verschlüsselten, anonymisierten Daten werden mithilfe von HTTPS an VMware übermittelt.

Sie können die Liste aller Felder einsehen, von denen Daten erhoben werden. Diese Liste gibt auch an, welche Felder anonymisiert werden. Weitere Informationen finden Sie unter [Von VMware erfasste globale View-Daten](#) sowie in den folgenden verwandten Themen.

Vorschau von vom Programm zur Verbesserung der Benutzerfreundlichkeit erfassten Daten

Sie können die Daten, die VMware empfangen würde, in einer Vorschau anzeigen, bevor diese verschlüsselt und übertragen werden. Wenn Sie diese Option aktivieren, schreibt View-Verbindungsserver den Datensatz auf Festplatte, anstatt die Daten zu verschlüsseln und an VMware zu senden.

Sie konfigurieren die Option zum Schreiben von CEIP-Daten auf Festplatte anstatt der Übertragung der Daten an VMware als globale Option im LDAP-Verzeichnis von View. Verwenden Sie zur Änderung von View LDAP das Dienstprogramm ADSI-Editor. Das Dienstprogramm ADSI-Editor ist zusammen mit der View-Verbindungsserver-Instanz installiert. Wenn Sie View LDAP auf einer View-Verbindungsserver-Instanz ändern, werden diese Änderungen auf alle replizierten View-Verbindungsserver-Instanzen übertragen.

Verfahren

- 1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem View-Verbindungsserver-Host.
- 2 Wählen Sie im Dialogfeld „Verbindungseinstellungen“ **DC=vdi**, **DC=vmware**, **DC=int** oder verbinden Sie sich damit.

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

Beispiel: localhost:389 or mycomputer.mydomain.com:389

- 4 Setzen Sie für das Objekt **CN=Common, OU=Global, OU=Properties** den Wert des Attributs **pae-ceipDumpOnly** auf 1.

- 5 Starten Sie View-Verbindungsserver neu.

Die CEIP-Datendateien werden im Nur-Text-JSON-Format in das Verzeichnis %PROGRAMFILES%\VMware\VMware View\Server\broker\temp\spool auf der View-Verbindungsserver-Instanz geschrieben.

Nächste Schritte

Um die Einstellung zurückzusetzen und mit dem Versenden von Daten an VMware zu beginnen, ändern Sie den Wert des Attributs **pae-ceipDumpOnly** auf 0 und starten Sie View-Verbindungsserver neu.

Zusätzliche Informationen über das Programm zur Verbesserung der Benutzerfreundlichkeit

Nachdem Sie sich für die Teilnahme am CEIP entschieden haben, werden die Daten auf der ersten View-Verbindungsserver-Instanz in einer View-Bereitstellung zusammengetragen. Die Konfigurationsdaten werden wöchentlich zusammengetragen. Die Leistungs- und Verwendungsdaten werden stündlich zusammengetragen. Wenn Ihre View-Verbindungsserver-Instanz nicht auf das Internet zugreifen kann, werden die Informationen auf der Festplatte gespeichert, bis die Internetverbindung das nächste Mal verfügbar ist.

Wenn Sie sich für die Teilnahme entscheiden, können Sie sich später abmelden. Sie können dem Programm jederzeit beitreten bzw. es verlassen, indem Sie die Einstellung **Anonyme Daten an VMware senden** auf der Seite „Produktlizenzierung und -verwendung“ in View Administrator bearbeiten. Starten Sie jede View-Verbindungsserver-Instanz in der Umgebung neu, damit die Änderung wirksam wird.

Die Datenerfassung nach dem CEIP wirkt sich nicht negativ auf die Leistung oder den Festplattenverbrauch in Ihrer View-Bereitstellung aus. Die von Ihnen zusammengestellten und an VMware gesendeten Informationen werden, unabhängig davon, ob die CEIP-Funktion aktiviert ist, an die View-Verbindungsserver-Instanz gesendet. Standardmäßig ist es möglich, dass durch die Aktivierung der Funktion bis zu 100 MB Speicherplatz auf der View-Verbindungsserver-Instanz beansprucht werden, bevor die Daten an VMware gesendet werden. Standardmäßig werden nicht gesendete Daten, die älter als acht Tage sind, verworfen.

Wenn Ihre View-Verbindungsserver-Instanzen von einer Firewall über den Zugang auf das Internet blockiert werden, können Sie immer noch das CEIP verwenden. Wenn das CEIP aktiviert ist, versuchen Ihre View-Verbindungsserver-Instanzen regelmäßig, eine Verbindung zur Datenerhebungs-URL unter Verwendung von HTTPS unter <https://ceip.vmware.com> herzustellen. Wenn die Verbindung gesperrt oder aufgrund einer Proxy-Server- bzw. Firewall-Einschränkung nicht auf sie zugegriffen werden kann, speichert der View-Verbindungsserver Ihre CEIP-Daten zwischen, bis die Datensätze das konfigurierte Höchstalter überschreiten (standardmäßig acht Tage) oder bis die insgesamt gesammelten Daten die konfigurierte maximale Spoolgröße (standardmäßig 100 MB) überschreiten.

Sie können den Standort, die maximale Größe und das Höchstalter des CEIP-Datenspools ändern. Der Standort und die Größe des Spools werden von den folgenden Einstellungen in der View LDAP-Datenbank bestimmt:

pae-ceipSpoolDirectory	Directory where CEIP data is cached before being sent to VMware. Default: Program Files\VMware\VMware View\Server\broker\temp\spool
pae-ceipMaxSpoolSize	Maximum size, in bytes, of temporary spool data. Default: 100 MB
pae-ceipMaxSpoolAge	Maximum age of records in the temporary local spool. Default: 8 days

Sie werden nicht kontaktiert bzw. erhalten keinen Spam, wenn Sie am CEIP teilnehmen. Das CEIP erfasst keine Kontaktinformationen wie Ihren Namen, Ihre Privatadresse, Ihre E-Mail-Adresse oder Ihre Telefonnummer. Das CEIP fordert Sie nicht auf, an Umfragen teilzunehmen oder Junk-E-Mails zu lesen. Zudem werden Sie auf keine andere Weise kontaktiert.

Von VMware erfasste globale View-Daten

Wenn Sie am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen, sammelt VMware globale Daten zur View-Umgebung. Felder mit vertraulichen Informationen werden anonymisiert.

Tabelle 6-6. Informationen zu globalen Konfigurationseinstellungen

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Maximale Laufzeit für eine View-Verbindungsserver-Sitzung (in Sekunden)	Nein	180,000
Zeitspanne (in Sekunden), nach deren Ablauf der View-Verbindungsserver die Trennung der Benutzer erzwingt, wenn keine Daten vom Client gesendet werden	Nein	36,000
Zeitspanne (in Sekunden), während der ein Benutzer im Leerlauf sein kann, bevor der View-Verbindungsserver die Single Sign-On-Anmeldeinformationen (SSO) des Benutzers sperrt	Nein	900
Zeitspanne (in Minuten), nach deren Ablauf die SSO-Anmeldeinformationen für einen Desktop-Start bereinigt werden	Nein	-1 (das bedeutet nie)
Zeitspanne (in Minuten), nach deren Ablauf die SSO-Anmeldeinformationen für einen Anwendungsstart bereinigt werden	Nein	-1 (das bedeutet nie)
Zeitüberschreitung für eine View Administrator-Konsolensitzung (in Sekunden)	Nein	3,000
Vor der Anmeldung gezeigte Meldung anzeigen, wenn Benutzer sich mit View-Verbindungsserver-Instanzen in diesem Pod verbinden	Nein	0 oder 1
Remote-Desktop kann ein Server-Betriebssystem ausführen	Nein	True oder False

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Mirage-Server ist aktiviert	Nein	True oder False
URL des Mirage-Servers, einschließlich Portnummer	Yes	Keine

Tabelle 6-7. Globale Statusinformationen

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
View Server können Kontakt zum Domänencontroller aufnehmen.	Nein	True oder False
DNS der Active Directory-Domäne	Yes	Keine
Es handelt sich um eine Domäne mit NT4.	Nein	True oder False
Name der Domäne	Yes	Keine
Status der Domäne	Nein	OK
Art der Vertrauensbeziehung mit der Domäne	Nein	Primäre Domäne, wechselseitig, wechselseitig mit mehreren Verzweigungen usw.

Von VMware erfasste View-Verbindungsserver-Daten

Wenn Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit beitreten, erhebt VMware Daten aus bestimmten View-Verbindungsserver-Feldern. Felder mit vertraulichen Informationen werden anonymisiert.

Tabelle 6-8. Aus dem View-Verbindungsserver erfasste Konfigurationsdaten

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Der allgemeine Name (CN) für den View-Verbindungsserver-Eintrag in View LDAP	Yes	Keine.
View-Verbindungsserver ist deaktiviert	Nein	True oder False
SecureID-Authentifizierung ist konfiguriert und aktiv	Nein	True oder False
RADIUS-Authentifizierung ist konfiguriert und aktiv	Nein	True oder False
SAML-Serverauthentifizierung ist zulässig, deaktiviert oder erforderlich	Nein	0 = Deaktiviert 1 = Zulässig 2 = Erforderlich
Art der View-Verbindungsserver-Installation	Nein	0 = View-Verbindungsserver 1 = Sicherheitsserver
Muss der Name der SecureID-Authentifizierung mit dem von Active Directory übereinstimmen?	Nein	True = Name der SecureID-Authentifizierung wird zugewiesen False = Name der SecureID-Authentifizierung wird nicht zugewiesen
Dürfen Clients den sicheren Tunnel umgehen?	Nein	True oder False

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Dürfen Clients das PCoIP Secure Gateway umgehen?	Nein	True oder False
Konfiguration der Smartcard-Authentifizierung	Nein	Aus, optional oder erforderlich
Dürfen Benutzer automatisch abgemeldet werden, wenn ihre Smartcard entfernt wird?	Nein	True oder False
Ordner, in dem View LDAP-Sicherungen gespeichert werden	Yes	Keine.
Einheiten der Zeit für das Festlegen der View LDAP-Sicherungshäufigkeit	Nein	Stunde, Tag oder Woche
Häufigkeit der View LDAP-Sicherungen	Nein	Ganzzahl
Zeitpunkt der View LDAP-Sicherung	Nein	Ganzzahl
Maximale Anzahl von zu speichernden View LDAP-Sicherungen	Nein	Ganzzahl
Zeitpunkt der letzten View LDAP-Sicherung	Nein	21. Februar 2014 12:00:10
Status der letzten View LDAP-Sicherung	Nein	OK
Ausstehende unmittelbare View LDAP-Sicherung	Nein	True oder False
Tags associated with the View-Verbindungsserver instance	Yes	Keine.
Angabe, ob die View-Verbindungsserver-Instanz mit einem Sicherheitsserver gekoppelt wird	Nein	0 = Nicht gekoppelt 1 = Gekoppelt
Der definierte Name (DN) der View-Verbindungsserver-Instanz in LDAP	Yes	Keine.
Zeitraum der Sicherheitsserver-Kopplung, in dem das Kennwort für die Paarbildung gültig ist	Nein	
Der Host-/Knotenname der View-Verbindungsserver-Instanz	Yes	Keine.
Die Versionsnummer nur der View-Verbindungsserver-Instanz	Nein	6.0.0
Die vollständige Build- und Versionsangabe für die View-Verbindungsserver-Instanz	Nein	6.0.0-123455
Automatisch erneut mit sicherem Gateway verbinden	Nein	True oder False
Tunnelclient-Protokoll	Nein	
Protokoll, das von der View-Verbindungsserver-Instanz oder dem Sicherheitsserver gelesen wird	Nein	

Tabelle 6-9. Aus dem View-Verbindungsserver erfasste Statusinformationen

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Die Buildnummer der View-Verbindungsserver-Instanz	Nein	123456
Der Name der replizierten Gruppe des View-Verbindungservers, in der Regel der erste Knotenname der View-Verbindungsserver-Instanz	Yes	Keine.
DNS-Name der View-Verbindungsserver-Instanz	Yes	Keine.
IP-Adresse der View-Verbindungsserver-Instanz	Yes	Keine.

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
NetBIOS-Hostname der View-Verbindungsserver-Instanz	Yes	Keine.
Die aktuelle Anzahl der Sitzungen auf der View-Verbindungsserver-Instanz	Nein	Ganzzahl
Die maximale Anzahl der Sitzungen auf der View-Verbindungsserver-Instanz	Nein	Ganzzahl
Die aktuelle Anzahl der View Composer-Sitzungen auf der View-Verbindungsserver-Instanz	Nein	Ganzzahl
Die maximale Anzahl der View Composer-Sitzungen auf der View-Verbindungsserver-Instanz	Nein	Ganzzahl
Die Version der View-Verbindungsserver-Instanz	Nein	6.0.0

Tabelle 6-10. Dynamische Verwendung von aus dem View-Verbindungsserver erfassten Daten

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Angabe, wie oft einzelne PowerShell-Cmdlets aufgerufen wurden	Nein	Liste von Ganzzahlen
Angabe, wie oft einzelne View API-Methoden in der vorherigen Minute aufgerufen wurden	Nein	Liste von Ganzzahlen
Anmelderate unter Verwendung von Kennwörtern im Laufe der Zeit	Nein	Gleitkommawert
Anmelderate unter Verwendung des SSL-Serverzertifikats im Laufe der Zeit	Nein	Gleitkommawert
Anmelderate unter Verwendung von delegierter Authentifizierung wie SAML im Laufe der Zeit	Nein	Gleitkommawert
Durchschnittliche prozentuale CPU-Nutzung	Nein	Ganzzahl
Durchschnittliche prozentuale Arbeitsspeicherauslastung	Nein	Ganzzahl
Durchschnittliche Anmeldungen mit und ohne Kennwörter, die für SSO verfügbar sind	Nein	Gleitkommawert
Angabe, wie oft Desktopverbindungen mit jedem Typ des Anzeigeprotokolls (PCoIP, RDP und Blast für HTML Access) gestartet wurden	Nein	Liste von Ganzzahlen
Angabe, wie oft neue Client-Verbindungen für eine Remoteanwendung für jeden Typ des Anzeigeprotokolls (PCoIP, RDP und Blast für HTML Access) vorgenommen wurden	Nein	Liste von Ganzzahlen
Angabe, wie oft das Starten einer Remoteanwendung zu einer neuen Verbindung, einer wiederverwendeten Verbindung, einer neuen Sitzungsverbindung und einer wiederverwendeten Sitzungsverbindung führt	Nein	Liste von Ganzzahlen
Angabe, wie oft Desktopverbindungen für einen Benutzer gestartet wurden, der für n Desktops berechtigt ist	Nein	Liste von Ganzzahlen wie eine Liste zur Anzahl der Benutzer, die für 1, 2, 3 Desktops usw. berechtigt sind

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Angabe, wie oft Anwendungsverbindungen für einen Benutzer gestartet wurden, der für n Anwendungen berechtigt ist	Nein	Liste von Ganzzahlen
Angabe, wie oft n Protokollsitzungen (wie PCoIP) vorhanden sind, wenn ein Benutzer eine andere Anwendung startet Beispiel: Ein Benutzer startet eine fünfte Anwendung, aber alle Anwendungen befinden sich in derselben Serverfarm. Nur eine Sitzung ist vorhanden.	Nein	Liste von Ganzzahlen wie eine Liste zur Anzahl der Benutzer, die über eine Sitzung verfügen, die über zwei Sitzungen verfügen usw.

Von VMware erfasste Sicherheitsserverdaten

Wenn Sie am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen, erhebt VMware Daten aus Sicherheitsserverfeldern. Felder mit vertraulichen Informationen werden anonymisiert.

Tabelle 6-11. Sicherheitsserverinformationen

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Die Anzahl an PCoIP-Sitzungen, die auf dem sicheren Gateway des Sicherheitsservers ausgeführt werden	Nein	Ganzzahl
Die Anzahl an Sitzungen eines beliebigen Typs, die auf dem sicheren Gateway des Sicherheitsservers ausgeführt werden	Nein	Ganzzahl
Die Buildnummer des Sicherheitsservers	Nein	123456
Der Hostname des Sicherheitsservers	Yes	Keine
IPsec ist aktiv	Nein	True oder False
Das sichere Gateway ist nicht verfügbar	Nein	True oder False
Die derzeitige Anzahl an Sitzungen	Nein	Ganzzahl
Die URL des sicheren Gateways	Yes	Keine
Die Versionsnummer des Sicherheitsservers	Nein	6.0.0

Von VMware erfasste Desktop-Pool-Daten

Wenn Sie am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen, erhebt VMware Daten aus bestimmten Desktop-Pool-Feldern. Felder mit vertraulichen Informationen werden anonymisiert.

Tabelle 6-12. Aus Desktop-Pools gesammelte Konfigurationsdaten

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Der allgemeine Name (CN) für den Desktop-Pool-Eintrag in View LDAP	Yes	Keine.
Der beschreibende Anzeigename des Desktop-Pools	Yes	Keine.
Der Desktop-Pool ist deaktiviert	Nein	True oder False

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Typ des Desktop-Pools	Nein	Eine der folgenden Optionen: IndividualVC, IndividualUnmanaged, Persistent, NonPersistent, SviPersistent, SviNonPersistent, ManualVCPersistent, Manual, ManualUnmanagedPersistent, ManualUnmanagedNonPersistent, TerminalService, OnRequestVcPersistent, OnRequestVcNonPersistent, OnRequestSviPersistent, OnRequestSviNonPersistent
Der View Administrator-Ordner, unter dem dieser Desktop-Pool gruppiert ist	Yes	Keine.
Die Liste der eindeutigen Namen (DNs) von virtuellen Maschinen, die zum Desktop-Pool gehören	Nein	Beispiel eines Listenelements: ["CN=8f11d7cf-b0ef-43ad-92ce-691aa929d3c4,OU=Server,DC=vdi,DC=vmware,DC=int"]
Sind mehrere Sitzungen im Desktop-Pool zulässig?	Nein	True oder False
Dürfen Benutzer dieses Desktop-Pools ihre virtuellen Maschinen zurücksetzen?	Nein	Aus, optional oder erforderlich
Zeit, nach der eine Meldung zum erzwungenen Abmelden angezeigt wird	Nein	True oder False
Der eindeutige Name (DN) der vCenter Server-Instanz, der die virtuellen Maschinen im Pool verwaltet	Nein	"CN=e7a718de-d0f7-444a-9452-156dce289028,OU=VirtualCenter,OU=Eigenschaften,DC=vdi,DC=vmware,DC=int"
Minimale Anzahl an virtuellen Maschinen im Desktop-Pool	Nein	Ganzzahl
Maximale Anzahl an virtuellen Maschinen im Desktop-Pool	Nein	Ganzzahl
Anzahl an bereitgestellten virtuellen Reservemaschinen im Desktop-Pool	Nein	Ganzzahl
Löschrichtlinie für den Desktop-Pool	Nein	Default, DeleteOnUse oder RefreshOnUse
Bei Bereitstellung verwendetes DNS-Suffix	Yes	Keine.
Das Benennungsmuster (Präfix), das für Namen von automatisch bereitgestellten virtuellen Maschinen verwendet werden soll	Yes	Keine.
Die Vorlage, von der aus virtuelle Maschinen geklont werden sollen	Yes	Keine.
Der Ordner in vCenter Server, in dem bereitgestellte virtuelle Maschinen gespeichert werden	Yes	Keine.
Der Ressourcenpool, der für die virtuellen Maschinen verwendet wird	Yes	Keine.

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Eine Liste mit Datenspeichern	Yes	Keine.
Die Anpassungsspezifikation, die zur Bereitstellung von virtuellen Maschinen verwendet wird	Yes	Keine.
Automatische Bereitstellung für den Desktop-Pool aktivieren	Nein	True oder False
Bei der Bereitstellung aufgetretene Fehler	Nein	
Bei Auftreten eines Fehlers Bereitstellung anhalten	Nein	True oder False
Bereitstellung starten	Nein	True oder False
Pool-Werte wurden berechnet	Nein	True oder False
Die übergeordnete virtuelle Maschine, die zur Bereitstellung von verknüpften Klonen verwendet wird	Yes	–
Der Snapshot-Name, der für die Bereitstellung von verknüpften Klonen verwendet wird	Yes	–
Die Snapshot-ID, die für die Bereitstellung von verknüpften Klonen verwendet wird	Nein	"snapshot-38685"
Bereitstellungsgruppen-ID, die vom VMware Horizon View Composer-Dienst verwendet wird	Nein	"7119316f-00a8-463d-bbba-c3000f105aeb"
Datenspeicherpfad für persistente Festplatten von View Composer	Yes	Keine.
Typ der View Composer-Festplatte	Nein	"SystemDisposable", UserProfile usw.
Die persistente Festplatte als Sparse-Festplatte erstellen	Nein	True oder False
Der Laufwerksbuchstabe für die persistente Festplatte oder löschbare Datenfestplatte	Nein	"*", "C" usw.
Zielgröße der persistenten Festplatte	Nein	Ganzzahl
Typ der Aktualisierungsrichtlinie	Nein	Immer, Nie oder Bedingt
Verwendungsgrenze für Aktualisierungsvorgänge	Nein	Ganzzahl
Zeitgrenze für Aktualisierungsvorgänge	Nein	Ganzzahl
Wert für die Speichermehrfachvergabe für einen Datenspeicher, der verknüpfte Klone speichert	Nein	Keine, Konservativ, Mäßig, Aggressiv
Datenspeicherpfad für einen Datenspeicher, der verknüpfte Klone speichert	Yes	Keine.
Liste mit IDs, für die dieser Datenspeicher verwendet wird	Nein	Liste mit GUIDs, wie beispielsweise folgende: ["7119316f-00a8-463d-bbba-c3000f105aeb"]
Status der virtuellen Maschine	Nein	Ready, Pre-provisioned, Cloning, Cloning Error, Customizing, Deleting, Maintenance, Error oder Logout
Eine virtuelle Maschine einem Benutzer zuweisen, wenn sich der Benutzer zum ersten Mal anmeldet	Nein	True oder False

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Flags für den Desktop-Pool	Nein	
Konfigurationseinstellungen für mehrere Monitore	Nein	svga.maxWidth:int, svga.vramSize:int, svga.maxHeight:int, svga.enable3d:bool, svga.numDisplays:int
Eine individuelle virtuelle Maschine wurde in einen manuellen Pool umgewandelt	Nein	True oder False
Der Pool mit verknüpften Klonen verwendet natives Snapshot-Klonen mit VAAI	Nein	True oder False
View-Speicherbeschleunigung (CBRC) ist aktiviert	Nein	True oder False
Häufigkeit, mit der der CBRC-Cache aktualisiert wird	Nein	Ganzzahl
CBRC-Cache-Aktualisierungssperrzeiten	Nein	Liste
Die Festplattentypen, die für CBRC (Betriebssystemfestplatten, persistente Festplatten) zwischengespeichert werden	Nein	Liste
Speicherplatzrückgewinnung von virtuellen Maschinen (SE-Sparse-Format) ist aktiviert	Nein	True oder False
Speicherplatzrückgewinnungsgrenze, in Byte	Nein	
Minimale Anzahl an virtuellen Maschinen, die während einer Neuanpassung bereit sind	Nein	
Der Desktop-Pool verwendet einen Virtual SAN-Datenspeicher	Nein	True oder False
Anzahl der Remote-Desktop-Berechtigungen für diesen Serverpool	Nein	0 or 1
Anzahl der Remoteanwendungsberechtigungen für diesen Pool	Nein	0 or 1
Standardanzeigeprotokoll	Nein	PCoIP oder RDP
Der Benutzer kann das verwendete Anzeigeprotokoll auswählen	Nein	True oder False
HTML Access ist aktiviert	Nein	True oder False
Flash-Qualitätsstufe	Nein	Keine verwendet, niedrig, mittel, hoch
Flash-Drosselungsstufe	Nein	Keine verwendet, konservativ, mäßig, aggressiv
Pool ist deaktiviert	Nein	True oder False
Pool ist zum Löschen gekennzeichnet	Nein	True oder False
Tags associated with the View-Verbindungsserver instance	Yes	Keine.
Einen anderen Mirage-Server verwenden als den, der in den globalen Einstellungen angegeben ist	Nein	True oder False
Mirage-Server ist aktiviert	Nein	True oder False
URL des Mirage-Servers, einschließlich Portnummer	Yes	Keine.

Von VMware erfasste Computerdaten

Wenn Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit beitreten, erhebt VMware Daten aus View und vCenter Server-Feldern, die virtuelle Maschinen beschreiben. Felder mit vertraulichen Informationen werden anonymisiert.

Tabelle 6-13. Von View erfasste Computerdaten

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Der Computer wurde als verunreinigt markiert. Die virtuelle Maschine wurde bei useonce=true verwendet und darf daher keine neuen Sitzungen akzeptieren	Nein	True oder False
Zuordnung der Geräte zum Ändern von IDs	Nein	Eine Gruppe von IDs wie folgende: 2000=01874583;01874583&2016=3910f513;3910f513
Eine Kennung für den Computer, der zum Korrelieren von Daten verwendet wird	Nein	vm-10
Sysprep-Anpassung wird für das Gastbetriebssystem verwendet	Nein	True oder False
Zeitüberschreitungswert. Die Zeitspanne, bevor der Computer getrennt wird.	Nein	Uhrzeit
Eine Zufalls-ID für den View Agent diesen Computer	Nein	GUID
Verschiedene Konfigurationswerte	Nein	Ganzzahlen und boolesche Werte (True oder False)
View LDAP-Kennung für die vorherige persistente Festplatte von View Composer	Nein	LDAP-Eintrag
ThinApps, die für den Computer berechtigt sind	Yes	Keine
ThinApps, für die eine Deinstallation aussteht	Yes	Keine
ThinApps, die auf dem Computer installiert sind	Yes	Keine
Der Status des Computers	Nein	Undefined, Pre-provisioned, Cloning, Cloning error, Customizing, Ready, Deleting, Maintenance, Error oder Logout
Zeitstempel, wann die Anpassung begann	Nein	Ganzzahl
Der Computer wird zur Anpassung eingeschaltet.	Nein	Ganzzahl. Die Werte lauten 0 oder 1.
Der Computer ist eingeschaltet.	Nein	True oder False
Der Computer wurde angehalten	Nein	True oder False
Der Computerstatus ändert sich	Nein	True oder False
Der Computer wurde konfiguriert	Nein	True oder False
Der Pfad zur virtuellen Maschine in vCenter Server	Yes	Keine
Anpassungsvorlage zum Anpassen des Computers	Yes	Keine
View Composer-Linked-Clone-ID für den Computer	Nein	GUID des verknüpften Klon
Die virtuelle Maschine ist in vCenter Server nicht vorhanden	Nein	True oder False

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Angabe, wie oft View versucht hat, den Computer auszuschalten	Nein	Ganzzahl
Status des CBRC (View-Speicherbeschleunigung)	Nein	Off, Current, Out of Date oder Error
Zeitpunkt der letzten CBRC-Aktualisierung	Nein	Datum
Zeitpunkt des letzten CBRC-Fehlers	Nein	Ganzzahl
Zeitpunkt des letzten unvollständigen Versuchs, den CBRC zu konfigurieren	Nein	Ganzzahl
Die auf dem Computer installierte View Agent-Version	Nein	6.0.0-551711
View Persona Management ist auf dem Computer aktiviert	Nein	True oder False
Letzte Größe des zurückgewonnenen Speicherplatzes des Computers (bei Verwendung des SE-Sparse-Formats)	Nein	
Zeitpunkt der letzten Rückgewinnung von Speicherplatz	Nein	Zeitstempel

Tabelle 6-14. Von vCenter Server erfasste Daten virtueller Maschinen

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Die Hardwareversion der virtuellen Maschine	Nein	v8
Die Menge an Arbeitsspeicher, die der virtuellen Maschine zugewiesen wird	Nein	1024
Die Anzahl virtueller CPUs, die in der virtuellen Maschine konfiguriert sind	Nein	Ganzzahl
Das auf der virtuellen Maschine installierte Betriebssystem	Nein	Microsoft Windows 7 (32 Bit), Microsoft Windows 8 (32 Bit), Microsoft Windows Server 2008 R2 (64 Bit) usw.

Von VMware erfasste vCenter Server-Daten

Wenn Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit beitreten, erhebt VMware Daten aus bestimmten vCenter Server-Feldern. Felder mit vertraulichen Informationen werden anonymisiert.

Tabelle 6-15. Von vCenter Server gesammelte Hostsystem-Informationen

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Die Uhrzeit, zu der View zuletzt mit dem vCenter Server-Host kommuniziert hat	Nein	Ganzzahl
Die URL der vCenter Server-Instanz	Yes	Keine
Die API-Version der vCenter Server-Instanz	Nein	5.0
Die Buildnummer der vCenter Server-Instanz	Nein	456789
Die Versionsnummer der vCenter Server-Instanz	Nein	5.0.0

Tabelle 6-16. Von vCenter Server gesammelte Hoststatus-Informationen

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Der interne Statuscode des Verbindungsstatus zwischen vCenter Server und View-Verbindungsserver	Nein	Status_Up
Beschreibung des Statuscodes der Verbindung	Nein	Verbunden
Das SSL-Zertifikat von vCenter Server ist gültig	Nein	True oder False
Der Grund, warum das SSL-Zertifikat nicht gültig ist	Nein	Nichtübereinstimmung bei Name, nicht vertrauenswürdig, Sperrüberprüfung nicht möglich usw.

Tabelle 6-17. Von vCenter Server erfasste Datenspeicher-Daten

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Festplattenkapazität dieses Datenspeichers	Nein	Ganzzahl
Freier Speicherplatz auf diesem Datenspeicher	Nein	Ganzzahl
Der Typ des Speichers	Nein	NFS, VMFS
Mehrere Hosts können gleichzeitig auf diesen Datenspeicher zugreifen.	Nein	True oder False

Tabelle 6-18. Informationen zum ESX-Knoten

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Bezeichner von vCenter Server, der einen bestimmten ESXi-Host verwaltet, zusammen mit einem Bezeichner für den ESXi-Host	Nein	1234-ADEE-BECF-41AA-4950BCDA-host-14

Tabelle 6-19. Informationen über den direkt angeschlossenen Speicher für einen ESXi-Host

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Hardwareanbieter der physischen Festplatte	Nein	SEAGATE
Modell der physischen Festplatte	Nein	ST9300653SS
SSD	Nein	True oder False
Kapazität in Bytes	Nein	
Bezeichner für den ESXi-Host	Nein	host-123
Bezeichner von vCenter Server, der einen bestimmten ESXi-Host verwaltet	Nein	1234-ADEE-BECF-41AA-4950BCDA

Von VMware erfasste ThinApp-Daten

Wenn Sie am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen, erhebt VMware Daten aus bestimmten ThinApp-Feldern. Felder mit vertraulichen Informationen werden anonymisiert.

Tabelle 6-20. ThinApp-Informationen

Beschreibung	Wird dieses Feld anonymisiert?	Werttyp
Anzeigenname des ThinApp-Pakets	Nein	
Anzahl der ThinApp zugewiesenen MSI-Pakete	Nein	Ganzzahl
Zählung „Zuordnung“ bei vollständiger Installation	Nein	Ganzzahl
Liste der Pools, die für die Verwendung der vollständigen Installation eingerichtet sind	Yes	Liste mit Hash für CN (common name, allgemeiner Name)
Remote-Desktops, die für die Verwendung der vollständigen Installation eingerichtet sind	Nein	Liste der Desktop-CNs (GUID)
Zählung „Zuordnung“ beim Streaming von ThinApp	Nein	Ganzzahl
Liste der Pools, die für das Streaming von ThinApp eingerichtet sind	Yes	Liste mit Hash für CN (common name, allgemeiner Name)
Remote-Desktops, die für das Streaming von ThinApp eingerichtet sind	Nein	Liste der Desktop-CNs (GUID)
ThinApps in einer Gruppe für Pools, die für die Verwendung der vollständigen Installation eingerichtet sind	Nein	Liste der ThinApp-IDs

Von VMware erfasste Cloud Pod Architecture-Daten

Wenn Sie dem Programm zur Verbesserung der Benutzerfreundlichkeit beitreten, erhebt VMware Daten aus bestimmten Cloud Pod Architecture-Feldern. Felder mit vertraulichen Informationen werden anonymisiert.

Tabelle 6-21. Zu Cloud Pod Architecture erfasste Daten

Beschreibung	Wird dieses Feld anonymisiert?	Beispiel oder Typ
Die Funktion Cloud Pod Architecture ist aktiviert	Nein	True oder False
Lokale Pod-ID	Nein	
Häufigkeit, mit der das System eine podübergreifende Systemzustandsprüfung durchführt (in Sekunden)	Nein	Ganzzahl
Maximal zulässiger Zeitunterschied zwischen den Pods (in Sekunden)	Nein	Ganzzahl
Allgemeiner Name der Site, zu der der Pod gehört	Nein	
Liste von globalen Berechtigungs-IDs (beispielsweise verfügt ein Pod über Desktop-Pools, die die globalen Berechtigungen unterstützen)	Nein	Liste der Strings
Allgemeiner Name des Pod-Endpunkts, bei dem es sich um eine View-Verbindungsserver-Instanz handelt	Yes	
Allgemeiner Name des Pods, der diesen Endpunkt enthält	Nein	
Der Pod-Endpunkt ist deaktiviert	Nein	True oder False

Beschreibung	Wird dieses Feld anonymisiert?	Beispiel oder Typ
Anzuwendende Gewichtung bei der zufälligen Auswahl von Endpunkten (View-Verbindungsserver-Instanzen) für Remote-Sitzungen	Nein	Ganzzahl
Die globale Berechtigung ist deaktiviert	Nein	True oder False
Die Desktop-Suche startet über die Start-Site eines Benutzers (Bei der Einstellung auf „false“ startet die Suche über den lokalen Pod)	Nein	True oder False
Die globale Berechtigung ist für einen zugewiesenen Desktop vorgesehen	Nein	0 = Nein 1 = Ja
Geltungsbereich, für den die vorhandene Sitzungssuche durchgeführt werden soll	Nein	ALLE, SITE oder LOKAL
Geltungsbereich, für den die neue Sitzungsplatzierung durchgeführt werden soll	Nein	ALLE, SITE oder LOKAL
Die Start-Site des Benutzers ist für die globale Berechtigung erforderlich	Nein	True oder False
Die automatische Sitzungsbereinigung ist aktiviert	Nein	True oder False

Durch VMware gesammelte Horizon Client-Daten

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

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

Tabelle 6-22. Von den Horizon Client-Instanzen gesammelte Daten für das Programm zur Verbesserung der Benutzerfreundlichkeit

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Unternehmen, das die Horizon Client-Anwendung entwickelte	Nein	VMware
Produktname	Nein	VMware Horizon Client
Client-Produktversion	Nein	(Das Format lautet x.x.x-yyyyyy, wobei x.x.x für die Client-Versionsnummer und yyyyyy für die Build-Nummer steht.)
Client-Binärarchitektur	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ i386 ■ x86_64 ■ arm

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Client-Build-Name	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ VMware-Horizon-View-Client-Win32-Windows ■ VMware-Horizon-View-Client-Linux ■ VMware-Horizon-View-Client-iOS ■ VMware-Horizon-View-Client-Mac ■ VMware-Horizon-View-Client-Android ■ VMware-Horizon-View-Client-WinStore
Host-Betriebssystem	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Windows 8.1 ■ Windows 7, Service Pack 1 für 64 Bit (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 10.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Host-Betriebssystemkernel	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ unbekannt (für Windows Store)
Host-Betriebssystemarchitektur	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ x86_64 ■ i386 ■ armv71 ■ ARM
Hostsystem-Modell	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Hostsystem-CPU	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ unbekannt (für iPad)
Anzahl der Cores bzw. Kerne im Prozessor des Hostsystems	Nein	Beispiel: 4
MB Arbeitsspeicher auf dem Hostsystem	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ 4096 ■ unbekannt (für Windows Store)
Anzahl der angeschlossenen USB-Geräte	Nein	2 (Die Umleitung von USB-Geräten wird nur für Linux-, Windows- und Mac OS X-Clients unterstützt.)

Beschreibung	Wird dieses Feld anonymisiert?	Beispielswert
Maximale Anzahl gleichzeitiger USB-Geräteverbindungen	Nein	2
Hersteller-ID des USB-Geräts	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Kingston ■ NEC ■ Nokia ■ Wacom
Produkt-ID des USB-Geräts	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ DataTraveler ■ Gamepad ■ Speicherlaufwerk ■ Kabellose Maus
USB-Gerätefamilie	Nein	Beispiele hierfür sind: <ul style="list-style-type: none"> ■ Sicherheit ■ Eingabegeräte ■ Bildverarbeitung
Nutzungszähler für das USB-Gerät	Nein	(Gibt an, wie oft das Gerät gemeinsam genutzt wurde)

Von VMware erfasste Daten

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

Tabelle 6-23. Für das Programm zur Verbesserung der Benutzerfreundlichkeit erfasste Clientdaten

Beschreibung	Feldname	Wird dieses Feld anonymisiert?	Beispielswert
Unternehmen, das die Anwendung hergestellt hat	<client-vendor>	Nein	VMware
Produktname	<client-product>	Nein	
Client-Produktversion	<client-version>	Nein	2.5.0-Buildnummer
Client-Binärarchitektur	<client-arch>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> ■ Browser ■ arm

Beschreibung	Feldname	Wird dieses Feld anonymisiert ?	Beispielswert
Systemeigene Architektur des Browsers	<browser-arch>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> ■ Win32 ■ Win64 ■ MacIntel ■ iPad
Zeichenfolge zum Browserbenutzer-Agent	<browser-user-agent>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 (KHTML, wie Gecko) ■ Chrome/3.0.1750 ■ Safari/703.00
Interne Versionszeichenfolge des Browsers	<browser-version>	Nein	Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> ■ 7.0.3 (für Safari), ■ 29.0 (für Firefox)
Core-Implementierung des Browsers	<browser-core>		Beispiele hierfür sind folgende Werte: <ul style="list-style-type: none"> ■ Chrome ■ Safari ■ Firefox ■ MSIE (für Internet Explorer)
Angabe, ob der Browser auf einem Handheld-Gerät ausgeführt wird	<browser-is-handheld>	Nein	true

Verwalten von virtuellen Linked-Clone-Maschinen

7

Mit View Composer können Sie virtuelle Linked-Clone-Maschinen aktualisieren, die Größe der Betriebssystemdaten reduzieren und eine Neuverteilung der virtuellen Linked-Clone-Maschinen auf die Festplattenlaufwerke vornehmen. Darüber hinaus können Sie die persistenten View Composer-Festplatten von verknüpften Klonen verwalten.

Dieses Kapitel enthält die folgenden Themen:

- [Reduzieren der Größe von verknüpften Klonen durch eine Maschinenaktualisierung](#)
- [Aktualisieren von Linked-Clone-Desktops](#)
- [Neuverteilen von virtuellen Linked-Clone-Maschinen](#)
- [Verwalten persistenter View Composer-Festplatten](#)

Reduzieren der Größe von verknüpften Klonen durch eine Maschinenaktualisierung

Bei einer Maschinenaktualisierung werden der ursprüngliche Status und die ursprüngliche Größe der Betriebssystemfestplatten der einzelnen verknüpften Klone wiederhergestellt und damit die Speicherkosten reduziert.

Planen Sie Aktualisierungsvorgänge wenn möglich außerhalb der Spitzenzeiten.

Richtlinien finden Sie unter [Computer-Aktualisierungen](#).

Voraussetzungen

- Legen Sie den Zeitpunkt für die Aktualisierung fest. Standardmäßig startet View Composer den Vorgang sofort.

Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur einen Vorgang zur Aktualisierung planen. Sie können mehrere Vorgänge zur Aktualisierung planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.

- Legen Sie fest, ob Sie das Abmelden aller Benutzer erzwingen möchten, sobald der Vorgang gestartet wird, oder ob gewartet werden soll, bis sich die einzelnen Benutzer abmelden, bevor der Desktop mit verknüpftem Klon des jeweiligen Benutzers aktualisiert wird.

Wenn Sie das Abmelden der Benutzer erzwingen, erhalten die Benutzer vor dem Trennen der Desktops eine Meldung von View, sodass sie ihre Anwendungen schließen und sich abmelden können.

Wenn Sie Benutzer zwingen, sich abzumelden, ist die maximale Anzahl an gleichzeitigen Aktualisierungsvorgängen für Remote-Desktops, für die Abmeldungen notwendig sind, der halbe Wert der Einstellung **Maximale parallele View Composer-Wartungsvorgänge**. Wenn Sie für diese Einstellung beispielsweise den Wert 24 konfigurieren und Benutzer zur Abmeldung zwingen, sind maximal 12 parallele Aktualisierungsvorgänge auf Remote-Desktops möglich, die Abmeldungen erfordern.

- Wenn Ihre Bereitstellung replizierte View-Verbindungsserver-Instanzen umfasst, überprüfen Sie, dass alle Instanzen in derselben Version vorliegen.

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Doppelklicken Sie zur Auswahl des Desktop-Pools für die Aktualisierung in der linken Spalte auf die Pool-ID.
- 3 Geben Sie an, ob mehrere virtuelle Maschinen oder eine einzelne virtuelle Maschine aktualisiert werden soll.

Option	Aktion
So aktualisieren Sie alle virtuellen Maschinen im Desktop-Pool	<ol style="list-style-type: none"> a Wählen Sie in View Administrator Katalog > Desktop-Pools aus. b Doppelklicken Sie zur Auswahl des Desktop-Pools für die Aktualisierung in der linken Spalte auf die Pool-ID. c Klicken Sie auf der Registerkarte Bestandsliste auf Computer. d Verwenden Sie die Strg- oder Umschalttaste, um alle Maschinen-IDs in der linken Spalte auszuwählen. e Wählen Sie Aktualisieren aus dem Dropdown-Menü View Composer.
So aktualisieren Sie eine einzelne virtuelle Maschine	<ol style="list-style-type: none"> a Wählen Sie in View Administrator Ressourcen > Computer aus. b Doppelklicken Sie zur Auswahl der Maschine für die Aktualisierung in der linken Spalte auf die Maschinen-ID. c Wählen Sie auf der Registerkarte Übersicht aus dem Dropdown-Menü View Composer die Option Aktualisieren aus.

- 4 Folgen Sie den Anweisungen des Assistenten.

Die ursprüngliche Größe der Betriebssystemfestplatten wird wiederhergestellt.

Der Fortschritt des Aktualisierungsvorgangs für die virtuellen Linked-Clone-Maschinen kann in vCenter Server überwacht werden.

Sie können den Vorgang in View Administrator überwachen, indem Sie **Katalog > Desktop-Pools** auswählen, auf die Pool-ID doppelklicken und auf die Registerkarte **Aufgaben** klicken. Sie können auf **Aufgabe abbrechen**, **Aufgabe pausieren** oder **Aufgabe fortsetzen** klicken, um eine Aufgabe zu beenden, eine Aufgabe anzuhalten oder mit einer angehaltenen Aufgabe fortzufahren.

Computer-Aktualisierungen

Wenn Benutzer mit verknüpften Klonen interagieren, steigt die Größe der Betriebssystemfestplatte der Klonen. Bei einer Computer-Aktualisierung werden der ursprüngliche Status und die ursprüngliche Größe der Betriebssystemfestplatte wiederhergestellt und damit die Speicherkosten reduziert.

Eine Aktualisierung hat keine Auswirkungen auf persistente View Composer-Festplatten.

Ein verknüpfter Klon verwendet weniger Speicherplatz als die übergeordnete virtuelle Maschine, welche die gesamten Betriebssystemdaten umfasst. Die Betriebssystemfestplatte eines Klon wird jedoch bei jedem Schreibvorgang für Daten aus dem Betriebssystem vergrößert.

Beim Erstellen eines verknüpften Klon durch View Composer wird ein Snapshot der Betriebssystemfestplatte des Klon erstellt. Der Snapshot kennzeichnet die virtuelle Linked-Clone-Maschine eindeutig. Bei einer Aktualisierung wird die Betriebssystemfestplatte anhand des Snapshots wiederhergestellt.

View Composer kann einen verknüpften Klon in der Hälfte der Zeit aktualisieren, die für das Löschen und erneute Erstellen des Klon benötigt wird.

Befolgen Sie bei Aktualisierungen die folgenden Richtlinien:

- Sie können einen Desktop-Pool nach Bedarf, als geplantes Ereignis oder beim Erreichen einer festgelegten Größe der Betriebssystemfestplatte aktualisieren.

Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur einen Vorgang zur Aktualisierung planen. Wenn Sie eine Aktualisierung umgehend starten, setzt der Vorgang zuvor geplante Aufgaben außer Kraft.

Sie können mehrere Vorgänge zur Aktualisierung planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.

Bevor Sie einen Vorgang zur Aktualisierung planen, müssen Sie zuvor geplante Aufgaben abbrechen.

- Sie können Pools mit dedizierter und mit dynamischer Zuweisung aktualisieren.
- Eine Aktualisierung kann nur ausgeführt werden, wenn die Benutzer von ihren Linked-Clone-Desktops getrennt sind.
- Bei der Aktualisierung werden die über QuickPrep oder Sysprep eingerichteten eindeutigen Computerinformationen beibehalten. Sysprep muss nach einer Aktualisierung nicht erneut ausgeführt werden, um die SID oder die GUIDs von auf dem Systemlaufwerk installierter Drittanbietersoftware wiederherzustellen.
- Nach der Neuzusammenstellung eines verknüpften Klon erstellt View einen neuen Snapshot der Betriebssystemfestplatte des verknüpften Klon. Bei zukünftigen Aktualisierungen werden die Betriebssystemdaten basierend auf diesem Snapshot wiederhergestellt, nicht anhand des Snapshots, der bei der ursprünglichen Erstellung des verknüpften Klon erstellt wurde.

Wenn Sie die VAAI-Technologie (Native NFS Snapshot) zum Generieren von verknüpften Klonen verwenden, nehmen die NAS-Geräte von bestimmten Anbietern Snapshots der Replikatfestplatte auf, wenn sie die Betriebssystemfestplatten der verknüpften Klone aktualisieren. Diese NAS-Geräte unterstützen das direkte Aufnehmen von Snapshots der Betriebssystemfestplatte jedes Klons nicht.

- Sie können eine Mindestanzahl bereiter, bereitgestellter Desktops festlegen, die für Benutzer verfügbar bleiben, damit sie sich während des Aktualisierungsvorgangs mit diesen verbinden können. Siehe hierzu „Bereitgestellt- und Bereithalten von Linked-Clone-Desktops während View Composer-Vorgängen“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Hinweis Sie können das Wachstum verknüpfter Klone verlangsamen, indem Sie die Auslagerungsdateien und temporären Systemdateien auf eine temporäre Festplatte umleiten. Beim Ausschalten eines verknüpften Klons ersetzt View die temporäre Festplatte durch eine Kopie der ursprünglichen temporären Festplatte, die View Composer mit dem Linked-Clone-Pool erstellt hat. Bei diesem Vorgang wird die temporäre Festplatte auf die ursprüngliche Größe reduziert.

Sie können diese Option beim Erstellen eines Linked-Clone-Desktop-Pools konfigurieren.

Aktualisieren von Linked-Clone-Desktops

Virtuelle Linked-Clone-Maschinen können aktualisiert werden, indem Sie ein neues Basis-Image für die übergeordnete virtuelle Maschine erstellen und das aktualisierte Image mithilfe der Neuzusammenstellungsfunktion an die verknüpften Klone verteilen.

- **Vorbereiten einer übergeordneten virtuellen Maschine für die Neuzusammenstellung von verknüpften Klonen**

Bevor Sie einen Linked-Clone-Desktop-Pool neu zusammenstellen, muss die übergeordnete virtuelle Maschine aktualisiert werden, die als Basis-Image für die verknüpften Klone verwendet wurde.

- **Neuzusammenstellung von virtuellen Linked-Clone-Maschinen**

Bei der Neuzusammenstellung von virtuellen Maschinen werden alle mit einer übergeordneten virtuellen Maschine verknüpften Linked-Clone-Maschinen gleichzeitig aktualisiert.

- **Aktualisieren verknüpfter Klone bei der Neuzusammenstellung**

Bei einer Neuzusammenstellung können Sie Betriebssystem-Patches bereitstellen, Anwendungen installieren bzw. aktualisieren oder die Hardwareeinstellungen der virtuellen Maschine in allen verknüpften Klonen in einem Desktop-Pool ändern.

- **Korrigieren einer nicht erfolgreichen Neuzusammenstellung**

Eine fehlgeschlagene Neuzusammenstellung kann korrigiert werden. Sie können zudem korrigierende Maßnahmen ergreifen, wenn Sie verknüpfte Klone versehentlich unter Verwendung eines falschen Basis-Images neu zusammenstellen.

Vorbereiten einer übergeordneten virtuellen Maschine für die Neuzusammenstellung von verknüpften Klonen

Bevor Sie einen Linked-Clone-Desktop-Pool neu zusammenstellen, muss die übergeordnete virtuelle Maschine aktualisiert werden, die als Basis-Image für die verknüpften Klone verwendet wurde.

View Composer bietet keine Unterstützung für die Neuzusammenstellung verknüpfter Klone in einer übergeordneten virtuellen Maschine, wenn der verknüpfte Klon ein anderes Betriebssystem verwendet als die übergeordnete virtuelle Maschine. Beispielsweise kann ein Snapshot einer übergeordneten virtuellen Maschine mit Windows 8, Windows 7 oder Windows Vista nicht verwendet werden, um einen verknüpften Klon mit Windows XP neu zusammenzustellen.

Verfahren

- 1 Aktualisieren Sie die übergeordnete virtuelle Maschine in vCenter Server für die Neuzusammenstellung.
 - Installieren Sie Betriebssystem-Patches oder Service Packs, neue Anwendungen, Anwendungs-Updates oder nehmen Sie andere Änderungen an der übergeordneten virtuellen Maschine vor.
 - Alternativ bereiten Sie eine andere virtuelle Maschine vor, die bei der Neuzusammenstellung als neue übergeordnete virtuelle Maschine verwendet werden soll.
- 2 Schalten Sie die aktualisierte oder neue übergeordnete virtuelle Maschine in vCenter Server aus.
- 3 Erstellen Sie in vCenter Server einen Snapshot der übergeordneten virtuellen Maschine.

Nächste Schritte

Stellen Sie den Linked-Clone-Desktop-Pool neu zusammen.

Neuzusammenstellung von virtuellen Linked-Clone-Maschinen

Bei der Neuzusammenstellung von virtuellen Maschinen werden alle mit einer übergeordneten virtuellen Maschine verknüpften Linked-Clone-Maschinen gleichzeitig aktualisiert.

Planen Sie Neuzusammenstellungen wenn möglich außerhalb der Spitzenzeiten.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen Snapshot der übergeordneten virtuellen Maschine verfügen. Siehe [Vorbereiten einer übergeordneten virtuellen Maschine für die Neuzusammenstellung von verknüpften Klonen](#).
- Machen Sie sich mit den Richtlinien zur Neuzusammenstellung vertraut. Siehe [Aktualisieren verknüpfter Klone bei der Neuzusammenstellung](#).
- Legen Sie den Zeitpunkt für die Neuzusammenstellung fest. Standardmäßig startet View Composer die Neuzusammenstellung sofort.

Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur eine Neuzusammenstellung planen. Sie können mehrere Neuzusammenstellungen planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.

- Legen Sie fest, ob Sie das Abmelden aller Benutzer erzwingen möchten, sobald die Neuzusammenstellung gestartet wird, oder ob gewartet werden soll, bis sich die einzelnen Benutzer abmelden, bevor für den Linked-Clone-Desktop des jeweiligen Benutzers eine Neuzusammenstellung vorgenommen wird.

Wenn Sie das Abmelden der Benutzer erzwingen, erhalten die Benutzer vor dem Trennen der Desktops eine Meldung von View, sodass sie ihre Anwendungen schließen und sich abmelden können.

Wenn Sie das Abmelden der Benutzer erzwingen, wird für die maximale Anzahl an parallelen Neuzusammenstellungsvorgängen auf Remote-Desktops, die das Abmelden erfordern, die Hälfte des Werts der Einstellung **Maximale parallele View Composer-Wartungsvorgänge** angezeigt. Wenn Sie für diese Einstellung beispielsweise den Wert 24 konfigurieren und Benutzer zur Abmeldung zwingen, sind maximal 12 parallele Neuzusammenstellungsvorgänge auf Remote-Desktops möglich, die Abmeldungen erfordern.

- Legen Sie fest, ob Sie die Bereitstellung beim ersten Fehler abbrechen möchten. Wenn Sie diese Option auswählen und bei der Bereitstellung eines verknüpften Klons durch View Composer ein Fehler auftritt, wird die Bereitstellung für alle Klone im Desktop-Pool abgebrochen. Sie können diese Option auswählen, um sicherzustellen, dass die Ressourcen wie Speicher nicht unnötigerweise beansprucht werden.

Die Auswahl der Option **Beim ersten Fehler stoppen** hat keinen Einfluss auf die Anpassung. Tritt ein Anpassungsfehler bei einem verknüpften Klon auf, wird die Bereitstellung und Anpassung für die anderen Klone weiter fortgeführt.

- Stellen Sie sicher, dass die Bereitstellung für den Desktop-Pool aktiviert ist. Wenn die Bereitstellung für den Desktop-Pool deaktiviert ist, verhindert View eine Anpassung der Desktops nach deren Neuzusammenstellung.
- Wenn Ihre Bereitstellung replizierte View-Verbindungsserver-Instanzen umfasst, überprüfen Sie, dass alle Instanzen in derselben Version vorliegen.

Verfahren

- 1 Legen Sie fest, ob der gesamte Desktop-Pool oder nur eine einzelne Maschine neu zusammengestellt werden soll.

Option	Aktion
Neuzusammenstellung aller virtuellen Maschinen im Desktop-Pool	<ol style="list-style-type: none"> a Wählen Sie in View Administrator Katalog > Desktop-Pools aus. b Doppelklicken Sie zur Auswahl des Desktop-Pools für die Neuzusammenstellung in der linken Spalte auf die Pool-ID. c Klicken Sie auf der Registerkarte Bestandsliste auf Computer. d Verwenden Sie die Strg-Taste oder die Umschalttaste, um alle VM-IDs in der linken Spalte auszuwählen. e Wählen Sie im Dropdown-Menü View Composer die Option Neu zusammenstellen.
Neuzusammenstellung ausgewählter virtueller Maschinen	<ol style="list-style-type: none"> a Wählen Sie in View Administrator Ressourcen > Computer aus. b Doppelklicken Sie zur Auswahl der VM für die Neuzusammenstellung in der linken Spalte auf die VM-ID. c Wählen Sie auf der Registerkarte Übersicht im Dropdown-Menü View Composer die Option Neu zusammenstellen.

- 2 Folgen Sie den Anweisungen des Assistenten.

Sie können eine neue virtuelle Maschine als übergeordnete VM für den Desktop-Pool festlegen.

Auf der Seite „Bereit zum Abschließen“ können Sie auf **Details anzeigen** klicken, um die Linked-Clone-Desktops anzuzeigen, die neu zusammengestellt werden.

Die virtuellen Linked-Clone-Maschinen werden aktualisiert. Die ursprüngliche Größe der Betriebssystemfestplatten wird wiederhergestellt.

In einem Pool mit dedizierter Zuweisung werden verknüpfte Klone ohne Zuweisung gelöscht und neu erstellt. Die angegebene Anzahl an Reserve-VMs wird beibehalten.

In einem Pool mit dynamischer Zuweisung werden alle ausgewählten verknüpften Klone neu zusammengestellt.

Der Fortschritt der Neuzusammenstellung für die virtuellen Linked-Clone-Maschinen kann in vCenter Server überwacht werden.

In View Administrator können Sie den Vorgang überwachen, indem Sie auf **Katalog > Desktop-Pools** klicken und dann auf die Pool-ID doppelklicken. Klicken Sie anschließend auf die Registerkarte **Aufgaben**. Sie können auf **Aufgabe abbrechen**, **Aufgabe pausieren** oder **Aufgabe fortsetzen** klicken, um eine Aufgabe zu beenden, eine Aufgabe anzuhalten oder mit einer angehaltenen Aufgabe fortzufahren.

Hinweis Wenn Sie bei der Erstellung des Desktop-Pools zur Anpassung der verknüpften Klone eine Sysprep-Anpassungsspezifikation verwendet haben, werden für die neu zusammengestellten virtuellen Maschinen möglicherweise neue SIDs generiert. Siehe hierzu „Neuzusammenstellung von mit Sysprep angepassten verknüpften Klonen“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Aktualisieren verknüpfter Klone bei der Neuzusammenstellung

Bei einer Neuzusammenstellung können Sie Betriebssystem-Patches bereitstellen, Anwendungen installieren bzw. aktualisieren oder die Hardwareeinstellungen der virtuellen Maschine in allen verknüpften Klonen in einem Desktop-Pool ändern.

Für die Neuzusammenstellung von virtuellen Maschinen mit verknüpften Klonen aktualisieren Sie die übergeordnete virtuelle Maschine in vCenter Server oder wählen eine andere virtuelle Maschine als neue übergeordnete Maschine aus. Anschließend erstellen Sie einen Snapshot der Konfiguration der neuen übergeordneten virtuellen Maschine.

Da die verknüpften Klone nicht direkt mit der übergeordneten virtuellen Maschine, sondern mit dem Replikat verknüpft sind, können Sie die übergeordnete virtuelle Maschine ändern, ohne dass sich dies auf die verknüpften Klone auswirkt.

Anschließend initiieren Sie die Neuzusammenstellung und wählen den Snapshot aus, der als neues Basis-Image für den Desktop-Pool verwendet werden soll. View Composer erstellt ein neues Replikat, kopiert die neu konfigurierte Betriebssystemfestplatte in die verknüpften Klone und koppelt die verknüpften Klone mit dem neuen Replikat.

Bei der Neuzusammenstellung werden auch die verknüpften Klone aktualisiert und die Größe der Betriebssystemfestplatten wird reduziert.

Desktop-Neuzusammenstellungen haben keine Auswirkungen auf persistente View Composer-Festplatten.

Befolgen Sie bei Neuzusammenstellungen die folgenden Richtlinien:

- Sie können Desktop-Pools mit dedizierter und mit dynamischer Zuweisung neu zusammenstellen.
- Sie können einen Desktop-Pool nach Bedarf oder als geplantes Ereignis neu zusammenstellen.

Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur eine Neuzusammenstellung planen. Bevor Sie eine Neuzusammenstellung planen können, müssen Sie alle zuvor geplanten Aufgaben abbrechen oder warten, bis der vorherige Vorgang abgeschlossen wurde. Um eine Neuzusammenstellung sofort zu starten, müssen Sie alle zuvor geplante Aufgaben abbrechen.

Sie können mehrere Neuzusammenstellungen planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.

- Sie können ausgewählte verknüpfte Klone oder alle verknüpften Klone in einem Desktop-Pool neu zusammenstellen.
- Wenn verschiedene verknüpfte Klone in einem Desktop-Pool von unterschiedlichen Snapshots des Basis-Images oder unterschiedlichen Basis-Images abgeleitet werden, umfasst der Desktop-Pool mehrere Replikate.
- Eine Neuzusammenstellung ist nur möglich, wenn die Benutzer sich von ihren Desktops mit verknüpften Klonen abgemeldet haben.
- Sie können keine Neuzusammenstellung für verknüpfte Klone in eine neue oder aktualisierte übergeordnete virtuelle Maschine durchführen, die ein anderes Betriebssystem verwendet.

- Sie können keine Neuzusammenstellung für verknüpfte Klone in eine Hardware-Version durchführen, die niedriger ist als die aktuelle Version. So können beispielsweise Klone mit der Hardware-Version 8 nicht in einer übergeordneten virtuellen Maschine neu zusammengestellt werden, die über die Hardware-Version 7 verfügt.
- Sie können eine Mindestanzahl bereiter, bereitgestellter Desktops festlegen, die für Benutzer verfügbar bleiben, damit sie sich während des Neuzusammenstellungsvorgangs mit diesen verbinden können. Siehe hierzu „Bereitgestellt- und Bereithalten von Linked-Clone-Desktops während View Composer-Vorgängen“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Hinweis Wenn Sie bei der Erstellung des Desktop-Pools zur Anpassung der verknüpften Klone eine Sysprep-Anpassungsspezifikation verwendet haben, werden für die neu zusammengestellten virtuellen Maschinen möglicherweise neue SIDs generiert. Siehe hierzu „Neuzusammenstellung von mit Sysprep angepassten verknüpften Klonen“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Korrigieren einer nicht erfolgreichen Neuzusammenstellung

Eine fehlgeschlagene Neuzusammenstellung kann korrigiert werden. Sie können zudem korrigierende Maßnahmen ergreifen, wenn Sie verknüpfte Klone versehentlich unter Verwendung eines falschen Basis-Images neu zusammenstellen.

Problem

Die virtuellen Maschinen weisen nach einer nicht erfolgreichen Neuzusammenstellung einen fehlerhaften oder veralteten Status auf.

Ursache

Möglicherweise ist während der Neuzusammenstellung auf dem vCenter Server-Host, in vCenter Server oder in einem Datenspeicher ein Systemfehler oder Problem aufgetreten.

Oder während der Neuzusammenstellung wurde ein VM-Snapshot mit einem anderen Betriebssystem verwendet als dem der ursprünglichen übergeordneten virtuellen Maschine. Beispiel: Sie haben möglicherweise einen Windows 7- oder neueren Snapshot zur Neuzusammenstellung eines verknüpften Windows XP-Klons verwendet.

Lösung

- 1 Wählen Sie den Snapshot aus, der für die letzte erfolgreiche Neuzusammenstellung verwendet wurde.

Sie können auch einen neuen Snapshot auswählen, um die verknüpften Klone mit einem neuen Status zu aktualisieren.

Der Snapshot muss dasselbe Betriebssystem aufweisen wie der Snapshot der ursprünglichen übergeordneten virtuellen Maschine.
- 2 Stellen Sie den Desktop-Pool neu zusammen.

View Composer erstellt anhand des Snapshots ein Basis-Image und erstellt die Linked-Clone-Betriebssystemfestplatten neu.

Persistente View Composer-Festplatten mit Benutzerdaten und -einstellungen werden bei der Neuzusammenstellung beibehalten.

Abhängig von den Bedingungen der nicht erfolgreichen Neuzusammenstellung können Sie die verknüpften Klone anstelle der oder zusätzlich zur Neuzusammenstellung aktualisieren oder neu verteilen.

Hinweis Wenn Sie keine persistenten View Composer-Festplatten konfigurieren, werden die von Benutzern generierten Änderungen in den virtuellen Linked-Clone-Maschinen durch die Neuzusammenstellungen gelöscht.

Neuverteilen von virtuellen Linked-Clone-Maschinen

Bei einem Vorgang zur Neuverteilung werden virtuelle Linked-Clone-Maschinen erneut auf die verfügbaren Datenspeicher verteilt.

Sie können den Vorgang zur Neuverteilung auch verwenden, um virtuelle Linked-Clone-Maschinen auf eine andere Datenbank zu migrieren. Verwenden Sie nicht vSphere Client bzw. vCenter Server, um virtuelle Linked-Clone-Maschinen zu migrieren oder zu verwalten. Siehe [Migrieren von virtuellen Maschinen mit verknüpften Klonen auf einen anderen Datenspeicher](#).

Planen Sie Vorgänge zur Neuverteilung wenn möglich außerhalb der Spitzenzeiten.

Richtlinien finden Sie unter [Neuverteilung verknüpfter Klone auf logische Laufwerke](#).

Voraussetzungen

- Machen Sie sich mit dem Vorgang zur Neuverteilung vertraut. Siehe [Neuverteilung verknüpfter Klone auf logische Laufwerke](#).
- Legen Sie den Zeitpunkt für die Neuverteilung fest. Standardmäßig startet View Composer den Vorgang sofort.

Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur einen Vorgang zur Neuverteilung planen. Sie können mehrere Vorgänge zur Neuverteilung planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.

- Legen Sie fest, ob Sie das Abmelden aller Benutzer erzwingen möchten, sobald der Vorgang gestartet wird, oder ob gewartet werden soll, bis sich die einzelnen Benutzer abmelden, bevor für den Linked-Clone-Desktop des jeweiligen Benutzers eine Neuverteilung vorgenommen wird.

Wenn Sie das Abmelden der Benutzer erzwingen, erhalten die Benutzer vor dem Trennen der Desktops eine Meldung von View, sodass sie ihre Anwendungen schließen und sich abmelden können.

Wenn Sie das Abmelden der Benutzer erzwingen, entspricht die maximale Anzahl an Vorgängen zur Neuverteilung auf Remote-Desktops, die eine Abmeldung erfordern, der Hälfte der Einstellung **Maximale parallele View Composer-Wartungsvorgänge**. Wenn diese Einstellung beispielsweise auf den Wert 24 konfiguriert ist und Sie die Benutzer zur Abmeldung zwingen, sind maximal 12 parallele Vorgänge zur Neuverteilung auf Remote-Desktops möglich, die Abmeldungen erfordern.

- Stellen Sie sicher, dass die Bereitstellung für den Desktop-Pool aktiviert ist. Wenn die Bereitstellung für den Pool deaktiviert ist, verhindert View eine Anpassung der virtuellen Maschinen nach deren Neuverteilung.
- Wenn Ihre Bereitstellung replizierte View-Verbindungsserver-Instanzen umfasst, überprüfen Sie, dass alle Instanzen in derselben Version vorliegen.

Verfahren

- 1 Legen Sie fest, ob der gesamte Pool oder nur eine einzelne virtuelle Maschine neu verteilt werden soll.

Option	Aktion
Neuverteilung aller virtuellen Maschinen im Pool	<ol style="list-style-type: none"> a Wählen Sie in View Administrator Katalog > Desktop-Pools aus. b Doppelklicken Sie zur Auswahl des Pools für die Neuverteilung in der linken Spalte auf die Pool-ID. c Klicken Sie auf der Registerkarte Bestandsliste auf Computer. d Verwenden Sie die Strg- oder Umschalttaste, um alle Computer-IDs in der linken Spalte auszuwählen. e Wählen Sie im Dropdown-Menü View Composer die Option Neu verteilen aus.
Neuverteilung einer einzelnen virtuellen Maschine	<ol style="list-style-type: none"> a Wählen Sie in View Administrator Ressourcen > Computer aus. b Doppelklicken Sie zur Auswahl des Computers für die Neuverteilung in der linken Spalte auf die Computer-ID. c Wählen Sie im Dropdown-Menü „View Composer“ auf der Registerkarte Übersicht die Option Neu zusammenstellen aus.

- 2 Folgen Sie den Anweisungen des Assistenten.

Die virtuellen Linked-Clone-Maschinen werden aktualisiert und neu verteilt. Die ursprüngliche Größe der Betriebssystemfestplatten wird wiederhergestellt.

Sie können den Vorgang in View Administrator überwachen, indem Sie **Katalog > Desktop-Pools** auswählen, auf die Pool-ID doppelklicken und auf die Registerkarte **Aufgaben** klicken. Sie können auf **Aufgabe abbrechen**, **Aufgabe pausieren** oder **Aufgabe fortsetzen** klicken, um eine Aufgabe zu beenden, eine Aufgabe anzuhalten oder mit einer angehaltenen Aufgabe fortzufahren.

Neuverteilung verknüpfter Klone auf logische Laufwerke

Bei einem Vorgang zur Neuverteilung werden virtuelle Maschinen mit verknüpften Klonen erneut gleichmäßig auf die verfügbaren logischen Laufwerke verteilt. Dadurch wird Speicherplatz auf überlasteten Laufwerken gespart und sichergestellt, dass Laufwerke optimal ausgelastet sind.

Wenn Sie große Linked-Clone-Desktop-Pools erstellen und mehrere LUNs (Logical Unit Number) verwenden, besteht das Risiko einer ineffizienten Speicherplatznutzung, wenn die anfängliche Größe nicht genau festgelegt wurde. Wird ein hoher Wert für die Speichermehrfachvergabe festgelegt, kann die Größe der verknüpften Klone rasch ansteigen, sodass der gesamte freie Speicherplatz im Datenspeicher möglicherweise schnell belegt ist.

Wenn die virtuellen Maschinen 95 % des Speicherplatzes im Datenspeicher belegen, generiert View einen Warnungsprotokolleintrag.

Bei der Neuverteilung werden auch die verknüpften Klone aktualisiert und die Größe der Betriebssystemfestplatten wird reduziert. Dieser Vorgang hat keine Auswirkungen auf persistente View Composer-Festplatten.

Befolgen Sie bei Neuverteilungen die folgenden Richtlinien:

- Sie können Desktop-Pools mit dedizierter und mit dynamischer Zuweisung neu verteilen.
- Sie können ausgewählte verknüpfte Klone oder alle Klone in einem Pool neu verteilen.
- Sie können einen Desktop-Pool nach Bedarf oder als geplantes Ereignis neu verteilen.

Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur einen Vorgang zur Neuverteilung planen. Wenn Sie eine Neuverteilung umgehend starten, setzt der Vorgang zuvor geplante Aufgaben außer Kraft.

Sie können mehrere Vorgänge zur Neuverteilung planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.

Bevor Sie einen Vorgang zur Neuverteilung planen, müssen Sie zuvor geplante Aufgaben abbrechen.

- Eine Neuverteilung kann nur für virtuelle Maschinen durchgeführt werden, deren Status Verfügbar, Fehler oder Wird angepasst lautet und für die weder Zeitpläne noch Aufhebungsvorgänge ausstehen.
- Als empfohlene Vorgehensweise sollten virtuelle Linked-Clone-Maschinen nicht mit anderen Typen virtueller Maschinen in einem Datenspeicher kombiniert werden. So kann View Composer alle virtuellen Maschinen im Datenspeicher neu verteilen.
- Wenn Sie einen Pool bearbeiten und den Host oder Cluster und die Datenspeicher ändern, auf denen verknüpfte Klone gespeichert werden, können Sie die verknüpften Klone nur dann neu verteilen, wenn der neu ausgewählte Host oder Cluster über Vollzugriff für die ursprünglichen und die neuen Datenspeicher verfügt. Alle Hosts im neuen Cluster müssen auf die ursprünglichen und neuen Datenspeicher zugreifen können.

Beispielsweise könnten Sie einen Desktop-Pool mit verknüpften Klonen auf einem eigenständigen Host erstellen und einen lokalen Datenspeicher zum Speichern der Klone auswählen. Wenn Sie den Desktop-Pool bearbeiten und einen Cluster und einen freigegebenen Datenspeicher auswählen, schlägt die Neuverteilung fehl, da die Hosts im Cluster nicht auf den ursprünglichen, lokalen Datenspeicher zugreifen können.

- Sie können eine Mindestanzahl bereiter, bereitgestellter virtueller Maschinen festlegen, die für Benutzer verfügbar bleiben, damit sie sich während des Neuverteilungsvorgangs mit diesen verbinden können. Siehe hierzu „Bereitgestellt- und Bereithalten von Linked-Clone-Desktops während View Composer-Vorgängen“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Wichtig Wenn Sie einen Virtual SAN-Datenspeicher verwenden, können Sie den Neuverteilungsvorgang nur verwenden, um alle virtuellen Maschinen in einem Desktop-Pool von einem Virtual SAN-Datenspeicher zu einem anderen Datentyp (oder umgekehrt) zu migrieren. Falls ein Desktop-Pool einen Virtual SAN-Datenspeicher verwendet, bietet Virtual SAN die Lastausgleichsfunktion und optimiert die Verwendung von Ressourcen über den ESXi-Cluster hinweg.

Migrieren von virtuellen Maschinen mit verknüpften Klonen auf einen anderen Datenspeicher

Um virtuelle Maschinen mit verknüpften Klonen von einem Datenspeichersatz auf einen anderen zu migrieren, verwenden Sie die Neuverteilung.

Wenn Sie die Neuverteilung verwenden, verwaltet View Composer das Verschieben der verknüpften Klone zwischen Datenspeichern. View Composer stellt sicher, dass der Zugriff von den verknüpften Klonen auf das Replikat während und nach der Neuverteilung aufrecht erhalten wird. Bei Bedarf erstellt View Composer eine Instanz des Replikats auf dem Zieldatenspeicher.

Hinweis Verwenden Sie nicht vSphere Client bzw. vCenter Server, um virtuelle Linked-Clone-Maschinen zu migrieren oder zu verwalten. Verwenden Sie Storage vMotion nicht, um virtuelle Maschinen mit verknüpften Klonen auf andere Datenspeicher zu migrieren.

Voraussetzungen

Machen Sie sich mit dem Vorgang zur Neuverteilung vertraut. Siehe [Neuverteilen von virtuellen Linked-Clone-Maschinen](#) und [Neuverteilung verknüpfter Klone auf logische Laufwerke](#).

Verfahren

- 1 Wählen Sie in View Administrator die Option **Katalog > Desktop-Pools** aus, dann den Desktop-Pool, den Sie migrieren möchten, und klicken Sie auf **Bearbeiten**.
- 2 Blättern Sie auf der Registerkarte **vCenter-Einstellungen** nach unten zu **Datenspeicher** und klicken Sie auf **Durchsuchen**.
- 3 Wählen Sie auf der Seite „Datenspeicher verknüpfter Klone auswählen“ die Datenspeicher aus, die derzeit die verknüpften Klone enthalten, wählen Sie die Zieldatenspeicher aus und klicken Sie auf **OK**.
- 4 Klicken Sie im Fenster **Bearbeiten** auf **OK**.
- 5 Wählen Sie auf der Seite „Desktop-Pools“ den Pool durch Doppelklicken auf die Pool-ID in der linken Spalte.

- 6** Wählen Sie die Option **Neu verteilen** aus dem Dropdown-Menü **View Composer** aus und folgen Sie den Anweisungen des Assistenten, um die virtuellen Maschinen mit verknüpften Klonen neu zu verteilen.

Die virtuellen Maschinen mit verknüpften Klonen werden aktualisiert und auf die Zieldatenspeicher migriert.

Dateinamen von Linked-Clone-Festplatten nach einer Neuverteilung

Wenn Sie virtuelle Linked-Clone-Maschinen neu verteilen, ändert vCenter Server die Dateinamen von persistenten View Composer-Festplatten und Festplatten für löschbare Dateien in verknüpften Klonen, die in einen neuen Datenspeicher verschoben werden.

Die ursprünglichen Dateinamen identifizieren den Festplattentyp. Die umbenannten Festplatten enthalten keine solche Kennzeichnung.

Eine ursprüngliche persistente Festplatte umfasst eine *user-disk*-Kennzeichnung: *Desktop-Name-vdm-user-disk-D-ID.vmdk*.

Eine ursprüngliche Festplatte für löschbare Dateien umfasst eine *disposable*-Kennzeichnung: *Desktop-Name-vdm-disposable-ID.vmdk*.

Wenn ein verknüpfter Klon nach einer Neuverteilung in einen neuen Datenspeicher verschoben wurde, verwendet vCenter Server die folgende gängige Dateinamenssyntax für beide Festplattentypen: *Desktop-Name_n.vmdk*.

Verwalten persistenter View Composer-Festplatten

Sie können eine persistente Festplatte von View Composer von einer virtuellen Maschine mit verknüpftem Klon trennen und an einen anderen verknüpften Klon anfügen. Mit dieser Funktion können Benutzerinformationen separat von virtuellen Maschinen mit verknüpftem Klon verwaltet werden.

Persistente View Composer-Festplatten

Mit View Composer können Betriebssystemdaten und Benutzerinformationen auf separaten Festplatten in virtuellen Linked-Clone-Maschinen konfiguriert werden. View Composer behält die Benutzerinformationen auf der persistenten Festplatte bei, wenn die Betriebssystemdaten aktualisiert oder neu verteilt werden.

Eine persistente View Composer-Festplatte enthält Benutzereinstellungen und andere von den Benutzern generierte Daten. Sie erstellen persistente Festplatten, wenn Sie einen Linked-Clone-Desktop-Pool erstellen. Siehe hierzu „Arbeitsblatt zum Erstellen eines Linked-Clone-Desktop-Pools“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Sie können eine persistente Festplatte von der zugehörigen virtuellen Linked-Clone-Maschine trennen und die Festplatte im ursprünglichen Datenspeicher oder in einem anderen Datenspeicher platzieren. Nach dem Trennen der Festplatte wird die virtuelle Linked-Clone-Maschine gelöscht. Eine getrennte persistente Festplatte ist nicht länger mit einer virtuellen Maschine verknüpft.

Sie können eine getrennte persistente Festplatte auf verschiedene Arten mit einer anderen virtuellen Linked-Clone-Maschine verknüpfen. Dies bietet verschiedene Möglichkeiten:

- Wenn ein verknüpfter Klon gelöscht wird, können Sie die Benutzerdaten erhalten.
- Verlässt ein Mitarbeiter das Unternehmen, kann ein anderer Mitarbeiter auf die Benutzerdaten dieses Mitarbeiters zugreifen.
- Ein Benutzer mit mehreren Remote-Desktops kann die Benutzerdaten auf einem einzigen Remote-Desktop konsolidieren.
- Wenn der Zugriff auf eine virtuelle Maschine in vCenter Server nicht länger möglich ist, die persistente Festplatte jedoch weiterhin intakt ist, können Sie die persistente Festplatte importieren und unter Verwendung dieser Festplatte einen neuen verknüpften Klon erstellen.

Hinweis Sie können eine persistente Festplatte nicht von einem verknüpften Windows XP-Klon trennen und die persistente Festplatte für einen verknüpften Windows 8-, Windows 7- oder Windows Vista-Klon neu erstellen oder mit diesem verknüpfen. Persistente Festplatten müssen mit dem Betriebssystem verbunden bleiben, das bei ihrer Erstellung verwendet wurde.

View kann persistente Festplatten von Linked-Clone-Pools verwalten, die in View 4.5 oder höher erstellt wurden. Persistente Festplatten, die in früheren Versionen von View erstellt wurden, können nicht verwaltet werden und werden auf der Seite „Persistente Festplatten“ in View Administrator nicht angezeigt.

Trennen einer persistenten View Composer-Festplatte

Wenn Sie eine persistente View Composer-Festplatte von einer virtuellen Linked-Clone-Maschine trennen, wird die Festplatte gespeichert und der verknüpfte Klon wird gelöscht. Indem Sie eine persistente Festplatte trennen, können Sie benutzerspezifische Informationen in einer anderen virtuellen Maschine speichern und wiederverwenden.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Persistente Festplatten** aus.
- 2 Wählen Sie die zu trennende persistente Festplatte aus und klicken Sie auf **Trennen**.

3 Legen Sie den Speicherort für die persistente Festplatte fest.

Option	Beschreibung
Aktuellen Datenspeicher verwenden	Zum Speichern der persistenten Festplatte im aktuellen Datenspeicher.
Den folgenden Datenspeicher verwenden	<p>Zum Auswählen eines neuen Datenspeichers für die persistente Festplatte. Klicken Sie auf Durchsuchen und auf den nach unten weisenden Pfeil, um im Menü Datenspeicher auswählen einen neuen Datenspeicher auszuwählen.</p> <p>Sie können keinen lokalen Datenspeicher auswählen, um eine getrennte persistente Festplatte zu speichern. Sie müssen einen freigegebenen Datenspeicher oder einen Virtual SAN-Datenspeicher verwenden.</p> <p>Wenn die persistente Festplatte ursprünglich auf einem Virtual SAN-Datenspeicher gespeichert war, können Sie einen Virtual SAN- oder einen Non-Virtual SAN-Datenspeicher auswählen, um die getrennte persistente Festplatte zu speichern. Gleichmaßen können Sie, wenn die persistente Festplatte auf einem Non-Virtual SAN-Datenspeicher gespeichert war, die Trennung dieser Festplatte auf einem Non-Virtual SAN- oder Virtual SAN-Datenspeicher ausführen.</p>

Die persistente View Composer-Festplatte wird im Datenspeicher gespeichert. Die virtuelle Linked-Clone-Maschine wird gelöscht und in View Administrator nicht mehr angezeigt.

Verbinden einer persistenten View Composer-Festplatte mit einem anderen verknüpften Klon

Sie können eine getrennte persistente Festplatte mit einer anderen virtuellen Maschine mit verknüpfem Klon verbinden. Nach dem Verbinden einer persistenten Festplatte sind die Benutzereinstellungen und -informationen auf der Festplatte für den Benutzer der anderen virtuellen Maschine verfügbar.

Getrennte persistente Festplatten werden als sekundäre Festplatte mit der virtuellen Maschine mit verknüpftem Klon verbunden. Der neue Benutzer des verknüpften Klons hat Zugriff auf die sekundäre Festplatte und auf die bestehenden Benutzerinformationen und -einstellungen.

Sie können eine persistente Festplatte, die auf einem Non-Virtual SAN-Datenspeicher gespeichert sind, mit einer virtuellen Maschine verbinden, die auf einem Virtual SAN-Datenspeicher gespeichert ist. Gleichmaßen können Sie keine Festplatte, die auf einem Virtual SAN gespeichert ist, mit einer virtuellen Maschine verbinden, die auf einem Non-Virtual SAN gespeichert ist. View Administrator verhindert, dass Sie virtuelle Maschinen auswählen können, die sich über Virtual SAN- und Non-Virtual SAN-Datenspeicher erstrecken.

Um eine getrennte persistente Festplatte von einem Non-Virtual SAN auf ein Virtual SAN zu verschieben, können Sie die Festplatte auf einer virtuellen Maschine, die auf einem Non-Virtual SAN-Datenspeicher gespeichert ist, neu erstellen und den Desktop-Pool der virtuellen Maschine auf einem Virtual SAN-Datenspeicher neu verteilen. Siehe [Neuerstellung eines verknüpfte Klons mit einer getrennten persistenten Festplatte](#).

Voraussetzungen

- Vergewissern Sie sich, dass die ausgewählte virtuelle Maschine dasselbe Betriebssystem verwendet wie der verknüpfte Klon, in dem die persistente Festplatte erstellt wurde.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Persistente Festplatten** aus.
- 2 Wählen Sie auf der Registerkarte **Getrennt** die persistente Festplatte aus und klicken Sie auf **Anhängen**.
- 3 Wählen Sie eine virtuelle Maschine mit verknüpftem Klon aus, mit dem die persistente Festplatte verbunden werden soll.
- 4 Wählen Sie **Als sekundäre Festplatte verknüpfen**.
- 5 Klicken Sie auf **Fertig stellen**.

Nächste Schritte

Stellen Sie sicher, dass der Benutzer des verknüpften Klons über ausreichende Berechtigungen zur Verwendung der verbundenen sekundären Festplatte verfügt. Wenn der ursprüngliche Benutzer beispielsweise über bestimmte Zugriffsberechtigungen für die persistente Festplatte verfügte und die persistente Festplatte auf dem neuen Desktop als Laufwerk D verbunden ist, muss der neue Benutzer des verknüpften Klons über die ursprünglichen Zugriffsberechtigungen für Laufwerk D verfügen.

Melden Sie sich als Administrator beim Gastbetriebssystem des verknüpften Klons an und weisen Sie dem neuen Benutzer geeignete Berechtigungen zu.

Bearbeiten des Pools oder Benutzers einer persistenten View Composer-Festplatte

Sie können eine getrennte persistente View Composer-Festplatte einem neuen Desktop-Pool oder Benutzer zuweisen, wenn der ursprüngliche Desktop-Pool oder Benutzer aus View gelöscht wurde.

Eine getrennte persistente Festplatte ist weiterhin mit dem ursprünglichen Desktop-Pool und Benutzer verknüpft. Wenn der Desktop-Pool oder Benutzer aus View gelöscht wurde, können Sie die persistente Festplatte nicht zur Neuerstellung einer virtuellen Linked-Clone-Maschine verwenden.

Indem Sie den Desktop-Pool und Benutzer bearbeiten, können Sie die getrennte persistente Festplatte zur Neuerstellung einer virtuellen Maschine im neuen Desktop-Pool verwenden. Die virtuelle Maschine wird dem neuen Benutzer zugewiesen.

Sie können einen neuen Desktop-Pool, einen neuen Benutzer oder beides auswählen.

Voraussetzungen

- Vergewissern Sie sich, dass der Desktop-Pool oder Benutzer der persistenten Festplatte aus View gelöscht wurde.
- Vergewissern Sie sich, dass der neue Desktop-Pool dasselbe Betriebssystem verwendet wie der Desktop-Pool, in dem die persistente Festplatte erstellt wurde.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Persistente Festplatten**.

- 2 Wählen Sie die persistente Festplatte aus, deren Benutzer oder Desktop-Pool gelöscht wurde, und klicken Sie auf **Bearbeiten**.
- 3 (Optional) Wählen Sie einen Linked-Clone-Desktop-Pool aus der Liste aus.
- 4 (Optional) Wählen Sie einen Benutzer für die persistente Festplatte aus.
Sie können Active Directory nach der Domäne und dem Benutzernamen durchsuchen.

Nächste Schritte

Führen Sie eine Neuerstellung einer virtuellen Linked-Clone-Maschine mit der getrennten persistenten Festplatte aus.

Neuerstellung eines verknüpfte Klons mit einer getrennten persistenten Festplatte

Wenn Sie eine persistente View Composer-Festplatte trennen, wird der verknüpfte Klon gelöscht. Der ursprüngliche Benutzer kann auf die Benutzereinstellungen und -informationen auf der getrennten Festplatte zugreifen, indem Sie die virtuelle Maschine mit verknüpftem Klon basierend auf der getrennten Festplatte neu erstellen.

Hinweis Wenn Sie eine virtuelle Maschine mit verknüpftem Klon in einem Desktop-Pool neu erstellen, dessen maximale Größe erreicht wurde, wird die neu erstellte virtuelle Maschine dennoch zum Desktop-Pool hinzugefügt. Die Größe des Desktop-Pools überschreitet die angegebene maximale Größe.

Wenn der ursprüngliche Desktop-Pool oder Benutzer einer persistenten Festplatte aus View gelöscht wurde, kann der persistenten Festplatte ein neuer Pool oder Benutzer zugewiesen werden. Siehe [Bearbeiten des Pools oder Benutzers einer persistenten View Composer-Festplatte](#).

View unterstützt keine Neuerstellung einer virtuellen Maschine mit einer persistenten Festplatte, die auf einem Non-Virtual SAN-Datenspeicher gespeichert ist, wenn die neue virtuelle Maschine auf einem Virtual SAN-Datenspeicher gespeichert ist. Gleichermaßen unterstützt View nicht die Neuerstellung einer virtuellen Maschine auf einem Non-Virtual SAN, wenn die persistente Festplatte auf einem Virtual SAN gespeichert ist.

Um eine getrennte persistente Festplatte von einem Non-Virtual SAN auf ein Virtual SAN zu verschieben, können Sie die Festplatte auf einer virtuellen Maschine, die auf einem Non-Virtual SAN-Datenspeicher gespeichert ist, neu erstellen und den Desktop-Pool der virtuellen Maschine auf einem Virtual SAN-Datenspeicher neu verteilen.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Persistente Festplatten** aus.
- 2 Wählen Sie auf der Registerkarte **Getrennt** die persistente Festplatte aus und klicken Sie auf **Computer neu erstellen**.

Sie können mehrere persistente Festplatten auswählen, um für jede Festplatte eine virtuelle Maschine mit verknüpftem Klon neu zu erstellen.

- 3 Klicken Sie auf **OK**.

View erstellt eine virtuelle Maschine mit verknüpftem Klon für jede ausgewählte persistente Festplatte und fügt die virtuelle Maschine zum ursprünglichen Desktop-Pool hinzu.

Die persistenten Festplatten werden weiterhin im ursprünglichen Datenspeicher gespeichert.

Wiederherstellen eines verknüpften Klons durch den Import einer persistenten Festplatte aus vSphere

Virtuelle Maschinen mit verknüpften Klonen, die mit einer persistenten View Composer-Festplatte konfiguriert wurden, können wiederhergestellt werden, wenn die Maschine in View nicht länger verfügbar ist. Sie können die persistente Festplatte aus einem vSphere-Datenspeicher in View importieren.

Die persistente Festplattendatei wird als getrennte persistente Festplatte in View importiert. Sie können die getrennte Festplatte entweder mit einer vorhandenen virtuellen Maschine verknüpfen oder den ursprünglichen verknüpften Klon in View erneut erstellen.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Persistente Festplatten** aus.
- 2 Klicken Sie auf der Registerkarte **Getrennt** auf **Aus vCenter importieren**.
- 3 Wählen Sie eine vCenter Server-Instanz.
- 4 Wählen Sie das Rechenzentrum, in dem sich die Festplattendatei befindet.
- 5 Wählen Sie einen Desktop-Pool mit verknüpften Klonen, in dem eine neue virtuelle Maschine mit verknüpftem Klon mit der persistenten Festplatte erstellt werden soll.
- 6 Klicken Sie im Feld **Persistente Festplattendatei** auf **Durchsuchen** und auf den nach unten weisenden Pfeil, um im Menü **Datenspeicher auswählen** einen Datenspeicher auszuwählen.

Sie können eine persistente Festplatte nicht aus einem lokalen Datenspeicher importieren. Es stehen nur freigegebene Datenspeicher zur Verfügung.
- 7 Klicken Sie auf den Datenspeichernamen, um die enthaltenen Festplattenspeicherdateien und Dateien virtueller Maschinen anzuzeigen.
- 8 Wählen Sie die zu importierende persistente Festplattendatei aus.
- 9 Klicken Sie im Feld **Benutzer** auf **Durchsuchen**, wählen Sie einen Benutzer zur Zuweisung zur virtuellen Maschine aus, und klicken Sie auf **OK**.

Die Festplattendatei wird in View als getrennte persistente Festplatte importiert.

Nächste Schritte

Um die virtuelle Maschine mit verknüpftem Klon wiederherzustellen, können Sie die ursprüngliche virtuelle Maschine neu erstellen oder die getrennte persistente Festplatte mit einer anderen virtuellen Maschine verknüpfen.

Weitere Informationen finden Sie unter [Neuerstellung eines verknüpften Klons mit einer getrennten persistenten Festplatte](#) und [Verbinden einer persistenten View Composer-Festplatte mit einem anderen verknüpften Klon](#).

Löschen einer getrennten persistenten View Composer-Festplatte

Wenn Sie eine getrennte persistente Festplatte löschen, können Sie die Festplatte entweder aus View entfernen und im Datenspeicher beibehalten oder sowohl aus View als auch aus dem Datenspeicher löschen.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Persistente Festplatten** aus.
- 2 Wählen Sie auf der Registerkarte **Getrennt** die persistente Festplatte aus und klicken Sie auf **Löschen**.
- 3 Legen Sie fest, ob die Festplatte nach dem Entfernen aus View aus dem Datenspeicher gelöscht oder im Datenspeicher beibehalten werden soll.

Option	Beschreibung
Von der Festplatte löschen	Die persistente Festplatte ist nach dem Löschvorgang nicht mehr vorhanden.
Nur aus View löschen	Die persistente Festplatte ist nach dem Löschvorgang in View nicht mehr verfügbar, im Datenspeicher jedoch weiterhin vorhanden.

- 4 Klicken Sie auf **OK**.

Verwalten von Desktop-Pools, Maschinen und Sitzungen

8

In View Administrator können Sie Desktop-Pools, VM-basierte Desktops, computerbasierte Desktops, Desktop-Sitzungen und Anwendungssitzungen verwalten.

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten von Desktop-Pools](#)
- [Verwalten von VM-basierten Desktops](#)
- [Verwalten von nicht verwalteten Computern](#)
- [Verwalten der Remote-Desktop- und Anwendungssitzungen](#)
- [Exportieren von View-Informationen in externe Dateien](#)

Verwalten von Desktop-Pools

Sie können Desktop-Pools in View Administrator bearbeiten, deaktivieren und löschen.

Bearbeiten eines Desktop-Pools

Sie können einen vorhandenen Desktop-Pool bearbeiten, um Einstellungen wie Anzahl an Reservecomputern, Datenspeicher und Anpassungsspezifikationen zu konfigurieren.

Voraussetzungen

Machen Sie sich mit den Desktop-Pool-Einstellungen vertraut, die Sie nach der Erstellung eines Desktop-Pools ändern können. Siehe [Ändern der Einstellungen in einem vorhandenen Desktop-Pool](#) und [Feste Einstellungen in einem vorhandenen Desktop-Pool](#).

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Wählen Sie einen Desktop-Pool aus und klicken Sie auf **Bearbeiten**.
- 3 Klicken Sie im Dialogfeld „Bearbeiten“ auf eine Registerkarte und konfigurieren Sie die Desktop-Pool-Optionen neu.
- 4 Klicken Sie auf **OK**.

Ändern der Einstellungen in einem vorhandenen Desktop-Pool

Nach dem Erstellen eines Desktop-Pools können bestimmte Konfigurationseinstellungen geändert werden.

Tabelle 8-1. Bearbeitbare Einstellungen in einem vorhandenen Desktop-Pool

Registerkarte „Konfiguration“	Beschreibung
Allgemein	<p>Bearbeiten von Optionen für die Pool-Benennung und Einstellungen zur Speicherrichtlinienverwaltung von Desktops. Einstellungen für die Speicherrichtlinienverwaltung legen fest, ob ein Virtual SAN-Datenspeicher verwendet werden soll. Falls Sie kein Virtual SAN verwenden, können Sie separate Datenspeicher für Replikat- und Betriebssystemfestplatten auswählen.</p> <p>Hinweis Wenn Sie später Virtual SAN verwenden möchten, müssen Sie mit einem Vorgang zur Neuverteilung alle virtuellen Maschinen im Desktop-Pool zum Virtual SAN-Datenspeicher migrieren.</p>
Desktop-Pool-Einstellungen	Bearbeiten von Maschineneinstellungen, z. B. die Betriebsrichtlinie, das Anzeigeprotokoll und Adobe Flash-Einstellungen.
Bereitstellungseinstellungen	<p>Bearbeiten von Optionen für die Pool-Bereitstellung von Desktops und Hinzufügen von Maschinen zum Desktop-Pool.</p> <p>Diese Registerkarte ist nur für automatisierte Desktop-Pools verfügbar.</p>
vCenter-Einstellungen	<p>Bearbeiten der VM-Vorlage oder des standardmäßigen Basis-Images. Hinzufügen oder Ändern von vCenter Server-Instanzen, ESXi-Hosts oder -Clustern, Datenspeichern und anderen vCenter-Funktionen.</p> <p>Die neuen Werte wirken sich nur auf virtuelle Maschinen aus, die nach dem Ändern der Einstellungen erstellt werden. Die neuen Einstellungen haben keine Auswirkungen auf vorhandene virtuelle Maschinen.</p> <p>Diese Registerkarte ist nur für automatisierte Desktop-Pools verfügbar.</p>

Registerkarte „Konfiguration“	Beschreibung
Gastanpassung	<p>Auswählen von Sysprep-Anpassungsspezifikationen.</p> <p>Wenn für die Anpassung eines Linked-Clone-Desktop-Pools QuickPrep verwendet wurde, können Sie die Active Directory-Domäne und den Active Directory-Container ändern und QuickPrep-Abschaltskripts sowie nach der Synchronisierung ausgeführte Skripts angeben.</p> <p>Diese Registerkarte ist nur für automatisierte Desktop-Pools verfügbar.</p>
Erweiterter Speicher	<p>Aktivieren oder deaktivieren Sie erweiterte Speicherfunktionen wie beispielsweise View-Speicherbeschleunigung, Zurückgewinnung von VM-Datenträgerplatz und systemeigene NFS-Snapshots (VAAI).</p> <p>Wenn Sie View-Speicherbeschleunigung verwenden aktivieren/deaktivieren oder neu planen, wenn die Digest-Dateien für die View-Speicherbeschleunigung neu generiert werden, haben die neuen Einstellungen Auswirkungen auf vorhandene virtuelle Maschinen. Weitere Informationen finden Sie unter „Konfigurieren der View-Speicherbeschleunigung für Desktop-Pools“ im Dokument <i>Einrichten von Desktop- und Anwendungspools in View</i>.</p> <hr/> <p>Hinweis Wenn Sie View-Speicherbeschleunigung verwenden für einen vorhandenen Desktop-Pool mit verknüpften Klonen auswählen und das Replikat zuvor nicht für die View-Speicherbeschleunigung aktiviert war, zieht diese Funktion möglicherweise nicht sofort Änderungen nach sich. Die View-Speicherbeschleunigung kann nicht aktiviert werden, solange das Replikat aktuell verwendet wird. Sie können die Aktivierung der View-Speicherbeschleunigung erzwingen, indem Sie den Desktop-Pool auf einer neuen übergeordneten virtuellen Maschine neu zusammenstellen.</p> <hr/> <p>Wenn Sie VM-Datenträgerplatz zurückgewinnen aktivieren oder deaktivieren oder den Zeitpunkt für die Zurückgewinnung von VM-Datenträgerplatz neu festlegen, wirken sich die neuen Einstellungen auf vorhandene virtuelle Maschinen aus, wenn sie mit platzsparenden Festplatten erstellt wurden. Siehe hierzu „Rückgewinnung von Datenträgerplatz auf Linked-Clone-VMs“ im Dokument <i>Einrichten von Desktop- und Anwendungspools in View</i>.</p> <p>Wenn Sie die Einstellung Systemeigene NFS-Snapshots (VAAI) verwenden aktivieren/deaktivieren, hat die neue Einstellung nur Auswirkung auf die virtuellen Maschinen, die nach der Einstellungsänderung erstellt werden. Sie können aus vorhandenen virtuellen Maschinen Native NFS-Snapshot-Klone machen, indem Sie den Desktop-Pool neu zusammenstellen oder bei Bedarf neu verteilen. Weitere Informationen finden Sie unter „Verwenden der View Composer Array Integration mit systemeigener NFS-Snapshot-Technologie“ im Dokument <i>Einrichten von Desktop- und Anwendungspools in View</i>.</p> <p>VAAI wird auf virtuellen Maschinen mit platzsparenden Festplatten nicht unterstützt. VAAI wird auf Maschinen mit der virtuellen Hardwareversion 9 oder höher nicht unterstützt, da diese Betriebssystemfestplatten immer speicherplatzsparend sind, sogar wenn Sie den Vorgang zur Rückgewinnung von Speicherplatz deaktivieren.</p>

Feste Einstellungen in einem vorhandenen Desktop-Pool

Nach dem Erstellen eines Desktop-Pools können bestimmte Konfigurationseinstellungen nicht geändert werden.

Tabelle 8-2. Feste Einstellungen in einem vorhandenen Desktop-Pool

Einstellung	Beschreibung
Pool type (Pool-Typ)	Nach der Erstellung eines automatisierten, manuellen oder RDS-Desktop-Pools kann der Pool-Typ nicht geändert werden.
Benutzerzuweisung	Ein Wechsel zwischen dedizierten und dynamischen Zuweisungen ist nicht möglich.
Type of virtual machine (Typ der virtuellen Maschine)	Sie können nicht zwischen vollständigen virtuellen Maschinen und Linked-Clone-VMs umschalten.
Pool-ID	Die Pool-ID kann nicht geändert werden.
Benennungs- und Bereitstellungsmethode für Maschinen	<p>Zum Hinzufügen von virtuellen Maschinen zu einem Desktop-Pool muss die Bereitstellungsmethode verwendet werden, die zur Erstellung des Pools verwendet wurde. Ein Wechsel zwischen der manuellen Angabe von Maschinennamen und der Verwendung eines Benennungsmusters ist nicht möglich.</p> <p>Bei der manuellen Angabe von Namen können Namen zur Liste der Maschinennamen hinzugefügt werden.</p> <p>Bei Verwendung eines Benennungsmusters kann die maximale Anzahl an Maschinen erhöht werden.</p>
vCenter settings (vCenter-Einstellungen)	<p>vCenter-Einstellungen für vorhandene virtuelle Maschinen können nicht geändert werden.</p> <p>Sie können vCenter-Einstellungen im Dialogfeld „Bearbeiten“ ändern, die Werte gelten jedoch nur für neue virtuelle Maschinen, die nach dem Ändern der Einstellungen erstellt werden.</p>
View Composer, persistente Festplatten	Nach der Erstellung eines Linked-Clone-Desktop-Pools ohne persistente Festplatten können keine persistenten Festplatten konfiguriert werden.
View Composer customization method (View Composer-Anpassungsmethode)	Nach der Anpassung eines Linked-Clone-Desktop-Pools mit QuickPrep oder Sysprep können Sie nicht zur anderen Anpassungsmethode wechseln, wenn Sie virtuelle Maschinen im Pool erstellen oder neu zusammenstellen.

Ändern der Größe eines automatisierten Pools, der über ein Benennungsmuster bereitgestellt wurde

Wenn Sie einen automatisierten Desktop-Pool über ein Benennungsmuster bereitstellen, können Sie die Größe des Pools erhöhen oder verringern, indem Sie die maximale Anzahl an Computern ändern.

Voraussetzungen

- Stellen Sie sicher, dass der Desktop-Pool über ein Benennungsmuster bereitgestellt wurde. Weitere Informationen zur manuellen Angabe von Computernamen finden Sie unter [Hinzufügen von Computern zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde](#).
- Stellen Sie sicher, dass der Desktop-Pool automatisiert ist.

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Wählen Sie den Pool aus und klicken Sie auf **Bearbeiten**.
- 3 Geben Sie auf der Registerkarte **Bereitstellungseinstellungen** die neue Anzahl an Computern im Desktop-Pool im Textfeld **Maximale Anzahl an Computern** ein.

Wenn Sie die Desktop-Pool-Größe erhöhen, können so lange neue Computer zum Pool hinzugefügt werden, bis die maximale Anzahl erreicht ist.

Beim Verringern der Größe eines Pools mit dynamischer Zuweisung werden nicht verwendete Computer gelöscht. Wenn mehr Benutzer am Pool angemeldet sind als der neue Höchstwert, wird die Pool-Größe nach dem Abmelden der Benutzer verringert.

Beim Verringern der Größe eines Pools mit dedizierter Zuweisung werden nicht zugewiesene Computer gelöscht. Wenn den Computern mehr Benutzer zugewiesen sind als der neue Höchstwert, wird die Pool-Größe nach dem Aufheben von Benutzerzuweisungen verringert.

Hinweis Beim Verringern der Desktop-Pool-Größe kann die tatsächliche Anzahl an Computern größer sein als der unter **Maximale Anzahl an Computern** angegebene Wert, wenn gegenwärtig mehr Benutzer angemeldet oder den Computern zugewiesen sind als unter **Maximale Anzahl an Computern** festgelegt.

Hinzufügen von Computern zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde

Zum Hinzufügen von Computern zu einem automatisierten Desktop-Pool, für dessen Bereitstellung manuell Computernamen angegeben wurden, stellen Sie eine alternative Liste mit neuen Computernamen bereit. Mit dieser Funktion können Sie einen Desktop-Pool erweitern und weiterhin die Benennungskonventionen Ihres Unternehmens verwenden.

Befolgen Sie beim manuellen Hinzufügen von Computernamen die folgenden Richtlinien:

- Geben Sie jeden Computernamen in einer separaten Zeile ein.
- Ein Computernamen kann bis zu 15 alphanumerische Zeichen umfassen.
- Sie können jedem Computer-Eintrag einen Benutzernamen hinzufügen. Mithilfe eines Kommas können Sie den Benutzernamen vom Computernamen trennen.

In diesem Beispiel werden zwei Computer hinzugefügt. Der zweite Computer ist mit einem Benutzer verknüpft:

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

Hinweis In einem Pool mit dynamischer Zuweisung können keine Benutzernamen mit Computernamen verknüpft werden. Die Computer werden den verknüpften Benutzern nicht dediziert zugewiesen. In einem Pool mit dynamischer Zuweisung bleiben alle derzeit ungenutzten Computer jedem Benutzer zugänglich, der sich anmeldet.

Voraussetzungen

Stellen Sie sicher, dass der Desktop-Pool durch die manuelle Angabe von Computernamen erstellt wurde. Wenn der Pool über die Bereitstellung eines Benennungsmusters erstellt wurde, können Computer nicht über die Angabe von neuen Computernamen hinzugefügt werden.

Verfahren

- 1 Erstellen Sie eine Textdatei mit der Liste zusätzlicher Computernamen.

Wenn nur einige wenige Computer hinzugefügt werden sollen, können Sie die Computernamen direkt im Assistenten **Desktop-Pool hinzufügen** eingeben. Sie müssen keine separate Textdatei erstellen.

- 2 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.

- 3 Wählen Sie den zu erweiternden Desktop-Pool aus.

- 4 Klicken Sie auf **Bearbeiten**.

- 5 Klicken Sie auf die Registerkarte **Bereitstellungseinstellungen**.

- 6 Klicken Sie auf **Computer hinzufügen**.

- 7 Kopieren Sie Ihre Liste mit Computernamen in die Seite **Computernamen eingeben** und klicken Sie auf **Weiter**.

Der Assistent **Computernamen eingeben** zeigt die Computer-Liste an und weist mit einem roten **X** auf Validierungsfehler hin.

- 8 Korrigieren Sie ungültige Computernamen.

- a Platzieren Sie Ihren Cursor auf einem ungültigen Namen, um die entsprechende Fehlermeldung im unteren Seitenbereich anzuzeigen.
- b Klicken Sie auf **Zurück**.
- c Bearbeiten Sie die fehlerhaften Namen, und klicken Sie auf **Weiter**.

- 9 Klicken Sie auf **Fertig stellen**.

- 10 Klicken Sie auf **OK**.

View fügt die neuen Computer zum Pool hinzu.

Die Erstellung der neuen virtuellen Maschinen kann in vCenter Server überwacht werden.

In View Administrator können Sie die Computer so anzeigen, wie sie dem Desktop-Pool hinzugefügt werden. Wählen Sie hierzu **Katalog > Desktop-Pools** aus.

Deaktivieren oder Aktivieren eines Desktop-Pools

Wenn Sie einen Desktop-Pool deaktivieren, wird der Pool den Benutzern nicht mehr angezeigt und die Pool-Bereitstellung wird gestoppt. Benutzer haben keinen Zugriff auf den Pool. Ein deaktivierter Pool kann erneut aktiviert werden.

Sie können einen Desktop-Pool deaktivieren, um Benutzer am Zugriff auf ihre Remote-Desktops zu hindern, während Sie die Desktops für ihre Verwendung vorbereiten. Wenn ein Desktop-Pool nicht länger benötigt wird, können Sie den Pool durch eine Deaktivierung außer Betrieb nehmen, ohne die Desktop-Pool-Definition aus View löschen zu müssen.

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Wählen Sie einen Desktop-Pool aus und ändern Sie den Status des Pools.

Option	Aktion
Deaktivieren des Pools	Wählen Sie im Dropdown-Menü Status die Option Desktop-Pool deaktivieren aus.
Aktivieren des Pools	Wählen Sie im Dropdown-Menü Status die Option Desktop-Pool aktivieren aus.

- 3 Klicken Sie auf **OK**.

Deaktivieren oder Aktivieren der Bereitstellung in einem automatisierten Desktop-Pool

Wenn Sie die Bereitstellung in einem automatisierten Desktop-Pool deaktivieren, stellt View die Bereitstellung neuer virtueller Maschinen für den Pool ein. Die Bereitstellung kann erneut aktiviert werden, nachdem sie deaktiviert wurde.

Bevor Sie die Konfiguration eines Desktop-Pools ändern, können Sie die Bereitstellung deaktivieren. Auf diese Weise ist sichergestellt, dass keine neuen Maschinen mit der alten Konfiguration erstellt werden. Sie können die Bereitstellung auch deaktivieren, um View an der Belegung von zusätzlichem Speicherplatz zu hindern, wenn ein Pool den verfügbaren Speicherplatz fast vollständig ausgeschöpft hat.

Wenn in einem Linked-Clone-Pool die Bereitstellung deaktiviert ist, stellt View die Bereitstellung neuer Maschinen ein und verhindert die Anpassung von Maschinen, nachdem diese neu zusammengestellt oder neu verteilt wurden.

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Wählen Sie einen Desktop-Pool aus und ändern Sie den Status des Pools.

Option	Aktion
Deaktivieren der Bereitstellung	Wählen Sie die Option Bereitstellung deaktivieren aus dem Dropdown-Menü Status aus.
Bereitstellung aktivieren	Wählen Sie die Option Bereitstellung aktivieren aus dem Dropdown-Menü Status aus.

- 3 Klicken Sie auf **OK**.

Konfigurieren der Adobe Flash-Qualität und -Drosselung

Sie können Modi für die Adobe Flash-Qualität und -Drosselung festlegen, um die von Adobe Flash-Inhalten in Remote-Desktops verwendete Bandbreite zu reduzieren. Durch diese Reduzierung kann die Browsing-Leistung insgesamt sowie die Reaktionsfähigkeit anderer im Remote-Desktop ausgeführter Anwendungen verbessert werden.

Voraussetzungen

Machen Sie sich mit den Adobe Flash-Qualitäts- und Drosselungseinstellungen vertraut. Siehe [Adobe Flash-Qualität und -Drosselung](#).

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Wählen Sie einen Desktop-Pool aus und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie auf der Registerkarte **Desktop-Pool-Einstellungen** einen Qualitätsmodus aus dem Menü **Adobe Flash-Qualität** und einen Drosselungsmodus aus dem Menü **Adobe Flash-Drosselung** aus.
- 4 Klicken Sie auf **OK**.

Hinweis Die Einstellungen zur Reduzierung der Adobe Flash-Bandbreitennutzung werden erst angewendet, wenn Horizon Client erneut eine Verbindung mit dem Remote-Desktop herstellt.

Adobe Flash-Qualität und -Drosselung

Sie können die höchste zulässige Qualitätsstufe für Adobe Flash-Inhalte festlegen, welche die Webseiteneinstellungen außer Kraft setzt. Wenn die Adobe Flash-Qualität für eine Webseite höher ist als die zulässige maximale Qualitätsstufe, wird die Qualität auf den angegebenen Höchstwert reduziert. Eine geringere Qualität führt zu größeren Bandbreiteinsparungen.

Um die Einstellungen zur Reduzierung der Adobe Flash-Bandbreite zu nutzen, darf Adobe Flash nicht im Vollbildmodus ausgeführt werden.

[Tabelle 8-3. Adobe Flash-Qualitätseinstellungen](#) zeigt die verfügbaren Einstellungen für die Adobe Flash-Anzeigequalität.

Tabelle 8-3. Adobe Flash-Qualitätseinstellungen

Qualitätseinstellung	Beschreibung
Nicht steuern	Die Qualität wird durch die Webseiteneinstellungen bestimmt.
Niedrig	Mit dieser Einstellung werden die höchsten Bandbreiteinsparungen erzielt.
Mittel	Mit dieser Einstellung werden mittlere Bandbreiteinsparungen erzielt.
Hoch	Mit dieser Einstellung werden die geringsten Bandbreiteinsparungen erzielt.

Wird keine maximale Qualitätsstufe angegeben, lautet der Standardwert des Systems **Niedrig**

Adobe Flash verwendet Zeitgeberdienste, um die Bildschirmanzeige zu aktualisieren. Ein typischer Wert für ein Adobe Flash-Zeitgeberintervall ist 4 bis 50 Millisekunden. Durch die Drosselung bzw. Verlängerung des Intervalls kann die Frame-Rate und damit die Bandbreitennutzung reduziert werden.

[Tabelle 8-4. Adobe Flash-Drosselungseinstellungen](#) zeigt die verfügbaren Einstellungen für die Adobe Flash-Drosselung.

Tabelle 8-4. Adobe Flash-Drosselungseinstellungen

Drosselungseinstellung	Beschreibung
Deaktiviert	Es erfolgt keine Drosselung. Das Zeitgeberintervall bleibt unverändert.
Konservativ	Das Zeitgeberintervall lautet 100 Millisekunden. Diese Einstellung führt zur geringsten Anzahl an verworfenen Frames.
Mäßig	Das Zeitgeberintervall lautet 500 Millisekunden.
Aggressiv	Das Zeitgeberintervall lautet 2500 Millisekunden. Diese Einstellung führt zur höchsten Anzahl an verworfenen Frames.

Die Audiogeswindigkeit bleibt unabhängig von der gewählten Drosselungseinstellung konstant.

Löschen eines Desktop-Pools

Wenn Sie einen Desktop-Pool löschen, können Benutzer keine neuen Remote-Desktops im Pool mehr starten.

Je nach Typ des Desktop-Pools haben Sie verschiedene Optionen, wie View mit persistenten Festplatten, vollständigen vCenter Server-VMs und aktiven Sitzungen von Benutzern umgeht.

Mit einem automatisierten Desktop-Pool von View Composer Linked-Clone-VMs löscht View immer die virtuellen Maschinen von der Festplatte.

Wichtig Löschen Sie die virtuellen Maschinen in vCenter Server erst, wenn Sie einen Desktop-Pool mit View Administrator gelöscht haben. Anderenfalls könnte dies dazu führen, dass die View-Komponenten einen inkonsistenten Status aufweisen.

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Wählen Sie einen Desktop-Pool aus und klicken Sie auf **Löschen**.

3 Geben Sie an, wie der Desktop-Pool gelöscht werden soll.

Pool	Optionen
Automatisierter Desktop-Pool von verknüpften Klonen ohne persistente Festplatten.	Keine verfügbaren Optionen. View löscht alle virtuellen Maschinen von der Festplatte. Die Sitzungen von Benutzern zu ihren Remote-Desktops werden beendet.
Automatisierter Desktop-Pool von verknüpften Klonen mit persistenten Festplatten.	<p>Legen Sie fest, ob die persistenten Festplatten nach dem Löschen der Linked-Clone-VMs getrennt oder gelöscht werden sollen.</p> <p>In beiden Fällen löscht View alle virtuellen Maschinen von der Festplatte, und die Sitzungen von Benutzern zu ihren Remote-Desktops werden beendet.</p> <p>Wenn Sie eine dauerhafte Festplatte trennen, kann die virtuelle Linked-Clone-Desktop, der die dauerhafte Festplatte enthalten hat, neu erstellt werden, oder die dauerhafte Festplatte kann mit einer anderen virtuellen Maschine verknüpft werden. Getrennte persistente Festplatten können in demselben Datenspeicher oder in einem anderen Datenspeicher platziert werden. Wenn Sie einen anderen Datenspeicher auswählen, können Sie getrennte persistente Festplatten nicht auf einem lokalen Datenspeicher speichern. Sie müssen einen freigegebenen Datenspeicher verwenden.</p> <p>Sie können nur dauerhafte Festplatten trennen, die in View 4.5 oder höheren Versionen erstellt wurden.</p>
Automatisierter Desktop-Pool mit vollständigen virtuellen Maschinen. Manueller Desktop-Pool von vCenter Server-VMs.	Legen Sie fest, ob die virtuellen Maschinen in vCenter Server beibehalten oder gelöscht werden sollen.
RDS-Desktop-Pool. Automatisierter Desktop-Pool mit vollständigen virtuellen Maschinen. Manueller Desktop-Pool.	Wenn Benutzer vorhanden sind, die mit ihren Remote-Desktops verbunden sind, geben Sie an, ob die Sitzungen der Benutzer aktiv bleiben oder beendet werden sollen. Beachten Sie, dass View-Verbindungsserver Sitzungen, die aktiv bleiben, nicht nachverfolgt.

Der Desktop-Pool wird von View entfernt. Selbst wenn Sie die virtuellen Maschinen in vCenter Server beibehalten, kann View nicht darauf zugreifen.

Beim Löschen eines Desktop-Pools werden Computerkonten von Linked-Clone-VMs aus Active Directory entfernt. Die Computerkonten vollständiger virtueller Maschinen sind weiterhin in Active Directory vorhanden. Diese Konten müssen manuell aus Active Directory entfernt werden.

Verwalten von VM-basierten Desktops

Bei einem VM-basierten Desktop handelt es sich um einen Desktop aus einem automatisierten bzw. manuellen Desktop-Pool, der vCenter Server-VMs enthält.

Sie können Desktop-Sitzungen anzeigen, trennen und abmelden, eine Meldung an das Client-Gerät senden sowie die virtuelle Maschine zurücksetzen, die den Remote-Desktop hostet. Siehe [Verwalten der Remote-Desktop- und Anwendungssitzungen](#).

Zuweisen einer Maschine zu einem Benutzer

In einem Pool mit dedizierter Zuweisung kann ein Benutzer als der Besitzer der virtuellen Maschine zugewiesen werden, die einen Remote-Desktop hostet. Nur der zugewiesene Benutzer kann sich anmelden und eine Verbindung mit dem Remote-Desktop herstellen.

View weist Maschinen Benutzern in diesen Situationen zu.

- Wenn Sie einen Desktop-Pool erstellen und die Einstellung **Automatische Zuweisung aktivieren** auswählen.

Hinweis Bei Auswahl der Einstellung **Automatische Zuweisung aktivieren** können Benutzern weiterhin manuell Maschinen zugewiesen werden.

- Wenn Sie einen automatisierten Pool erstellen, die Einstellung **Desktop-Namen manuell angeben** auswählen und mit den Maschinennamen Benutzernamen angeben.

Wenn Sie für einen Pool mit dedizierter Zuweisung keine der beiden Einstellungen festlegen, können die Benutzer nicht auf die Remote-Desktops zugreifen. In diesem Fall muss jedem Benutzer manuell eine Maschine zugewiesen werden.

Maschinen können Benutzern auch mithilfe des Befehls `vdmadmin` zugewiesen werden. Siehe [Zuweisen von dedizierten Computern unter Verwendung der Option „-L“](#).

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine des Remote-Desktops zu einem Pool mit dedizierter Zuweisung gehört. Desktop-Pool-Zuweisungen werden in View Administrator in der Spalte des Desktop-Pools auf der Seite „Computer“ angezeigt.

Verfahren

- 1 Wählen Sie in View Administrator die Option **Ressourcen > Computer** oder wählen Sie **Katalog > Desktop-Pools**, doppelklicken Sie auf eine Pool-ID und klicken Sie auf die Registerkarte **Bestandsliste**.
- 2 Wählen Sie die Maschine aus.
- 3 Wählen Sie die Option **Benutzer zuweisen** aus dem Dropdown-Menü **Weitere Befehle**.
- 4 Wählen Sie, ob nach Benutzern oder nach Gruppen gesucht werden soll, wählen Sie eine Domäne und geben Sie im Textfeld **Name** oder **Beschreibung** eine Suchzeichenfolge ein.
- 5 Wählen Sie den Benutzer- oder Gruppennamen und klicken Sie auf **OK**.

Aufheben der Benutzerzuweisung für eine dedizierte Maschine

In einem Pool mit dedizierter Zuweisung kann die Maschinenzuweisung eines Benutzers entfernt werden.

Der Befehl `vdmadmin` kann ebenfalls verwendet werden, um die Zuweisung einer Maschine zu einem Benutzer zu entfernen. Siehe [Zuweisen von dedizierten Computern unter Verwendung der Option „-L“](#).

Verfahren

- 1 Wählen Sie in View Administrator die Option **Ressourcen > Maschinen** oder **Katalog > Desktop-Pools** aus, doppelklicken Sie auf eine Pool-ID und klicken Sie auf die Registerkarte **Bestandsliste**.
- 2 Wählen Sie die Maschine aus.
- 3 Wählen Sie die Option **Benutzerzuweisung aufheben** aus dem Dropdown-Menü **Weitere Befehle** aus.
- 4 Klicken Sie auf **OK**.

Die Maschine ist verfügbar und kann einem anderen Benutzer zugewiesen werden.

Anpassen von vorhandenen Computern im Wartungsmodus

Nach der Erstellung eines Desktop-Pools können einzelne Computer angepasst, geändert oder getestet werden, indem Sie sie in den Wartungsmodus versetzen. Wenn sich ein Computer im Wartungsmodus befindet, können die Benutzer nicht auf den VM-Desktop zugreifen.

Vorhandene Computer werden nacheinander in den Wartungsmodus versetzt. Der Wartungsmodus mehrerer Computer kann in einem Vorgang beendet werden.

Beim Erstellen eines Desktop-Pools können Sie alle Computer in diesem Pool im Wartungsmodus starten, wenn Sie die Computernamen manuell angeben. Weitere Informationen finden Sie im Thema „Anpassen von Desktops im Wartungsmodus“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Computer** oder **Katalog > Desktop-Pools** aus, doppelklicken Sie auf eine Pool-ID und wählen Sie die Registerkarte **Bestandsliste** aus.
- 2 Wählen Sie einen Computer aus.
- 3 Wählen Sie im Dropdown-Menü **Weitere Befehle** die Option **In den Wartungsmodus wechseln** aus.
- 4 Passen Sie den VM-Desktop an oder ändern bzw. testen Sie ihn.
- 5 Wiederholen Sie [Schritt 2](#) bis [Schritt 4](#) für alle virtuelle Maschinen, die Sie anpassen möchten.
- 6 Wählen Sie die angepassten Computer aus und wählen Sie im Dropdown-Menü **Weitere Befehle** die Option **Wartungsmodus beenden** aus.

Die geänderten VM-Desktops sind nun für die Benutzer verfügbar.

Überwachen des Status von VM-Desktops

Sie können den Status von VM-Desktops in Ihrer View-Bereitstellung problemlos über das View Administrator-Dashboard überwachen. Beispielsweise können alle getrennten virtuellen Maschinen oder virtuelle Maschinen im Wartungsmodus angezeigt werden.

Voraussetzungen

Machen Sie sich mit den VM-Status vertraut. Siehe [Status von vCenter Server-VMs](#).

Verfahren

- 1 Klicken Sie in View Administrator auf **Dashboard**.
- 2 Erweitern Sie im Fenster „Computerstatus“ einen Statusordner.

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

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

Auf der Seite „Computer“ werden alle virtuellen Maschinen mit dem ausgewählten Status angezeigt.

Nächste Schritte

Klicken Sie auf einen Computernamen, um Einzelheiten zu dieser virtuellen Maschine anzuzeigen, oder klicken Sie in View Administrator auf „Zurück“, um erneut auf die Dashboard-Seite zu wechseln.

Status von vCenter Server-VMs

Virtuelle Maschinen, die von vCenter Server verwaltet werden, können in verschiedenen Betriebs- und Verfügbarkeitszuständen vorhanden sein. In View Administrator können Sie den Status von Maschinen in der rechten Spalte der Seite „Computer“ nachverfolgen.

[Tabelle 8-5. Status von virtuellen Maschinen, die von vCenter Server verwaltet werden](#) zeigt die Betriebsstatus von VM-Desktops, die in View Administrator angezeigt werden. Ein Desktop kann jeweils nur einen Status aufweisen.

Tabelle 8-5. Status von virtuellen Maschinen, die von vCenter Server verwaltet werden

Status	Beschreibung
Wird bereitgestellt	Die virtuelle Maschine wird gegenwärtig bereitgestellt.
Wird angepasst	Die virtuelle Maschine in einem automatisierten Pool wird angepasst.
Wird gelöscht	Die virtuelle Maschine ist für den Löschvorgang gekennzeichnet. View löscht die virtuelle Maschine in Kürze.
Warten auf Agent	View-Verbindungsserver wartet auf die Kommunikation mit View Agent in einer virtuellen Maschine in einem manuellen Pool.
Wartungsmodus	Die virtuelle Maschine befindet sich im Wartungsmodus. Benutzer können sich nicht an der virtuellen Maschine anmelden oder diese verwenden.

Status	Beschreibung
Starten	View Agent wurde auf der virtuellen Maschine gestartet, andere erforderliche Dienste (z.B. das Anzeigeprotokoll) werden jedoch gegenwärtig noch gestartet. View Agent kann beispielsweise erst eine RDP-Verbindung mit Clientcomputern herstellen, wenn der RDP-Startvorgang abgeschlossen wurde. Während des View Agent-Starts können auch andere Prozesse (z. B. Protokolldienste) gestartet werden.
Agent deaktiviert	Dieser Status tritt in zwei Fällen auf. Das erste mögliche Szenario ist, wenn ein Benutzer sich in einem Desktop-Pool mit aktivierter Einstellung Computer bei Abmeldung löschen oder aktualisieren oder Computer nach Abmeldung löschen von einer Desktop-Sitzung abmeldet, die virtuelle Maschine jedoch noch nicht aktualisiert oder gelöscht wird. Die zweite Möglichkeit ist, dass der View-Verbindungsserver View Agent unmittelbar vor dem Senden einer Anforderung zum Ausschalten der virtuellen Maschine deaktiviert. Mit diesem Status wird sichergestellt, dass keine neuen Desktop-Sitzungen für die virtuelle Maschine gestartet werden können.
Agent nicht erreichbar	View-Verbindungsserver kann nicht mit View Agent in einer virtuellen Maschine kommunizieren.
Ungültige IP	Der Registrierungseintrag der Subnetzmaske wird auf der virtuellen Maschine konfiguriert, und keine aktiven Netzwerkadapter haben eine IP-Adresse innerhalb des konfigurierten Bereichs.
Agent muss neu gestartet werden	Eine View-Komponente wurde aktualisiert und die virtuelle Maschine muss neu gestartet werden, damit View Agent mit der aktualisierten Komponente interagieren kann.
Protokollfehler	Ein Anzeigeprotokoll konnte vor dem Ende des View Agent-Startzeitraums nicht gestartet werden. Hinweis View Administrator zeigt Computer möglicherweise mit dem Status Protokollfehler an, wenn für ein Protokoll ein Fehler aufgetreten ist, andere Protokolle jedoch erfolgreich gestartet wurden. Der Status Protokollfehler wird z. B. möglicherweise angezeigt, wenn kein HTML Access möglich ist, PCoIP und RDP jedoch ordnungsgemäß funktionieren. In diesem Fall sind die Computer verfügbar und Horizon Client-Geräte können über PCoIP oder RDP darauf zugreifen.
Domänenfehler	Die Domäne ist für die virtuelle Maschine nicht erreichbar. Es konnte nicht auf den Domänenserver zugegriffen werden oder die Domänenauthentifizierung ist fehlgeschlagen.
Bereits verwendet	In einem Desktop-Pool mit aktivierter Einstellung Computer bei Abmeldung löschen oder aktualisieren oder Computer nach Abmeldung löschen ist keine VM-Sitzung aktiv, der Benutzer hat sich jedoch nicht von der Sitzung abgemeldet. Diese Situation kann eintreten, wenn eine virtuelle Maschine unerwartet heruntergefahren wird oder der Benutzer die Maschine während einer aktiven Sitzung zurücksetzt. Wenn eine virtuelle Maschine diesen Status aufweist, verhindert View standardmäßig, dass andere Horizon Client-Geräte auf den Desktop zugreifen.
Konfigurationsfehler	Das Anzeigeprotokoll, z.B. RDP oder PCoIP, ist nicht aktiviert.
Bereitstellungsfehler	Während der Bereitstellung ist ein Fehler aufgetreten.
Fehler	In der virtuellen Maschine ist ein unbekannter Fehler aufgetreten.
Nicht zugewiesener Benutzer verbunden	Ein Benutzer, bei dem es sich nicht um den zugewiesenen Benutzer handelt, ist an einer virtuellen Maschine in einem dedizierten Pool angemeldet. Dieser Status kann beispielsweise auftreten, wenn ein Administrator vSphere Client startet, eine Konsole in der virtuellen Maschine öffnet und sich anmeldet.

Status	Beschreibung
Nicht zugewiesener Benutzer getrennt	Ein Benutzer, bei dem es sich nicht um den zugewiesenen Benutzer handelt, ist angemeldet und von einer virtuellen Maschine in einem Pool mit dedizierter Zuweisung getrennt.
Unbekannt	Die virtuelle Maschine weist einen unbekannten Status auf.
Bereitgestellt	Die virtuelle Maschine ist ausgeschaltet oder wurde angehalten.
Verfügbar	Die virtuelle Maschine ist eingeschaltet und kann für eine Verbindung verwendet werden. In einem dedizierten Pool wird die virtuelle Maschine einem Benutzer zugewiesen und bei der Anmeldung des Benutzers gestartet.
Verbunden	Die virtuelle Maschine befindet sich in einer Sitzung und hat eine Remote-Verbindung zum Horizon Client-Gerät.
Verbindung getrennt	Die virtuelle Maschine befindet sich in einer Sitzung, die Verbindung zum Horizon Client-Gerät ist aber getrennt.
Vorgang läuft	Die virtuelle Maschine weist während eines Wartungsvorgangs einen Übergangstatus auf.

Wenn eine Maschine einen bestimmten Status aufweist, können weitere Bedingungen gelten. View Administrator zeigt diese Bedingungen als Suffixe des Maschinenstatus an. Ein möglicher Status in View Administrator ist z.B. `Wird angepasst (fehlt)`.

[Tabelle 8-6. Bedingungen des Maschinenstatus](#) zeigt diese zusätzlichen Bedingungen.

Tabelle 8-6. Bedingungen des Maschinenstatus

Bedingung	Beschreibung
Fehlt)	Die virtuelle Maschine ist in vCenter Server nicht vorhanden. Typischerweise wurde die virtuelle Maschine in vCenter Server gelöscht, in der View LDAP-Konfiguration ist jedoch noch ein Eintrag für die Maschine vorhanden.
Aufgabe angehalten	Ein View Composer-Vorgang, z.B. eine Aktualisierung, Neuzusammenstellung oder Neuverteilung, wurde angehalten. Weitere Informationen zur Fehlerbehebung bei Neuzusammenstellungen finden Sie unter Korrigieren einer nicht erfolgreichen Neuzusammenstellung . Details zu den Fehlerzuständen von View Composer finden Sie unter „View Composer-Bereitstellungsfehler“ im Dokument <i>Einrichten von Desktop- und Anwendungspools in View</i> . Die Bedingung <code>Aufgabe angehalten</code> gilt für alle virtuellen Maschinen, die für den Vorgang ausgewählt wurden, für die der Vorgang jedoch noch nicht gestartet wurde. Auf virtuelle Maschinen innerhalb des Pools, die nicht für den Vorgang ausgewählt wurden, wird die Bedingung <code>Aufgabe angehalten</code> nicht angewendet.

Ein Maschinenstatus kann beide Bedingungen aufweisen (`fehlt`, `Aufgabe angehalten`), wenn eine View Composer-Aufgabe angehalten wurde und die virtuelle Maschine nicht in vCenter Server vorhanden ist.

Löschen von VM-Desktops

Wenn Sie einen VM-Desktop löschen, können die Benutzer nicht länger auf den Desktop zugreifen. Beim VM-Desktop handelt es sich entweder um eine virtuelle Maschine von vCenter Server oder um eine nicht verwaltete virtuelle Maschine.

Wenn Sie die virtuellen Maschinen in vCenter Server beibehalten, können Benutzer mit derzeit aktiven Sitzungen Desktops auf Grundlage vollständiger virtueller Maschinen weiterhin verwenden. Nach der Abmeldung der Benutzer können diese nicht auf die gelöschten VM-Desktops zugreifen.

Bei virtuellen Linked-Clone-Computern löscht vCenter Server die virtuellen Maschinen immer von der Festplatte.

Hinweis Löschen Sie die virtuellen Maschinen in vCenter Server erst, wenn Sie die VM-Desktops mit View Administrator gelöscht haben. Anderenfalls könnte dies dazu führen, dass die View-Komponenten einen inkonsistenten Status aufweisen.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Computer** aus.
- 2 Wählen Sie die Registerkarte **vCenter-VMs** oder die Registerkarte **Andere** aus.
- 3 Wählen Sie einen oder mehrere Computer aus und klicken Sie auf **Entfernen**.
- 4 Geben Sie an, wie der VM-Desktop gelöscht werden sollen.

Option	Beschreibung
Pool that contains full virtual-machine desktops (Pool mit Desktops auf Grundlage vollständiger virtueller Maschinen)	<p>Legen Sie fest, ob die virtuellen Maschinen in vCenter Server beibehalten oder gelöscht werden sollen.</p> <p>Wenn Sie die virtuellen Maschinen von der Festplatte löschen, werden Benutzer mit aktiven Sitzungen von ihren Desktops getrennt.</p> <p>Wenn Sie die virtuellen Maschinen in vCenter Server beibehalten, legen Sie fest, ob Benutzer mit aktiven Sitzungen mit ihren Desktops verbunden bleiben oder getrennt werden sollen.</p>
Linked-clone pool with View Composer persistent disks (Linked-Clone-Pool mit persistenten View Composer-Festplatten)	<p>Legen Sie fest, ob die dauerhaften Festplatten nach dem Löschen der Desktops mit virtuellen Maschinen getrennt oder gelöscht werden sollen.</p> <p>In beiden Fällen löscht vCenter Server die virtuellen Linked-Clone-Maschinen von der Festplatte. Benutzer mit derzeit aktiven Sitzungen werden von ihren Remote-Desktops getrennt.</p> <p>Wenn Sie eine dauerhafte Festplatte trennen, kann die virtuelle Linked-Clone-Desktop, der die dauerhafte Festplatte enthalten hat, neu erstellt werden, oder die dauerhafte Festplatte kann mit einer anderen virtuellen Maschine verknüpft werden. Getrennte persistente Festplatten können in demselben Datenspeicher oder in einem anderen Datenspeicher platziert werden. Wenn Sie einen anderen Datenspeicher auswählen, können Sie getrennte persistente Festplatten nicht auf einem lokalen Datenspeicher speichern. Sie müssen einen freigegebenen Datenspeicher verwenden.</p> <p>Sie können nur dauerhafte Festplatten trennen, die in View 4.5 oder höheren Versionen erstellt wurden.</p>
Linked-clone pool without View Composer persistent disks (Linked-Clone-Pool ohne persistente View Composer-Festplatten)	<p>vCenter Server löscht die virtuellen Linked-Clone-Maschinen von der Festplatte. Benutzer mit derzeit aktiven Sitzungen werden von ihren Remote-Desktops getrennt.</p>

Die Computer werden aus dem View-Verbindungsserver entfernt. Wenn Sie die virtuellen Maschinen in vCenter Server beibehalten, kann View nicht darauf zugreifen.

Beim Löschen von VM-Desktops werden Linked-Clone-Computerkonten der virtuellen Maschine aus Active Directory entfernt. Die Konten vollständiger virtueller Maschinen sind weiterhin in Active Directory vorhanden. Diese Konten müssen manuell aus Active Directory entfernt werden.

Verwalten von nicht verwalteten Computern

In View Administrator können Sie nicht verwaltete Computer zu manuellen Desktop-Pools hinzufügen oder daraus entfernen und außerdem registrierte Computer aus View entfernen. Unter nicht verwalteten Computern sind physische Computer und virtuelle Maschinen zu verstehen, die nicht von vCenter Server verwaltet werden.

Weitere Informationen zum Löschen eines Desktop-Pools, der nicht verwaltete Computer enthält, finden Sie unter [Löschen eines Desktop-Pools](#).

Wenn Sie eine Einstellung neu konfigurieren, die einen nicht verwalteten Computer betrifft, kann es bis zu 10 Minuten dauern, bis die neue Einstellung wirksam wird. Wenn Sie z. B. den Sicherheitsmodus für Nachrichten in den globalen Einstellungen oder die Einstellung **Nach Verbindungstrennung automatisch abmelden** für einen Pool ändern, kann es bis zu 10 Minuten dauern, bis View die betroffenen nicht verwalteten Computer neu konfiguriert.

Hinweis RDS-Hosts sind ebenfalls nicht verwaltete Computer, da sie weder aus einer übergeordneten virtuellen Maschine oder Vorlage erstellt noch von vCenter Server verwaltet werden. RDS-Hosts unterstützen sitzungsbasierte Desktops und Anwendungen und werden als separate Kategorie behandelt. Siehe [Verwalten von RDS-Hosts](#).

Hinzufügen eines nicht verwalteten Computers zu einem manuellen Pool

Die Größe eines manuellen Desktop-Pools kann erhöht werden, indem nicht verwaltete Computer zum Pool hinzugefügt werden.

Voraussetzungen

Stellen Sie sicher, dass View Agent auf dem nicht verwalteten Computer installiert ist. Weitere Informationen zur Vorbereitung eines nicht verwalteten Computers finden Sie unter „Installieren von View Agent auf einem nicht verwalteten Computer“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Doppelklicken Sie auf die Pool-ID des manuellen Pools.
- 3 Klicken Sie auf der Registerkarte **Bestandsliste** auf **Hinzufügen**.
- 4 Wählen Sie im Fenster **Desktops hinzufügen** nicht verwaltete Computer aus und klicken Sie auf **OK**.

Die nicht verwalteten Computer werden zu dem Pool hinzugefügt.

Entfernen eines nicht verwalteten Computers aus einem manuellen Desktop-Pool

Die Größe eines manuellen Desktop-Pools kann verringert werden, indem nicht verwaltete Computer aus dem Pool entfernt werden.

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Doppelklicken Sie auf die Pool-ID des manuellen Pools.
- 3 Wählen Sie die Registerkarte **Bestandsliste** aus.
- 4 Wählen Sie die zu entfernenden nicht verwalteten Computer aus.
- 5 Klicken Sie auf **Entfernen**.
- 6 Wenn Benutzer bei den nicht verwalteten, VM-basierten Desktops angemeldet sind, legen Sie fest, ob die Sitzungen beendet werden oder aktiv bleiben sollen.

Option	Beschreibung
Aktiv lassen	Aktive Sitzungen bleiben bestehen, bis der Benutzer sich abmeldet. View-Verbindungsserver verfolgt diese Sitzungen nicht nach.
Beenden	Aktive Sitzungen werden sofort beendet.

- 7 Klicken Sie auf **OK**.

Die nicht verwalteten Computer werden aus dem Pool entfernt.

Entfernen von registrierten Maschinen aus View

Falls Sie eine registrierte Maschine nicht erneut verwenden möchten, können Sie sie aus View entfernen.

Es gibt zwei Typen von registrierten Maschinen in View: RDS-Hosts und Andere. Nicht verwaltete Maschinen fallen unter die Kategorie „Andere“. Unter nicht verwalteten Maschinen sind physische Computer und virtuelle Maschinen zu verstehen, die nicht von vCenter Server verwaltet werden. Sie werden zur Bildung von manuellen Desktop-Pools verwendet, die keine vCenter Server-VMs enthalten.

Nachdem Sie eine registrierte Maschine entfernt haben, ist sie in View nicht mehr verfügbar. Damit Ihnen die Maschine wieder zur Verfügung steht, müssen Sie View Agent neu installieren.

Voraussetzungen

Stellen Sie sicher, dass die registrierten Maschinen, die Sie entfernen möchten, nicht in einem Desktop-Pool verwendet werden.

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration > Registrierte Computer** aus.
- 2 Klicken Sie auf die Registerkarte **Andere**.

- 3 Wählen Sie einen oder mehrere Computer aus und klicken Sie auf **Entfernen**.

Sie können nur Maschinen auswählen, die nicht von einem Desktop-Pool verwendet werden.

- 4 Klicken Sie zum Bestätigen auf **OK**.

Status nicht verwalteter Computer

Nicht verwaltete Computer, bei denen es sich um physische Computer oder virtuelle Maschinen handelt, die nicht von vCenter Server verwaltet werden, können verschiedene Betriebs- und Verfügbarkeitsstatus aufweisen. In View Administrator können Sie den Status nicht verwalteter Computer in der rechten Spalte der Seite „Computer“ auf der Registerkarte **Andere** verfolgen.

Tabelle 8-7. Status nicht verwalteter Computer zeigt die Betriebsstatus von nicht verwalteten Computern an, die in View Administrator angezeigt werden. Ein Computer kann jeweils nur einen Status aufweisen.

Tabelle 8-7. Status nicht verwalteter Computer

Status	Beschreibung
Starten	View Agent wurde auf dem Computer gestartet, andere erforderliche Dienste (z. B. das Anzeigeprotokoll) werden jedoch gegenwärtig noch gestartet. Während des View Agent-Starts können auch andere Prozesse (z. B. Protokolldienste) gestartet werden.
Validierung läuft	Dieser Status tritt auf, nachdem der View-Verbindungsserver zunächst den Computer erkennt, d. h. in der Regel nach dem Start oder Neustart des View-Verbindungsservers und vor der ersten erfolgreichen Kommunikation mit View Agent auf dem Computer. Der Status ist in der Regel vorübergehend. Dabei handelt es sich nicht um denselben nicht erreichbaren Agent-Status, der ein Kommunikationsproblem anzeigt.
Agent deaktiviert	Dieser Status tritt auf, wenn der View-Verbindungsserver den View Agent deaktiviert. Mit diesem Status wird sichergestellt, dass keine neue Desktop-Sitzung für den Computer gestartet werden kann.
Agent nicht erreichbar	View-Verbindungsserver kann nicht mit View Agent auf dem Computer kommunizieren. Der Computer wird möglicherweise ausgeschaltet.
Ungültige IP	Die Registrierungseinstellung für die Subnetzmaske ist auf dem Computer konfiguriert und keine aktiven Netzwerkadapter verfügen über eine IP-Adresse innerhalb des konfigurierten Bereichs.
Agent muss neu gestartet werden	Eine View-Komponente wurde aktualisiert und der Computer muss neu gestartet werden, damit View Agent mit der aktualisierten Komponente interagieren kann.
Protokollfehler	Ein Anzeigeprotokoll konnte vor dem Ende des View Agent-Startzeitraums nicht gestartet werden. Hinweis View Administrator zeigt Computer möglicherweise mit dem Status Protokollfehler an, wenn für ein Protokoll ein Fehler aufgetreten ist, andere Protokolle jedoch erfolgreich gestartet wurden. Der Status Protokollfehler wird z. B. möglicherweise angezeigt, wenn kein HTML Access möglich ist, PCoIP und RDP jedoch ordnungsgemäß funktionieren. In diesem Fall sind die Computer verfügbar und Horizon Client-Geräte können über PCoIP oder RDP darauf zugreifen.
Domänenfehler	Die Domäne ist für den Computer nicht erreichbar. Es konnte nicht auf den Domänenserver zugegriffen werden oder die Domänenauthentifizierung ist fehlgeschlagen.
Konfigurationsfehler	Das Anzeigeprotokoll, z. B. RDP oder ein anderes Protokoll, ist nicht aktiviert.

Status	Beschreibung
Nicht zugewiesener Benutzer verbunden	Ein Benutzer, bei dem es sich nicht um den zugewiesenen Benutzer handelt, ist an einem Computer in einem dedizierten Pool angemeldet. Beispiel: Dieser Status kann auftreten, wenn ein Administrator sich bei einem nicht verwalteten Computer ohne Verwendung von Horizon Client anmeldet.
Nicht zugewiesener Benutzer getrennt	Ein Benutzer, bei dem es sich nicht um den zugewiesenen Benutzer handelt, ist angemeldet und von einem Computer in einem dedizierten Pool getrennt.
Unbekannt	Der Computer weist einen unbekannten Status auf.
Verfügbar	Der als Desktop-Quelle eingesetzte Computer ist eingeschaltet und es kann eine Verbindung mit dem Desktop hergestellt werden. In einem dedizierten Pool wird der Desktop einem Benutzer zugewiesen. Der Desktop wird bei der Anmeldung des Benutzers gestartet.
Verbunden	Der Desktop befindet sich in einer Sitzung und verfügt über eine Remote-Verbindung mit einem Horizon Client-Gerät.
Verbindung getrennt	Der Desktop befindet sich in einer Sitzung, ist jedoch vom Horizon Client-Gerät getrennt.

Verwalten der Remote-Desktop- und Anwendungssitzungen

Wenn ein Benutzer einen Remote-Desktop oder eine Remoteanwendung startet, wird eine Sitzung erstellt. Sie können Sitzungen trennen und abmelden, Nachrichten an Clients senden und virtuelle Maschinen wiederherstellen.

Verfahren

- 1 Navigieren Sie in View Administrator zur Anzeige der Sitzungsinformationen.

Sitzungstyp	Navigation
Remote-Desktop-Sitzungen	Wählen Sie Katalog > Desktop-Pools aus, doppelklicken Sie auf eine Pool-ID und klicken Sie auf die Registerkarte Sitzungen .
Remote-Desktop-Sitzungen und Remoteanwendungssitzungen	Wählen Sie Überwachung > Sitzungen aus.
Mit einem Benutzer oder einer Benutzergruppe verknüpfte Sitzungen	<ul style="list-style-type: none"> ■ Wählen Sie Benutzer und Gruppen aus. ■ Doppelklicken Sie auf einen Namen eines Benutzers oder einer Benutzergruppe. ■ Klicken Sie auf die Registerkarte Sitzungen.

- 2 Wählen Sie eine Sitzung aus.

Um eine Nachricht an Benutzer zu senden, können Sie mehrere Sitzungen auswählen. Sie können die anderen Vorgänge jeweils nur für eine Sitzung ausführen.

- 3 Geben Sie an, ob die Desktops getrennt, die Benutzer abgemeldet, eine Nachricht gesendet oder eine virtuelle Maschine wiederhergestellt werden soll.

Option	Beschreibung
Sitzung trennen	Trennt den Benutzer von der Sitzung.
Logoff Session (Von Sitzung abmelden)	Meldet den Benutzer von der Sitzung ab. Die nicht gespeicherten Daten gehen verloren.
Virtuelle Maschine zurücksetzen	Startet die virtuelle Maschine ohne ordnungsgemäßes Herunterfahren neu. Diese Aktion gilt nur für eine Desktop-Sitzung in einem automatisierten Pool oder in einem manuellen Pool, der virtuelle Maschinen von vCenter Server enthält.
Nachricht senden	Senden Sie eine Meldung an Horizon Client. Sie können die Nachricht als Info , Warnung oder Fehler kennzeichnen.

- 4 Klicken Sie auf **OK**.

Exportieren von View-Informationen in externe Dateien

In View Administrator können View-Tabelleninformationen in externe Dateien exportiert werden. Sie können die Tabellen mit Benutzern und Gruppen, Pools, Maschinen, persistenten View Composer-Festplatten, ThinApp-Anwendungen, Ereignissen und VDI-Sitzungen exportieren. Anschließend können diese Informationen in einer Kalkulationstabelle oder in einem anderen Tool angezeigt und verwaltet werden.

Sie können beispielsweise Informationen zu Maschinen erfassen, die von mehreren View-Verbindungsserver-Instanzen oder Gruppen aus replizierten View-Verbindungsserver-Instanzen verwaltet werden. Die Tabelle „Maschinen“ kann über jede View Administrator-Schnittstelle exportiert und in einer Tabellenkalkulation angezeigt werden.

Beim Export einer View Administrator-Tabelle wird diese als kommagetrennte Datei (CSV) gespeichert. Über diese Funktion werden nicht einzelne Seiten, sondern die gesamte Tabelle exportiert.

Verfahren

- 1 Zeigen Sie die zu exportierende Tabelle in View Administrator an.
Klicken Sie beispielsweise auf **Ressourcen > Maschinen**, um die Maschinentabelle anzuzeigen.
- 2 Klicken Sie in der oberen rechten Ecke der Tabelle auf das Exportsymbol.
Wenn Sie auf das Symbol zeigen, wird die Quickinfo Tabelleninhalte exportieren angezeigt.
- 3 Geben Sie im Dialogfeld „Speicherort für Download auswählen“ einen Dateinamen für die CSV-Datei ein.
Der standardmäßige Dateiname lautet `global_table_data_export.csv`.
- 4 Navigieren Sie zu einem Verzeichnis zum Speichern der Datei.
- 5 Klicken Sie auf **Speichern**.

Nächste Schritte

Öffnen Sie eine Tabellenkalkulation oder ein anderes Tool, um die CSV-Datei anzuzeigen.

Verwalten von Anwendungspools, Farmen und RDS-Hosts

9

In View Administrator können Sie Verwaltungsvorgänge wie das Konfigurieren oder Löschen von Desktop-Pools, Farmen oder RDS-Hosts durchführen.

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten von Anwendungspools](#)
- [Verwalten von Farmen](#)
- [Verwalten von RDS-Hosts](#)

Verwalten von Anwendungspools

Sie können Anwendungspools in View Administrator hinzufügen, bearbeiten, löschen oder Berechtigungen dazu erteilen.

Informationen zum Hinzufügen eines Anwendungspools finden Sie unter „Erstellen von Anwendungspools“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*. Informationen zum Erteilen von Berechtigungen für einen Anwendungspool finden Sie unter „Berechtigen von Benutzern und Gruppen“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Bearbeiten eines Anwendungspools

Sie können einen vorhandenen Anwendungspool bearbeiten, um Einstellungen wie z. B. Anzeigename, Version, Veröffentlicher, Pfad, Startordner, Parameter und Beschreibung zu konfigurieren. Sie können die ID oder Zugriffsgruppe eines Anwendungspools nicht ändern.

Voraussetzungen

Machen Sie sich mit den Einstellungen eines Anwendungspools vertraut. Siehe hierzu „Erstellen von Anwendungspools“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Anwendungspools**.
- 2 Wählen Sie einen Pool aus und klicken Sie auf **Bearbeiten**.
- 3 Nehmen Sie die gewünschten Änderungen an den Pool-Einstellungen vor.

- 4 Klicken Sie auf **OK**.

Löschen eines Anwendungspools

Nach dem Löschen eines Anwendungspools können Benutzer die Anwendung im Pool nicht mehr starten.

Sie können einen Anwendungspool auch dann löschen, wenn Benutzer gerade auf die Anwendung zugreifen. Nach dem Schließen der Anwendung können die betreffenden Benutzer nicht mehr darauf zugreifen.

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Anwendungspools**.
- 2 Wählen Sie einen oder mehrere Anwendungspools und klicken Sie auf **Löschen**.
- 3 Klicken Sie zum Bestätigen auf **OK**.

Verwalten von Farmen

In View Administrator können Sie Farmen hinzufügen, bearbeiten, löschen, aktivieren und deaktivieren.

Informationen zum Hinzufügen einer Farm finden Sie unter „Erstellen von Farmen“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*. Informationen zu Zugriffsgruppen finden Sie unter [Kapitel 4 Konfigurieren der rollenbasierten Verwaltungsdelegierung](#).

Nach dem Erstellen einer Farm können Sie RDS-Hosts hinzufügen oder entfernen, um mehr oder weniger Benutzer zu unterstützen.

Bearbeiten einer Farm

Im Fall einer bestehenden Farm können Sie Einstellungen wie „Beschreibung“, „Zugriffsgruppe“ und „Zeitüberschreitung bei leerer Sitzung“ konfigurieren.

Voraussetzungen

Machen Sie sich mit den Einstellungen einer Farm vertraut. Siehe hierzu „Erstellen von Farmen“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Farmen**.
- 2 Wählen Sie eine Farm aus und klicken Sie auf **Bearbeiten**.
- 3 Nehmen Sie die gewünschten Änderungen an den Farmeinstellungen vor.
- 4 Klicken Sie auf **OK**.

Löschen einer Farm

Sie können eine Farm löschen, falls Sie sie nicht mehr benötigen oder Sie eine neue mit unterschiedlichen RDS-Hosts erstellen möchten. Sie können nur Farmen löschen, die nicht mit einem RDS-Desktop-Pool oder einem Anwendungspool verknüpft sind.

Voraussetzungen

Stellen Sie sicher, dass die Farm keinem RDS-Desktop-Pool oder Anwendungspool zugewiesen ist.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Farmen**.
- 2 Wählen Sie eine oder mehrere Farmen aus und klicken Sie auf **Löschen**.
- 3 Klicken Sie zum Bestätigen auf **OK**.

Aktivieren oder Deaktivieren einer Farm

Wenn Sie eine Farm deaktivieren, können Benutzer keine RDS-Desktops oder Anwendungen mehr aus den RDS-Desktop-Pools und Anwendungspools starten, die dieser Farm zugeordnet sind. Die Benutzer können weiterhin RDS-Desktops und Anwendungen verwenden, die derzeit geöffnet sind.

Sie können eine Farm deaktivieren, wenn Sie planen, Wartungsarbeiten auf den RDS-Hosts in der betreffenden Farm oder auf den RDS-Desktop- und Anwendungspools durchzuführen, die dieser Farm zugeordnet sind. Nach der Deaktivierung einer Farm kann es vorkommen, dass einige Benutzer weiterhin RDS-Desktops oder Anwendungen verwenden, die noch vor der Deaktivierung dieser Farm geöffnet wurden.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Farmen**.
- 2 Wählen Sie eine oder mehrere Farmen aus und klicken Sie auf **Weitere Befehle**.
- 3 Klicken Sie auf **Aktivieren** oder **Deaktivieren**.
- 4 Klicken Sie zum Bestätigen auf **OK**.

Die RDS-Desktop-Pools sowie die Anwendungspools, die dieser Farm zugeordnet sind, weisen nun den Status „Nicht verfügbar“ auf. Sie können den Status der Pools anzeigen, indem Sie **Katalog > Desktop-Pools** bzw. **Katalog > Anwendungspools** auswählen.

Verwalten von RDS-Hosts

Sie können einen RDS-Host in View Administrator bearbeiten, entfernen, aktivieren und deaktivieren.

Nachdem Sie einen RDS-Host eingerichtet haben, wird er automatisch bei View-Verbindungsserver registriert. Sie können einen RDS-Host nicht manuell bei View-Verbindungsserver registrieren.

Informationen finden Sie unter „Einrichten von Remote-Desktop-Sitzungshosts“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Bearbeiten eines RDS-Hosts

Sie können die Anzahl der Verbindungen ändern, die ein RDS-Host unterstützt. Dies ist die einzige Einstellung, die geändert werden kann. Der Standardwert lautet 150. Sie können ihn auf jede positive Zahl oder auf unbegrenzt setzen.

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration > Registrierte Computer** aus.
- 2 Wählen Sie einen RDS-Host aus und klicken Sie auf **Bearbeiten**.
- 3 Geben Sie einen Wert für die Einstellung **Anzahl der Verbindungen** an.
- 4 Klicken Sie auf **OK**.

Entfernen eines RDS-Hosts von einer Farm

Sie können einen RDS-Host aus einer Farm entfernen, um die Skalierung einer Farm nach unten zu verändern, um Wartungsaufgaben am RDS-Host durchzuführen oder aus anderen Gründen. Es hat sich bewährt, die RDS-Hosts zu deaktivieren und sicherzustellen, dass Benutzer von aktiven Sitzungen abgemeldet sind, bevor Sie einen Host aus einer Farm entfernen.

Sofern Benutzer derzeit mit Anwendungs- oder Desktop-Sitzungen auf diesen Hosts, die Sie entfernen möchten, interagieren, bleiben die Sitzungen aktiv, werden allerdings von View nicht mehr nachverfolgt. Ein Benutzer, der die Verbindung zu einer Sitzung trennt, kann sich anschließend nicht erneut mit ihr verbinden, und sämtliche nicht gespeicherten Daten gehen möglicherweise verloren.

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Farmen**.
- 2 Klicken Sie auf die Registerkarte **RDS-Hosts**.
- 3 Wählen Sie einen oder mehrere RDS-Hosts aus.
- 4 Klicken Sie auf **Von Farm entfernen**.
- 5 Klicken Sie auf **OK**.

Entfernen eines RDS-Hosts aus View

Sie können einen RDS-Host aus View entfernen, den Sie nicht mehr verwenden möchten. Sie können nur RDS-Hosts entfernen, die zu keiner Farm gehören.

Voraussetzungen

Stellen Sie sicher, dass der RDS-Host zu keiner Farm gehört.

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration > Registrierte Computer** aus.
- 2 Wählen Sie einen RDS-Host aus und klicken Sie auf **Entfernen**.

3 Klicken Sie auf **OK**.

Nachdem Sie einen wiederzuverwendenden RDS-Host entfernt haben, müssen Sie View Agent neu installieren. Weitere Informationen finden Sie unter „Einrichten von Remote-Desktop-Sitzungshosts“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Deaktivieren oder Aktivieren eines RDS-Hosts

Wenn Sie einen RDS-Host deaktivieren, wird dieser von View nicht mehr als Host für neue RDS-Desktops oder Anwendungen verwendet. Die Benutzer können weiterhin RDS-Desktops und Anwendungen verwenden, die derzeit geöffnet sind.

Verfahren

- 1 Wählen Sie in View Administrator **View-Konfiguration > Registrierte Computer** aus.
- 2 Wählen Sie einen RDS-Host und klicken Sie auf **Weitere Befehle**.
- 3 Klicken Sie auf **Aktivieren** oder **Deaktivieren**.
- 4 Klicken Sie auf **OK**.

Wenn Sie den RDS-Host aktivieren, wird in der Spalte „Aktiviert“ ein Häkchen angezeigt und in der Spalte „Status“ wird „verfügbar“ angezeigt. Wenn Sie den RDS-Host deaktivieren, bleibt die Spalte „Aktiviert“ leer und in der Spalte „Status“ wird „deaktiviert“ angezeigt.

Überwachen von RDS-Hosts

Sie können den Status von RDS-Hosts überwachen und deren Eigenschaften in View Administrator anzeigen.

Verfahren

- ◆ Navigieren Sie in View Administrator zur Seite mit den Eigenschaften, die Sie anzeigen möchten.

Eigenschaften	Aktion
RDS-Host, Farm, Desktop-Pool, Agent-Version, Sitzungen, Status	<ul style="list-style-type: none"> ■ Wählen Sie in View Administrator Ressourcen > Maschinen aus. ■ Klicken Sie auf die Registerkarte RDS-Hosts.
DNS-Name, Typ, RDS-Farm, Maximale Anzahl an Verbindungen, Agent-Version, Aktiviert, Status	<ul style="list-style-type: none"> ■ Wählen Sie in View Administrator View-Konfiguration > Registrierte Computer aus. ■ Klicken Sie auf die Registerkarte RDS-Hosts.

Die Eigenschaften werden angezeigt und haben folgende Bedeutung:

Eigenschaft	Beschreibung
RDS-Host	Name des RDS-Hosts.
Farm	Farm, zu welcher der RDS-Host gehört.
Desktop-Pool	Der dieser Farm zugewiesene RDS-Desktop-Pool.
Agent-Version	Version des View Agent, der auf dem RDS-Host ausgeführt wird.

Eigenschaft	Beschreibung
Sitzungen	Anzahl der Client-Sitzungen.
DNS-Name	DNS-Name des RDS-Hosts.
Typ	Version von Windows Server, der auf dem RDS-Host ausgeführt wird.
RDS-Farm	Farm, zu welcher der RDS-Host gehört.
Maximale Anzahl an Verbindungen	Maximale Anzahl an Verbindungen, die der RDS-Host unterstützt.
Aktiviert	Angabe, ob der RDS-Host aktiviert ist.
Status	Status des RDS-Hosts. Eine Beschreibung der möglichen Status finden Sie unter Status von RDS-Hosts .

Status von RDS-Hosts

Ein RDS-Host kann sich ab dem Zeitpunkt seiner Initialisierung in verschiedenen Status befinden. Es hat sich bewährt, sicherzustellen, dass sich die RDS-Hosts im erwarteten Status befinden, bevor und nachdem Sie auf ihnen Aufgaben bzw. Vorgänge ausführen.

Tabelle 9-1. Status eines RDS-Hosts

Status	Beschreibung
Starten	View Agent wurde auf dem RDS-Host gestartet, andere erforderliche Dienste (z. B. das Anzeigeprotokoll) werden jedoch gegenwärtig noch gestartet. Während des View Agent-Starts können auch andere Prozesse (z. B. Protokolldienste) gestartet werden.
Deaktivierung wird ausgeführt	Der RDS-Host wird gerade deaktiviert, während Sitzungen immer noch auf dem Host ausgeführt werden. Wenn die Sitzungen beendet werden, ändert sich der Status auf „Deaktiviert“.
Deaktiviert	Das Deaktivieren des RDS-Hosts ist abgeschlossen.
Validierung läuft	Tritt auf, nachdem der View-Verbindungsserver zunächst den RDS-Host erkennt, d. h. in der Regel nach dem Start oder Neustart des View-Verbindungsservers und vor der ersten erfolgreichen Kommunikation mit View Agent auf dem RDS-Host. Der Status ist in der Regel vorübergehend. Bei diesem Status handelt es sich nicht um denselben Agent-Status der Nichterreichbarkeit, der ein Kommunikationsproblem anzeigt.
Agent deaktiviert	Tritt auf, wenn der View-Verbindungsserver den View Agent deaktiviert. Dieser Status stellt sicher, dass keine neue Desktop- oder Anwendungssitzung auf dem RDS-Host gestartet werden kann.
Agent nicht erreichbar	Der View-Verbindungsserver kann mit View Agent nicht auf einem RDS-Host kommunizieren.
Ungültige IP	Die Registrierungseinstellung für die Subnetzmaske ist auf dem RDS-Host konfiguriert, und keine aktiven Netzwerkadapter verfügen über eine IP-Adresse innerhalb des konfigurierten Bereichs.
Agent muss neu gestartet werden	Eine View-Komponente wurde aktualisiert und der RDS-Host muss neu gestartet werden, damit View Agent mit der aktualisierten Komponente interagieren kann.
Protokollfehler	Das RDP-Anzeigeprotokoll wird nicht korrekt ausgeführt. Wenn RDP nicht ausgeführt und PCoIP ausgeführt wird, können Clients weder RDP noch PCoIP verwenden. Wenn RDP jedoch ausgeführt und PCoIP nicht ausgeführt wird, können Clients mithilfe von RDP eine Verbindung herstellen.
Domänenfehler	Beim Erreichen der Domäne durch den RDS-Host ist ein Problem aufgetreten. Es konnte nicht auf den Domänenserver zugegriffen werden oder die Domänenauthentifizierung ist fehlgeschlagen.
Konfigurationsfehler	Die RDS-Rolle ist auf dem Server nicht aktiviert.

Status	Beschreibung
Unbekannt	Der RDS-Host befindet sich in einem unbekannten Status.
Verfügbar	Der RDS-Host ist verfügbar. Wenn sich der Host in einer Farm befindet und die Farm mit einem RDS- oder Anwendungspool verknüpft wird, wird er verwendet, um Benutzern RDS-Desktops oder Anwendungen bereitzustellen.

Konfigurieren der Adobe Flash-Drosselung in Internet Explorer für RDS-Desktops

Um sicherzustellen, dass die Adobe Flash-Drosselung in Internet Explorer für RDS-Desktops funktioniert, müssen Benutzer Browsererweiterungen von Drittanbietern aktivieren.

Verfahren

- 1 Starten Sie Horizon Client und melden Sie sich bei einem Remote-Desktop des Benutzers an.
- 2 Klicken Sie in Internet Explorer auf **Extras > Internetoptionen**.
- 3 Klicken Sie auf die Registerkarte **Erweitert**, wählen Sie **Browsererweiterungen von Drittanbietern aktivieren** und klicken Sie auf **OK**.
- 4 Starten Sie Internet Explorer neu.

Verwalten von ThinApp-Anwendungen in View Administrator

10

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

Zur Verwendung der ThinApp-Verwaltungsfunktion in View 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 Workspace verwenden.

Dieses Kapitel enthält die folgenden Themen:

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

View-Anforderungen für ThinApp-Anwendungen

Beim Erfassen und Speichern von ThinApp-Anwendungen zur Verteilung an Remote-Desktops in View 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 View-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 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-Namespaces 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 View 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 View 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. View 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 View Administrator an Remote-Desktops und -Pools verteilt werden, müssen Sie eine Windows-Netzwerkfreigabe erstellen.

3 Registrieren eines Anwendungs-Repositorys

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

4 Hinzufügen von ThinApp-Anwendungen zu View Administrator

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

5 Erstellen einer ThinApp-Vorlage

Sie können in View 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
```

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 View Administrator an Remote-Desktops und -Pools verteilt werden, müssen Sie eine Windows-Netzwerkfreigabe erstellen.

Voraussetzungen

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

Verfahren

- 1 Erstellen Sie eine Ordnerfreigabe auf einem Computer in einer Active Directory-Domäne, auf die Ihr View-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 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 View Administrator.

Registrieren eines Anwendungs-Repositorys

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

Sie können auch mehrere Anwendungs-Repositorys registrieren.

Voraussetzungen

Erstellen Sie eine Windows-Netzwerkfreigabe.

Verfahren

- 1 Wählen Sie in View 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 View Administrator zu registrieren.

Hinzufügen von ThinApp-Anwendungen zu View Administrator

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

Voraussetzungen

Registrieren Sie ein Anwendungs-Repository mit View Administrator.

Verfahren

- 1 Wählen Sie in View 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 View 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**.

View Administrator zeigt den Status der einzelnen Suchvorgänge und die Anzahl an ThinApp-Anwendungen an, die zu View Administrator hinzugefügt wurden. Bei Auswahl einer Anwendung, die sich bereits in View Administrator befindet, wird diese nicht erneut hinzugefügt.
- 6 Klicken Sie auf **Fertig stellen**.

Die neuen ThinApp-Anwendungen werden auf der Registerkarte **Übersicht** angezeigt.

Nächste Schritte

(Optional) Erstellen Sie ThinApp-Vorlagen.

Erstellen einer ThinApp-Vorlage

Sie können in View 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 View 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 View 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 View Administrator hinzu.

Verfahren

- 1 Wählen Sie in View 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 View Administrator einer Maschine oder einem Desktop-Pool zu.

Wenn Sie einer Maschine eine ThinApp-Anwendung zuweisen, beginnt View Administrator wenige Minuten später mit der Installation der Anwendung auf der virtuellen Maschine. Wenn Sie einem Desktop-Pool eine ThinApp-Anwendung zuweisen, beginnt View Administrator mit der Installation der Anwendung, sobald sich ein Benutzer erstmalig bei einem Remote-Desktop im Pool anmeldet.

Streaming	View 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	View 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 RDS-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 View 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 View 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. View 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

Durchsuchen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu View Administrator hinzu. Siehe [Hinzufügen von ThinApp-Anwendungen zu View Administrator](#).

Verfahren

- 1 Wählen Sie in View 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.

View Administrator beginnt wenige Minuten später mit der Installation der ThinApp-Anwendung. Nach der Installation steht die Anwendung allen Benutzern der Remote-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

Durchsuchen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu View Administrator hinzu. Siehe [Hinzufügen von ThinApp-Anwendungen zu View Administrator](#).

Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Computer** 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.

View Administrator beginnt wenige Minuten später mit der Installation der ThinApp-Anwendungen. Nach der Installation stehen die Anwendungen allen Benutzern des Remote-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 View Administrator die Anwendung erneut. Eine manuelle Neuinstallation der Anwendung ist nicht erforderlich.

Voraussetzungen

Durchsuchen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu View Administrator hinzu. Siehe [Hinzufügen von ThinApp-Anwendungen zu View Administrator](#).

Verfahren

- 1 Wählen Sie in View Administrator **Katalog > ThinApps** und anschließend die ThinApp-Anwendung aus.

- 2 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 .

- 3 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.

- 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.

View 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 View Administrator die Anwendung erneut. Eine manuelle Neuinstallation der Anwendung ist nicht erforderlich.

Voraussetzungen

Durchsuchen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu View Administrator hinzu. Siehe [Hinzufügen von ThinApp-Anwendungen zu View Administrator](#).

Verfahren

- 1 Wählen Sie in View 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.

View 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 View 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 View 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.

Wenn Sie einer Maschine eine ThinApp-Vorlage zuweisen, beginnt View Administrator wenige Minuten später mit der Installation der in der Vorlage enthaltenen Anwendungen. Wenn Sie einem Desktop-Pool eine ThinApp-Vorlage zuweisen, beginnt View 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 View 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> <hr/> <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 View Administrator den Status der Installation an.

[Tabelle 10-1. Installationsstatus für ThinApp-Anwendungen](#) beschreibt die einzelnen Statuswerte.

Tabelle 10-1. Installationsstatus für ThinApp-Anwendungen

Status	Beschreibung
Zugewiesen	Die ThinApp-Anwendung wurde dem Computer zugewiesen.
Fehler bei der Installation	Als View Administrator versucht hat, die ThinApp-Anwendung zu installieren, ist ein Fehler aufgetreten.
Fehler bei der Deinstallation	Als View Administrator versucht hat, die ThinApp-Anwendung zu deinstallieren, ist ein Fehler aufgetreten.
Installiert	Die ThinApp-Anwendung wurde installiert.

Status	Beschreibung
Ausstehende Installation	View 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	View Administrator versucht, die ThinApp-Anwendung zu deinstallieren.

Anzeigen von MSI-Paketinformationen

Nach dem Hinzufügen einer ThinApp-Anwendung zu View Administrator können Sie Informationen zu den MSI-Paketen anzeigen.

Verfahren

- 1 Wählen Sie in View 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**.

Warten von ThinApp-Anwendungen in View Administrator

Das Verwalten von ThinApp-Anwendungen in View 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 View Administrator**

Wenn Sie eine ThinApp-Anwendung aus View 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 View 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 View 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.

View Administrator beginnt wenige Minuten später mit der Deinstallation der ThinApp-Anwendung.

Wichtig Wenn ein Endbenutzer die ThinApp-Anwendung verwendet, während View Administrator versucht, die Anwendung zu deinstallieren, schlägt die Deinstallation fehl und der Anwendungsstatus ändert sich in Uninstall Error (Fehler bei der Deinstallation). Wenn dieser Fehler auftritt, müssen Sie die ThinApp-Anwendungsdateien zunächst manuell von dem Computer deinstallieren und anschließend in View Administrator auf **Löschen der Zuweisung erzwingen** 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 View Administrator **Ressourcen > Computer** und doppelklicken Sie in der Spalte „Computer“ auf den Namen des Computers.
- 2 Wählen Sie auf der Registerkarte **Übersicht** die ThinApp-Anwendung und klicken Sie im ThinApps-Fensterbereich auf **Zuweisung entfernen**.

Wiederholen Sie diesen Schritt, um eine weitere Anwendungszuweisung zu entfernen.

View Administrator beginnt wenige Minuten später mit der Deinstallation der ThinApp-Anwendung.

Wichtig Wenn ein Endbenutzer die ThinApp-Anwendung verwendet, während View 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 von dem Computer deinstallieren und anschließend in View Administrator auf **Löschen der Zuweisung erzwingen** 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 View 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.

View 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 View 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.

View Administrator deinstalliert die ThinApp-Anwendungen, wenn ein Benutzer sich das erste Mal bei einem Remote-Desktop im Pool anmeldet.

Entfernen einer ThinApp-Anwendung aus View Administrator

Wenn Sie eine ThinApp-Anwendung aus View 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 View 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 View 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 View 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 View 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 View Administrator kann nicht geändert werden.

Verfahren

- 1 Wählen Sie in View 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 View Administrator

View Administrator protokolliert mit der ThinApp-Anwendungsverwaltung verbundene Ereignisse in der Datenbank für Ereignisse und Berichterstellung. Diese Ereignisse werden in View 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 View Administrator entfernt
- Eine ThinApp-Anwendung wird zu View 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 View Administrator registrieren.

Problem

Beim Versuch, ein Anwendungs-Repository in View Administrator zu registrieren, wird eine Fehlermeldung ausgegeben.

Ursache

Der View-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 View-Verbindungsserver-Host aus zugegriffen werden kann, oder die Berechtigungen für die Netzwerkfreigabe wurden nicht ordnungsgemäß eingerichtet.

- 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 View-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 View Administrator möglich

View Administrator kann keine ThinApp-Anwendungen zu View Administrator zuweisen.

Problem

Beim Klicken auf **Neue ThinApps untersuchen** in View Administrator sind keine MSI-Pakete verfügbar.

Ursache

Die Anwendungspakete liegen entweder nicht im MSI-Format vor oder der View-Verbindungsserver-Host kann nicht auf die Verzeichnisse auf der Netzwerkfreigabe zugreifen.

- Stellen Sie sicher, dass die Anwendungspakete im Anwendungs-Repository im MSI-Format vorliegen.
- Stellen Sie sicher, dass die Netzwerkfreigabe die View-Anforderungen für ThinApp-Anwendungen erfüllt. Weitere Informationen finden Sie unter [View-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 View-Verbindungsserver aufgeführt. View-Verbindungsserver-Protokolldateien befinden sich auf dem View-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

View 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.

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

View 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 View-Verbindungsserver-Host und Computer bzw. zwischen View-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 View Agent- und View-Verbindungsserver-Protokolldateien finden Sie weitere Informationen zur Ursache des Problems.

View 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).

View-Verbindungsserver-Protokolldateien befinden sich auf dem View-Verbindungsserver-Host im Verzeichnis *Laufwerk:*\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs.

Lösung

- 1 Wählen Sie in View 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

View 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 View Administrator versucht hat, sie zu deinstallieren.
- Die Netzwerkverbindung zwischen View-Verbindungsserver-Host und Computer wurde getrennt.

In den View Agent- und View-Verbindungsserver-Protokolldateien finden Sie weitere Informationen zur Ursache des Problems.

View 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).

View-Verbindungsserver-Protokolldateien befinden sich auf dem View-Verbindungsserver-Host im Verzeichnis *Laufwerk:*\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs.

Lösung

- 1 Wählen Sie in View 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 **Löschen der Zuweisung erzwingen**.

Über diesen Befehl wird die ThinApp-Anwendungszuweisung in View 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

View Administrator meldet ein ungültiges MSI-Paket in einem Anwendungs-Repository.

Problem

View 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 paketierte. Sie müssen ThinApp Version 4.6 oder höher verwenden.

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.

View 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 View-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 View Administrator.
- 6 Durchsuchen Sie die MSI-Pakete im Anwendungs-Repository in View Administrator und fügen Sie ausgewählte ThinApp-Anwendungen zu View 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 Pool-Zuweisungen schnell an bestimmte Abteilungen oder Benutzer verteilen.

- 8 Wählen Sie in View 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 View Administrator den Installationsstatus der ThinApp-Anwendungen.

Einrichten von Clients im Kiosk-Modus

11

Sie können unbeaufsichtigte Clients einrichten, die über View 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 View-Verbindungsserver-Instanz herzustellen und eine Remote-Sitzung zu starten. Endbenutzer müssen sich typischerweise nicht für den Zugriff auf das Clientgerät anmelden. Der Remote-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 Umleitung von USB-Geräten an die Remote-Sitzung und die standortbasierte Druckfunktion.

View verwendet die Funktion zur flexiblen Authentifizierung in View 4.5 und höher, um anstelle des Endbenutzers ein Client-Gerät im Kiosk-Modus zu authentifizieren. Eine View-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 View-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 View 4.5 und höher nicht zulässig.

Die empfohlene Vorgehensweise ist das Verwenden dedizierter View-Verbindungsserver-Instanzen zur Verarbeitung von Clients im Kiosk-Modus und das Erstellen dedizierter Organisationseinheiten und Gruppen in Active Directory für die Konten dieser Clients. 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 View 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 View 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 View 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 View-Verbindungsserver-Gruppe hinzugefügt werden. Nach dem Hinzufügen eines Clients kann dieser mit einer View-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 View-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 View-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 View 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.

View 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 View Administrator den von den Clients verwendeten Desktop-Pool und berechnen 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 Berechnen Sie einen Client oder eine Gruppe nicht für mehrere Desktop-Pools. Anderenfalls weist View nach dem Zufallsprinzip einen Remote-Desktop aus den Pools zu, für die ein Client berechnen ist, und es wird eine Warnung generiert.

- 5 Wenn für die Clients der standortbasierte Druck eingerichtet werden soll, konfigurieren Sie die Active Directory-Gruppenrichtlinieneinstellung Automatische standortbasierte Druckfunktion für 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 View-Verbindungsserver-Instanzen in der Gruppe mit der View-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 View-Verbindungsserver-Instanzen innerhalb einer Gruppe verwendet.

Verfahren

- ◆ Legen Sie die Standardwerte für Clients fest.

```
vdmadmin
-Q
-clientauth
-setdefaults [-b authentication_arguments] [-ouDN] [ -expirepassword | -noexpirepassword ]
[-groupgroup_name | -nogroup]
```

Option	Beschreibung
<code>-expirepassword</code>	Gibt an, dass die Ablaufzeit für Kennwörter der Clientkonten mit der Ablaufzeit für die View-Verbindungsserver-Gruppe übereinstimmt. Wenn für die Gruppe keine Ablaufzeit definiert ist, laufen Kennwörter nicht ab.
<code>-group Gruppenname</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 DN</code>	Specifies the distinguished name of the default organizational unit to which client accounts are added. For example: OU=kiosk-ou,DC=myorg,DC=com Hinweis You cannot use the command to change the configuration of an organizational unit.

The command updates the default values for clients in the View Connection Server group.

Beispiel: Setting Default Values for Cients in Kiosk Mode

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

Nächste Schritte

Find out the MAC addresses of client devices that use their MAC address for authentication.

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 View-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 View-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 `vdadmin` können Clientkonten zur Konfiguration einer View-Verbindungsserver-Gruppe hinzugefügt werden. Nach dem Hinzufügen eines Clients kann dieser mit einer View-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 `vdadmin` muss für eine der View-Verbindungsserver-Instanzen in der Gruppe mit der View-Verbindungsserver-Instanz ausgeführt werden, welche die Clients zum Herstellen einer Verbindung mit ihren Remote-Desktops verwenden.

Beim Hinzufügen von Clients im Kiosk-Modus erstellt View ein Benutzerkonto für den Client in Active Directory. Wenn Sie für einen Client einen Namen angeben, muss dieser Name mit einer bekannten 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 View einen Namen aus der für das Clientgerät angegebenen MAC-Adresse. Wenn die MAC-Adresse beispielsweise 00:10:db:ee:76:80 lautet, wird der Kontoname cm-00_10_db_ee_76_80 generiert. Diese Konten können nur mit View-Verbindungsserver-Instanzen verwendet werden, die für die Authentifizierung von Clients aktiviert sind.

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 [-bauthentication_arguments] -domaindomain_name-clientidclient_id [-password
"password" | -genpassword] [-ouDN] [-expirepassword | -noexpirepassword] [-groupgroup_name | -nogroup]
[-description "description_text"]
```

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 View-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.

Option	Beschreibung
-ou <i>DN</i>	Specifies the distinguished name of the organizational unit to which the client's account is added. For example: OU=kiosk-ou,DC=myorg,DC=com
-password "<i>password</i>"	Specifies an explicit password for the client's account.

The command creates a user account in Active Directory for the client in the specified domain and group (if any).

Beispiel: Adding Accounts for Clients

Add an account for a client specified by its MAC address to the MYORG domain, using the default settings for the group kc-grp.

```
vdadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

Add an account for a client specified by its MAC address to the MYORG domain, using an automatically generated password.

```
vdadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword
```

Add an account for a named client, and specify a password to be used with the client.

```
vdadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Add an account for a named client, using an automatically generated password.

```
vdadmin -Q -clientauth -add -domain MYORG -clientid custom-Kiosk11 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Kiosk 11"
```

Nächste Schritte

Enable authentication of the clients.

Authentifizierung von Clients im Kiosk-Modus aktivieren

Mithilfe des Befehls `vdadmin` kann die Authentifizierung von Clients aktiviert werden, die versuchen, über eine View-Verbindungsserver-Instanz eine Verbindung mit ihren Remote-Desktops herzustellen.

Der Befehl `vdadmin` muss für eine der View-Verbindungsserver-Instanzen in der Gruppe mit der View-Verbindungsserver-Instanz ausgeführt werden, welche die Clients zum Herstellen einer Verbindung mit ihren Remote-Desktops verwenden.

Wenngleich die Authentifizierung für eine einzelne View-Verbindungsserver-Instanz aktiviert wird, gelten die anderen Einstellungen für die Clientauthentifizierung für alle View-Verbindungsserver-Instanzen innerhalb einer Gruppe. Das Konto für einen Client muss nur einmal hinzugefügt werden. Alle aktivierten View-Verbindungsserver-Instanzen innerhalb einer View-Verbindungsserver-Gruppe können den Client authentifizieren.

Wenn Sie den Kiosk-Modus zusammen mit einem sitzungsbasierten View-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 View-Verbindungsserver-Instanz.

```
vdmadmin
-Q
-enable [-bauthentication_arguments] -sconnection_server [-requirepassword]
```

Option	Beschreibung
-requirepassword	Gibt an, dass Clients Kennwörter angeben müssen. Wichtig Bei Angabe dieser Option kann die View-Verbindungsserver-Instanz keine Clients authentifizieren, die über automatisch generierte Kennwörter verfügen. Wenn Sie die Konfiguration einer View-Verbindungsserver-Instanz ändern und diese Option angeben, können diese Clients nicht authentifiziert werden und der Fehler <code>Unknown username or bad password</code> (Unbekannter Benutzername oder falsches Kennwort) wird ausgegeben.
-s connection_server	Gibt den NetBIOS-Namen der View-Verbindungsserver-Instanz an, für welche die Authentifizierung von Clients aktiviert werden soll.

Der Befehl aktiviert die angegebene View-Verbindungsserver-Instanz für die Authentifizierung von Clients.

- 2 Wenn der Remote-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 View Server dem Benutzerkonto `custom-11` die Berechtigung für einen sitzungsbasierten View-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 View-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 View-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 View-Verbindungsserver-Instanzen und Clients.

Überprüfen der Konfiguration von Clients im Kiosk-Modus

Mithilfe des Befehls `vdadmin` können Informationen zu Clients im Kiosk-Modus und zu View-Verbindungsserver-Instanzen angezeigt werden, die zur Authentifizierung dieser Clients konfiguriert sind.

Der Befehl `vdadmin` muss für eine der View-Verbindungsserver-Instanzen in der Gruppe mit der View-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.

```
vdadmin
-Q
-clientauth
-list [-b authentication_arguments] [-xml]
```

Der Befehl zeigt Informationen zu Clients im Kiosk-Modus und zu den View-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 View-Verbindungsserver-Instanz CONSVR2 akzeptiert Authentifizierungsanforderungen von Clients mit automatisch generierten Kennwörtern. CONSVR1 akzeptiert keine Authentifizierungsanforderungen von Clients im Kiosk-Modus.

```
C:\> vdadmin -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 OS X-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>Verbindungsserver</i> Gibt die IP-Adresse oder den FQDN der View-Verbindungsserver-Instanz an, die Horizon Client zur Herstellung einer Verbindung mit einem Remote-Desktop verwendet. Wenn Sie die IP-Adresse oder den FQDN der View-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 View-Verbindungsserver-Instanz.</p> <p>-userName<i>Benutzername</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.</p>
Linux	<p>Geben Sie vmware-view --unattended -s <i>Verbindungsserver</i> [--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. Anderenfalls 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 View-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 bei View

Zur Diagnose und Behandlung von Problemen bei der Verwendung von View können Sie zwischen verschiedenen Vorgehensweisen wählen. Sie können die Vorgehensweisen zur Fehlerbehebung nutzen, um die Ursachen dieser Probleme zu ermitteln. Anschließend können Sie versuchen, die Probleme selbst zu behandeln, oder sich an den technischen Support von VMware wenden, um Unterstützung zu erhalten.

Informationen zur Fehlerbehebung bei Desktop-Pools finden Sie im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Dieses Kapitel enthält die folgenden Themen:

- [Überwachen des Systemzustands](#)
- [Überwachen von Ereignissen in View](#)
- [Sammeln von Diagnoseinformationen für View](#)
- [Aktualisieren von Supportanfragen](#)
- [Fehlerbehebung einer nicht erfolgreichen Sicherheitsserver-Kombination mit View-Verbindungsserver](#)
- [Fehlerbehebung der View Server-Zertifikatssperrüberprüfung](#)
- [Fehlerbehebung bei der Smartcard-Zertifikatssperrüberprüfung](#)
- [Weitere Informationen zur Fehlerbehebung](#)

Überwachen des Systemzustands

Mithilfe des Dashboards zum Systemzustand in View Administrator können Sie rasch Probleme ermitteln, die sich auf die Ausführung von View oder den Benutzerzugriff auf Remote-Desktops auswirken können.

Das Dashboard zum Systemzustand befindet sich oben links in der View Administrator-Anzeige und bietet verschiedene Links, um Berichte zur Ausführung von View 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 View 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 View 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 der Status von View-Komponenten, vSphere-Komponenten, Domänen, Desktops und Informationen zur Datenspeichernutzung zusammengefasst 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 View

In der Ereignisdatenbank werden Informationen zu Ereignissen gespeichert, die im View-Verbindungsserver-Host oder in der View Connection Server-Gruppe, in den View Agent-Instanzen und in View Administrator auftreten. Sie werden im Dashboard über die Anzahl an Ereignissen benachrichtigt. Im Ereignisbildschirm können Sie die Ereignisse im Detail untersuchen.

Hinweis Ereignisse werden in der View Administrator-Oberfläche 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 *Integration von View*.

Neben der Überwachung von Ereignissen in View Administrator können Sie View-Ereignisse im SysLog-Format generieren, sodass die Analysesoftware auf die Ereignisdaten zugreifen kann. Weitere Informationen finden Sie unter [Generieren von View-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-l“](#) und „Konfigurieren der Ereignisprotokollierung für Syslog-Server“ im Dokument *Installation von View*.

Voraussetzungen

Erstellen und konfigurieren Sie die Ereignisdatenbank. Die erforderlichen Schritte sind im Dokument *Installation von View* beschrieben.

Verfahren

- 1 Wählen Sie in View 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.

View-Ereignismeldungen

View 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.

[Tabelle 12-1. Von View angezeigte Ereignistypen](#) zeigt die Ereignistypen, die in View angezeigt werden.

Tabelle 12-1. Von View 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 View vornimmt.
Fehler	Zeigt einen fehlgeschlagenen View-Vorgang an.
Information	Zeigt normale Vorgänge innerhalb von View 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 View

Sie können Diagnoseinformationen sammeln, um den technischen Support von VMware bei der Diagnose und Behandlung von Problemen mit View zu unterstützen.

Sie können Diagnoseinformationen für verschiedene View-Komponenten sammeln. Wie diese Informationen gesammelt werden, ist je nach View-Komponente unterschiedlich.

- [Erstellen eines Data Collection Tool-Pakets für View Agent](#)

Um den technischen Support von VMware bei der Fehlerbehebung für View Agent zu unterstützen, müssen Sie möglicherweise den Befehl `vdmaadmin` zum Erstellen eines DCT-Pakets (Data Collection Tool) verwenden. Sie können das DCT-Paket auch manuell abrufen, ohne `vdmaadmin` zu verwenden.

- [Speichern von Diagnoseinformationen für Horizon Client](#)

Wenn bei Verwendung von Horizon Client Probleme auftreten, die sich mithilfe der allgemeinen Verfahren zur Behandlung von Netzwerkproblemen nicht lösen lassen, können Sie eine Kopie der Protokolldateien und 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 View-Verbindungsserver mithilfe des Supporttools](#)

Mithilfe des Supporttools können Sie Protokollierungsebenen festlegen und Protokolldateien für View-Verbindungsserver generieren.

- [Sammeln von Diagnoseinformationen für View Agent, Horizon Client oder View-Verbindungsserver von der Konsole](#)

Wenn Sie über direkten Zugriff auf die Konsole verfügen, können Sie die Supportskripts zur Generierung von Protokolldateien für View-Verbindungsserver, Horizon Client oder für Remote-Desktops verwenden, auf denen View 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 View Agent

Um den technischen Support von VMware bei der Fehlerbehebung für View 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 View-Verbindungsserver-Instanz verwenden, um ein DCT-Paket von einem Remote-Desktop anzufordern. Das Paket wird an View-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 das Betriebssystem des Remote-Desktops Windows 8 oder Windows 7 ist und die Benutzerkontensteuerung (User Account Control, UAC) aktiviert ist, müssen Sie das DCT-Paket auf diese Weise abrufen.

Verfahren

- 1 Melden Sie sich als Benutzer mit entsprechenden Rechten an.

Option	Aktion
Auf View-Verbindungsserver mit „vdmadmin“	Melden Sie sich an einer Standard- oder Replikatinstanz des View-Verbindungs_servers als Benutzer mit der Rolle Administratoren an.
Auf dem Remote-Desktop	Melden Sie sich auf dem Remote-Desktop als Benutzer mit Administratorrechten an.

- Öffnen Sie eine Eingabeaufforderung und führen Sie den Befehl zum Generieren des DCT-Pakets aus.

Option	Aktion
Auf View-Verbindungsserver mit „vdmadmin“	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 [-bauthentication_arguments] -getDCT-outfile local_file-ddesktop-mmachine</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>

Der Befehl schreibt das Paket in die angegebene Ausgabedatei.

Beispiel: Beispiel für die Verwendung von „vdmadmin“ zum Erstellen einer Paketdatei für View 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

Wenn bei Verwendung von Horizon Client Probleme auftreten, die sich mithilfe der allgemeinen Verfahren zur Behandlung von Netzwerkproblemen nicht lösen lassen, können Sie eine Kopie der Protokolldateien und Informationen zur Konfiguration speichern.

Sie können versuchen, Verbindungsprobleme mit Horizon Client zu lösen, bevor Sie die Diagnoseinformationen speichern und sich an den technischen Support von VMware wenden. Weitere Informationen finden Sie unter „Verbindungsprobleme zwischen View Client und View-Verbindungsserver“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Verfahren

- Klicken Sie in Horizon Client auf **Supportinformationen** oder wählen Sie im Remote-Desktop-Menü **Optionen > Supportinformationen** aus.
- 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 View-Verbindungsserver-Instanzen ein, für die Sie die Konfiguration von Horizon Client testen möchten. Aktivieren Sie ggf. die Option zum Generieren von Diagnose-Dumps der View-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 View-Verbindungsserver mithilfe des Supporttools

Mithilfe des Supporttools können Sie Protokollierungsebenen festlegen und Protokolldateien für View-Verbindungsserver generieren.

Das Supporttool sammelt Protokollierungsdaten für View-Verbindungsserver. Diese Informationen erleichtern den Mitarbeitern des technischen Supports von VMware die Diagnose von Problemen im Zusammenhang mit View-Verbindungsserver. Das Supporttool ist nicht geeignet, um Diagnoseinformationen für Horizon Client oder View Agent zu sammeln. Für diese Komponenten muss stattdessen das Supportskript verwendet werden. Siehe [Sammeln von Diagnoseinformationen für View Agent, Horizon Client oder View-Verbindungsserver von der Konsole](#).

Voraussetzungen

Melden Sie sich bei einer Standard- oder Replikatinstanz des View-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 View-Verbindungservers 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 View-Verbindungsserver-Instanz.

- 4 Senden Sie über die Supportseite der VMware-Website eine Supportanfrage und fügen Sie die Ausgabedateien an.

Sammeln von Diagnoseinformationen für View Agent, Horizon Client oder View-Verbindungsserver von der Konsole

Wenn Sie über direkten Zugriff auf die Konsole verfügen, können Sie die Supportskripts zur Generierung von Protokolldateien für View-Verbindungsserver, Horizon Client oder für Remote-Desktops verwenden, auf denen View 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 View Agent melden Sie sich an der virtuellen Maschine an, auf der View Agent installiert ist.
- Melden Sie sich für Horizon Client beim System mit installiertem Horizon Client an.
- Für View-Verbindungsserver melden Sie sich am View-Verbindungsserver-Host an.

Verfahren

- 1 Öffnen Sie ein Eingabeaufforderungsfenster und wechseln Sie in das entsprechende Verzeichnis der View-Komponente, für die Diagnoseinformationen gesammelt werden sollen.

Option	Beschreibung
View 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 View Agent und Horizon Client).
5	Legt die Debug-Protokollierung für PCoIP fest (nur bei View Agent und Horizon Client).
6	Legt die Protokollierung von Informationen für virtuelle Kanäle fest (nur bei View Agent und Horizon Client).
7	Legt die Debug-Protokollierung für virtuelle Kanäle fest (nur bei View Agent und Horizon Client).
8	Legt die Ablaufprotokollierung für virtuelle Kanäle fest (nur bei View 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.

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 Supportanfragenummer 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 Sicherheitsserver-Kombination mit View-Verbindungsserver

Ein Sicherheitsserver funktioniert womöglich nicht, wenn keine erfolgreiche Kombination mit einer View-Verbindungsserver-Instanz erfolgte.

Problem

Es können die folgenden Sicherheitsserverprobleme auftreten, wenn ein Sicherheitsserver keine Kombination mit View-Verbindungsserver herstellen konnte:

- Wenn Sie versuchen, den Sicherheitsserver ein zweites Mal zu installieren, kann sich der Sicherheitsserver nicht mit View-Verbindungsserver verbinden.

- Horizon Client kann sich nicht mit View verbinden. Die folgende Fehlermeldung wird angezeigt: Die Authentifizierung der View-Verbindungsserver-Instanz 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 View 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.

Wenn Sie beabsichtigen, den Sicherheitsserver in Ihrer View-Umgebung zu behalten, führen Sie folgende Schritte aus:

- 1 Wählen Sie in View 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 View-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 View-Umgebung zu entfernen, führen Sie den Befehl `vdmadmin -S` aus.

Beispiel: `vdmadmin -S -r -s security_server_name`

Fehlerbehebung der View Server-Zertifikatssperrüberprüfung

Ein Sicherheitsserver oder eine View-Verbindungsserver-Instanz, die für sichere Horizon Client-Verbindungen verwendet wird, kann in View Administrator rot angezeigt werden, wenn eine Zertifikatssperrüberprüfung beim SSL-Zertifikat des Servers nicht durchgeführt werden kann.

Problem

Ein Sicherheitsserver- oder View-Verbindungsserver-Symbol ist im View Administrator-Dashboard rot. Der Status des View-Servers meldet Folgendes: Das Serverzertifikat kann nicht geprüft werden.

Ursache

Die Zertifikatssperrüberprüfung kann fehlschlagen, wenn Ihr Unternehmen für den Internetzugriff einen Proxy-Server verwendet oder wenn eine View-Verbindungsserver-Instanz die Server, die die Sperrüberprüfung durchführen, aufgrund von Firewalls oder anderen Kontrollen nicht erreichen kann.

Eine View-Verbindungsserver-Instanz führt die Zertifikatssperrüberprüfung für ihr eigenes Zertifikat und für das der Sicherheitsserver durch, die mit ihr kombiniert sind. Der VMware View-Verbindungsserver-Dienst wird standardmäßig mit dem Konto LocalSystem gestartet. Wenn sie unter LocalSystem ausgeführt wird, kann eine View-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 View-Verbindungsserver-Instanz zu importieren, sodass der Server auf die Websites für die Zertifikatssperrüberprüfung im Internet zugreifen kann.

Lösung

- 1 Öffnen Sie auf dem View-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 View-Verbindungsserver-Computer keine Verbindung zum Internet herstellen, wenn Ihr Unternehmen 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 View-Verbindungsserver-Computer importiert.

- 6 Überprüfen Sie die Proxy-Einstellungen durch Eingabe von **show proxy**.
- 7 Restart the VMware Horizon View-Verbindungsserver service.
- 8 Überprüfen Sie im View Administrator-Dashboard, dass das Sicherheitsserver- oder View-Verbindungsserver-Symbol grün ist.

Fehlerbehebung bei der Smartcard-Zertifikatssperrüberprüfung

Die View-Verbindungsserver-Instanz oder der Sicherheitsserver, mit der bzw. dem die Smartcard verbunden ist, kann die Zertifikatssperrüberprüfung für das SSL-Zertifikat des Servers nur dann durchführen, wenn Sie die Smartcard-Zertifikatssperrüberprüfung konfiguriert haben.

Problem

Die Zertifikatssperrüberprüfung kann fehlschlagen, wenn Ihr Unternehmen für den Internetzugriff einen Proxy-Server verwendet oder wenn eine View-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 Zertifikatssperrlistendatei auf dem neuesten Stand ist.

Ursache

View unterstützt die Zertifikatssperrüberprüfung mit Zertifikatssperrlisten und dem Online Certificate Status Protocol (OCSP). Eine Zertifikatssperrliste ist eine Liste mit gesperrten Zertifikaten, die von der Zertifizierungsstelle veröffentlicht wird, die das Zertifikat ausgestellt hat. OCSP ist ein Zertifikatüberprüfungsprotokoll, das zum Abrufen des Sperrstatus eines X.509-Zertifikats verwendet wird. Der Zugriff auf die Zertifizierungsstelle muss über den View-Verbindungsserver- oder Sicherheitsserverhost möglich sein. Dieses Problem kann nur auftreten, wenn Sie die Zertifikatssperrüberprüfung für Smartcard-Zertifikate konfiguriert haben. Siehe [Verwenden der Smartcard-Zertifikatssperrüberprüfung](#).

Lösung

- 1 Erstellen Sie eine eigene (manuelle) Vorgehensweise für das Herunterladen einer aktuellen Zertifikatssperrliste von der Website der Zertifizierungsstelle in ein Verzeichnis auf Ihrem View Server.
- 2 Erstellen oder bearbeiten Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf dem View-Verbindungsserver- oder dem Sicherheitsserverhost.

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 Zertifikatssperrliste gespeichert ist.
- 4 Starten Sie den View-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 View finden Sie in den KB-Artikeln auf der VMware KB-Website:

<http://kb.vmware.com/selfservice/microsites/microsite.do>

Verwenden des Befehls „vdmadmin“

13

Über den Befehl `vdmadmin` kann eine Vielzahl von Verwaltungsaufgaben für eine View-Verbindungsserver-Instanz ausgeführt werden.

Mithilfe von `vdmadmin` ist das Ausführen von Verwaltungsaufgaben möglich, die nicht über die View Administrator-Benutzeroberfläche ausgeführt werden können oder die automatisch über Skripts ausgeführt werden müssen.

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

- **Verwendung des Befehls „vdmadmin“**

Die Syntax des Befehls `vdmadmin` bestimmt seine Ausführung.

- **Konfigurieren der Protokollierung in View Agent unter Verwendung der Option „-A“**

Sie können den Befehl `vdmadmin` mit der Option `-A` verwenden, um die Protokollierung in View Agent zu konfigurieren.

- **Außerkräftsetzen von IP-Adressen unter Verwendung der Option „-A“**

Sie können den Befehl `vdmadmin` mit der Option `-A` verwenden, um die von einer View Agent-Instanz angegebene IP-Adresse außer Kraft zu setzen.

- **Festlegen des Namens einer View-Verbindungsserver-Gruppe unter Verwendung der Option „-C“**

Sie können den Befehl `vdmadmin` mit der Option `-C` verwenden, um den Namen einer View Connection Server-Gruppe festzulegen. Zur Identifizierung der Gruppe in Microsoft System Center Operations Manager (SCOM) wird dieser Name in der SCOM-Konsole angezeigt.

- **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 unter Verwendung der Option „-H“**

Mithilfe der Option `-H` des Befehls `vdmadmin` können die vorhandenen Systemüberwachungen angezeigt werden, um Instanzen für View-Komponenten zu überwachen und die Einzelheiten für eine bestimmte Systemüberwachung oder eine bestimmte Überwachungsinstanz anzuzeigen.

- **Auflisten und Anzeigen von Berichten zum View-Betrieb unter Verwendung der Option „-I“**

Sie können den Befehl `vdmadmin` mit der Option `-I` verwenden, um die verfügbaren Berichte zum View-Betrieb aufzulisten und die Ergebnisse beim Ausführen eines dieser Berichte anzuzeigen.

- **Generieren von View-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-I“**

Sie können den Befehl `vdmadmin` zusammen mit der Option `-I` verwenden, um View-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 unter Verwendung 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 mit 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. View 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 View Administrator angegeben ist.

- **Konfigurieren von Domänenfiltern unter Verwendung der Option „-N“**

Sie können den Befehl `vdmadmin` mit der Option `-N` zum Steuern der Domänen verwenden, die View für die Endbenutzer zur Verfügung stellt.

- **Konfigurieren von Domänenfiltern**

Domänenfilter können Sie zur Einschränkung der Anzahl der Domänen, die eine View-Verbindungsserver-Instanz oder ein Sicherheitsserver den Endbenutzern zur Verfügung stellt, konfigurieren.

- **Anzeigen der Maschinen und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“**

Sie können den Befehl `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.

- **Konfigurieren von Clients im Kiosk-Modus unter Verwendung 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 unter Verwendung 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 View-Verbindungsserver-Instanz oder einen Sicherheitsserver mit der Option „-S“**

Sie können den Befehl `vdmadmin` mit der Option `-S` verwenden, um den Eintrag für eine View-Verbindungsserver-Instanz oder einen Sicherheitsserver aus der View-Konfiguration zu entfernen.

- **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 unter Verwendung der Option „-V“**

Sie können den Befehl `vdmadmin` mit der Option `-V` verwenden, um virtuelle Maschinen im Rechenzentrum zu sperren oder zu entsperren.

- **Ermitteln und Lösen von Konflikten bei LDAP-Einträgen mit der Option „-X“**

Sie können den Befehl `vdmadmin` mit der Option `-X` verwenden, um Konflikte bei LDAP-Einträgen auf replizierten View-Verbindungsserver-Instanzen in einer Gruppe zu ermitteln und zu 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
command_option [additional_optionargument] ...
```

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 View Administrator verwenden, um einem Benutzer die Rolle **Administrators (Administratoren)** zuzuweisen. Siehe [Kapitel 4 Konfigurieren der rollenbasierten Verwaltungsdelegation](#).

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
  username
  domain [password | *]
```

```
-b
  username@domain [password | *]
```

```
-b
  domain\username [password | *]
```

Wenn Sie anstelle eines Kennworts ein Sternchen (*) angeben, werden Sie zur Eingabe des Kennworts aufgefordert. 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.

[Tabelle 13-1. Optionen für die Auswahl des Ausgabeformats](#) zeigt einige Optionen des Befehls `vdmadmin` für die Ausgabeformatierung.

Tabelle 13-1. 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.

Tabelle 13-2. Optionen des Befehls „vdmadmin“ zeigt die Befehlsoptionen, die Sie mit dem Befehl `vdmadmin` zum Steuern und Untersuchen des View-Vorgangs verwenden können.

Tabelle 13-2. Optionen des Befehls „vdmadmin“

Option	Beschreibung
-A	Steuert die Informationen, die von einer View Agent-Instanz in den entsprechenden Protokolldateien aufgezeichnet werden. Siehe Konfigurieren der Protokollierung in View Agent unter Verwendung der Option „-A“ . Setzt die von einer View Agent-Instanz angegebene IP-Adresse außer Kraft. Siehe Außerkräftsetzen von IP-Adressen unter Verwendung der Option „-A“
-C	Legt den Namen einer View-Verbindungsserver-Gruppe fest. Siehe Festlegen des Namens einer View-Verbindungsserver-Gruppe unter Verwendung der Option „-C“ .
-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 View-Dienste an. Siehe Auflisten und Anzeigen von Systemüberwachungen unter Verwendung der Option „-H“ .
-I	Generiert Berichte zu View-Vorgängen. Siehe Auflisten und Anzeigen von Berichten zum View-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 unter Verwendung der Option „-M“ .
-N	Konfiguriert die Domänen, die eine View-Verbindungsserver-Instanz oder -Gruppe für Horizon Client verfügbar macht. Siehe Konfigurieren von Domänenfiltern unter Verwendung 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“ .

Option	Beschreibung
-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 View ein Client-Gerät im Kiosk-Modus. Siehe Konfigurieren von Clients im Kiosk-Modus unter Verwendung der Option „-Q“ .
-R	Gibt den ersten Benutzer an, der auf einen Remote-Desktop zugegriffen hat. Siehe Anzeigen des ersten Benutzers einer Maschine unter Verwendung der Option „-R“ .
-S	Entfernt einen Konfigurationseintrag für eine View-Verbindungsserver-Instanz aus der Konfiguration von View. Siehe Entfernen des Eintrags für eine View-Verbindungsserver-Instanz oder einen Sicherheitsserver mit der Option „-S“ .
-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 unter Verwendung der Option „-V“ .
-X	Ermittelt und löst Konflikte bei LDAP-Einträgen auf replizierten View-Verbindungsserver-Instanzen. Siehe Ermitteln und Lösen von Konflikten bei LDAP-Einträgen mit der Option „-X“ .

Konfigurieren der Protokollierung in View Agent unter Verwendung der Option „-A“

Sie können den Befehl `vdmadmin` mit der Option `-A` verwenden, um die Protokollierung in View Agent zu konfigurieren.

Syntax

```
vdmadmin
-A [-b authentication_arguments] -getDCT-outfile local_file -d desktop -m machine
```

```
vdmadmin
-A [-b authentication_arguments] -getlogfile logfile-outfile local_file -d desktop -m machine
```

```
vdmadmin
-A [-b authentication_arguments] -getloglevel [-xml] -d desktop [-m machine]
```

```
vdmadmin
-A [-b authentication_arguments] -getstatus [-xml] -d desktop [-m machine]
```

```
vdmadmin
-A [-b authentication_arguments] -getversion [-xml] -d desktop [-m machine]
```

```
vdmadmin
-A [-b authentication_arguments] -list [-xml] [-w | -n] -d desktop -m machine
```

```
vdmadmin
-A [-b authentication_arguments] -setloglevel level -d desktop [-m machine]
```

Nutzungshinweise

Um den technischen Support von VMware bei der Fehlerbehebung für eine View Agent-Instanz zu unterstützen, können Sie ein DCT-Paket (Data Collection Tool) erstellen. Darüber hinaus können Sie die Protokollierungsebene ändern, die Version und den Status von View Agent anzeigen und einzelne Protokolldateien auf der lokalen Festplatte speichern.

Optionen

[Tabelle 13-3. Optionen für die Konfiguration der Protokollierung in View Agent](#) zeigt die verfügbaren Optionen für die Konfiguration der Protokollierung in View Agent.

Tabelle 13-3. Optionen für die Konfiguration der Protokollierung in View 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.

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 View Agent an.
<code>-getstatus</code>	Zeigt den Status von View Agent an.
<code>-getversion</code>	Zeigt die Version von View Agent an.
<code>-list</code>	Zeigt eine Liste der Protokolldateien für View Agent an.
<code>-m <i>Maschine</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 View Agent fest.
	debug Protokolliert Fehler-, Warnungs- und Debugging-Ereignisse. normal Protokolliert Fehler- und Warnungseignisse. trace Protokolliert Fehler-, Informations- und Debugging-Ereignisse.

Beispiele

Zeigen Sie die Agent-Protokollierungsebene für die Maschine **machine1** im Desktop-Pool **dtpool2** an.

```
vdadmin -A -d dtpool2 -m machine1 -getloglevel
```

Legen Sie die View Agent-Protokollierungsebene für die Maschine **machine1** im Desktop-Pool **dtpool2** auf **Debug** fest.

```
vdadmin -A -d dtpool2 -m machine1 -setloglevel debug
```

Zeigen Sie die Liste der View Agent-Protokolldateien für die Maschine **machine1** im Desktop-Pool **dtpool2** an.

```
vdadmin -A -d dtpool2 -m machine1 -list
```

Speichern Sie eine Kopie der View Agent-Protokolldatei `log-2009-01-02.txt` für die Maschine **machine1** im Desktop-Pool **dtpool2** als `C:\mycopiedlog.txt`.

```
vdadmin -A -d dtpool2 -m machine1 -getlogfile log-2009-01-02.txt -outfile C:\mycopiedlog.txt
```

Zeigen Sie die Version der View Agent-Instanz für die Maschine **machine1** im Desktop-Pool **dtpool2** an.

```
vdadmin -A -d dtpool2 -m machine1 -getversion
```

Zeigen Sie den Status der View Agent-Instanz für die Maschine **machine1** im Desktop-Pool **dtpool2** an.

```
vdadmin -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.

```
vdadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

Außerkräftsetzen von IP-Adressen unter Verwendung der Option „-A“

Sie können den Befehl `vdadmin` mit der Option `-A` verwenden, um die von einer View Agent-Instanz angegebene IP-Adresse außer Kraft zu setzen.

Syntax

```
vdadmin
-A [-bauthentication_arguments] -override-ip_or_dns-ddesktop-mmachine
```

```
vdadmin
-A [-bauthentication_arguments] -override-list-ddesktop-mmachine
```

```
vdadmin
-A [-bauthentication_arguments] -override-r-ddesktop [-mmachine]
```

Nutzungshinweise

Eine View Agent-Instanz gibt die ermittelte IP-Adresse der Maschine, auf der sie ausgeführt wird, an die View-Verbindungsserver-Instanz zurück. In Konfigurationen, in denen die View-Verbindungsserver-Instanz den von der View Agent-Instanz bereitgestellten Wert nicht als vertrauenswürdig einstuft, können Sie diesen Wert außer Kraft setzen und die IP-Adresse festlegen, welche die verwaltete Maschine verwenden sollte. Wenn die von View Agent angegebene Adresse einer Maschine nicht mit der definierten Adresse übereinstimmt, kann nicht über Horizon Client auf die Maschine zugegriffen werden.

Optionen

[Tabelle 13-4. Optionen für das Außerkräftsetzen von IP-Adressen](#) zeigt die verfügbaren Optionen zum Außerkräftsetzen von IP-Adressen.

Tabelle 13-4. 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
```

Festlegen des Namens einer View-Verbindungsserver-Gruppe unter Verwendung der Option „-C“

Sie können den Befehl `vdadmin` mit der Option `-C` verwenden, um den Namen einer View Connection Server-Gruppe festzulegen. Zur Identifizierung der Gruppe in Microsoft System Center Operations Manager (SCOM) wird dieser Name in der SCOM-Konsole angezeigt.

Syntax

```
vdadmin
-C [-b authentication_arguments] [-c groupname]
```

Nutzungshinweise

Wenn zur Überwachung und Verwaltung von View-Komponenten SCOM verwendet werden soll, muss eine View-Verbindungsservergruppe benannt werden. In View Administrator wird der Name einer Gruppe nicht angezeigt. Führen Sie den Befehl auf einem Mitglied der Gruppe aus, der Sie einen Namen zuweisen möchten.

Wenn Sie keinen Namen für die Gruppe angeben, gibt der Befehl die GUID der Gruppe zurück, zu der die lokale View-Verbindungsserver-Instanz gehört. Anhand der GUID können Sie überprüfen, ob eine View-Verbindungsserver-Instanz Mitglied derselben View-Verbindungsserver-Gruppe ist wie eine andere View-Verbindungsserver-Instanz.

Die Verwendung von SCOM mit View ist im Dokument *Integration von View* beschrieben.

Optionen

Die Option `-c` gibt den Namen der View-Verbindungsserver-Gruppe an. Wenn Sie diese Option nicht angeben, gibt der Befehl die GUID der Gruppe zurück.

Beispiele

Legen Sie den Namen einer View Connection Server-Gruppe auf **VCSG01** fest.

```
vdmadmin -C -c VCSG01
```

Geben Sie die GUID der Gruppe zurück.

```
vdmadmin -C
```

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.

Syntax

```
vdmadmin  
-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 unter Verwendung der Option „-H“

Mithilfe der Option `-H` des Befehls `vdadmin` können die vorhandenen Systemüberwachungen angezeigt werden, um Instanzen für View-Komponenten zu überwachen und die Einzelheiten für eine bestimmte Systemüberwachung oder eine bestimmte Überwachungsinstanz anzuzeigen.

Syntax

```
vdadmin
-H [-b authentication_arguments] -list-xml [-w | -n]
```

```
vdadmin
-H [-b authentication_arguments] -list-monitorid monitor_id -xml [-w | -n]
```

```
vdadmin
-H [-b authentication_arguments] -monitorid monitor_id -instanceid instance_id -xml [-w | -n]
```


Nutzungshinweise

Tabelle 13-5. Systemüberwachungen zeigt die von View hinsichtlich des Zustands der Komponenten verwendeten Systemüberwachungen.

Tabelle 13-5. Systemüberwachungen

Überwachungsinstanz	Beschreibung
CBMonitor	Überwacht den Zustand von View-Verbindungsserver-Instanzen.
DBMonitor	Überwacht den Zustand der Ereignisdatenbank.
DomainMonitor	Überwacht den Zustand der lokalen Domäne und aller vertrauenswürdigen Domänen des View-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 View eine separate Überwachungsinstanz für die Überwachung jeder einzelnen Komponenteninstanz.

Der Befehl gibt sämtliche Informationen zu Systemüberwachungen und Überwachungsinstanzen im XML-Format aus.

Optionen

Tabelle 13-6. Optionen für das Auflisten und Anzeigen von Systemüberwachungen zeigt die verfügbaren Optionen zum Auflisten und Anzeigen von Systemüberwachungen.

Tabelle 13-6. 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.

```
vdmin -H -list -xml
```

Listen Sie alle Instanzen der vCenter-Überwachung (VCMonitor) im XML-Format mit ASCII-Zeichen auf.

```
vdmin -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 View-Betrieb unter Verwendung der Option „-l“

Sie können den Befehl `vdadmin` mit der Option `-l` verwenden, um die verfügbaren Berichte zum View-Betrieb aufzulisten und die Ergebnisse beim Ausführen eines dieser Berichte anzuzeigen.

Syntax

```
vdadmin
-I [-b authentication_arguments] -list [-xml] [-w | -n]
```

```
vdadmin
-I [-b authentication_arguments] -report report -view view [-startdate yyyy-MM-dd-HH:mm:ss]
[-enddate yyyy-MM-dd-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 View für einen angegebenen Bericht oder eine angegebene Ansicht aufgezeichnet hat.

Sie können den Befehl `vdadmin` auch mit der Option `-l` verwenden, um View-Protokollmeldungen im `syslog`-Format zu erzeugen. Siehe [Generieren von View-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-l“](#).

Optionen

[Tabelle 13-7. Optionen für das Auflisten und Anzeigen von Berichten und Ansichten](#) zeigt die verfügbaren Optionen zum Auflisten und Anzeigen von Berichten und Ansichten.

Tabelle 13-7. Optionen für das Auflisten und Anzeigen von Berichten und Ansichten

Option	Beschreibung
<code>-enddate yyyy-MM-dd-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 yyyy-MM-dd-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.

```
vdmadmin -I -list -xml -w
```

Zeigen Sie eine Liste der Benutzerereignisse seit dem 1. August 2010 im CSV-Format mit ASCII-Zeichen an.

```
vdmadmin -I -report events -view user_events -startdate 2010-08-01-00:00:00 -csv -n
```

Generieren von View-Ereignisprotokollmeldungen im Syslog-Format mit der Option „-l“

Sie können den Befehl `vdmadmin` zusammen mit der Option `-I` verwenden, um View-Ereignismeldungen in den Ereignisprotokolldateien im Format SysLog aufzuzeichnen. Viele Analyseprodukte von Drittanbietern erfordern Flatfile-SysLog-Daten als Eingabe für die Analysevorgänge.

Syntax

```
vdmadmin
-I
-eventSyslog
-disable
```

```
vdmadmin
-I
-eventSyslog
-enable
-localOnly
```

```
vdmadmin
-I
-eventSyslog
-enable
-path
path
```

```
vdmadmin
-I
-eventSyslog
-enable
-path
```

```

path
-user
DomainName\username
-password
password

```

Nutzungshinweise

Sie können den Befehl verwenden, um View-Ereignisprotokollmeldungen im Syslog-Format zu generieren. View-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 View-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 View 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 *Installation von View*.

Tabelle 13-8. Optionen zum Generieren von View-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 View-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 <i>Kennwort</i></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 <i>Domänenname\Benutzername</i></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 View-Ereignissen im Syslog-Format:

```
vdadmin -I -eventSyslog -disable
```

Leiten der Syslog-Ausgabe von View-Ereignissen nur auf das lokale System:

```
vdmadmin -I -eventSyslog -enable -localOnly
```

Leiten der Syslog-Ausgabe von View-Ereignissen auf einen angegebenen Pfad:

```
vdmadmin -I -eventSyslog -enable -path path
```

Leiten der Syslog-Ausgabe von View-Ereignissen auf einen angegebenen Pfad, der Zugriff durch einen autorisierten Domänenbenutzer erfordert:

```
vdmadmin -I -eventSyslog -enable -path \\logserver\share\ViewEvents -user mydomain\myuser
-passwd mypassword
```

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.

Syntax

```
vdmadmin
-L [-bauthentication_arguments] -ddesktop-m machine-udomain\user
```

```
vdmadmin
-L [-bauthentication_arguments] -ddesktop [-mmachine | -udomain\user] -r
```

Nutzungshinweise

View 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 View 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 eines einzelnen Computers 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 View-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 View 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 `vdmadmin -L` weist persistenten View Composer-Festplatten keine Besitzrechte zu. Um Benutzern Linked-Clone-Desktops mit persistenten Festplatten zuzuweisen, verwenden Sie die Menüoption **Benutzer zuweisen** in View Administrator oder das View PowerCLI-Cmdlet `Update-UserOwnership`.

Wenn Sie `vdmadmin -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

Tabelle 13-9. Optionen für die Zuweisung dedizierter Desktops zeigt die Optionen an, die Sie für die Zuweisung eines Benutzers zu einem Desktop oder zum Entfernen einer Zuweisung festlegen können.

Tabelle 13-9. 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.

```
vdmadmin -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`.

```
vdmadmin -L -d dtpool1 -u Corp\Jo -r
```

Entfernen Sie sämtliche Benutzerzuweisungen für die Maschine `machine1` im Desktop-Pool `dtpool3`.

```
vdmadmin -L -d dtpool3 -m machine1 -r
```

Anzeigen von Informationen zu Maschinen unter Verwendung 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.

Der Maschinenstatus kann einen der folgenden Werte haben: `UNDEFINED`, `PRE_PROVISIONED`, `CLONING`, `CLONINGERROR`, `CUSTOMIZING`, `READY`, `DELETING`, `MAINTENANCE`, `ERROR`, `LOGOUT`.

Der Befehl zeigt nicht alle dynamischen Maschinenstati an, wie beispielsweise `Connected` oder `Disconnected`, die in View 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

[Tabelle 13-10. Optionen für das Anzeigen von Informationen zu Maschinen](#) zeigt die verfügbaren Optionen zum Angeben der Maschine, für die Details angezeigt werden sollen.

Tabelle 13-10. 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.

```
vdadmin -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.

```
vdadmin -M -m machine3 -csv
```

Rückgewinnung von Datenträgerplatz auf virtuellen Maschinen mit der Option „-M“

Sie können den Befehl `vdadmin` zusammen mit der Option `-M` verwenden, um eine virtuelle Linked-Clone-Maschine für die Rückgewinnung von Datenträgerplatz zu markieren. View 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 View Administrator angegeben ist.

Syntax

```
vdadmin
-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 `vdadmin` mit der Option `-M` zurückgewinnen können:

- Vergewissern Sie sich, dass View 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.
- Überprüfen Sie in View Administrator, dass die Option **Zurückgewinnung von Datenträgerplatz** für vCenter Server ausgewählt ist. Siehe [Zulassen, dass vSphere Speicherplatz auf virtuellen Maschinen mit verknüpften Klonen freigibt](#).
- Überprüfen Sie in View Administrator, dass die Option **VM-Datenträgerplatz zurückgewinnen** für den Desktop-Pool ausgewählt wurde. Siehe hierzu „Rückgewinnung von Datenträgerplatz auf Linked-Clone-Desktops“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.
- Überprüfen Sie, dass die virtuelle Maschine eingeschaltet ist, bevor Sie den Vorgang zur Rückgewinnung von Speicherplatz initiieren.
- Überprüfen Sie, dass keine Ausfallperiode wirksam ist. Siehe hierzu „Festlegen von Ausfallzeiten für ESXi-Vorgänge auf Remote-Desktops“ im Dokument *Einrichten von Desktop- und Anwendungspools in View*.

Optionen

Tabelle 13-11. 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 unter Verwendung der Option „-N“

Sie können den Befehl `vdmadmin` mit der Option `-N` zum Steuern der Domänen verwenden, die View für die Endbenutzer zur Verfügung stellt.

Syntax

```
vdmadmin
```

```
-N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -add [-s connsvr]
```

```
vdadmin
-N [-b authentication_arguments] -domains-list [-w | -n] [-xml]
```

```
vdadmin
-N [-b authentication_arguments] -domains-list-active [-w | -n] [-xml]
```

```
vdadmin
-N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -remove [-s connsvr]
```

```
vdadmin
-N [-b authentication_arguments] -domains {-exclude | -include | -search} -removeall [-s connsvr]
```

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

[Tabelle 13-12. Optionen für die Konfiguration von Domänenfiltern](#) zeigt die verfügbaren Optionen zum Konfigurieren von Domänenfiltern.

Tabelle 13-12. Optionen für die Konfiguration von Domänenfiltern

Option	Beschreibung
<code>-add</code>	Fügt eine Domäne zu einer Liste hinzu.
<code>-domain <i>Domäne</i></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.

Option	Beschreibung
-list	Zeigt die Domänen an, die in der Ausschlussliste für die Suche, in der Ausschlussliste und in der Aufnahmeliste für die einzelnen View-Verbindungsserver-Instanzen und für die View-Verbindungsserver-Gruppe konfiguriert sind.
-list -active	Zeigt die verfügbaren Domänen für die View-Verbindungsserver-Instanz an, auf welcher der Befehl ausgeführt wird.
-remove	Entfernt eine Domäne aus einer Liste.
-removeall	Entfernt alle Domänen aus einer Liste.
-s <i>Verbindungsserver</i>	Gibt an, dass der Vorgang für die Domänenfilter einer View-Verbindungsserver-Instanz ausgeführt wird. Die View-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 View-Verbindungsserver-Instanzen innerhalb der Gruppe übernommen.
-search	Gibt einen Vorgang für eine Ausschlussliste für die Suche an.

Beispiele

Fügen Sie die Domäne FARDOM zur Ausschlussliste für die Suche für die View-Verbindungsserver-Instanz csvr1 hinzu.

```
vdadmin -N -domains -search -domain FARDOM -add -s csvr1
```

Fügen Sie die Domäne NEARDOM zur Ausschlussliste für eine View-Verbindungsserver-Gruppe hinzu.

```
vdadmin -N -domains -exclude -domain NEARDOM -add
```

Zeigen Sie die Konfiguration für die Domänensuche auf beiden View-Verbindungsserver-Instanzen in der Gruppe und für die Gruppe 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 :
```

View schränkt die Domänensuche auf allen View-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 View 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 View auf der lokalen View-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 View-Verbindungsserver-Gruppe.

```
vdadmin -N -domains -exclude -domain NEARDOM -remove
```

Entfernen Sie sämtliche Domänen aus der Aufnahmeliste für die View-Verbindungsserver-Instanz csvr1.

```
vdadmin -N -domains -include -removeall -s csvr1
```

Konfigurieren von Domänenfiltern

Domänenfilter können Sie zur Einschränkung der Anzahl der Domänen, die eine View-Verbindungsserver-Instanz oder ein Sicherheitsserver den Endbenutzern zur Verfügung stellt, konfigurieren.

View ermittelt die für den Zugriff verfügbaren Domänen, indem – beginnend mit der Domäne, in der sich eine View-Verbindungsserver-Instanz oder ein Sicherheitsserver befindet – die vorhandenen Vertrauensbeziehungen durchlaufen werden. Bei einer kleinen, gut verbundenen Gruppe von Domänen kann View 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 View-Suchergebnisse können Domänen enthalten, die Sie Benutzern nicht anbieten möchten, wenn sich diese mit ihren Remote-Desktops verbinden.

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 View-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 View-Verbindungsserver-Instanz ausgeführt werden, auf der dieser Schlüssel festgelegt ist.

Tabelle 13-13. Typen von Domänenlisten zeigt die Typen von Domänenlisten, die Sie zur Konfiguration der Domänenfilterung angeben können.

Tabelle 13-13. Typen von Domänenlisten

Domänenlistentyp	Beschreibung
Ausschlussliste für die Suche	Gibt die Domänen an, die View 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 View aus den Ergebnissen einer Domänensuche ausschließt. Die primäre Domäne kann nicht ausgeschlossen werden.
Aufnahmeliste	Gibt die Domänen an, die View 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. View wählt die erste nicht leere Ausschluss- oder Aufnahmeliste mit dieser Reihenfolge aus.

- 1 Die für die View-Verbindungsserver-Instanz konfigurierte Ausschlussliste.
- 2 Die für die View-Verbindungsserver-Gruppe konfigurierte Ausschlussliste.
- 3 Die für die View-Verbindungsserver-Instanz konfigurierte Aufnahmeliste.
- 4 Die für die View-Verbindungsserver-Gruppe konfigurierte Aufnahmeliste.

View wendet lediglich die erste ausgewählte Liste auf die Suchergebnisse an.

Wenn Sie eine Domäne in die Aufnahmeliste aufnehmen, deren Domänencontroller nicht verfügbar ist, nimmt View diese Domäne nicht in die Liste aktiver Domänen auf.

Die primäre Domäne, zu der eine View-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 View nicht aus den Ergebnissen einer Domänensuche ausschließt. Mit Ausnahme der primären Domäne werden alle anderen Domänen entfernt.

Eine View-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 View-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 View-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
```

View 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 mithilfe einer Aufnahmeliste die Domänen angeben, die View aus den Ergebnissen einer Domänensuche ausschließt.

Eine Gruppe aus zwei View-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 View-Verbindungsserver-Gruppe in der Domäne MYDOM zugreifen können.

Zeigen Sie die derzeit aktiven Domänen für ein Mitglied der View-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 View-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 View-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 :
```

View schränkt die Domänensuche auf allen View-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 View 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 authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

```
vdmadmin
-P [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

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

Tabelle 13-14. Optionen für das Anzeigen der Maschinen und Richtlinien nicht berechtigter Benutzer zeigt die verfügbaren Optionen zum Anzeigen der virtuellen Maschinen und Richtlinien nicht berechtigter Benutzer auf.

Tabelle 13-14. 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.

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 13-15. 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 13-15. 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.

```
vdadmin -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.

```
vdadmin -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.

```
vdadmin -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.

```
vdadmin -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.

```
vdadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xml" > up-output.html
```

Konfigurieren von Clients im Kiosk-Modus unter Verwendung 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 authentication_arguments] -domain domain_name-clientid client_id [-password "password"
| -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-groupgroup_name | -nogroup] [-description
"description_text"]
```

```
vdmadmin
-Q
-disable [-b authentication_arguments] -s connection_server
```

```
vdmadmin
-Q
-enable [-b authentication_arguments] -s connection_server [-requirepassword]
```

```
vdmadmin
-Q
-clientauth
-getdefaults [-b authentication_arguments] [-xml]
```

```
vdmadmin
-Q
-clientauth
-list [-b authentication_arguments] [-xml]
```

```
vdmadmin
-Q
-clientauth
-remove [-b authentication_arguments] -domain domain_name-clientid client_id
```

```
vdmadmin
-Q
```

```
-clientauth
-removeall [-b authentication_arguments] [-force]
```

```
vdmadmin
-Q
-clientauth
-setdefaults [-b authentication_arguments] [-ou DN] [ -expirepassword | -noexpirepassword ] [-group
group_name | -nogroup]
```

```
vdmadmin
-Q
-clientauth
-update [-b authentication_arguments] -domain domain_name-clientid client_id [-password
"password" | -genpassword] [-description "description_text"]
```

Nutzungshinweise

Der Befehl `vdmadmin` muss für eine der View-Verbindungsserver-Instanzen in der Gruppe mit der View-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 View-Verbindungsserver-Instanzen innerhalb einer Gruppe verwendet.

Beim Hinzufügen von Clients im Kiosk-Modus erstellt View 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 angeben, und zwar unter `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` in ADAM in einer View-Verbindungsserver-Instanz. Vermeiden Sie, diese Präfixe bei normalen Benutzerkonten zu verwenden.

Wenn Sie keinen Namen für den Client angeben, generiert View einen Namen aus der für das Clientgerät angegebenen MAC-Adresse. Wenn die MAC-Adresse beispielsweise `00:10:db:ee:76:80` lautet, wird der Kontoname `cm-00_10_db_ee_76_80` generiert. Diese Konten können nur mit View-Verbindungsserver-Instanzen verwendet werden, die für die Authentifizierung von Clients aktiviert sind.

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 View 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 View-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 View-Verbindungsserver-Instanz aktiviert oder deaktiviert wird, gelten die anderen Einstellungen für die Clientauthentifizierung für alle View-Verbindungsserver-Instanzen innerhalb einer Gruppe. Ein Client muss nur einmal hinzugefügt werden, damit alle View-Verbindungsserver-Instanzen in einer Gruppe Anforderungen von diesem Client akzeptieren.

Wenn Sie beim Aktivieren der Authentifizierung die Option `-requirepassword` angeben, kann die View-Verbindungsserver-Instanz keine Clients authentifizieren, die über automatisch generierte Kennwörter verfügen. Wenn Sie die Konfiguration einer View-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

Tabelle 13-16. Optionen für die Konfiguration von Clients im Kiosk-Modus zeigt die verfügbaren Optionen für die Konfiguration von Clients im Kiosk-Modus.

Tabelle 13-16. 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>Beschreibungstext</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 View-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 View-Verbindungsserver-Instanz.
<code>-expirepassword</code>	Gibt an, dass die Ablaufzeit für Kennwörter der Clientkonten mit der Ablaufzeit für die View-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.

Option	Beschreibung
<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 Gruppenname</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 View-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 DN</code>	Specifies the distinguished name of the organizational unit to which client accounts are added. For example: OU=kiosk-ou,DC=myorg,DC=com Hinweis You cannot use the <code>-setdefaults</code> option to change the configuration of an organizational unit.
<code>-password "password"</code>	Specifies an explicit password for the client's account.
<code>-remove</code>	Removes the account for a client in kiosk mode.
<code>-removeall</code>	Removes the accounts of all clients in kiosk mode.
<code>-requirepassword</code>	Specifies that clients in kiosk mode must provide passwords. View will not accept generated passwords for new connections.
<code>-s connection_server</code>	Specifies the NetBIOS name of the View Connection Server instance on which to enable or disable the authentication of clients in kiosk mode.
<code>-setdefaults</code>	Sets the default values that are used for adding client accounts.
<code>-update</code>	Updates an account for a client in kiosk mode.

Examples

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

Get the current default values for clients in plain text format.

```
vdmadmin -Q -clientauth -getdefaults
```

Get the current default values for clients in XML format.

```
vdmadmin -Q -clientauth -getdefaults -xml
```

Add an account for a client specified by its MAC address to the MYORG domain, and use the default settings for the group kc-grp.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

Add an account for a client specified by its MAC address to the MYORG domain, and use an automatically generated password.

```
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
```

Add an account for a named client, and specify a password to be used with the client.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

Update an account for a client, specifying a new password and descriptive text.

```
vdmadmin -Q -clientauth -update -domain MYORG -clientid custom-Terminal21 -password "Secret1!" -description "Foyer Entry Workstation"
```

Remove the account for a kiosk client specified by its MAC address from the MYORG domain.

```
vdmadmin -Q -clientauth -remove -domain MYORG -clientid 00:10:db:ee:54:12
```

Remove the accounts of all clients without prompting to confirm the removal.

```
vdmadmin -Q -clientauth -removeall -force
```

Enable authentication of clients for the View Connection Server instance csvr-2. Clients with automatically generated passwords can authenticate themselves without providing a password.

```
vdmadmin -Q -enable -s csvr-2
```

Enable authentication of clients for the View Connection Server instance csvr-3, and require that the clients specify their passwords to Horizon Client. Clients with automatically generated passwords cannot authenticate themselves.

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

Disable authentication of clients for the View Connection Server instance csvr-1.

```
vdmadmin -Q -disable -s csvr-1
```

Display information about clients in text format. Client cm-00_0c_29_0d_a3_e6 has an automatically generated password, and does not require an end user or an application script to specify this password to Horizon Client. Client cm-00_22_19_12_6d_cf has an explicitly specified password, and requires the end user to provide this. The View Connection Server instance CONSVR2 accepts authentication requests from clients with automatically generated passwords. CONSVR1 does not accept authentication requests from clients in kiosk mode.

```
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 unter Verwendung 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` zusammen mit der Option `-R` funktioniert nur auf virtuellen Maschinen, die eine ältere Version als View Agent 5.1 aufweisen. Auf virtuellen Maschinen, auf denen View Agent 5.1 und höhere Versionen ausgeführt werden, 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 View-Verbindungsserver-Instanz oder einen Sicherheitsserver mit der Option „-S“

Sie können den Befehl `vdmadmin` mit der Option `-S` verwenden, um den Eintrag für eine View-Verbindungsserver-Instanz oder einen Sicherheitsserver aus der View-Konfiguration zu entfernen.

Syntax

```
vdmadmin  
-S [-b authentication_arguments] -r-s server
```

Nutzungshinweise

Um Hochverfügbarkeit zu gewährleisten, ermöglicht View die Konfiguration einer oder mehrerer View-Verbindungsserver-Replikatinstanzen in einer View-Verbindungsserver-Gruppe. Wenn Sie eine View-Verbindungsserver-Instanz in einer Gruppe deaktivieren, bleibt der Eintrag für den Server in der View-Konfiguration erhalten.

Sie können auch den Befehl `vdmadmin` mit der Option `-S` verwenden, um einen Sicherheitsserver aus Ihrer View-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 View-Verbindungsserver-Instanz oder den Sicherheitsserver vom Windows Server-Computer, indem Sie das View-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 `vdadmin` auf einer anderen View-Verbindungsserver-Instanz, um den Eintrag für die deinstallierte View-Verbindungsserver-Instanz oder den Sicherheitsserver aus der Konfiguration zu entfernen.

Wenn Sie View auf den entfernten Systemen erneut installieren möchten, ohne die View-Konfiguration der ursprünglichen Gruppe zu replizieren, starten Sie vor der erneuten Installation alle View-Verbindungsserver-Hosts in der ursprünglichen Gruppe neu. Dadurch wird verhindert, dass die erneut installierten View-Verbindungsserver-Instanzen die Konfigurationsaktualisierungen ihrer ursprünglichen Gruppe erhalten.

Optionen

Die Option `-s` gibt den NetBIOS-Namen der View-Verbindungsserver-Instanz oder des Sicherheitsservers an, die bzw. der entfernt werden soll.

Beispiele

Entfernen Sie den Eintrag für die View-Verbindungsserver-Instanz `connsvr3`.

```
vdadmin -S -r -s connsvr3
```

Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U“

Sie können den Befehl `vdadmin` mit der Option `-U` verwenden, um detaillierte Informationen zu Benutzern anzuzeigen.

Syntax

```
vdadmin
-U [-b authentication_arguments] -u domain\user [-w | -n] [-xml]
```

Nutzungshinweise

Der Befehl zeigt Informationen zu einem Benutzer aus Active Directory und View an.

- Active Directory-Informationen zum Konto des Benutzers.
- Mitgliedschaft in Active Directory-Gruppen.
- Computer-Berechtigungen, einschließlich Computer-ID, Anzeigenname, 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.

```
vdadmin -U -u CORP\Jo -n -xml
```

Entsperren oder Sperren von virtuellen Maschinen unter Verwendung der Option „-V“

Sie können den Befehl `vdadmin` mit der Option `-V` verwenden, um virtuelle Maschinen im Rechenzentrum zu sperren oder zu entsperren.

Syntax

```
vdadmin
-V [-b authentication_arguments] -e-d desktop-mmachine [-m machine] ...
```

```
vdadmin
-V [-b authentication_arguments] -e-vcdn vCenter_dn-vmpath inventory_path
```

```
vdadmin
-V [-b authentication_arguments] -p-d desktop -m machine [-mmachine] ...
```

```
vdadmin
-V [-b authentication_arguments] -p-vcdn vCenter_dn-vmpath inventory_path
```

Nutzungshinweise

Sie sollten ausschließlich den Befehl `vdadmin` 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

Tabelle 13-17. Optionen für das Entsperren oder Sperren von virtuellen Maschinen zeigt die Optionen, die Sie zum Entsperren oder Sperren von virtuellen Maschinen angeben können.

Tabelle 13-17. 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.
<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 mit der Option „-X“

Sie können den Befehl `vdadmin` mit der Option `-X` verwenden, um Konflikte bei LDAP-Einträgen auf replizierten View-Verbindungsserver-Instanzen in einer Gruppe zu ermitteln und zu lösen.

Syntax

```
vdadmin
-X [-bauthentication_arguments] -collisions [-resolve]
```

Nutzungshinweise

Wenn auf mindestens zwei View-Verbindungsserver-Instanzen dieselben LDAP-Einträge erstellt wurden, kann dies zu Integritätsproblemen von LDAP-Daten in View führen. Dies kann passieren, wenn ein Upgrade durchgeführt wird, während die LDAP-Replikation nicht verwendet wird. Auch wenn View in regelmäßigen Abständen nach dieser Fehlerbedingung sucht, können Sie den Befehl `vdadmin` auf den View-Verbindungsserver-Instanzen in der Gruppe ausführen, um Konflikte bei LDAP-Einträgen manuell zu ermitteln und diese zu lösen.

Optionen

[Tabelle 13-18. Optionen zum Ermitteln und Lösen von Konflikten bei LDAP-Einträgen](#) zeigt die Optionen, die Sie angeben können, um Konflikte bei LDAP-Einträgen zu ermitteln und zu lösen.

Tabelle 13-18. Optionen zum Ermitteln und Lösen von Konflikten bei LDAP-Einträgen

Option	Beschreibung
-collisions	Legt einen Vorgang zum Ermitteln von LDAP-Konflikten in einer View-Verbindungsserver-Gruppe fest.
-resolve	Löst alle ermittelten LDAP-Konflikte.

Beispiele

Ermitteln Sie Konflikte bei LDAP-Einträgen in einer View-Verbindungsserver-Gruppe.

```
vdmadmin -X -collisions
```

Ermitteln und lösen Sie Konflikte bei LDAP-Einträgen.

```
vdmadmin -X -collisions -resolve
```