

# Einrichten von Desktop- und Anwendungspools für 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](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://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](http://www.vmware.com/de)

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

# Inhalt

|   |           |
|---|-----------|
| Einrichten von Desktop- und Anwendungspools in View   | 11        |
| <b>1 Einführung in Desktop- und Anwendungspools</b>   | <b>12</b> |
| Farmen, RDS-Hosts und Desktop- und Anwendungspools  | 12        |
| Vorteile von Desktop-Pools  | 13        |
| Desktop-Pools für bestimmte Nutzertypen   | 14        |
| Pools für Sachbearbeiter  | 15        |
| Pools für Büroanwender und Hauptbenutzer  | 16        |
| Pools für Kioskbenutzer   | 17        |
| Vorteile von Anwendungspools  | 18        |
| <b>2 Vorbereiten nicht verwalteter Maschinen</b>  | <b>20</b> |
| Vorbereiten eines nicht verwalteten Computers für die Remote-Desktop-Bereitstellung                                     | 20        |
| Installieren von View Agent auf einer nicht verwalteten Maschine  | 21        |
| Benutzerdefinierte Setup-Optionen für View Agent für nicht verwaltete Maschinen   | 22        |
| <b>3 Erstellen und Vorbereiten virtueller Maschinen</b>   | <b>25</b> |
| Erstellen virtueller Maschinen für die Remote-Desktop-Bereitstellung  | 25        |
| Erstellen einer virtuellen Maschine für die Remote-Desktop-Bereitstellung   | 26        |
| Installieren eines Gastbetriebssystems  | 29        |
| Vorbereiten eines Gastbetriebssystems für die Remote-Desktop-Bereitstellung   | 30        |
| Vorbereiten von Windows Server 2008 R2 für Desktop-Verwendung   | 33        |
| Installieren von „Desktopdarstellung“ auf Windows Server 2008 R2  | 34        |
| Installieren von View Agent auf einer virtuellen Maschine   | 34        |
| Benutzerdefinierte Setup-Optionen für View Agent  | 36        |
| Unbeaufsichtigte Installation von View Agent  | 40        |
| Befehlszeilenoptionen für Microsoft Windows Installer   | 42        |
| Eigenschaften für die unbeaufsichtigte Installation von View Agent  | 44        |
| Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent                                      | 47        |
| Optimieren der Leistung des Gastbetriebssystems für alle Windows-Versionen  | 47        |
| Optimieren der Leistung des Windows 7- und Windows 8-Gastbetriebssystems  | 49        |
| Deaktivieren des Windows-Programms zur Verbesserung der Benutzerfreundlichkeit  | 50        |
| Optimieren von Windows 7 und Windows 8 für virtuelle Maschinen mit verknüpftem Klon                                     | 51        |
| Vorteile der Deaktivierung von Diensten und Aufgaben unter Windows 7 und Windows 8                                      | 51        |
| Überblick über Windows 7- und Windows 8-Dienste und -Aufgaben, die zu einem Wachstum von verknüpften Klonen führen      | 52        |
| Deaktivieren der geplanten Datenträgerdefragmentierung auf übergeordneten virtuellen Windows 7- und Windows 8-Maschinen | 56        |

|  |            |
|--|------------|
| Deaktivieren des Windows Update-Dienstes auf virtuellen Windows 7- und Windows 8-Maschinen             | 57         |
| Deaktivieren des Diagnoserichtliniendienstes auf virtuellen Windows 7- und Windows 8-Maschinen         | 58         |
| Deaktivieren der Vorabruf- und SuperFetch-Funktionen auf virtuellen Windows 7- und Windows 8-Maschinen | 59         |
| Deaktivieren der Sicherung der Windows-Registrierung auf virtuellen Windows 7- und Windows 8-Maschinen | 59         |
| Deaktivieren der Systemwiederherstellung auf virtuellen Windows 7- und Windows 8-Maschinen             | 60         |
| Deaktivieren von Windows Defender auf virtuellen Windows 7- und Windows 8-Maschinen                    | 60         |
| Deaktivieren der Microsoft-Feeds-Synchronisierung auf virtuellen Windows 7- und Windows 8-Maschinen    | 61         |
| Vorbereiten virtueller Maschinen für View Composer   | 62         |
| Vorbereiten einer übergeordneten virtuellen Maschine   | 62         |
| Aktivieren von Windows auf virtuellen Linked-Clone-Computern   | 65         |
| Deaktivieren des Windows-Ruhezustands in der übergeordneten virtuellen Maschine                        | 66         |
| Konfigurieren einer übergeordneten virtuellen Maschine zur Verwendung des lokalen Speichers            | 67         |
| Protokollieren der Auslagerungsdateigröße für die übergeordnete virtuelle Maschine                     | 68         |
| Erhöhen des Zeitüberschreitungslimits für QuickPrep-Anpassungsskripts                                  | 69         |
| Erstellen von Vorlagen virtueller Maschinen  | 70         |
| Erstellen von Anpassungsspezifikationen  | 70         |
| <b>4 Erstellen automatisierter Desktop-Pools mit vollständigen virtuellen Maschinen</b>                | <b>72</b>  |
| Automatisierte Pools mit vollständigen virtuellen Maschinen  | 72         |
| Arbeitsblatt zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen          | 72         |
| Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen                           | 76         |
| Desktop-Einstellungen für automatisierte Pools mit vollständigen virtuellen Maschinen                  | 78         |
| <b>5 Erstellen von Linked-Clone-Desktop-Pools</b>  | <b>80</b>  |
| Pools von Linked-Clone-Desktops  | 80         |
| Arbeitsblatt zum Erstellen eines Linked-Clone-Desktop-Pools  | 80         |
| Erstellen eines Linked-Clone-Desktop-Pools   | 92         |
| Desktop-Pool-Einstellungen für Linked-Clone-Desktop-Pools  | 94         |
| View Composer-Unterstützung für Linked-Clone-SIDs und Drittanbieteranwendungen                         | 95         |
| Wählen von QuickPrep oder Sysprep zum Anpassen von Linked-Clone-Maschinen                              | 97         |
| Linked-Clone-Maschinen während View Composer-Vorgängen bereitgestellt und einsatzbereit halten         | 101        |
| Verwenden vorhandener Active Directory-Computerkonten für verknüpfte Klone                             | 102        |
| <b>6 Erstellen von manuellen Desktop-Pools</b>   | <b>105</b> |
| Manuelle Desktop-Pools   | 105        |
| Arbeitsblatt zum Erstellen eines manuellen Desktop-Pools   | 105        |

- [Erstellen eines manuellen Desktop-Pools](#) 108
- [Erstellen eines manuellen Pools mit einem Computer](#) 109
- [Desktop-Pool-Einstellungen für manuelle Pools](#) 110

## **7 Einrichten von Remote-Desktop-Dienste-Hosts** 113

- [RDS-Hosts](#) 113
  - [Installieren von „Remotedesktopdienste“ auf Windows Server 2008 R2](#) 115
  - [Installieren von Remotedesktopdiensten auf Windows Server 2012 oder Windows Server 2012 R2](#) 116
  - [Installieren von „Desktopdarstellung“ auf Windows Server 2008 R2](#) 117
  - [Installieren von „Desktopdarstellung“ auf Windows Server 2012 oder Windows Server 2012 R2](#) 117
  - [Einschränken von Benutzern auf eine einzelne Sitzung](#) 118
  - [Installation von View Agent auf einem Remote-Desktop-Dienste-Host](#) 118
    - [Benutzerdefinierte Setup-Optionen für View Agent für einen RDS-Host](#) 120
  - [Aktivieren der Zeitzone-Umleitung für RDS-Desktop- und Anwendungssitzungen](#) 121
  - [Aktivieren des Windows-Basisdesigns für Anwendungen](#) 121
  - [Konfigurieren der Gruppenrichtlinie zum Ausführen von Start Runonce.exe](#) 122
  - [RDS-Host-Performance-Optionen](#) 123

## **8 Erstellen von Farmen** 124

- [Farmen](#) 124
  - [Arbeitsblatt zum Erstellen einer Farm](#) 125
  - [Erstellen einer Farm](#) 126

## **9 Erstellen von Anwendungspools** 128

- [Anwendungspools](#) 128
  - [Arbeitsblatt zum manuellen Erstellen eines Anwendungspools](#) 129
  - [Erstellen eines Anwendungspools](#) 129

## **10 Erstellen von RDS-Desktop-Pools** 131

- [Grundlegendes zu RDS-Desktop-Pools](#) 131
- [Erstellen eines RDS-Desktop-Pools](#) 132
- [Desktop-Pool-Einstellungen für RDS-Desktop-Pools](#) 133
- [Konfigurieren der Adobe Flash-Drosselung mit Internet Explorer für RDS-Desktop-Pools](#) 133

## **11 Bereitstellen von Desktop-Pools** 134

- [Benutzerzuweisung in Desktop-Pools](#) 134
- [Manuelles Benennen von Computern oder Bereitstellen eines Benennungsmusters](#) 135
  - [Angaben einer Liste von Maschinennamen](#) 137
  - [Verwenden eines Benennungsmusters für automatisierte Desktop-Pools](#) 139
  - [Beispiel für die Maschinenbenennung](#) 140
  - [Hinzufügen von Computern zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde](#) 141

|   |            |
|---|------------|
| Manuelles Anpassen von Maschinen  | 143        |
| Anpassen von Maschinen im Wartungsmodus   | 143        |
| Anpassen einzelner Maschinen  | 144        |
| Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen  | 144        |
| Adobe Flash-Qualität und -Drosselung  | 148        |
| Einstellen von Betriebsrichtlinien für Desktop-Pools  | 149        |
| Betriebsrichtlinien für Desktop-Pools   | 150        |
| Konfigurieren von speziellen Maschinen zum Anhalten nach Trennung der Verbindung durch Benutzer | 153        |
| Auswirkungen von Betriebsrichtlinien auf automatisierte Desktop-Pools                           | 153        |
| Beispiele für Betriebsrichtlinien für automatisierte Pools mit dynamischer Zuweisung            | 154        |
| Beispiel für Betriebsrichtlinien für automatisierte Pools mit dedizierter Zuweisung             | 155        |
| Verhindern von Betriebsrichtlinienkonflikten  | 156        |
| Konfigurieren von 3D-Rendern auf Windows 7- oder neueren Desktops                               | 156        |
| 3D-Render-Optionen  | 158        |
| Empfohlene Vorgehensweise für das Konfigurieren des 3D-Renderns                                 | 159        |
| Prüfen der GPU-Ressourcen auf einem ESXi-Host   | 161        |
| Verhindern vom Zugriff auf View-Desktops durch RDP  | 161        |
| Bereitstellen großer Desktop-Pools  | 162        |
| Konfigurieren von Desktop-Pools auf Clustern mit mehr als acht Hosts                            | 162        |
| Zuweisen mehrerer Netzwerkbezeichnungen zu einem Desktop-Pool                                   | 163        |
| <b>12 Berechtigen von Benutzern und Gruppen</b>   | <b>164</b> |
| Hinzufügen von Berechtigungen zu einem Desktop- oder Anwendungspool                             | 164        |
| Entfernen von Berechtigungen für einen Desktop- oder Anwendungspool                             | 165        |
| Überprüfen von Desktop-Pool- und Anwendungspool-Berechtigungen                                  | 166        |
| Einschränken des Zugriffs auf Remote-Desktops   | 166        |
| Beispiel für eingeschränkte Berechtigungen  | 167        |
| Kennzeichenabgleich   | 168        |
| Überlegungen und Einschränkungen bei eingeschränkten Berechtigungen                             | 169        |
| Zuweisen von Kennzeichen zu einer View-Verbindungsserver-Instanz                                | 170        |
| Zuweisen von Kennzeichen zu einem Desktop-Pool  | 170        |
| <b>13 Konfigurieren von Remote-Desktop-Funktionen</b>   | <b>172</b> |
| Konfigurieren von Unity Touch   | 172        |
| Systemanforderungen für Unity Touch   | 173        |
| Konfigurieren von Favoritenanwendungen durch Unity Touch  | 173        |
| Konfigurieren der Flash-URL-Umleitung für das Multicast- oder Unicast-Streaming                 | 176        |
| Systemanforderungen für die Flash-URL-Umleitung   | 177        |
| Sicherstellen, dass die Flash-URL-Umleitung installiert ist                                     | 179        |
| Einrichten der Webseiten zur Bereitstellung von Multicast- oder Unicast-Streams                 | 179        |
| Einrichten von Clientgeräten für die Flash-URL-Umleitung  | 180        |

|   |            |
|---|------------|
| Deaktivieren oder Aktivieren der Flash-URL-Umleitung  | 180        |
| Konfigurieren von Echtzeit-Audio/Video  | 181        |
| Konfigurationsmöglichkeiten für Echtzeit-Audio/Video  | 182        |
| Systemanforderungen für Echtzeit-Audio/Video  | 182        |
| Sicherstellen, dass anstelle der USB-Umleitung Echtzeit-Audio/Video verwendet wird  | 183        |
| Auswählen von bevorzugten Webcams und Mikrofonen  | 184        |
| Konfigurieren von Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video  | 194        |
| Bandbreite für Echtzeit-Audio/Video   | 198        |
| Konfigurieren der Scannerumleitung  | 199        |
| Systemanforderungen für Scannerumleitung  | 199        |
| Bedienung der Scannerumleitung durch den Benutzer   | 200        |
| Konfigurieren der Gruppenrichtlinieneinstellungen für Scannerumleitung  | 201        |
| Verwalten des Zugriffs auf die Multimedia-Umleitung von Windows (MMR)   | 205        |
| Aktivieren von Multimedia-Umleitung in View   | 206        |
| Systemanforderungen für Windows Media MMR   | 206        |
| Unterstützung der Multimedia-Umleitung auf Desktop-Betriebssystemen   | 207        |
| Sicherstellen, dass Clients Windows 7 MMR initiieren können   | 208        |
| <b>14 Verwenden von USB-Geräten mit Remote-Desktops</b>   | <b>210</b> |
| Einschränkungen in Bezug auf USB-Gerätetypen  | 211        |
| Überblick über das Einrichten der USB-Umleitung   | 212        |
| Netzwerkdatenverkehr und USB-Umleitung  | 213        |
| Automatische Verbindungen mit USB-Geräten   | 214        |
| Deaktivieren der USB-Umleitung  | 215        |
| Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs  | 216        |
| Verwenden von Richtlinien zum Steuern der USB-Umleitung   | 217        |
| Konfigurieren der Gerätesplittingrichtlinieneinstellungen für Composite USB-Geräte  | 218        |
| Konfigurieren der Filterrichtlinieneinstellungen für USB-Geräte   | 221        |
| USB-Gerätefamilien  | 226        |
| USB-Einstellungen in der ADM-Vorlage für die View Agent-Konfiguration   | 226        |
| Fehlerbehebung bei Problemen mit der USB-Umleitung  | 229        |
| <b>15 Reduzieren und Verwalten von Speicheranforderungen</b>  | <b>232</b> |
| Verwalten des Speichers mit vSphere   | 232        |
| Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung  | 234        |
| Standardmäßige Speicherrichtlinienprofile für Virtual SAN-Datenspeicher   | 236        |
| Reduzieren von Speicheranforderungen mit View Composer  | 237        |
| Speichergrößen für Linked-Clone-Desktop-Pools   | 240        |
| Größenrichtlinien für Linked-Clone-Pools  | 240        |
| Größenformeln für Linked-Clone-Pools  | 243        |
| Formeln zur Größenberechnung von verknüpften Klonen beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern | 244        |

|  |            |
|--|------------|
| Speichermehrfachvergabe für virtuellen Linked-Clone-Computer   | 246        |
| Festlegen des Werts für die Speichermehrfachvergabe für virtuelle Linked-Clone-Computer                                    | 247        |
| Datenfestplatten von verknüpften Klonen  | 248        |
| Speichern von verknüpften Klonen auf lokalen Datenspeichern  | 250        |
| Speichern von View Composer-Replikaten und verknüpften Klonen in separaten Datenspeichern                                  | 251        |
| Überlegungen zur Verfügbarkeit beim Speichern von Replikaten in einem separaten oder in gemeinsam genutzten Datenspeichern | 252        |
| Konfigurieren der View-Speicherbeschleunigung für Desktop-Pools  | 253        |
| Rückgewinnung von Festplattenspeicherplatz auf virtuellen Linked-Clone-Maschinen   | 254        |
| Verwenden der View Composer Array Integration mit systemeigener NFS-Snapshot-Technologie (VAAI)                            | 257        |
| Festlegen von Ausfallzeiten für ESXi-Vorgänge auf View-VMs   | 258        |
| <b>16 Konfigurieren von Richtlinien für Desktop- und Anwendungspools</b>   | <b>260</b> |
| Festlegen von Richtlinien in View Administrator  | 260        |
| Konfigurieren globaler Richtlinieneinstellungen  | 261        |
| Konfigurieren von Richtlinien für Desktop-Pools  | 261        |
| Konfigurieren von Richtlinien für Benutzer   | 262        |
| View-Richtlinien   | 262        |
| Verwenden von Active Directory-Gruppenrichtlinien  | 263        |
| Erstellen einer OU für Remote-Desktops   | 264        |
| Aktivieren der Loopback-Verarbeitung für Remote-Desktops   | 264        |
| Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien (ADM) für View  | 264        |
| ADM- und ADMX-Vorlagendateien für View   | 265        |
| ADM-Vorlageneinstellungen für die View Agent-Konfiguration   | 266        |
| An View-Desktops gesendete Clientsysteminformationen   | 269        |
| Ausführen von Befehlen auf View-Desktops   | 272        |
| ADM-Vorlageneinstellungen für View-PCoIP-Sitzungsvariablen   | 273        |
| Allgemeine View-PCoIP-Sitzungsvariablen  | 274        |
| View-PCoIP-Sitzungsbandbreitenvariablen  | 283        |
| View-PCoIP-Sitzungsvariablen für die Tastatur  | 286        |
| View PCoIP Build-to-Lossless-Funktion  | 287        |
| Verwenden von Gruppenrichtlinien für Remote-Desktop-Dienste  | 288        |
| Hinzufügen der ADMX-Dateien der Remote-Desktop-Dienste zu Active Directory   | 288        |
| Einstellungen zur Kompatibilität der RDS-Anwendung   | 289        |
| Einstellungen zu RDS-Verbindungen  | 291        |
| Einstellungen zur Umleitung von RDS-Geräten und Ressourcen   | 291        |
| Einstellungen zur RDS-Lizenzierung   | 292        |
| Einstellungen zu RDS-Profilen  | 294        |
| Umgebungseinstellungen zur RDS-Remote-Sitzung  | 297        |
| RDS-Sicherheitseinstellungen   | 297        |
| Einstellungen zu temporären RDS-Ordern   | 298        |



|  |            |
|--|------------|
| Einrichten des standortbasierten Drucks  | 300        |
| Registrieren der Gruppenrichtlinien-DLL für den standortbasierten Druck                    | 301        |
| Konfigurieren der Gruppenrichtlinie für den standortbasierten Druck                        | 302        |
| Syntax einer Gruppenrichtlinieneinstellung für den standortbasierten Druck                 | 303        |
| Beispiel einer Active Directory-Gruppenrichtlinie  | 305        |
| Erstellen einer OU für View-Computer   | 306        |
| Erstellen von GPOs für View-Gruppenrichtlinien   | 307        |
| Hinzufügen von View-ADM-Vorlagen zu einem GPO  | 308        |
| Aktivieren der Loopback-Verarbeitung für Remote-Desktops                                   | 309        |
| <b>17 Konfigurieren von Benutzerprofilen mit View Persona Management</b>                   | <b>310</b> |
| Bereitstellen von Benutzerpersonas in View   | 310        |
| Verwenden von View Persona Management mit eigenständigen Systemen                          | 311        |
| Migration von Benutzerprofilen mit View Persona Management                                 | 312        |
| Persona-Verwaltung und servergespeicherte Windows-Profile                                  | 316        |
| Konfigurieren einer View Persona Management Bereitstellung                                 | 316        |
| Übersicht über das Einrichten einer View Persona Management Bereitstellung                 | 316        |
| Konfigurieren eines Benutzerprofil-Repositorys   | 317        |
| Installieren von View Agent mit der View Persona Management Option                         | 320        |
| Installieren eines eigenständigen View Persona Management                                  | 321        |
| Hinzufügen der View Persona Management ADM-Vorlagendatei                                   | 323        |
| Konfigurieren von View Persona Management-Richtlinien                                      | 325        |
| Erstellen von Desktop-Pools, die Persona Management verwenden                              | 327        |
| Empfohlene Vorgehensweisen beim Konfigurieren einer View Persona Management Bereitstellung | 328        |
| Konfigurieren von Benutzerprofilen unter Einschluss von ThinApp Sandbox-Ordnern            | 331        |
| Konfigurieren von persistenten View Composer-Festplatten mit View Persona Management       | 331        |
| Verwalten von Benutzerprofilen auf eigenständigen Laptops                                  | 332        |
| Gruppenrichtlinieneinstellungen für View Persona Management                                | 333        |
| Gruppenrichtlinieneinstellungen für Serverspeicherung und Synchronisierung                 | 334        |
| Gruppenrichtlinieneinstellungen für Ordnerumleitung  | 338        |
| Gruppenrichtlinieneinstellungen für Desktop-Benutzeroberfläche                             | 342        |
| Protokollieren von Gruppenrichtlinieneinstellungen   | 342        |
| <b>18 Fehlerbehebung bei Computern und Desktop-Pools</b>                                   | <b>344</b> |
| Anzeigen problematischer Computer  | 344        |
| Senden von Nachrichten an Desktop-Benutzer   | 345        |
| Fehlerbehebung bei Problemen während der Desktop-Pool-Erstellung                           | 346        |
| Fehler bei der Pool-Erstellung, wenn keine Anpassungsspezifikationen gefunden werden       | 346        |
| Fehler bei der Pool-Erstellung aufgrund eines Berechtigungsproblems                        | 346        |
| Fehler bei der Pool-Bereitstellung aufgrund eines Konfigurationsproblems                   | 347        |

|   |     |
|---|-----|
| Fehler bei der Pool-Bereitstellung, da eine View-Verbindungsserver-Instanz keine Verbindung mit einer vCenter-Instanz herstellen kann | 348 |
| Fehler bei der Pool-Bereitstellung aufgrund von Datenspeicherproblemen  | 349 |
| Fehler bei der Pool-Bereitstellung, da vCenter Server überlastet ist  | 349 |
| Virtuelle Maschinen können den Bereitstellungsstatus nicht verlassen  | 350 |
| Virtuelle Maschinen können den Anpassungsstatus nicht verlassen   | 350 |
| Entfernen verwaister oder gelöschter verknüpfter Klone  | 351 |
| Fehlerbehebung bei Computern, die wiederholt gelöscht und neu erstellt werden   | 352 |
| Beheben von Fehlern bei der QuickPrep-Anpassung   | 353 |
| Suchen und Aufheben des Schutzes von nicht verwendeten View Composer-Replikaten   | 354 |
| Fehler beim Hinzufügen von verknüpften Windows XP-Klonen zur Domäne   | 356 |
| View Composer-Bereitstellungsfehler   | 357 |
| Fehlerbehebung bei Problemen mit der Netzwerkverbindung   | 359 |
| Connection Problems Between Machines and View-Verbindungsserver Instances   | 359 |
| Verbindungsprobleme zwischen Horizon Client und dem PCoIP Secure Gateway  | 360 |
| Connection Problems Between Machines and View-Verbindungsserver Instances   | 362 |
| Verbindungsprobleme aufgrund einer falschen Zuweisung von IP-Adressen zu geklonten Computern  | 364 |
| Fehlerbehebung bei Problemen mit der USB-Umleitung  | 364 |
| Fehlerbehebung von GINA-Problemen auf Windows XP-Computern  | 366 |
| Verwalten von Maschinen und Richtlinien für nicht berechtigte Benutzer  | 367 |
| Weitere Informationen zur Fehlerbehebung  | 368 |

# Einrichten von Desktop- und Anwendungspools in View

In *Einrichten von Desktop- und Anwendungspools in View* wird die Erstellung und Bereitstellung von Maschinen-Pools beschrieben sowie die Erstellung von Pools mit Remoteanwendungen, die auf RDS-Hosts (Remote-Desktop-Dienste von Microsoft) ausgeführt werden. Dieser Abschnitt enthält Informationen zur Vorbereitung der Maschinen sowie zur Konfiguration der Richtlinien, zur Vergabe von Berechtigungen an Benutzer und Gruppen, zur Konfiguration von Remote-Desktop-Funktionen und zur Konfiguration von Benutzerprofilen über View Persona Management.

## Zielgruppe

Diese Informationen sind für alle Benutzer gedacht, die Desktop- und Anwendungspools erstellen und bereitstellen möchten. Die Informationen wurden für erfahrene Windows-Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Rechenzentrum-Vorgängen vertraut sind.

# Einführung in Desktop- und Anwendungspools

1

Mithilfe von VMware Horizon mit View können Sie Desktop-Pools erstellen, die einen, Hunderte oder sogar Tausende virtueller Desktops enthalten. Sie können Desktops bereitstellen, die auf virtuellen Maschinen, physischen Computern und Windows-Remote-Desktop-Dienste-Hosts ausgeführt werden. Wenn Sie eine virtuelle Maschine als Basis-Image erstellen, kann View einen Pool virtueller Desktops anhand dieses Images generieren. Außerdem können Sie Anwendungspools erstellen, die Benutzern Remote-Zugriff auf Anwendungen verschaffen.

Dieses Kapitel enthält die folgenden Themen:

- [Farmen, RDS-Hosts und Desktop- und Anwendungspools](#)
- [Vorteile von Desktop-Pools](#)
- [Desktop-Pools für bestimmte Nutzertypen](#)
- [Vorteile von Anwendungspools](#)

## Farmen, RDS-Hosts und Desktop- und Anwendungspools

Mit View können Sie Desktop- und Anwendungspools erstellen, um Benutzern Remote-Zugang zu VM-basierten Desktops, sitzungsbasierten Desktops, physischen Computern und Anwendungen zu gewähren. View nutzt die Technologien von Microsoft-Remote-Desktop-Dienste (RDS) und VMware PC-over-IP (PCoIP), um Benutzern hochwertigen Remote-Zugriff zu bieten.

### RDS-Hosts

RDS-Hosts sind Server-Computer, auf denen Windows-Remote-Desktop-Dienste und View Agent installiert sind. Diese Server hosten Hostanwendungen und Desktop-Sitzungen, auf die Benutzer remote zugreifen können. Um RDS-Desktop-Pools oder -Anwendungen zu verwenden, müssen Ihre Endbenutzer über Zugang zu Horizon Client 3.0 oder höher verfügen.

### Desktop-Pools

Es gibt drei Typen von Desktop-Pools: Automatisiert, manuell und RDS. Automatisierte Desktop-Pools verwenden eine Vorlage virtueller Maschinen von vCenter Server oder einen Snapshot, um einen Pool identischer virtueller Maschinen zu erstellen. Bei manuellen Desktop-Pools handelt es sich um eine Sammlung vorhandener virtueller Maschinen von vCenter Server, physische Computer oder virtuelle Maschinen von Drittanbietern. In automatisierten oder manuellen Pools kann ein Benutzer auf jeden

Windows-Computer gleichzeitig remote zugreifen. Bei RDS-Desktop-Pools handelt es sich um keine Sammlung von Windows-Computern. Stattdessen stellen Sie Benutzer mit Desktop-Sitzungen auf RDS-Hosts bereit. Mehrere Benutzer können gleichzeitig über Desktop-Sitzungen auf einem RDS-Host verfügen.

## Anwendungspools

Anwendungspools ermöglichen Ihnen, Anwendungen vielen Benutzern bereitzustellen. Diese Anwendungen im Anwendungspool werden auf einer Farm von RDS-Hosts ausgeführt.

## Farmen

Farmen sind Sammlungen von RDS-Hosts und vereinfachen die Verwaltung dieser Hosts. Farmen können eine Variablennummer von RDS-Hosts enthalten und Benutzern einen gängigen Satz von Anwendungen oder RDS-Desktops bereitstellen. Wenn Sie einen RDS-Desktop-Pool oder einen Anwendungspool erstellen, müssen Sie eine Farm festlegen. Die RDS-Hosts in der Farm stellen Benutzern Desktop- und Anwendungssitzungen bereit.

## Vorteile von Desktop-Pools

View bietet als Grundlage eines zentralen Managements die Möglichkeit, Pools mit Desktops zu bilden und bereitzustellen.

Sie können einen Remote-Desktop-Pool aus folgenden Quellen erstellen:

- Ein physisches System, wie beispielsweise ein physischer Desktop-PC oder ein RDS-Host
- Eine virtuelle Maschine, die auf einem ESXi-Host gehostet und von vCenter Server verwaltet wird
- Eine virtuelle Maschine, die auf einer anderen Virtualisierungsplattform als vCenter Server ausgeführt wird, die View Agent unterstützt

Wenn Sie eine virtuelle vSphere-Maschine als Desktop-Quelle verwenden, können Sie den Prozess der Erstellung der gewünschten Anzahl identischer virtueller Desktops automatisieren. Sie können eine minimale und maximale Anzahl an virtuellen Desktops festlegen, die für den Pool erstellt werden soll. Durch Festlegen dieser Parameter wird sichergestellt, dass Sie stets über eine ausreichende Anzahl von Remote-Desktops zur unmittelbaren Verwendung verfügen, ohne die verfügbaren Ressourcen zu überlasten.

Durch die Verwendung von Pools zur Verwaltung von Desktops wird das Anwenden von Einstellungen oder das Bereitstellen von Anwendungen auf allen Remote-Desktops in einem Pool ermöglicht. Die folgenden Beispiele zeigen einige der verfügbaren Einstellungen:

- Geben Sie an, welches Remote-Anzeigeprotokoll als Standard für den Remote-Desktop verwendet werden soll und ob Benutzer die Standardeinstellung außer Kraft setzen dürfen.
- Geben Sie beim Verwenden einer virtuellen Maschine an, ob die virtuelle Maschine ausgeschaltet werden soll, wenn sie nicht verwendet wird, und ob sie vollständig gelöscht werden soll.

- Geben Sie an, ob eine Microsoft Sysprep-Anpassungsspezifikation oder QuickPrep von VMware verwendet werden soll. Sysprep generiert eine eindeutige SID und GUID für jede virtuelle Maschine im Pool.

Darüber hinaus bietet das Verwenden von Desktop-Pools viele Vorteile.

|  |   |
|--|---|
| <b>Pools mit fester Zuweisung</b>      | Jedem Benutzer wird ein bestimmter Remote-Desktop zugewiesen, zu dem er bei jeder Anmeldung zurückkehrt. Benutzer können ihre Desktops individuell anpassen, Anwendungen installieren und Daten speichern.  |
| <b>Pools mit dynamischer Zuweisung</b> | <p>Der Remote-Desktop wird nach jeder Verwendung optional gelöscht und erneut erstellt, wodurch eine hohe Kontrolle der Umgebung möglich ist. Ein Desktop mit dynamischer Zuweisung entspricht einer Test- oder Kioskumgebung, in der die benötigten Anwendungen auf alle Desktops aufgespielt werden und alle Desktops Zugriff auf die benötigten Daten haben.</p> <p>Pools mit dynamischer Zuordnung ermöglichen auch das Erstellen eines Pools mit Desktops, die von Benutzern in Schichten genutzt werden können. Ein Pool mit 100 Desktops kann beispielsweise von 300 Benutzern verwendet werden, wenn diese in drei Schichten mit je 100 Benutzern arbeiten.</p> |

## Desktop-Pools für bestimmte Nutzertypen

View bietet viele Funktionen, mit deren Hilfe Sie Speicherplatz sparen und die für verschiedene Anwendungsfälle erforderliche Verarbeitungsleistung reduzieren können. Viele dieser Funktionen stehen als Pool-Einstellung zur Verfügung.

Die wichtigste Frage lautet, ob ein bestimmter Nutzertyp ein zustandsbehaftetes Desktop-Image oder ein zustandsloses Desktop-Image benötigt. Benutzer, die ein zustandsbehaftetes Desktop-Image benötigen, haben möglicherweise Daten im Betriebssystem-Image abgelegt, die gespeichert, gewartet und gesichert werden müssen. Beispielsweise installieren diese Benutzer eigene Anwendungen oder verwenden Daten, die nicht außerhalb der virtuellen Maschine, also auf einem Dateiserver oder in einer Anwendungsdatenbank, gespeichert werden können.

|   |   |
|---|---|
| <b>Zustandslose Desktop-Images</b>      | <p>Zustandslose Architekturen bieten viele Vorteile: Sie lassen sich z. B. leichter unterstützen und verursachen geringere Speicherkosten. Außerdem müssen virtuelle Maschinen auf der Basis verknüpfter Klone nur begrenzt gesichert werden, und die Disaster Recovery- und Business Continuity-Optionen sind weniger komplex und kostengünstiger.</p> |
| <b>Zustandsbehaftete Desktop-Images</b> | <p>Für diese Images sind eventuell herkömmliche Methoden zur Image-Verwaltung erforderlich. Zustandsbehaftete Images können in Verbindung mit bestimmten Speichersystemtechnologien geringe Speicherkosten verursachen. Sicherungs- und Wiederherstellungstechnologien wie VMware Consolidated Backup und VMware Site Recovery Manager sind</p>         |

bei der Erwägung von Sicherungs-, Disaster Recovery- und Business Continuity-Strategien von großer Bedeutung.

Sie können mit View Composer zustandslose Desktop-Images erstellen, indem Sie Pools mit dynamischer Zuweisung aus virtuellen Maschinen auf Basis verknüpfter Klone erstellen.

Zustandsbehaftete Desktop-Images werden erstellt, indem Sie Pools mit fester Zuweisung aus virtuellen Linked-Clone-Maschinen oder vollständigen virtuellen Maschinen erstellen. Wenn Sie virtuelle Linked-Clone-Maschinen verwenden, können Sie die persistenten Festplatten sowie die Ordnerumleitung in View Composer konfigurieren. Einige Speicherhersteller bieten kostengünstige Speicherlösungen für zustandsbehaftete Desktop-Images an. Diese Hersteller haben oft ihre eigenen empfohlenen Vorgehensweisen und Bereitstellungsdienstprogramme. Für den Einsatz eines dieser Produkte müssen Sie möglicherweise einen manuellen Pool mit fester Zuweisung erstellen.

## Pools für Sachbearbeiter

Sie können für Sachbearbeiter standardmäßig zustandslose Desktop-Images verwenden, damit das Image immer in einer bekannten und leicht unterstützbaren Konfiguration vorliegt und die Nutzer sich immer an einem beliebigen verfügbaren Desktop anmelden können.

Da Sachbearbeiter sich wiederholende Aufgaben in einer überschaubaren Anzahl an Anwendungen durchführen, können Sie zustandslose Desktop-Images erstellen. So benötigen Sie weniger Speicherplatz und Verarbeitungsleistung. Verwenden Sie folgende Pool-Einstellungen:

- Erstellen Sie einen automatisierten Pool, damit Desktops zusammen mit dem Pool erstellt oder je nach Pool-Auslastung nach Bedarf generiert werden können.
- Verwenden Sie die dynamische Zuweisung, damit Benutzer sich an jedem verfügbaren Desktop anmelden können. Durch diese Einstellung wird die Anzahl erforderlicher Desktops reduziert, wenn nicht alle gleichzeitig angemeldet sein müssen.
- Erstellen Sie View Composer-Linked-Clone-Desktops, damit Desktops dasselbe Basis-Image nutzen und weniger Speicherplatz im Rechenzentrum beanspruchen als vollständige virtuelle Maschinen.
- Legen Sie gegebenenfalls die Aktion fest, die beim Abmelden des Benutzers ausgeführt werden soll. Festplatten werden mit der Zeit größer. Sie können Speicherplatz sparen, indem Sie den Desktop auf den ursprünglichen Zustand aktualisieren, sobald der Benutzer sich abmeldet. Außerdem können Sie einen Zeitplan zur regelmäßigen Aktualisierung von Desktops festlegen. Zum Beispiel können Sie einstellen, dass Desktops täglich, wöchentlich oder monatlich aktualisiert werden.
- Verwenden Sie gegebenenfalls Virtual SAN-Datenspeicher. Virtual SAN virtualisiert die lokalen physischen Speicherfestplatten, die auf den ESXi-Hosts verfügbar sind, in einem einzelnen Datenspeicher, der von allen Hosts in einem vSphere-Cluster gemeinsam verwendet wird. Mithilfe von Virtual SAN können Sie auch den Speicher und die Leistung von virtuellen Maschinen verwalten, indem Sie Profile mit Speicherrichtlinien verwenden. Weitere Informationen finden Sie unter [Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung](#).

- Bei Bedarf sollten Sie erwägen, Desktops auf lokalen ESXi-Datenspeichern zu speichern. Diese Strategie kann verschiedene Vorteile bieten, so z.B. eine kostengünstige Hardware, eine schnelle Bereitstellung von virtuellen Maschinen, mehrere hochleistungsfähige Vorgänge zum Ändern des Betriebsstatus und eine vereinfachte Verwaltung. Eine Aufstellung der Beschränkungen finden Sie unter [Speichern von verknüpften Klonen auf lokalen Datenspeichern](#).
- Verwenden Sie die Persona-Verwaltungsfunktion, damit die Benutzer wie bei den Windows-Benutzerprofilen immer auf ihre bevorzugten Desktop-Anzeigeeinstellungen und Anwendungseinstellungen zugreifen können. Wenn Ihre Desktops bei der Abmeldung nicht aktualisiert oder gelöscht werden, können Sie die Persona so konfigurieren, dass sie bei der Abmeldung entfernt wird.

---

**Wichtig** View Persona Management erleichtert die Implementierung eines Pools mit dynamischer Zuweisung für die Benutzer, die die Einstellungen zwischen den Sitzungen beibehalten möchten. Bisher bestand eine der Einschränkungen von Desktops mit dynamischer Zuweisung darin, dass alle Konfigurationseinstellungen und alle auf dem Remote-Desktop gespeicherten Daten des Endbenutzers verloren gingen, wenn sich dieser abmeldete.

Bei jeder Anmeldung des Benutzers wurde der Desktophintergrund auf das Standard-Hintergrundbild zurückgesetzt, und alle Voreinstellungen für die einzelnen Anwendungen mussten erneut konfiguriert werden. Mit View Persona Management kann der Endbenutzer eines Desktops mit dynamischer Zuweisung nicht zwischen der eigenen Sitzung und der Sitzung auf einem Desktop mit fester Zuweisung unterscheiden.

---

## Pools für Büroanwender und Hauptbenutzer

Büroanwender müssen komplexe Dokumente erstellen und dauerhaft auf dem Desktop speichern können. Hauptbenutzer müssen ihre eigenen Anwendungen dauerhaft installieren können. Je nach Art und Menge der zu speichernden persönlichen Daten kann es sich um einen zustandslosen oder einen zustandsbehafteten Desktop handeln.

Da Hauptbenutzer und Büroanwender, zum Beispiel Buchhalter, Vertriebsleiter und Marktforscher, Dokumente und Einstellungen erstellen und speichern können müssen, erstellen Sie für diese Benutzer Desktops mit fester Zuweisung. Für Büroanwender, die benutzerinstallierte Anwendungen höchstens vorübergehend benötigen, können Sie zustandslose Desktop-Images erstellen und alle persönlichen Daten außerhalb der virtuellen Maschine auf einem Dateiserver oder in einer Anwendungsdatenbank speichern. Für andere Büroanwender und für Hauptanwender können Sie zustandsbehaftete Desktop-Images erstellen. Verwenden Sie folgende Pool-Einstellungen:

- Verwenden Sie Pools mit dedizierter Zuweisung, damit jeder Büroanwender oder Hauptbenutzer sich jedes Mal an demselben Desktop anmeldet.
- Verwenden Sie die Persona-Verwaltungsfunktion, damit die Benutzer wie bei den Windows-Benutzerprofilen immer auf ihre bevorzugten Desktop-Anzeigeeinstellungen und Anwendungseinstellungen zugreifen können.
- Verwenden Sie vStorage Thin Provisioning, damit jeder Desktop zunächst nur so viel Speicherplatz beansprucht wie die Festplatte für den anfänglichen Betrieb benötigt.



- Für Hauptbenutzer und Büroanwender, die ihre eigenen Anwendungen installieren müssen und so der Festplatte mit dem Betriebssystem Daten hinzufügen, erstellen Sie Desktops mit vollständigen virtuellen Maschinen. Verwenden Sie Mirage, um Anwendungen bereitzustellen und zu aktualisieren, ohne die von den Benutzern installierten Anwendungen zu überschreiben.
- Wenn Büroanwender benutzerinstallierte Anwendungen höchstens vorübergehend benötigen, können Sie View Composer-Linked-Clone-Desktops erstellen. Die Desktop-Images nutzen dasselbe Basis-Image und benötigen weniger Speicherplatz als vollständige virtuelle Maschinen.
- Wenn Sie View Composer mit virtuellen Desktops der Version vSphere 5.1 oder höher verwenden, aktivieren Sie die Funktion zur Rückgewinnung von Speicherplatz für vCenter Server und für den Desktop-Pool. Bei Verwendung der Funktion zur Rückgewinnung von Datenträgerplatz wird der Speicherplatz veralteter oder gelöschter Daten innerhalb eines Gastbetriebssystems mit einem Bereinigungs- oder Verkleinerungsprozess automatisch zurückgewonnen.
- Wenn Sie Linked-Clone-Desktops aus View Composer verwenden, implementieren Sie View Persona Management, servergespeicherte Profile oder andere Profilverwaltungslösungen.

Konfigurieren Sie persistente Festplatten, sodass Sie die Linked-Clone-Betriebssystemfestplatten aktualisieren und neu zusammenstellen und eine Kopie des Benutzerprofils auf den persistenten Festplatten speichern können.

## Pools für Kioskbenutzer

Zu Kioskbenutzern gehören zum Beispiel Kunden an Checkin-Schaltern von Fluggesellschaften, Schüler in Klassenräumen oder Bibliotheken, medizinisches Personal an Eingabestationen für medizinische Daten oder Kunden an öffentlichen Zugangspunkten. Konten, die nicht mit Benutzern, sondern mit Clientgeräten verknüpft sind, können diese Desktop-Pools verwenden, da Benutzer sich nicht anmelden müssen, um das Clientgerät oder den Remote-Desktop zu nutzen. Dennoch müssen Benutzer für manche Anwendungen Anmeldeinformationen zur Authentifizierung bereitstellen.

Desktops auf virtuellen Maschinen, die für die Ausführung im Kioskmodus eingestellt sind, verwenden zustandslose Desktop-Images, weil Benutzerdaten nicht auf der Betriebssystemfestplatte gespeichert werden müssen. Desktops im Kioskmodus werden mit Thin Client-Geräten oder gesperrten PCs mit eingeschränkten Funktionen verwendet. Sie müssen sicherstellen, dass die Desktop-Anwendung den Authentifizierungsmechanismus für sichere Transaktionen implementiert, dass das physische Netzwerk vor Sabotage und Überwachung geschützt ist und dass alle mit dem Netzwerk verbundenen Geräte vertrauenswürdig sind.

Es hat sich bewährt, dedizierte View-Verbindungsserver-Instanzen für die Verwaltung von Clients im Kioskmodus einzusetzen und dedizierte Organisationseinheiten und Gruppen in Active Directory für die Konten dieser Clients zu erstellen. Bei dieser Vorgehensweise werden die Systeme nicht nur partitioniert und gegen unberechtigten Zugriff geschützt, sondern gleichzeitig wird die Konfiguration und Verwaltung der Clients vereinfacht.

Zum Einrichten des Kioskmodus müssen Sie die Befehlszeilenschnittstelle `vdmadmin` verwenden und mehrere Verfahren durchführen, die im Dokument *Verwaltung von View* unter den Themen zum Kioskmodus dokumentiert sind. Im Zuge dieser Einrichtung können Sie die folgenden Pool-Einstellungen verwenden.

- Erstellen Sie einen automatisierten Pool, damit Desktops zusammen mit dem Pool erstellt oder je nach Pool-Auslastung nach Bedarf generiert werden können.
- Verwenden Sie die dynamische Zuweisung, damit Benutzer auf jeden verfügbaren Desktop im Pool zugreifen können.
- Erstellen Sie View Composer-Linked-Clone-Desktops, damit Desktops dasselbe Basis-Image nutzen und weniger Speicherplatz im Rechenzentrum beanspruchen als vollständige virtuelle Maschinen.
- Richten Sie eine Aktualisierungsrichtlinie ein, damit der Desktop häufig aktualisiert wird, beispielsweise bei jeder Benutzerabmeldung.
- Verwenden Sie gegebenenfalls Virtual SAN-Datenspeicher. Virtual SAN virtualisiert die lokalen physischen Speicherfestplatten, die auf den ESXi-Hosts verfügbar sind, in einem einzelnen Datenspeicher, der von allen Hosts in einem vSphere-Cluster gemeinsam verwendet wird. Mithilfe von Virtual SAN können Sie auch den Speicher und die Leistung von virtuellen Maschinen verwalten, indem Sie Profile mit Speicherrichtlinien verwenden. Weitere Informationen finden Sie unter [Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung](#).
- Bei Bedarf sollten Sie erwägen, Desktops auf lokalen ESXi-Datenspeichern zu speichern. Diese Strategie kann verschiedene Vorteile bieten, so z.B. eine kostengünstige Hardware, eine schnelle Bereitstellung von virtuellen Maschinen, mehrere hochleistungsfähige Vorgänge zum Ändern des Betriebsstatus und eine vereinfachte Verwaltung. Eine Aufstellung der Beschränkungen finden Sie unter [Speichern von verknüpften Klonen auf lokalen Datenspeichern](#).
- Verwenden Sie ein Active Directory-Gruppenrichtlinienobjekt zum Konfigurieren der standortbasierten Druckfunktion, damit der Desktop den nächstgelegenen Drucker verwendet. Eine vollständige Liste und Beschreibung der über Gruppenrichtlinien-ADM-Vorlagen verfügbaren Einstellungen finden Sie unter [Kapitel 16 Konfigurieren von Richtlinien für Desktop- und Anwendungspools](#).
- Mit einem Gruppenrichtlinienobjekt können Sie die Standardrichtlinie außer Kraft setzen, die das Anschließen lokaler USB-Geräte am Desktop gestattet, wenn der Desktop gestartet wird oder wenn USB-Geräte an den Clientcomputer angeschlossen werden.

## Vorteile von Anwendungspools

Mithilfe von Anwendungspools gewähren Sie Benutzern Zugriff auf Anwendungen, die auf Servern in einem Rechenzentrum ausgeführt werden, d. h. nicht auf ihren eigenen PCs oder Geräten.

Anwendungspools bieten mehrere wichtige Vorteile:

- **Barrierefreiheit**  
Benutzer können von jedem Gerät im Netzwerk aus auf Anwendungen zugreifen. Außerdem können Sie den sicheren Netzwerkzugriff konfigurieren.

- Unabhängigkeit der Geräte

Anwendungspools unterstützen zahlreiche Clientgeräte, wie zum Beispiel Smartphones, Tablets, Laptops, Thin Clients und PCs. Auf den Clientgeräten können verschiedene Betriebssysteme ausgeführt werden, wie zum Beispiel Windows, iOS, Mac OS oder Android.

- Zugriffssteuerung

Sie können einem Benutzer oder einer Benutzergruppe schnell und einfach den Zugriff auf Anwendungen gewähren oder verweigern.

- Schnellere Bereitstellung

Mithilfe von Anwendungspools lässt sich die Bereitstellung von Anwendungen beschleunigen, da Sie Anwendungen nur auf Servern in einem Rechenzentrum bereitstellen und jeder Server mehrere Benutzer unterstützen kann.

- Verwaltbarkeit

Die Verwaltung von Software, die auf Clientcomputern und Clientgeräten bereitgestellt wurde, ist in der Regel sehr ressourcenintensiv. Zu den Verwaltungsaufgaben zählen Bereitstellung, Konfiguration, Wartung, Support sowie Upgrades. Mithilfe von Anwendungspools können Sie die Softwareverwaltung in einem Unternehmen vereinfachen, da die Software auf Servern in einem Rechenzentrum ausgeführt wird, wodurch weniger installierte Kopien erforderlich sind.

- Sicherheit und Einhaltung gesetzlicher Bestimmungen

Mithilfe von Anwendungspools können Sie die Sicherheit verbessern, da Anwendungen und die zugehörigen Daten sich zentral in einem Rechenzentrum befinden. Zentralisierte Daten bieten bessere Möglichkeiten, um Sicherheitsprobleme zu vermeiden und die Einhaltung gesetzlicher Bestimmungen zu gewährleisten.

- Niedrigere Kosten

Je nach den Bestimmungen von Software-Lizenzverträgen kann das Hosting von Anwendungen in einem Rechenzentrum kostengünstiger sein. Auch andere Faktoren wie eine schnellere Bereitstellung und eine bessere Verwaltbarkeit tragen dazu bei, dass die Softwarekosten im Unternehmen gesenkt werden können.

# Vorbereiten nicht verwalteter Maschinen

# 2

Benutzer können auf Remote-Desktops zugreifen, die über nicht von vCenter Server verwaltete Maschinen bereitgestellt werden. Diese nicht verwalteten Maschinen können physische Computer und virtuelle Maschinen beinhalten, die auf anderen Virtualisierungsplattformen außer vCenter Server ausgeführt werden. Sie müssen eine nicht verwaltete Maschine vorbereiten, um den Zugriff auf einen Remote-Desktop bereitzustellen.

Informationen zur Vorbereitung von Maschinen, die als RDS-Hosts (Remotedesktopdienste) verwendet werden, finden Sie unter [Kapitel 7 Einrichten von Remote-Desktop-Dienste-Hosts](#).

Dieses Kapitel enthält die folgenden Themen:

- [Vorbereiten eines nicht verwalteten Computers für die Remote-Desktop-Bereitstellung](#)
- [Installieren von View Agent auf einer nicht verwalteten Maschine](#)

## Vorbereiten eines nicht verwalteten Computers für die Remote-Desktop-Bereitstellung

Zur Vorbereitung eines nicht verwalteten Computers für die Remote-Desktop-Bereitstellung müssen bestimmte Aufgaben ausgeführt werden.

### Voraussetzungen

- Vergewissern Sie sich, dass Sie über Administratorrechte für den nicht verwalteten Computer verfügen.
- Um sicherzustellen, dass Remote-Desktop-Benutzer zur lokalen Gruppe der Remote-Desktop-Benutzer des nicht verwalteten Computers hinzugefügt werden, erstellen Sie eine eingeschränkte Gruppe der Remote-Desktop-Benutzer in Active Directory. Weitere Informationen finden Sie im Dokument *Installation von View*.

### Verfahren

- 1 Schalten Sie den nicht verwalteten Computer ein und stellen Sie sicher, dass die View-Verbindungsserver-Instanz auf diesen Computer zugreifen kann.
- 2 Fügen Sie den nicht verwalteten Computer der Active Directory-Domäne für Ihre Remote-Desktops hinzu.

- 3 Konfigurieren Sie die Windows-Firewall so, dass Remote-Desktop-Verbindungen mit dem nicht verwalteten Computer zulässig sind.

#### Nächste Schritte

Installieren Sie View Agent auf dem nicht verwalteten Computer. Siehe [Installieren von View Agent auf einer nicht verwalteten Maschine](#).

## Installieren von View Agent auf einer nicht verwalteten Maschine

Sie müssen View Agent auf allen nicht verwalteten Maschinen installieren. View kann nicht verwaltete Maschinen nur dann verwalten, wenn View Agent installiert ist.

Um View Agent auf mehreren physischen Windows-Computern zu installieren, ohne auf Eingabeaufforderungen des Assistenten reagieren zu müssen, kann View Agent unbeaufsichtigt installiert werden. Siehe [Unbeaufsichtigte Installation von View Agent](#).

#### Voraussetzungen

- Vergewissern Sie sich, dass Sie über Administratorrechte für den nicht verwalteten Computer verfügen.
- Um eine nicht verwaltete Windows Server 2008 R2-Maschine als Remote-Desktop anstatt als RDS-Host zu verwenden, führen Sie die in [Vorbereiten von Windows Server 2008 R2 für Desktop-Verwendung](#) beschriebenen Schritte durch.
- Machen Sie sich mit den benutzerdefinierten Setup-Optionen für View Agent für nicht verwaltete Maschinen vertraut. Siehe [Benutzerdefinierte Setup-Optionen für View Agent für nicht verwaltete Maschinen](#).
- Machen Sie sich mit den TCP-Ports vertraut, die das View Agent-Installationsprogramm in der Firewall öffnet. Weitere Informationen finden Sie im Dokument *Planung der View-Architektur*.
- Laden Sie die View Agent-Installationsdatei von der VMware-Produktseite unter <http://www.vmware.com/products/> herunter.

#### Verfahren

- 1 Zum Starten des View Agent-Installationsprogramms doppelklicken Sie auf die Installationsdatei. Der Dateiname des Installationsprogramms lautet VMware-viewagent-y.y.y-xxxxxx.exe oder VMware-viewagent-x86\_64-y.y.y-xxxxxx.exe, wobei y.y.y die Versionsnummer und xxxxxx die Build-Nummer ist.
- 2 Stimmen Sie den Lizenzbedingungen von VMware zu.
- 3 Wählen Sie Ihre benutzerdefinierten Setup-Optionen.
- 4 Übernehmen oder ändern Sie den Zielordner.

- 5 Geben Sie im Textfeld **Server** den Hostnamen oder die IP-Adresse eines View-Verbindungsserver-Hosts ein.

Während der Installation registriert das Installationsprogramm die nicht verwaltete Maschine bei dieser View-Verbindungsserver-Instanz. Nach der Registrierung können die angegebene View-Verbindungsserver-Instanz sowie alle zusätzlichen Instanzen in derselben View-Verbindungsserver-Gruppe mit der nicht verwalteten Maschine kommunizieren.

- 6 Wählen Sie eine Authentifizierungsmethode zur Registrierung der nicht verwalteten Maschine für die View-Verbindungsserver-Instanz.

| Option   | Aktion   |
|--|--|
| <b>Authentifizierung als aktuell angemeldeter Benutzer</b> | Die Textfelder <b>Benutzername</b> und <b>Kennwort</b> sind deaktiviert und die Anmeldung an der View-Verbindungsserver-Instanz erfolgt über die aktuellen Anmeldeinformationen. |
| <b>Angeben von Administratoranmeldeinformationen</b>       | In die Textfelder <b>Benutzername</b> und <b>Kennwort</b> müssen der Benutzername und das Kennwort eines View-Verbindungsserver-Administrators eingegeben werden.                |

The user account must be a domain user with access to View LDAP on the View-Verbindungsserver instance. Ein lokales Benutzerkonto funktioniert nicht.

- 7 Befolgen Sie die Anweisungen im View Agent-Installationsprogramm und schließen Sie die Installation ab.
- 8 Wenn Sie die USB-Umleitungsoption ausgewählt haben, starten Sie die nicht verwaltete Maschine neu, um die USB-Unterstützung zu aktivieren.

Es wird möglicherweise auch der Assistent **Neue Hardware gefunden** gestartet. Befolgen Sie die Anweisungen des Assistenten zum Konfigurieren der Hardware, bevor Sie die nicht verwaltete Maschine neu starten.

Der VMware Horizon View Agent-Dienst wird auf der nicht verwalteten Maschine gestartet.

### Nächste Schritte

Verwenden Sie die nicht verwaltete Maschine, um einen Remote-Desktop zu erstellen. Siehe [Manuelle Desktop-Pools](#).

## Benutzerdefinierte Setup-Optionen für View Agent für nicht verwaltete Maschinen

Wenn Sie View Agent auf einer nicht verwalteten Maschine installieren, können Sie bestimmte benutzerdefinierte Setup-Optionen aus- oder abwählen. Zusätzlich installiert View Agent bestimmte Funktionen automatisch auf allen Gastbetriebssystemen, die diese Funktionen unterstützen. Diese Funktionen sind nicht optional.

**Tabelle 2-1. Benutzerdefinierte Setup-Optionen für View Agent für nicht verwaltete Maschinen (optional)**

| Option                  | Beschreibung  |
|-------------------------|---|
| USB-Umleitung           | <p>Gibt Benutzern Zugriff auf lokal verbundene USB-Geräte auf ihren Desktops.</p> <p>Die USB-Umleitung wird auf Remote-Desktops unterstützt, die auf Computern für Einzelbenutzer bereitgestellt sind, jedoch nicht auf Remote-Desktops, die auf RDS-Hosts basieren.</p> <p><b>Hinweis</b> Sie können mithilfe von Gruppenrichtlinieneinstellungen die USB-Umleitung für spezifische Benutzer deaktivieren.</p> |
| View Persona Management | Synchronisiert das Benutzerprofil auf dem lokalen Desktop mit einem Remote-Profil-Repository, damit die Benutzer immer Zugriff auf ihre Profile haben, wenn sie sich bei einem Desktop anmelden.  |
| PCoIP-Smartcard         | <p>Ermöglicht Benutzern die Authentifizierung per Smartcard, wenn sie das PCoIP-Anzeigeprotokoll verwenden.</p> <p>PCoIP-Smartcard wird auf Remote-Desktops unterstützt, die auf Computern für Einzelbenutzer bereitgestellt sind, jedoch nicht auf Remote-Desktops, die auf RDS-Hosts basieren.</p>  |

**Tabelle 2-2. View Agent-Funktionen, die automatisch auf nicht verwalteten Maschinen installiert werden (nicht optional)**

| Funktion                        | Beschreibung   |
|---------------------------------|--|
| PCoIP-Agent                     | <p>Ermöglicht Benutzern die Verbindungsherstellung mit dem Remote-Desktop über das PCoIP-Anzeigeprotokoll.</p> <p>Die PCoIP Agent-Funktion wird auf physischen Computern unterstützt, die mit einer Teradici TERA-Hostkarte konfiguriert sind.</p> <p><b>Hinweis</b> Wenn Sie unter Windows Vista die PCoIP Agent-Komponente installieren, wird die Windows-Gruppenrichtlinie <b>Software-SAS deaktivieren oder aktivieren</b> aktiviert und auf <b>Dienste</b> und <b>Anwendungen für die erleichterte Bedienung</b> gesetzt. Wenn Sie diese Einstellung ändern, funktioniert SSO nicht mehr ordnungsgemäß.</p> |
| Wyse-Multimedia-Umleitung (MMR) | Bietet eine Multimedia-Umleitung für Windows XP- und Windows Vista-Desktops und -Clients. Diese Funktion leitet einen Multimedia-Stream direkt an den Clientcomputer um, sodass der Multimedia-Stream nicht auf dem Remote-ESXi-Host, sondern auf der Clienthardware verarbeitet wird.   |
| Lync                            | Bietet Unterstützung für Microsoft Lync 2013-Client auf Remote-Desktops.   |

| Funktion                | Beschreibung   |
|-------------------------|--|
| Unity Touch             | Ermöglicht Tablet- und Smartphone-Benutzern eine einfache Interaktion über Windows-Anwendungen, die auf dem Remote-Desktop ausgeführt werden. Die Benutzer können Windows-Anwendungen und -Dateien bequem durchsuchen, suchen und öffnen, Lieblingsanwendungen und -dateien auswählen und bequem zwischen ausgeführten Anwendungen wechseln, ohne das Start-Menü oder die Taskleiste zu verwenden. |
| Virtueller Audiotreiber | Bietet einen virtuellen Audio-Treiber auf dem Remote-Desktop.  |



# Erstellen und Vorbereiten virtueller Maschinen

# 3

Sie können über vCenter Server verwaltete virtuelle Maschinen dazu verwenden, Remote-Desktops bereitzustellen und zu verteilen und bereitzustellen. Sie können eine virtuelle Maschine, die von vCenter Server verwaltet wird, als Vorlage für einen automatisierten Pool, für ein übergeordnetes Element für einen Pool mit verknüpften Klonen oder für eine Maschine in einem manuellen Pool verwenden. Sie müssen virtuelle Maschinen vorbereiten, um den Zugriff auf einen Remote-Desktop bereitzustellen.

Dieses Kapitel enthält die folgenden Themen:

- [Erstellen virtueller Maschinen für die Remote-Desktop-Bereitstellung](#)
- [Installieren von View Agent auf einer virtuellen Maschine](#)
- [Unbeaufsichtigte Installation von View Agent](#)
- [Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent](#)
- [Optimieren der Leistung des Gastbetriebssystems für alle Windows-Versionen](#)
- [Optimieren der Leistung des Windows 7- und Windows 8-Gastbetriebssystems](#)
- [Optimieren von Windows 7 und Windows 8 für virtuelle Maschinen mit verknüpftem Klon](#)
- [Vorbereiten virtueller Maschinen für View Composer](#)
- [Erstellen von Vorlagen virtueller Maschinen](#)
- [Erstellen von Anpassungsspezifikationen](#)

## Erstellen virtueller Maschinen für die Remote-Desktop-Bereitstellung

Mit der ersten virtuellen Maschine wird ein virtuelles Hardwareprofil und ein Betriebssystem eingerichtet, die für die schnelle Bereitstellung von Remote-Desktops verwendet werden.

### Verfahren

#### 1 [Erstellen einer virtuellen Maschine für die Remote-Desktop-Bereitstellung](#)

Verwenden Sie vSphere Client zum Erstellen virtueller Maschinen in vCenter Server für Remote-Desktops.

## 2 Installieren eines Gastbetriebssystems

Nachdem Sie eine virtuelle Maschine erstellt haben, müssen Sie ein Gastbetriebssystem installieren.

## 3 Vorbereiten eines Gastbetriebssystems für die Remote-Desktop-Bereitstellung

Sie müssen bestimmte Aufgaben durchführen, um ein Gastbetriebssystem für die Remote-Desktop-Bereitstellung vorzubereiten.

## 4 Vorbereiten von Windows Server 2008 R2 für Desktop-Verwendung

Um eine virtuelle Maschine von Windows Server 2008 R2 als View-Desktop für nur eine Sitzung (anstatt eines RDS-Hosts) zu verwenden, müssen Sie vor der Installation von View Agent in der virtuellen Maschine bestimmte Schritte durchführen. Sie müssen auch View Administrator konfigurieren, um Windows Server 2008 R2 als unterstütztes Betriebssystem für die Desktop-Verwendung von View zu behandeln.

## 5 Installieren von „Desktopdarstellung“ auf Windows Server 2008 R2

Für RDS-Desktops und -Anwendungen und für VDI-Desktops, die auf Einzelbenutzer-VMs mit Windows Server bereitgestellt werden, erfordert die Scannerumleitung, dass Sie die Funktion „Desktopdarstellung“ auf den RDS-Hosts und den Einzelbenutzer-VMs installieren.

# Erstellen einer virtuellen Maschine für die Remote-Desktop-Bereitstellung

Verwenden Sie vSphere Client zum Erstellen virtueller Maschinen in vCenter Server für Remote-Desktops.

### Voraussetzungen

- Laden Sie eine ISO-Image-Datei des Gastbetriebssystems in einen Datenspeicher auf Ihren ESXi-Server hoch.
- Machen Sie sich mit den benutzerdefinierten Konfigurationsparametern für virtuelle Maschinen vertraut. Siehe [Benutzerdefinierte Konfigurationsparameter für die virtuelle Maschine](#).

### Verfahren

- 1 Melden Sie sich in vSphere Client am vCenter Server-System an.
- 2 Wählen Sie **Datei > Neu > Virtuelle Maschine** aus, um den Assistenten **Neue virtuelle Maschine** zu starten.
- 3 Wählen Sie **Benutzerdefiniert** aus und konfigurieren Sie benutzerdefinierte Konfigurationsparameter.

- 4 Wählen Sie **Einstellungen virtueller Maschinen vor Abschluss bearbeiten** aus und klicken Sie auf **Weiter**, um die Hardwareeinstellungen zu konfigurieren.
  - a Fügen Sie ein CD-/DVD-Laufwerk hinzu, legen Sie den Medientyp auf die Verwendung einer ISO-Image-Datei fest, wählen Sie das ISO-Image des Gastbetriebssystems, das Sie in Ihren Datenspeicher hochgeladen haben, und wählen Sie **Beim Einschalten verbinden**.
  - b Wenn Sie ein Windows XP-Gastbetriebssystem installieren, fügen Sie ein Diskettenlaufwerk hinzu und legen Sie **Gerätetyp** auf **Clientgerät** fest.
  - c Legen Sie **Startverzögerung nach dem Einschalten** auf 10.000 Millisekunden fest.
- 5 Klicken Sie auf **Fertig stellen**, um die virtuelle Maschine zu erstellen.

### Nächste Schritte

Installieren Sie ein Gastbetriebssystem auf der virtuellen Maschine.

## Benutzerdefinierte Konfigurationsparameter für die virtuelle Maschine

Sie können benutzerdefinierte VM-Konfigurationsparameter als grundlegende Einstellungen für das Erstellen virtueller Maschinen in Ihrer Remote-Desktop-Bereitstellung verwenden.

Sie können bestimmte Einstellungen ändern, wenn Sie View Administrator verwenden, um Desktop-Pools aus der virtuellen Maschine bereitzustellen.

**Tabelle 3-1. Benutzerdefinierte Konfigurationsparameter**

| Parameter                | Beschreibung und Empfehlungen  |
|--------------------------|--|
| Name and Location        | Der Name und der Speicherort der virtuellen Maschine.<br>Wenn Sie die virtuelle Maschine als Vorlage verwenden möchten, weisen Sie ihr einen allgemeinen Namen zu. Der Speicherort kann ein beliebiger Ordner in der Bestandsliste des Rechenzentrums sein.  |
| Host/Cluster             | Der ESXi-Server oder der Cluster an Serverressourcen, auf dem die virtuelle Maschine ausgeführt wird.<br>Wenn die virtuelle Maschine als Vorlage verwendet werden soll, gibt der Speicherort der ersten virtuellen Maschine nicht zwangsläufig an, wo sich die zukünftigen virtuellen Maschinen befinden, die anhand dieser Vorlage erstellt wurden. |
| Resource Pool            | Wenn die physischen ESXi-Serverressourcen in Ressourcenpools unterteilt werden, können Sie sie der virtuellen Maschine zuweisen.   |
| Datastore                | Der Speicherort der mit der virtuellen Maschine verknüpften Dateien.   |
| Hardware Machine Version | Die verfügbare Hardware-Maschinenversion hängt von der ausgeführten ESXi-Version ab. Als optimale Vorgehensweise hat sich herausgestellt, die neueste verfügbare Hardware-Maschinenversion auszuwählen, die die meisten VM-Funktionen bereitstellt. Bestimmte View-Funktionen erfordern minimale Hardware-Maschinenversionen.                        |

| Parameter              | Beschreibung und Empfehlungen   |
|------------------------|---|
| Guest Operating System | Die Art des Betriebssystems, das Sie auf der virtuellen Maschine installieren.  |
| CPUs                   | Die Anzahl an virtuellen Prozessoren in der virtuellen Maschine.<br>Für die meisten Gastbetriebssysteme ist ein einzelner Prozessor ausreichend.  |
| Memory                 | Die Arbeitsspeichergröße, die der virtuellen Maschine zugewiesen wird.<br>In den meisten Fällen reicht 512 MB aus.  |
| Network                | <p>Die Anzahl an virtuellen Netzwerkkarten (Network Interface Cards, NICs) in der virtuellen Maschine.</p> <p>Eine Netzwerkkarte reicht im Allgemeinen aus. Der Netzwerkname sollte in allen virtuellen Infrastrukturen konsistent sein. Ein falscher Netzwerkname in einer Vorlage kann zu Fehlern während der Anpassungsphasen der Instanz führen.</p> <p>Wenn Sie View Agent auf einer virtuellen Maschine installieren, die mehr als eine Netzwerkkarte besitzt, müssen Sie das von View Agent verwendete Subnetz konfigurieren. Weitere Informationen finden Sie unter <a href="#">Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent</a>.</p> <hr/> <p><b>Wichtig</b> Für die Betriebssysteme Windows 8, Windows 7, Windows Vista und Windows Server 2008 R2 müssen Sie den Netzwerkadapter „VMXNET 3“ auswählen. Die Verwendung des standardmäßigen E1000-Adapters kann zu Zeitüberschreitungsfehlern bei der Anpassung auf virtuellen Maschinen führen. Zur Verwendung des VMXNET 3-Adapters müssen Sie einen Microsoft-Hotfix-Patch installieren:</p> <ul style="list-style-type: none"> <li>■ Für Windows 7 SP1: <a href="http://support.microsoft.com/kb/2550978">http://support.microsoft.com/kb/2550978</a></li> <li>■ Für Windows 7-Versionen vor SP1: <a href="http://support.microsoft.com/kb/2344941">http://support.microsoft.com/kb/2344941</a></li> </ul> |

| Parameter       | Beschreibung und Empfehlungen  |
|-----------------|--|
| SCSI Controller | <p>Der Typ des SCSI-Adapters, der mit der virtuellen Maschine verwendet wird.</p> <p>Für die Gastbetriebssysteme Windows 8, Windows 7 und Windows XP sollten Sie den LSI Logic-Adapter angeben. Der LSI Logic-Adapter zeigt eine bessere Leistung und arbeitet mit generischen SCSI-Geräten besser zusammen.</p> <p>LSI Logic SAS ist nur für virtuelle Maschinen mit der Hardwareversion 7 und höher verfügbar.</p> <hr/> <p><b>Hinweis</b> Windows XP umfasst keinen Treiber für den LSI Logic-Adapter. Sie müssen den Treiber von der LSI Logic-Website herunterladen.</p>                |
| Select a Disk   | <p>Die Festplatte zur Verwendung mit der virtuellen Maschine.</p> <p>Erstellen Sie eine neue virtuelle Festplatte basierend auf der Größe des lokalen Speichers, den Sie jedem Benutzer zuweisen möchten. Berücksichtigen Sie ausreichend Speicherplatz für die Betriebssysteminstallation, Patches sowie lokal installierten Anwendungen.</p> <p>Um den Bedarf an Speicherplatz und die Verwaltung lokaler Daten zu reduzieren, wird empfohlen, die Informationen, das Profil und die Dokumente des Benutzers statt auf eine lokale Festplatte auf freigegebene Netzwerke zu speichern.</p> |

## Installieren eines Gastbetriebssystems

Nachdem Sie eine virtuelle Maschine erstellt haben, müssen Sie ein Gastbetriebssystem installieren.

### Voraussetzungen

- Überprüfen Sie, ob sich eine ISO-Image-Datei des Gastbetriebssystems auf einem Datenspeicher auf Ihrem ESXi-Server befindet.
- Vergewissern Sie sich, dass das CD-/DVD-Laufwerk in der virtuellen Maschine auf die ISO-Image-Datei des Gastbetriebssystems weist und dass das CD-/DVD-Laufwerk für die Verbindung beim Einschalten konfiguriert ist.
- Wenn Sie Windows XP installieren und den LSI Logic-Adapter für die virtuelle Maschine ausgewählt haben, laden Sie den Treiber für den LSI20320-R-Controller von der LSI Logic-Website herunter, erstellen Sie eine Disketten-Image-Datei (.flp), die den Treiber enthält, und laden Sie die Datei in einen Datenspeicher auf Ihrem Server hoch.

### Verfahren

- 1 Melden Sie sich in vSphere Client am vCenter Server-System an, auf dem sich die virtuelle Maschine befindet.

- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie **Einschalten/Ausschalten** und **Einschalten** aus, um die virtuelle Maschine zu starten.

Da Sie das CD-/DVD-Laufwerk so konfiguriert haben, dass es auf das ISO-Image weist und beim Einschalten verbunden wird, startet die Installation des Gastbetriebssystems automatisch.

- 3 Klicken Sie auf die Registerkarte **Konsole** und folgen Sie den Installationsanweisungen des Betriebssystemanbieters.
- 4 Wenn Sie Windows XP installieren und den LSI Logic-Adapter für die virtuelle Maschine ausgewählt haben, installieren Sie den LSI Logic-Treiber während des Windows-Setups.
  - a Drücken Sie F6, um zusätzliche SCSI-Treiber auszuwählen.
  - b Geben Sie **S** ein, um ein zusätzliches Gerät anzugeben.
  - c Klicken Sie in der vSphere Client-Symbolleiste auf **Diskette verbinden**, um die Diskettenimagedatei des LSI Logic-Treibers (.flp) auszuwählen.
  - d Kehren Sie zum Windows-Installationsbildschirm zurück und drücken Sie die Eingabetaste, um mit dem Windows-Installationsvorgang fortzufahren.
  - e Wenn der Windows-Installationsvorgang abgeschlossen wurde, trennen Sie die Verbindung zum virtuellen Diskettenlaufwerk.
- 5 Wenn Sie Windows 7 oder Windows 8 installieren, aktivieren Sie Windows online.

#### Nächste Schritte

Bereiten Sie das Gastbetriebssystem für die View-Desktop-Bereitstellung vor.

## Vorbereiten eines Gastbetriebssystems für die Remote-Desktop-Bereitstellung

Sie müssen bestimmte Aufgaben durchführen, um ein Gastbetriebssystem für die Remote-Desktop-Bereitstellung vorzubereiten.

#### Voraussetzungen

- Erstellen Sie eine virtuelle Maschine und installieren Sie ein Gastbetriebssystem.
- Konfigurieren Sie einen Active Directory-Domänencontroller für Ihre Remote-Desktops. Weitere Informationen finden Sie im Dokument *Installation von View*.
- Um sicherzustellen, dass Desktop-Benutzer zur lokalen Gruppe „Remote-Desktop-Benutzer“ der virtuellen Maschine hinzugefügt werden, erstellen Sie eine eingeschränkte Gruppe „Remote-Desktop-Benutzer“ in Active Directory. Weitere Informationen finden Sie im Dokument *Installation von View*.
- Stellen Sie sicher, dass die Remotedesktopdienste, in Windows XP-Systemen als „Terminaldienste“ bezeichnet, auf der virtuellen Maschine gestartet werden. Die Remotedesktopdienste sind

erforderlich für die Installation von View Agent, SSO und andere View-Vorgänge. Sie können den RDP-Zugriff auf Ihre View-Desktops durch Konfiguration der Desktop-Pool-Einstellungen und Gruppenrichtlinieneinstellungen deaktivieren. Siehe [Verhindern vom Zugriff auf View-Desktops durch RDP](#).

- Stellen Sie sicher, dass Sie auf dem Gastbetriebssystem über Administratorberechtigungen verfügen.
- In Windows Vista-Betriebssystemen muss sichergestellt werden, dass der Windows Update-Dienst aktiviert ist. Wird dieser Dienst in Windows Vista deaktiviert, kann das View Agent-Installationsprogramm den USB-Treiber nicht installieren.
- Bereiten Sie unter Windows Server 2008 R2 das Betriebssystem für die Desktop-Verwendung vor. Siehe [Vorbereiten von Windows Server 2008 R2 für Desktop-Verwendung](#).
- Wenn Sie das Rendern von 3D-Grafiken für Desktop-Pools konfigurieren möchten, machen Sie sich mit der Einstellung **3D-Unterstützung aktivieren** für virtuelle Maschinen vertraut.

Diese Einstellung ist auf Betriebssystemen der Version Windows 7 und höher aktiviert. Auf Hosts der Version ESXi 5.1 und höher können Sie zudem festlegen, wie der 3D-Renderer auf dem ESXi-Host verwaltet wird. Einzelheiten finden Sie im Dokument *Verwaltung virtueller vSphere-Maschinen*.

## Verfahren

- 1 Melden Sie sich in vSphere Client am vCenter Server-System an, auf dem sich die virtuelle Maschine befindet.
- 2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie **Einschalten/Ausschalten** und **Einschalten** aus, um die virtuelle Maschine zu starten.
- 3 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie **Gast** und **VMware Tools installieren/aktualisieren** aus, um die aktuelle Version von VMware Tools zu installieren.

---

**Hinweis** Die Funktion zum virtuellen Drucken wird nur unterstützt, wenn Sie diese von View Agent aus installieren. Das virtuelle Drucken wird nicht unterstützt, wenn Sie die Funktion mit VMware Tools installieren.

---

- 4 Verwenden Sie die VMware Tools-Funktion zur Uhrzeitsynchronisierung, um sicherzustellen, dass die virtuelle Maschine mit ESXi synchronisiert ist.

ESXi muss mit einer externen NTP-Quelle synchronisiert werden, beispielsweise mit derselben Uhrzeitquelle wie Active Directory.

Deaktivieren Sie andere Uhrzeitsynchronisierungsmechanismen wie z. B. den Windows-Zeitdienst.

Die VMware Tools-Online-Hilfe stellt Informationen zum Konfigurieren der Uhrzeitsynchronisierung zwischen Gast und Host bereit.

- 5 Installieren Sie Service Packs und Updates.
- 6 Installieren Sie eine Antivirensoftware.

- 7 Installieren Sie weitere Anwendungen und Software, z. B. Smartcard-Treiber, wenn Sie die Smartcard-Authentifizierung verwenden.

Wenn Sie vorhaben, Workspace zu verwenden, um einen Katalog mit ThinApp-Anwendungen anzubieten, müssen Sie Workspace für Windows installieren.

In Windows XP-Systemen müssen alle Drittanbieter- und Softwareanwendungen (außer Microsoft .NET Framework) vor der Installation von View Agent installiert werden.

---

**Wichtig** Wenn Sie Microsoft .NET Framework installieren möchten, müssen Sie die Installation nach der Installation von View Agent durchführen.

---

- 8 Wenn Horizon Client-Geräte sich über das PCoIP-Anzeigeprotokoll mit der virtuellen Maschine verbinden, legen Sie die Energieoption **Anzeige deaktivieren** auf **Nie** fest.

Wenn Sie diese Einstellung nicht deaktivieren, verbleibt die Anzeige bei Aktivierung des Energiesparmodus im letzten Status und scheint nicht mehr zu reagieren.

- 9 Wenn sich Horizon Client-Geräte über das PCoIP-Anzeigeprotokoll mit der virtuellen Maschine verbinden, navigieren Sie zu **Systemsteuerung > System > Erweiterte Systemeinstellungen > Leistungseinstellungen** und ändern Sie die Einstellung für **Visuelle Effekte** in **Für optimale Leistung anpassen**.

Wenn Sie stattdessen die Einstellung **Für optimale Darstellung anpassen** oder **Optimale Einstellung automatisch auswählen** verwenden und Windows Darstellung statt Leistung wählt, wird die Leistung negativ beeinflusst.

- 10 Wenn in Ihrer Netzwerkumgebung ein Proxy-Server verwendet wird, konfigurieren Sie die Proxy-Einstellungen für das Netzwerk.

- 11 Konfigurieren Sie die Eigenschaften für Netzwerkverbindungen.

- a Weisen Sie eine statische IP-Adresse zu oder geben Sie eine IP-Adresse an, die durch einen DHCP-Server vergeben wurde.

View bietet keine Unterstützung für verbindungslokale Adressen (169.254.x.x) für View-Desktops.

- b Legen Sie die bevorzugte und alternative DNS-Serveradressen auf Ihre Active Directory-Serveradresse fest.

- 12 Fügen Sie die virtuelle Maschine der Active Directory-Domäne für Ihre Remote-Desktops hinzu.

Eine übergeordnete virtuelle Maschine, die Sie für View Composer verwenden, muss entweder zu derselben Active Directory-Domäne wie die Domäne gehören, mit der sich die Linked-Clone-Desktops verbinden, oder sie muss Mitglied der lokalen ARBEITSGRUPPE sein.

- 13 Konfigurieren Sie die Windows-Firewall so, dass Remote-Desktop-Verbindungen mit der virtuellen Maschine zulässig sind.

- 14 (Optional) Deaktivieren Sie Hotplug-PCI-Geräte.

Dieser Schritt verhindert, dass Benutzer versehentlich das virtuelle Netzwerkgerät (vNIC) von der virtuellen Maschine trennen.



**15** (Optional) Konfigurieren Sie Skripte für die Benutzeranpassung.

### Nächste Schritte

Installieren Sie View Agent. Siehe [Installieren von View Agent auf einer virtuellen Maschine](#).

## Vorbereiten von Windows Server 2008 R2 für Desktop-Verwendung

Um eine virtuelle Maschine von Windows Server 2008 R2 als View-Desktop für nur eine Sitzung (anstatt eines RDS-Hosts) zu verwenden, müssen Sie vor der Installation von View Agent in der virtuellen Maschine bestimmte Schritte durchführen. Sie müssen auch View Administrator konfigurieren, um Windows Server 2008 R2 als unterstütztes Betriebssystem für die Desktop-Verwendung von View zu behandeln.

### Voraussetzungen

Machen Sie sich mit den Schritten zur Installation der Funktion „Desktopdarstellung“ in Windows Server 2008 R2 vertraut. Siehe [Installieren von „Desktopdarstellung“ auf Windows Server 2008 R2](#).

### Verfahren

- 1** Stellen Sie sicher, dass die Remotedesktopdienste-Rolle nicht installiert ist.  
  
Wenn die Remotedesktopdienste-Rolle nicht vorhanden ist, fordert das View Agent-Installationsprogramm Sie dazu auf, die Installation von View Agent im Desktop-Modus zu bestätigen. Wenn die Remotedesktopdienste-Rolle nicht vorhanden ist, zeigt das View Agent-Installationsprogramm diese Aufforderung nicht an und behandelt den Windows Server 2008 R2-Computer als RDS-Host anstatt als View-Desktop für nur eine Sitzung.
- 2** Installieren Sie Windows Server 2008 R2 Service Pack 1 (SP1).  
  
Wenn Sie SP1 nicht installieren, tritt bei der Installation von View Agent ein Fehler auf.
- 3** (Optional) Installieren Sie die Funktion „Desktopdarstellung“, wenn Sie beabsichtigen, die folgenden Funktionen zu verwenden:
  - HTML Access
  - Scannerumleitung
  - Windows Aero
- 4** (Optional) Um Windows Aero auf einem Windows Server 2008 R2-Desktop zu verwenden, starten Sie den Design-Dienst.  
  
Wenn Sie einen Desktop-Pool erstellen oder bearbeiten, können Sie das 3D-Grafikrendering für Ihre Desktops konfigurieren. Die Einstellung „3D-Renderer“ bietet eine Software-Option, die Benutzern das Ausführen von Windows Aero auf den Desktops im Pool ermöglicht.

- 5 Konfigurieren Sie View Administrator, um Windows Server 2008 R2 als unterstütztes Betriebssystem des Desktops zu behandeln.

Wenn Sie diesen Schritt nicht durchführen, können Sie die Computer von Windows Server 2008 R2 nicht für die Desktop-Verwendung in View Administrator auswählen.

- a Wählen Sie in View Administrator **View-Konfiguration > Globale Einstellungen** aus.
- b Klicken Sie im Bereich „Allgemein“ auf **Bearbeiten**.
- c Wählen Sie das Kontrollkästchen **Windows Server 2008 R2-Desktops aktivieren** aus und klicken Sie auf **OK**.

Wenn Sie Windows Server 2008 R2-Desktops in View Administrator aktivieren, zeigt View Administrator alle verfügbaren Windows Server 2008 R2-Computer, einschließlich Computer, auf denen View-Verbindungsserver installiert sind, als mögliche Computer für die Desktop-Verwendung an. Sie können View Agent nicht auf Computern installieren, auf denen andere View-Softwarekomponenten installiert sind.

## Installieren von „Desktopdarstellung“ auf Windows Server 2008 R2

Für RDS-Desktops und -Anwendungen und für VDI-Desktops, die auf Einzelbenutzer-VMs mit Windows Server bereitgestellt werden, erfordert die Scannerumleitung, dass Sie die Funktion „Desktopdarstellung“ auf den RDS-Hosts und den Einzelbenutzer-VMs installieren.

### Verfahren

- 1 Melden Sie sich als Administrator an.
- 2 Starten Sie Server Manager.
- 3 Klicken Sie auf **Features**.
- 4 Klicken Sie auf **Features hinzufügen**.
- 5 Aktivieren Sie auf der Seite „Features auswählen“ das Kontrollkästchen **Desktopdarstellung**.
- 6 Lesen Sie die Informationen zu anderen Funktionen, die die Funktion „Desktopdarstellung“ benötigt, und klicken Sie auf **Erforderliche Features hinzufügen**.
- 7 Folgen Sie den Anweisungen und schließen Sie die Installation ab.

## Installieren von View Agent auf einer virtuellen Maschine

Sie müssen View Agent installieren, damit View-Verbindungsserver mit den über vCenter Server verwalteten virtuellen Maschinen kommunizieren kann. Installieren Sie View Agent auf allen virtuellen Maschinen, die Sie als Vorlage für automatisierte Desktop-Pools, übergeordnete Elemente für Linked-Clone-Desktop-Pools und Computer in manuellen Desktop-Pools verwenden.

Um View Agent auf mehreren virtuellen Windows-Maschinen zu installieren, ohne auf Eingabeaufforderungen des Assistenten reagieren zu müssen, kann View Agent unbeaufsichtigt installiert werden. Siehe [Unbeaufsichtigte Installation von View Agent](#).

Die View Agent-Software darf nicht auf derselben virtuellen Maschine oder demselben physischen Computer wie eine andere View-Softwarekomponente vorliegen, Sicherheitsserver, View-Verbindungsserver, View Composer oder Horizon Client eingeschlossen.

### Voraussetzungen

- Bereiten Sie das Gastbetriebssystem für die Remote-Desktop-Bereitstellung vor. Siehe [Vorbereiten eines Gastbetriebssystems für die Remote-Desktop-Bereitstellung](#).
- Um eine virtuelle Maschine von Windows Server 2008 R2 als Remote-Desktop (anstelle eines RDS-Hosts) zu verwenden, führen Sie die in [Vorbereiten von Windows Server 2008 R2 für Desktop-Verwendung](#) beschriebenen Schritte durch.
- Laden Sie die View Agent-Installationsdatei von der VMware-Produktseite unter <http://www.vmware.com/products/> herunter.
- Vergewissern Sie sich, dass Sie über Administratorrechte für die virtuelle Maschine verfügen.
- Machen Sie sich mit den benutzerdefinierten Setup-Optionen für View Agent vertraut. Siehe [Benutzerdefinierte Setup-Optionen für View Agent](#).
- Machen Sie sich mit den TCP-Ports vertraut, die das View Agent-Installationsprogramm in der Firewall öffnet. Weitere Informationen finden Sie im Dokument *Planung der View-Architektur*.
- Wenn Sie die benutzerdefinierte Setup-Option für View Composer Agent auswählen, stellen Sie sicher, dass Sie über eine Lizenz zur Verwendung von View Composer verfügen.

### Verfahren

- 1 Zum Starten des View Agent-Installationsprogramms doppelklicken Sie auf die Installationsdatei.  
Der Dateiname des Installationsprogramms lautet VMware-viewagent-y.y.y-xxxxxx.exe oder VMware-viewagent-x86\_64-y.y.y-xxxxxx.exe, wobei y.y.y die Versionsnummer und xxxxxx die Build-Nummer ist.
- 2 Stimmen Sie den Lizenzbedingungen von VMware zu.
- 3 Wenn Sie View Agent auf einem Windows Server-Computer installieren, auf dem die Rolle „Remote-Desktop-Sitzungshost“ (RDSH) nicht installiert ist, wählen Sie **VMware Horizon View Agent im 'Desktop-Modus' installieren** aus.  
  
Mit der Auswahl dieser Option wird der Windows Server-Computer als View-Desktop für Einzelbenutzer statt als RDS-Host konfiguriert. Wenn der Computer als RDS-Host fungieren soll, gehen Sie wie folgt vor: Brechen Sie die Installation von View Agent ab, installieren Sie die RDSH-Rolle auf dem Computer und starten Sie die View Agent-Installation neu.
- 4 Wählen Sie Ihre benutzerdefinierten Setup-Optionen.  
  
Wählen Sie zum Bereitstellen von Linked-Clone-Desktops die Option **View Composer Agent** aus.
- 5 Übernehmen oder ändern Sie den Zielordner.

- 6 Befolgen Sie die Anweisungen im View Agent-Installationsprogramm und schließen Sie die Installation ab.

---

**Hinweis** Wenn Sie während der Vorbereitung des Gastbetriebssystems nicht die Remote-Desktop-Unterstützung aktiviert haben, werden Sie nun vom View Agent-Installationsprogramm aufgefordert, dies nachzuholen. Wenn Sie die Remote-Desktop-Unterstützung während der View Agent-Installation nicht aktivieren, müssen Sie die Aktivierung nach Abschluss der Installation manuell vornehmen.

---

- 7 Wenn Sie die USB-Umleitungsoption ausgewählt haben, starten Sie die virtuelle Maschine neu, um die USB-Unterstützung zu aktivieren.

Es wird möglicherweise auch der Assistent **Neue Hardware gefunden** gestartet. Befolgen Sie die Anweisungen des Assistenten zum Konfigurieren der Hardware, bevor Sie die virtuelle Maschine neu starten.

Der VMware Horizon View Agent-Dienst wird auf der virtuellen Maschine gestartet.

Wenn Sie die Option **View Composer Agent** ausgewählt haben, wird der VMware Horizon View Composer Guest Agent Server-Dienst auf der virtuellen Maschine gestartet.

#### Nächste Schritte

Wenn die virtuelle Maschine über mehrere Netzwerkkarten verfügt, konfigurieren Sie das Subnetz, das View Agent verwendet. Siehe [Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent](#).

## Benutzerdefinierte Setup-Optionen für View Agent

Wenn Sie View Agent auf einer virtuellen Maschine installieren, können Sie benutzerdefinierte Setup-Optionen auswählen oder ihre Auswahl aufheben. Zusätzlich installiert View Agent bestimmte Funktionen automatisch auf allen Gastbetriebssystemen, die diese Funktionen unterstützen. Diese Funktionen sind nicht optional.

Weitere Informationen dazu, welche Gastbetriebssysteme welche Funktionen unterstützen, finden Sie unter „Funktionsunterstützungs-Matrix für View Agent“ im Dokument *Planung der View-Architektur*.

Alle benutzerdefinierten Setup-Optionen bis auf PCoIP-Smartcard und Scannerumleitung sind auf Windows Server-Gastbetriebssystemen standardmäßig ausgewählt.

**Tabelle 3-2. Benutzerdefinierte Setup-Optionen für View Agent**

| Option               | Beschreibung   |
|----------------------|--|
| USB-Umleitung        | <p>Gibt Benutzern Zugriff auf lokal verbundene USB-Geräte auf ihren Desktops.</p> <p>Die USB-Umleitung wird auf Remote-Desktops unterstützt, die auf Computern für Einzelbenutzer bereitgestellt sind, jedoch nicht auf Remote-Desktops, die auf RDS-Hosts basieren.</p> <hr/> <p><b>Hinweis</b> Sie können mithilfe von Gruppenrichtlinieneinstellungen die USB-Umleitung für spezifische Benutzer deaktivieren.</p>  |
| HTML Access          | <p>Ermöglicht dem Benutzer die Verbindungsherstellung mit View-Desktops über HTML Access. Der HTML Access Agent muss auf View-Desktops installiert sein, damit Benutzer Verbindungen mit HTML Access herstellen können.</p>  |
| View Composer Agent  | <p>View Agent wird auf den Linked-Clone-Desktops ausgeführt, die von dieser virtuellen Maschine bereitgestellt werden.</p>   |
| Echtzeit-Audio/Video | <p>Leitet Webcams und Audiogeräte um, die mit dem Clientsystem verbunden sind, sodass diese auf dem Remote-Desktop eingesetzt werden können.</p>   |
| Scannerumleitung     | <p>Leitet Scan- und Bildverarbeitungsgeräte um, die mit dem Clientsystem verbunden sind, sodass sie auf dem Remote-Desktop bzw. in der Remote-Anwendung verwendet werden können.</p> <p>Diese Setup-Option ist auf Windows Desktop-Gastbetriebssystemen standardmäßig aktiviert.</p> <p>Auf Windows Server-Gastbetriebssystemen ist die Option nicht standardmäßig aktiviert. Um sie zu installieren, müssen Sie die Option auswählen.</p> <p>Die Scannerumleitung ist in den Versionen Horizon 6.0.2 und höher verfügbar.</p> |

| Option                           | Beschreibung  |
|----------------------------------|---|
| Virtuelles Drucken               | <p>Benutzer können mit jedem beliebigen Drucker drucken, der auf ihren Clientcomputern zur Verfügung steht. Benutzer müssen keine zusätzlichen Treiber auf ihren Desktops installieren.</p> <p>In Horizon 6.0.1 und höher wird das virtuelle Drucken von den folgenden Desktops und Anwendungen unterstützt:</p> <ul style="list-style-type: none"> <li>■ Desktops, die auf Computern für Einzelbenutzer bereitgestellt werden, z. B. Windows Desktop- und Windows Server 2008 R2-Maschinen</li> <li>■ Desktops, die auf RDS-Hosts bereitgestellt werden, wobei die RDS-Hosts virtuelle Maschinen sind</li> <li>■ Gehostete Apps</li> <li>■ Gehostete Apps, die von Horizon Client in Remote-Desktops gestartet werden</li> </ul> <p>In Horizon 6.0 und früher wird das virtuelle Drucken auf Desktops unterstützt, die auf Windows Desktop-Maschinen für Einzelbenutzer bereitgestellt werden.</p> <p>Die Funktion zum virtuellen Drucken wird nur unterstützt, wenn Sie diese von View Agent aus installieren. Sie wird nicht unterstützt, wenn Sie die Funktion mit VMware Tools installieren.</p> |
| vCenter Operations Manager Agent | <p>Bietet Informationen, die es vCenter Operations Manager für View ermöglichen, View-Desktops zu überwachen.</p>   |
| View Persona Management          | <p>Synchronisiert das Benutzerprofil auf dem lokalen Desktop mit einem Remote-Profil-Repository, damit die Benutzer immer Zugriff auf ihre Profile haben, wenn sie sich bei einem Desktop anmelden.</p>   |
| PCoIP-Smartcard                  | <p>Ermöglicht Benutzern die Authentifizierung per Smartcard, wenn sie das PCoIP-Anzeigeprotokoll verwenden. Diese Option ist nicht standardmäßig ausgewählt.</p> <p>PCoIP-Smartcard wird auf Remote-Desktops unterstützt, die auf Computern für Einzelbenutzer bereitgestellt sind, jedoch nicht auf Remote-Desktops, die auf RDS-Hosts basieren.</p>   |

**Tabelle 3-3. Automatisch installierte View Agent-Funktionen (nicht optional)**

| Funktion                                 | Beschreibung   |
|--|--|
| PCoIP-Agent                              | <p>Ermöglicht Benutzern, mithilfe des PCoIP-Anzeigeprotokolls eine Verbindung zum View-Desktop herzustellen.</p> <p>Wenn Sie die Funktion „PCoIP-Agent“ installieren, wird auf Windows 8-, Windows 7- und Windows Vista-Desktops der Energiesparmodus und auf Windows XP-Desktops der Standbymodus deaktiviert. Wenn ein Benutzer zum Menü für die Energieoptionen oder das Abschalten wechselt, wird der Energiesparmodus oder Standbymodus als inaktiv angezeigt. Desktops wechseln nach der standardmäßig angegebenen Leerlaufzeit nicht in den Energiespar- oder Standbymodus. Desktops verbleiben im aktiven Modus.</p> <p><b>Hinweis</b> Wenn Sie unter Windows Vista die Funktion „PCoIP-Agent“ installieren, wird die Windows-Gruppenrichtlinie <b>Software-SAS deaktivieren oder aktivieren</b> aktiviert und auf <b>Dienste</b> und <b>Anwendungen für die erleichterte Bedienung</b> gesetzt. Wenn Sie diese Einstellung ändern, funktioniert SSO nicht mehr ordnungsgemäß.</p> |
| Wyse-Multimedia-Umleitung (MMR)          | <p>Bietet eine Multimedia-Umleitung für Windows XP- und Windows Vista-Desktops und -Clients. Diese Funktion leitet einen Multimedia-Stream direkt an den Clientcomputer um, sodass der Multimedia-Stream nicht auf dem Remote-ESXi-Host, sondern auf der Clienthardware verarbeitet wird.</p>  |
| Windows Media-Multimedia-Umleitung (MMR) | <p>Erweitert die Multimedia-Umleitung auf Desktops und Clients, die auf Windows 7 oder neueren Windows-Versionen basieren. Diese Funktion leitet einen Multimedia-Stream direkt an den Clientcomputer um, sodass der Multimedia-Stream nicht auf dem Remote-ESXi-Host, sondern auf der Clienthardware verarbeitet wird.</p> <p>Mit Horizon 6.0.2 und höher wird Windows Media-MMR auf Windows 7- und Windows 8/8.1-Desktops installiert. Mit Horizon 6.0.1 und älteren Versionen wird Windows 7-Multimedia-Umleitung auf Windows 7-Desktops installiert.</p>   |
| Lync                                     | <p>Bietet Unterstützung für Microsoft Lync 2013-Client auf View-Desktops.</p>  |
| Virtuelles Drucken mit PCoIP             | <p>Bietet eine virtuelle Druckfunktion über PCoIP. Mithilfe dieser Funktion können Benutzer mit einem beliebigen Drucker drucken, der auf ihren Windows-Clientcomputern zur Verfügung steht. Benutzer müssen keine zusätzlichen Treiber auf ihren Desktops installieren.</p>   |
| Unity Touch                              | <p>Ermöglicht Tablet- und Smartphone-Benutzern eine einfache Interaktion über Windows-Anwendungen, die auf dem Remote-Desktop ausgeführt werden. Die Benutzer können Windows-Anwendungen und -Dateien bequem durchsuchen, suchen und öffnen, bevorzugte Anwendungen und Dateien auswählen und bequem zwischen ausgeführten Anwendungen wechseln, ohne das Start-Menü oder die Taskleiste zu verwenden.</p>   |

| Funktion                | Beschreibung  |
|-------------------------|---|
| Virtueller Videotreiber | Bietet einen virtuellen Video-Treiber auf dem Remote-Desktop. |
| Virtueller Audiotreiber | Bietet einen virtuellen Audiotreiber auf dem Remote-Desktop.  |

## Unbeaufsichtigte Installation von View Agent

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, View Agent auf mehreren virtuellen Windows-Maschinen oder physischen Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Wenn Sie nicht alle Funktionen installieren möchten, die automatisch oder standardmäßig installiert werden, können Sie die MSI-Eigenschaft ADDLOCAL verwenden, um bestimmte Setup-Optionen und Funktionen selektiv zu installieren. Weitere Informationen zur Eigenschaft ADDLOCAL finden Sie unter [Tabelle 3-5. MSI-Befehlszeilenoptionen und MSI-Eigenschaften](#).

### Voraussetzungen

- Bereiten Sie das Gastbetriebssystem für die Desktop-Bereitstellung vor. Siehe [Vorbereiten eines Gastbetriebssystems für die Remote-Desktop-Bereitstellung](#).
- Um Windows Server 2008 R2 als Einzelsitzungs-Remote-Desktop (anstelle eines RDS-Hosts) zu verwenden, führen Sie die in [Vorbereiten von Windows Server 2008 R2 für Desktop-Verwendung](#) beschriebenen Schritte durch.

- Laden Sie die View Agent-Installationsdatei von der VMware-Produktseite unter <http://www.vmware.com/products/> herunter.

Der Dateiname des Installationsprogramms lautet VMware-viewagent-y.y.y-xxxxxx.exe oder VMware-viewagent-x86\_64-y.y.y-xxxxxx.exe, wobei y.y.y die Versionsnummer und xxxxxx die Build-Nummer ist.

- Stellen Sie sicher, dass Sie auf der virtuellen Maschine oder auf dem physischen Computer über Administratorberechtigungen verfügen.
- Machen Sie sich mit den benutzerdefinierten Setup-Optionen für View Agent vertraut. Siehe [Benutzerdefinierte Setup-Optionen für View Agent](#).
- Wenn Sie die benutzerdefinierte Setup-Option für View Composer Agent auswählen, stellen Sie sicher, dass Sie über eine Lizenz zur Verwendung von View Composer verfügen.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe [Befehlszeilenoptionen für Microsoft Windows Installer](#).
- Machen Sie sich mit den verfügbaren Eigenschaften für die unbeaufsichtigte Installation von View Agent vertraut. Siehe [Eigenschaften für die unbeaufsichtigte Installation von View Agent](#).



- Machen Sie sich mit den TCP-Ports vertraut, die das View Agent-Installationsprogramm in der Firewall öffnet. Weitere Informationen finden Sie im Dokument *Planung der View-Architektur*.
- Stellen Sie sicher, dass die neuesten Windows Update-Patches auf den Gastbetriebssystemen installiert sind, auf denen Sie View Agent unbeaufsichtigt installieren möchten. In bestimmten Fällen ist möglicherweise eine interaktive Installation durch einen Administrator erforderlich, um ausstehende Windows Update-Patches auszuführen. Stellen Sie sicher, dass alle Vorgänge im Betriebssystem und nachfolgende Neustarts abgeschlossen wurden.

## Verfahren

- 1 Öffnen Sie auf der virtuellen Maschine oder auf einem physischen Computer eine Windows-Eingabeaufforderung.
- 2 Geben Sie den Installationsbefehl in einer Zeile ein.

In diesem Beispiel wird View Agent in einer virtuellen Maschine installiert, die von vCenter Server verwaltet wird. Das Installationsprogramm konfiguriert die benutzerdefinierten Setup-Optionen für View Composer Agent, die Funktion für den virtuellen Druck, die USB-Umleitung, HTML Access und Echtzeit-Audio/Video sowie die nicht optionalen Funktionen, die automatisch installiert werden.

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1  
ADDLOCAL=Core,SVIAgent,ThinPrint,USB,HtmlAccess,RTAV"
```

In diesem Beispiel wird View Agent auf einem nicht verwalteten Computer installiert und der Desktop mit dem angegebenen View-Verbindungsserver `cs1.companydomain.com` registriert. Mit dem Installationsprogramm werden die benutzerdefinierten Setup-Optionen für die Funktion für den virtuellen Druck und die USB-Umleitung konfiguriert.

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=0  
VDM_SERVER_NAME=cs1.companydomain.com VDM_SERVER_USERNAME=admin.companydomain.com  
VDM_SERVER_PASSWORD=secret ADDLOCAL=Core,ThinPrint,USB"
```

Wenn Sie View Agent auf einem Windows Server-Computer installieren und den Computer als View-Desktop für Einzelbenutzer statt als RDS-Host konfigurieren möchten, müssen Sie im Installationsbefehl die Eigenschaftseinstellung `VDM_FORCE_DESKTOP_AGENT=1` angeben. Diese Anforderung gilt für Computer, die von vCenter Server verwaltet werden, und für nicht verwaltete Computer.

Der VMware View Agent-Dienst wird auf der virtuellen Maschine gestartet.

Wenn Sie die Option **View Composer Agent** ausgewählt haben, wird der VMware View Composer Guest Agent Server-Dienst auf der virtuellen Maschine gestartet.

## Nächste Schritte

Wenn die virtuelle Maschine über mehrere Netzwerkkarten verfügt, konfigurieren Sie das Subnetz, das View Agent verwendet. Siehe [Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent](#).

## Befehlszeilenoptionen für Microsoft Windows Installer

Zur unbeaufsichtigten Installation von View-Komponenten müssen Sie die Befehlszeilenoptionen und Eigenschaften von Microsoft Windows Installer (MSI) verwenden. Die Installationsprogramme für View-Komponenten sind MSI-Programme und verwenden standardmäßige MSI-Funktionen.

Einzelheiten zu MSI finden Sie auf der Website von Microsoft. Informationen zu MSI-Befehlszeilenoptionen finden Sie auf der Website der MSDN-Bibliothek (Microsoft Developer Network), wenn Sie nach MSI-Befehlszeilenoptionen suchen. Informationen zur Verwendung der MSI-Befehlszeile erhalten Sie, indem Sie auf dem Computer mit der View-Komponente eine Eingabeaufforderung öffnen und `msiexec /?` eingeben.

Für die unbeaufsichtigte Installation einer View-Komponente deaktivieren Sie zunächst das Bootstrap-Programm, mit dem das Installationsprogramm in ein temporäres Verzeichnis extrahiert und eine interaktive Installation gestartet wird.

An der Befehlszeile müssen Sie die Befehlszeilenoptionen eingeben, die das Bootstrap-Programm des Installers steuern.

**Tabelle 3-4. Befehlszeilenoptionen für das Bootstrap-Programm einer View-Komponente**

| Option                                     | Beschreibung   |
|--|--|
| <code>/s</code>                            | <p>Deaktiviert den Bootstrap-Splash-Bildschirm und das Dialogfeld für die Extraktion, wodurch die Anzeige interaktiver Dialogfelder unterbunden wird.</p> <p>Beispiel: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s</code></p> <p>Die Option <code>/s</code> ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.</p>   |
| <code>/v"MSI-Befehlszeilenoptionen"</code> | <p>Weist den Installer an, die in doppelten Anführungszeichen eingeschlossene Zeichenfolge, die Sie an der Befehlszeile eingeben, als Befehlssatz zur Interpretation durch MSI zu übergeben. Sie müssen Ihre Befehlszeileneinträge in doppelte Anführungszeichen einschließen. Geben Sie ein doppeltes Anführungszeichen nach <code>/v</code> und am Ende der Befehlszeile ein.</p> <p>Beispiel: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"MSI-Befehlszeilenoptionen"</code></p> <p>Damit das MSI-Installationsprogramm eine Zeichenfolge mit Leerzeichen richtig auswertet, müssen Sie die Zeichenfolge in zwei Sätze doppelter Anführungszeichen einschließen. Angenommen, Sie möchten die View-Komponente in einem Pfad installieren, dessen Name Leerzeichen enthält.</p> <p>Beispiel: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"MSI-Befehlszeilenoptionen" INSTALLDIR=""d:\abc\mein Ordner""</code></p> <p>In diesem Beispiel übergibt das MSI-Installationsprogramm den Verzeichnispfad für die Installation und versucht nicht, die Zeichenfolge als Befehlszeilenoptionen auszuwerten. Beachten Sie die zweifach gesetzten doppelten Anführungszeichen, die die gesamte Befehlszeile umschließen.</p> <p>Die Option <code>/v"MSI-Befehlszeilenoptionen"</code> ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.</p> |

Sie steuern die verbleibenden Schritte einer unbeaufsichtigten Installation, indem Sie Befehlszeilenoptionen und MSI-Eigenschaftswerte an den MSI Installer, `msiexec.exe`, übergeben. Das MSI-Installationsprogramm umfasst den Installationscode der View-Komponente. Der Installer verwendet die in die Befehlszeile eingegebenen Werte und Optionen, um die Installationsauswahl und die für die View-Komponente spezifischen Setup-Optionen auszuwerten.

**Tabelle 3-5. MSI-Befehlszeilenoptionen und MSI-Eigenschaften**

| MSI-Option oder -Eigenschaft | Beschreibung   |
|------------------------------|--|
| /qn                          | <p>Weist den MSI Installer an, keine Seiten des Installations-Assistenten anzuzeigen.</p> <p>Angenommen, Sie möchten View Agent unbeaufsichtigt installieren und nur standardmäßige Setup-Optionen und Funktionen verwenden:</p> <pre>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"</pre> <p>Alternativ können Sie die Option /qb zur Anzeige der Assistentenseiten in einer nicht interaktiven, automatisierten Installation verwenden. Während die Installation durchgeführt wird, werden die Assistentenseiten angezeigt, Sie können jedoch keine Eingaben vornehmen.</p> <p>Die Option /qn oder /qb ist erforderlich, um eine unbeaufsichtigte Installation durchzuführen.</p>  |
| INSTALLDIR                   | <p>Gibt einen alternativen Installationspfad für die View-Komponente an.</p> <p>Verwenden Sie das Format <i>INSTALLDIR=Pfad</i>, um den Installationspfad anzugeben. Sie können diese MSI-Eigenschaft ignorieren, wenn Sie die View-Komponente im Standardpfad installieren möchten.</p> <p>Diese MSI-Eigenschaft ist optional.</p>  |
| ADDLOCAL                     | <p>Legt die komponentenspezifischen Optionen fest, die installiert werden sollen.</p> <p>Bei einer interaktiven Installation zeigt das View-Installationsprogramm benutzerdefinierte Setup-Optionen an, die Sie aus- oder abwählen können. Bei einer unbeaufsichtigten Installation können Sie mithilfe der ADDLOCAL-Eigenschaft bestimmte Setup-Optionen selektiv installieren, indem Sie die Optionen in der Befehlszeile angeben. Optionen, die Sie nicht explizit angeben, werden nicht installiert.</p> <p>Bei der interaktiven und der unbeaufsichtigten Installation werden bestimmte Funktionen automatisch vom View-Installationsprogramm installiert. Mit der ADDLOCAL-Eigenschaft können Sie nicht festlegen, ob diese nicht optionalen Funktionen installiert werden sollen.</p> <p>Geben Sie ADDLOCAL=ALL ein, um alle benutzerdefinierten Setup-Optionen, die standardmäßig installiert werden, sowie alle Funktionen, die automatisch installiert werden, (unter unterstützten Gastbetriebssystemen) zu installieren.</p> <p>Beispiel: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</code></p> <p>Wenn Sie die Eigenschaft ADDLOCAL nicht verwenden, werden die standardmäßigen Setup-Optionen und die automatisch installierten Funktionen installiert. Die Eingabe von ADDLOCAL=ALL hat dieselbe Wirkung wie der Verzicht auf die Eigenschaft ADDLOCAL.</p> <p>Zur Festlegung einzelner Setup-Optionen geben Sie eine Liste der Setup-Optionen ein. Trennen Sie hierbei die Namen der Optionen durch Kommata. Verwenden Sie zwischen den Namen keine Leerzeichen. Verwenden Sie das Format <i>ADDLOCAL=Wert,Wert,Wert....</i></p> <p>Angenommen, Sie möchten View Agent zusammen mit View Composer Agent und der Funktion für den virtuellen Druck unter einem Gastbetriebssystem installieren:</p> <pre>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,ThinPrint"</pre> <p>Die MSI-Eigenschaft ADDLOCAL ist optional.</p> |

| MSI-Option oder -Eigenschaft | Beschreibung  |
|------------------------------|---|
| REBOOT                       | Sie können die Option REBOOT=ReallySuppress verwenden, um die Ausführung von Systemkonfigurationsaufgaben zuzulassen, bevor das System neu gestartet wird.<br>Diese MSI-Eigenschaft ist optional.   |
| /l*v <i>Protokolldatei</i>   | Schreibt ausführliche Protokollinformationen in die angegebene Protokolldatei.<br>Beispiel: /l*v ""%TEMP%\vmmsi.log""<br>In diesem Beispiel wird eine detaillierte Protokolldatei generiert, die dem Protokoll ähnelt, das während einer interaktiven Installation erstellt wird.<br>Sie können diese Option dazu verwenden, benutzerdefinierte Funktionen aufzuzeichnen, die möglicherweise nur für Ihre Installation gelten. Sie können die aufgezeichneten Informationen dazu verwenden, Installationsfunktionen für unbeaufsichtigte Installationen anzugeben.<br>Die Option /l*v ist optional. |

## Eigenschaften für die unbeaufsichtigte Installation von View Agent

Sie können spezifische Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation von View Agent über die Befehlszeile durchführen. Sie müssen das Format *EIGENSCHAFT=Wert* verwenden, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

**Tabelle 3-6. MSI-Eigenschaften für die unbeaufsichtigte Installation von View Agent** zeigt die Eigenschaften für eine unbeaufsichtigte Installation von View Agent, die Sie an der Befehlszeile verwenden können.

**Tabelle 3-6. MSI-Eigenschaften für die unbeaufsichtigte Installation von View Agent**

| MSI-Eigenschaft | Beschreibung  | Standardwert                            |
|-----------------|---|---|
| INSTALLDIR      | Der Pfad und der Ordner, in dem die View Agent-Software installiert wird.<br>Beispiel: INSTALLDIR=""D:\abc\mein Ordner""<br>Die zweifach gesetzten doppelten Anführungszeichen um den Pfad sorgen dafür, dass das MSI-Installationsprogramm das Leerzeichen im Pfad ignoriert.<br>Diese MSI-Eigenschaft ist optional. | %ProgramFiles%\VMware\VMware View Agent |
| RDPCHOICE       | Legt fest, ob RDP (Remote Desktop Protocol) auf dem Desktop aktiviert werden soll.<br>Mit dem Wert 1 wird RDP aktiviert. Mit dem Wert 0 wird die RDP-Einstellung deaktiviert.<br>Diese MSI-Eigenschaft ist optional.  | 1                                       |

| MSI-Eigenschaft         | Beschreibung  | Standardwert |
|-------------------------|---|--------------|
| UNITY_DEFAULT_APPS      | <p>Gibt eine Standardliste mit bevorzugten Anwendungen an, die in der Unity Touch-Sidebar auf einem mobilen Gerät angezeigt werden. Diese Eigenschaft wurde zur Unterstützung der Unity Touch-Komponente erstellt. Es handelt sich nicht um eine allgemeine MSI-Eigenschaft.</p> <p>Informationen zum Konfigurieren einer Standardliste mit bevorzugten Anwendungen und zu Syntax und Format dieser Eigenschaft finden Sie unter <a href="#">Konfigurieren von Favoritenanwendungen durch Unity Touch</a>.</p> <p>Diese MSI-Eigenschaft ist optional.</p> |              |
| VDM_FORCE_DESKTOP_AGENT | Konfiguriert die Maschine als View-Desktop für Einzelbenutzer statt als RDS-Host, wenn Sie View Agent auf einem Windows Server-Betriebssystem installieren.   | 1            |
| VDM_VC_MANAGED_AGENT    | <p>Legt fest, ob vCenter Server die virtuelle Maschine verwaltet, auf der View Agent installiert ist.</p> <p>Mit dem Wert 1 wird der Desktop als von vCenter Server verwaltete virtuelle Maschine konfiguriert.</p> <p>Mit dem Wert 0 wird der Desktop ohne Verwaltung durch vCenter Server konfiguriert.</p> <p>Diese MSI-Eigenschaft ist erforderlich.</p>  | –            |
| VDM_SERVER_NAME         | <p>Der Hostname oder die IP-Adresse des View-Verbindungsserver-Computers, auf dem das View Agent-Installationsprogramm einen nicht verwalteten Desktop registriert. Diese Eigenschaft gilt nur für nicht verwaltete Desktops.</p> <p>Beispiel: VDM_SERVER_NAME=10.123.01.01</p> <p>Diese MSI-Eigenschaft ist für nicht verwaltete Desktops erforderlich.</p> <p>Verwenden Sie diese MSI-Eigenschaft nicht für VM-Desktops, die von vCenter Server verwaltet werden.</p>   | –            |
| VDM_SERVER_USERNAME     | <p>Der Benutzername des Administrators auf dem View-Verbindungsserver-Computer. Diese MSI-Eigenschaft gilt nur für nicht verwaltete Desktops.</p> <p>Beispiel: VDM_SERVER_USERNAME=admin.companydomain.com</p> <p>Diese MSI-Eigenschaft ist für nicht verwaltete Desktops erforderlich.</p> <p>Verwenden Sie diese MSI-Eigenschaft nicht für VM-Desktops, die von vCenter Server verwaltet werden.</p>  | –            |
| VDM_SERVER_PASSWORD     | <p>Das Benutzerkennwort des View-Verbindungsserver-Administrators.</p> <p>Beispiel: VDM_SERVER_PASSWORD=secret</p> <p>Diese MSI-Eigenschaft ist für nicht verwaltete Desktops erforderlich.</p> <p>Verwenden Sie diese MSI-Eigenschaft nicht für VM-Desktops, die von vCenter Server verwaltet werden.</p>  | –            |

In einem Befehl für die unbeaufsichtigte Installation können Sie mit der MSI-Eigenschaft ADDLOCAL= Optionen angeben, die das View Agent-Installationsprogramm konfiguriert.

**Tabelle 3-7. Optionen für die unbeaufsichtigte View Agent-Installation und benutzerdefinierte Setup-Optionen bei einer interaktiven Installation (optional)** zeigt die Optionen von View Agent an, die Sie an der Befehlszeile eingeben können. Für diese Optionen gibt es entsprechende Setup-Optionen, die Sie bei einer interaktiven Installation deaktivieren bzw. aktivieren können. Weitere Informationen zu den benutzerdefinierten Setup-Optionen finden Sie unter [Benutzerdefinierte Setup-Optionen für View Agent](#).

Bei einer interaktiven Installation werden all diese Optionen außer der PCoIP-Smartcard standardmäßig installiert.

**Tabelle 3-7. Optionen für die unbeaufsichtigte View Agent-Installation und benutzerdefinierte Setup-Optionen bei einer interaktiven Installation (optional)**

| Option für die unbeaufsichtigte Installation | Benutzerdefinierte Setup-Option in einer interaktiven Installation                                       |
|--|--|
| USB  | USB-Umleitung  |
| HtmlAccess                                   | HTML Access Agent  |
| SVIAgent                                     | View Composer Agent  |
| RTAV   | Echtzeit-Audio/Video   |
| ScannerRedirection                           | Scannerumleitung   |
| ThinPrint                                    | Virtuelles Drucken   |
| V4V  | vCenter Operations Manager for View  |
| VPA  | View Persona Management  |
| Smartcard                                    | PCoIP-Smartcard. Standardmäßig wird diese Funktion nicht in einer interaktiven Installation installiert. |

**Tabelle 3-8. Funktionen für die unbeaufsichtigte View Agent-Installation, die automatisch installiert werden (nicht optional)** zeigt die View Agent-Funktionen an, die automatisch installiert werden. Die Funktionen werden auf allen Gastbetriebssystemen installiert, auf denen sie unterstützt werden. Diese Funktionen sind nicht optional. Mit der ADDLOCAL=-Eigenschaft können Sie nicht steuern, ob sie installiert werden.

**Tabelle 3-8. Funktionen für die unbeaufsichtigte View Agent-Installation, die automatisch installiert werden (nicht optional)**

| Funktion für die unbeaufsichtigte Installation | Beschreibung   |
|--|--|
| Core   | Die View Agent-Hauptfunktionen.<br>Wenn Sie ADDLOCAL=ALL angeben, werden alle Core-Funktionen installiert. |
| ThinPrintPCoIP                                 | Virtuelles Drucken mit PCoIP   |
| PCoIP  | Agent des PCoIP-Protokolls   |
| VmVideo  | Virtueller Videotreiber  |
| VmwVaudio                                      | Virtueller Audiotreiber  |

| Funktion für die unbeaufsichtigte Installation | Beschreibung  |
|--|---|
| UnityTouch                                     | Unity Touch   |
| MMR  | <p>Windows Media-Multimedia-Umleitung (MMR) wird als Bestandteil von Horizon 6.0.2 und höher auf Windows 7- oder Windows 8/8.1-Desktops installiert.</p> <p>Windows 7-Multimedia-Umleitung (MMR) wird als Bestandteil von Horizon 6.0.1 und älteren Versionen auf Windows 7-Desktops installiert.</p> |

Installieren Sie die Flash-URL-Umleitung, indem Sie das Befehlszeilenargument `FlashURLRedirection` in einer unbeaufsichtigten Installation eingeben. Diese Funktion wird während einer interaktiven Installation oder bei der Verwendung von `ADDLOCAL=ALL` in einer unbeaufsichtigten Installation nicht installiert.

Beispiel: `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1 ADDLOCAL=Core,SVIAgent,ThinPrint,USB,HtmlAccess,FlashURLRedirection,RTAV"`

## Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent

Wenn Sie View Agent auf einer virtuellen Maschine installieren, die mehr als eine Netzwerkkarte besitzt, müssen Sie das von View Agent verwendete Subnetz konfigurieren. Mit dem Subnetz wird festgelegt, welche Netzwerkadresse View Agent der View-Verbindungsserver-Instanz für Clientprotokollverbindungen bereitstellt.

### Verfahren

- ◆ Öffnen Sie auf der virtuellen Maschine, auf der View Agent installiert ist, eine Eingabeaufforderung, geben Sie **regedit.exe** ein und erstellen Sie einen Registrierungseintrag, um das Subnetz zu konfigurieren.

Beispiel:

`HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = n.n.n.n/m (REG_SZ)`

In diesem Beispiel steht *n.n.n.n* für das TCP/IP-Subnetz und *m* für die Anzahl der Bits in der Subnetzmaske.

## Optimieren der Leistung des Gastbetriebssystems für alle Windows-Versionen

Sie können bestimmte Schritte ausführen, um die Leistung des Gastbetriebssystems für eine Remote-Desktop-Bereitstellung zu optimieren. Die Schritte gelten für alle Windows-Betriebssysteme. Alle genannten Schritte sind optional.

Es wird u. a. empfohlen, den Bildschirmschoner auszuschalten und keinen Ruhezustandstimer anzugeben. Möglicherweise verlangt Ihr Unternehmen die Verwendung eines Bildschirmschoners. So sorgt beispielsweise eine GPO-verwaltete Sicherheitsrichtlinie dafür, dass ein Desktop nach Ablauf einer bestimmten Zeit nach dem Starten des Bildschirmschoners gesperrt wird. Verwenden Sie in einem solchen Fall einen leeren Bildschirmschoner.

## Voraussetzungen

Bereiten Sie ein Gastbetriebssystem für die Remote-Desktop-Bereitstellung vor.

## Verfahren

- ◆ Deaktivieren Sie alle nicht verwendeten Ports, beispielsweise COM1, COM2 und LPT.
- ◆ Passen Sie die Anzeigeeigenschaften an.
  - a Wählen Sie ein Basisdesign.
  - b Legen Sie den Hintergrund auf eine Volltonfarbe fest.
  - c Legen Sie den Bildschirmschoner auf **Keiner** fest.
  - d Stellen Sie sicher, dass die Hardwarebeschleunigung aktiviert ist.
- ◆ Wählen Sie eine Betriebsoption mit hoher Leistung aus und legen Sie keinen Wechsel in den Energiesparmodus fest.
- ◆ Deaktivieren Sie den Indexdienst.

---

**Hinweis** Die Indizierung verbessert die Suche, indem Dateien katalogisiert werden. Deaktivieren Sie diese Funktion nicht bei Benutzern, die die Suche häufig verwenden.

---

- ◆ Entfernen Sie Systemwiederherstellungspunkte, oder reduzieren Sie diese auf ein Mindestmaß.
- ◆ Deaktivieren Sie den Systemschutz für C:\.
- ◆ Deaktivieren Sie alle nicht benötigten Dienste.
- ◆ Legen Sie das Soundschema auf **Keine Sounds** fest.
- ◆ Legen Sie die visuellen Effekte auf **Für optimale Leistung anpassen** fest.
- ◆ Öffnen Sie Windows Media Player und verwenden Sie die Standardeinstellungen.
- ◆ Deaktivieren Sie die automatische Computerwartung.
- ◆ Passen Sie die Leistungseinstellungen für eine optimale Leistung an.
- ◆ Löschen Sie alle versteckten Ordner für die Deinstallation unter C:\Windows, beispielsweise \$NtUninstallKB893756\$.
- ◆ Löschen Sie alle Ereignisprotokolle.
- ◆ Führen Sie eine Datenträgerbereinigung zum Entfernen temporärer Dateien durch, leeren Sie den Papierkorb und entfernen Sie Systemdateien und andere Elemente, die nicht mehr benötigt werden.
- ◆ Führen Sie eine Datenträgerdefragmentierung aus, um fragmentierte Daten neu anzuordnen.



- ◆ Wenn Benutzer auf Desktops in einer vSphere 5.1-Umgebung Videos im Vollbildmodus wiedergeben oder 3D-Anwendungen ausführen, befolgen Sie die Anweisungen zum Ändern der Registrierung, die im Microsoft KB-Artikel 235257 beschrieben sind.

Der Titel dieses Microsoft KB-Artikels lautet „Der Server verwendet beim Streaming von Dateien mit Bitraten von über 100 Kbit/s nicht die gesamte verfügbare Bandbreite“ und befindet sich unter <http://support.microsoft.com/kb/235257>. Starten Sie die virtuelle Maschine neu, damit die geänderten Registrierungseinstellung wirksam werden.

Ohne diese Optimierung kommt es bei der Anzeige möglicherweise zu Standbildern oder Verzögerungen.

---

**Hinweis** Wenn Sie diese Optimierungsschritte ausführen, wird die Leistung sowohl in ESXi 5.x als auch in ESXi 5.1 verbessert; für ESXi 5.1 ist dies jedoch erforderlich.

---

### Nächste Schritte

Führen Sie auf Windows 7- und Windows 8-Gastbetriebssystemen zusätzliche Schritte zur Optimierung aus. Siehe [Optimieren der Leistung des Windows 7- und Windows 8-Gastbetriebssystems](#).

## Optimieren der Leistung des Windows 7- und Windows 8-Gastbetriebssystems

Sie können zusätzliche Schritte ausführen, um die Leistung des Windows 7- und Windows 8-Gastbetriebssystems für eine Remote-Desktop-Bereitstellung zu optimieren. Alle genannten Schritte sind optional.

### Voraussetzungen

- Führen Sie die Schritte zur Leistungsoptimierung für das Gastbetriebssystem aus, die für alle Windows-Betriebssysteme gelten. Siehe [Optimieren der Leistung des Gastbetriebssystems für alle Windows-Versionen](#).
- Machen Sie sich mit der Vorgehensweise für das Deaktivieren des Windows-Programms zur Verbesserung der Benutzerfreundlichkeit vertraut. Siehe [Deaktivieren des Windows-Programms zur Verbesserung der Benutzerfreundlichkeit](#).

### Verfahren

- 1 Deinstallieren Sie Tablet PC-Komponenten – es sei denn, diese werden benötigt.
- 2 Deaktivieren Sie IPv6, sofern diese Funktion nicht benötigt wird.
- 3 Verwenden Sie den Dateisystembefehl (fsutil), um die Nachverfolgung des letzten Zugriffszeitpunkts für eine Datei zu deaktivieren.

Beispiel: `fsutil behavior set disablelastaccess 1`

- 4 Starten Sie den Registrierungs-Editor (regedit.exe) und ändern Sie den REG\_WORD-Eintrag **TimeOutValue** in HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\Disk auf **0x000000be(190)**.

- 5 Deaktivieren Sie das Windows-Programm zur Verbesserung der Benutzerfreundlichkeit und deaktivieren Sie verbundene Aufgaben im Taskplaner.
- 6 Fahren Sie das Gastbetriebssystem herunter und schalten Sie die virtuelle Maschine aus.
- 7 Schalten Sie die virtuelle Maschine ein.

#### Nächste Schritte

Siehe [Optimieren von Windows 7 und Windows 8 für virtuelle Maschinen mit verknüpftem Klon](#), um Informationen zu erhalten, wie Sie durch das Deaktivieren bestimmter Windows 7- und Windows 8-Dienste und -Aufgaben das Wachstum von virtuellen View Composer-Maschinen mit verknüpften Klonen verlangsamen können. Das Deaktivieren bestimmter Dienste und Tasks kann außerdem die Leistung vollständiger virtueller Maschinen verbessern.

## Deaktivieren des Windows-Programms zur Verbesserung der Benutzerfreundlichkeit

Das Deaktivieren des Windows-Programms zur Verbesserung der Benutzerfreundlichkeit und der damit verbundenen Taskplaner-Aufgaben, die dieses Programm steuern, können die Windows 7- und Windows 8-Systemleistung in großen Desktop-Pools verbessern.

#### Verfahren

- 1 Starten Sie im Windows 7- oder Windows 8-Gastbetriebssystem die Systemsteuerung und klicken Sie auf **Wartungscenter > Wartungscentereinstellungen ändern**.
- 2 Klicken Sie auf **Einstellungen für das Programm zur Verbesserung der Benutzerfreundlichkeit**.
- 3 Wählen Sie **Nein, ich möchte nicht am Windows-Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen** und dann auf **Änderungen speichern**.
- 4 Starten Sie die Systemsteuerung und klicken Sie auf **Verwaltungstools > Taskplaner**.
- 5 Erweitern Sie im Bereich Aufgabenplanung (Lokal) des Dialogfelds **Taskplaner** die Knoten Aufgabenplanungsbibliothek **Microsoft > Windows** und öffnen Sie den Ordner **Anwendungserfahrung**.
- 6 Deaktivieren Sie die Aufgaben **AITAgent** und **ProgramDataUpdater**.
- 7 Öffnen Sie im Knoten **Aufgabenplanungsbibliothek > Microsoft > Windows** den Ordner **Programm zur Verbesserung der Benutzerfreundlichkeit**.
- 8 Deaktivieren Sie die Aufgaben **Konsolidator**, **KernelCEIPTask** und **CEIP verwenden**.

#### Nächste Schritte

Führen Sie andere Windows 7- oder Windows 8-Optimierungsaufgaben durch. Siehe [Optimieren der Leistung des Windows 7- und Windows 8-Gastbetriebssystems](#).

## Optimieren von Windows 7 und Windows 8 für virtuelle Maschinen mit verknüpftem Klon

Durch das Deaktivieren bestimmter Windows 7- oder Windows 8-Dienste und -Aufgaben können Sie das Wachstum von virtuellen View Composer-Maschinen mit verknüpftem Klon verlangsamen. Das Deaktivieren bestimmter Dienste und Tasks kann außerdem die Leistung vollständiger virtueller Maschinen verbessern.

### Vorteile der Deaktivierung von Diensten und Aufgaben unter Windows 7 und Windows 8

Windows 7 und Windows 8 planen die Ausführung von Diensten und Aufgaben, die verknüpfte View Composer-Klone anwachsen lassen können, selbst wenn die Maschinen mit verknüpften Klonen sich im Leerlauf befinden. Das inkrementelle Wachstum von Linked-Clone-Betriebssystemfestplatten kann die Speichereinsparungen zunichte machen, die Sie durch das Erstellen von Maschinen mit verknüpften Klonen erzielen. Sie können das Wachstum von Linked-Clone-Desktops verringern, indem Sie diese Windows-Dienste deaktivieren.

Unter Windows 7 und Windows 8 werden verschiedene neu eingeführte Dienste und ältere Dienste, wie beispielsweise die Datenträgerdefragmentierung, zur standardmäßigen Ausführung geplant. Diese Dienste werden im Hintergrund ausgeführt, wenn Sie sie nicht deaktivieren.

Dienste, die sich auf das Wachstum der Betriebssystemfestplatte auswirken, erhöhen außerdem die Anzahl an E/A-Vorgängen pro Sekunde auf den virtuellen Windows 7- oder Windows 8-Maschinen. Durch das Deaktivieren dieser Dienste kann die Anzahl an E/A-Vorgängen pro Sekunde verringert und die Leistung auf vollständigen virtuellen Maschinen und verknüpften Klonen verbessert werden.

Das Deaktivieren bestimmter Dienste kann sich auch auf den Betriebssystemen Windows XP und Windows Vista positiv auswirken.

Die hier vorgestellten empfohlenen Vorgehensweisen zur Optimierung von Windows 7 und Windows 8 gelten für die meisten Benutzerumgebungen. Sie müssen jedoch die Auswirkung der Deaktivierung einzelner Dienste auf Ihre Benutzer, Anwendungen und Desktops berücksichtigen. Bestimmte Dienste müssen möglicherweise ausgeführt werden.

Beispielsweise ist ein Deaktivieren des Windows Update-Dienstes sinnvoll, wenn Sie verknüpfte Klone aktualisieren und neu zusammenstellen. Bei einer Aktualisierung werden die Betriebssystemfestplatten im Zustand der letzten Snapshots wiederhergestellt, und alle automatischen Windows-Updates seit Erstellung des letzten Snapshots werden gelöscht. Bei einer Neuzusammenstellung werden die Betriebssystemfestplatten unter Verwendung eines neuen Snapshots erneut erstellt. Da dieser neue Snapshot die aktuellen Windows-Updates möglicherweise bereits umfasst, sind automatische Windows-Updates überflüssig.

Wenn Sie Aktualisierungen und Neuzusammenstellungen nicht regelmäßig ausführen, sollten Sie den Windows Update-Dienst möglicherweise weiterhin ausführen.

## Überblick über Windows 7- und Windows 8-Dienste und -Aufgaben, die zu einem Wachstum von verknüpften Klonen führen

Bestimmte Windows 7- und Windows 8-Dienste und -Aufgaben können dazu führen, dass die Linked-Clone-Betriebssystemfestplatten inkrementell anwachsen, selbst wenn die Linked-Clone-Computer sich im Leerlauf befinden. Wenn Sie diese Dienste und Tasks deaktivieren, können Sie das Wachstum der Betriebssystemfestplatten kontrollieren.

Dienste, die sich auf das Wachstum der Betriebssystemfestplatten auswirken, erzeugen auch eine höhere Anzahl an E/A-Vorgängen pro Sekunde auf den virtuellen Windows 7- und Windows 8-Maschinen. Sie sollten auswerten, welche Vorteile eine Deaktivierung dieser Dienste auf vollständigen virtuellen Maschinen und verknüpften Klonen bietet.

Bevor Sie die Windows 7- oder Windows 8-Dienste deaktivieren, die in [Tabelle 3-9. Auswirkung von Windows 7 und Windows 8-Diensten und -Aufgaben auf das Wachstum von Betriebssystemfestplatten und E/A-Vorgängen pro Sekunde, wenn das Betriebssystem sich im Leerlauf befindet](#) angezeigt werden, führen Sie die Optimierungsschritte unter [Optimieren der Leistung des Gastbetriebssystems für alle Windows-Versionen](#) und [Optimieren der Leistung des Windows 7- und Windows 8-Gastbetriebssystems](#) durch.

**Tabelle 3-9. Auswirkung von Windows 7 und Windows 8-Diensten und -Aufgaben auf das Wachstum von Betriebssystemfestplatten und E/A-Vorgängen pro Sekunde, wenn das Betriebssystem sich im Leerlauf befindet**

| Dienst oder Task                             | Beschreibung   | Standardhäufigkeit oder -start  | Auswirkung auf Linked-Clone-Betriebssystemfestplatten  | Auswirkung auf E/A-Vorgänge pro Sekunde   | Dienst oder Task deaktivieren?   |
|--|--|---|--|---|--|
| Windows-Ruhezustand                          | Versetzt das System in einen Zustand zur Energieeinsparung, indem offene Dokumente und Programme in einer Datei gespeichert werden, bevor der Computer ausgeschaltet wird. Die Datei wird erneut in den Arbeitsspeicher geladen, wenn der Computer neu gestartet wird, und es wird der Zustand vor Auslösung des Ruhezustands wiederhergestellt. | Ruhezustand ist in den Einstellungen des standardmäßigen Energiesparplans deaktiviert | Hoch.<br>Standardmäßig entspricht die Größe der Datei für den Ruhezustand, hiberfil.sys, der des installierten Arbeitsspeichers auf der virtuellen Maschine. Diese Funktion betrifft alle Gastbetriebssysteme. | Hoch.<br>Beim Auslösen des Ruhezustands erstellt das System die Datei hiberfil.sys, die so groß ist wie der installierte Arbeitsspeicher. | Ja<br>Der Ruhezustand bietet in einer virtuellen Umgebung keine Vorteile.<br>Anweisungen finden Sie unter <a href="#">Deaktivieren des Ruhezustands in der übergeordneten virtuellen Maschine.</a> |
| Geplante Windows-Datenträgerdefragmentierung | Die Datenträgerdefragmentierung ist als Hintergrundprozess geplant.  | Einmal pro Woche  | Hoch.<br>Wiederholte Defragmentierungsvorgänge können die Linked-Clone-Betriebssystemfestplatten um mehrere GB anwachsen lassen und verbessern den Festplattenzugriff auf verknüpfte Klone nur unwesentlich.   | Hoch  | Ja   |

| Dienst oder Task                  | Beschreibung  | Standardhäufigkeit oder -start                                  | Auswirkung auf Linked-Clone-Betriebssystemfestplatten  | Auswirkung auf E/A-Vorgänge pro Sekunde | Dienst oder Task deaktivieren?  |
|-----------------------------------|---|---|--|---|---|
| Windows Update-Dienst             | Sorgt für Ermittlung, Download und Installation von Updates für Windows und andere Programme.   | Automatischer Start   | Mittel bis hoch.<br>Verursacht häufige Schreibvorgänge auf den Linked-Clone-Betriebssystemfestplatten, da häufig auf Updates geprüft wird. Die Auswirkung richtet sich nach den Updates, die heruntergeladen werden. | Mittel bis hoch                         | Ja, wenn Sie View Composer-Neuzusammenstellungen zum Installieren von Windows-Updates und Aktualisierungen dazu verwenden, um Betriebssystemfestplatten in den Zustand ihrer ursprünglichen Snapshots zurückzusetzen. |
| Windows-Diagnoserichtliniendienst | Ermittlung, Fehlerbehebung und Lösung von Problemen in Windows-Komponenten. Wenn Sie diesen Dienst anhalten, ist eine Diagnose nicht länger möglich.    | Automatischer Start   | Mittel bis hoch.<br>Der Dienst wird bei Bedarf gestartet. Die Häufigkeit von Schreibvorgängen variiert je nach Bedarf.   | Gering bis mittel                       | Ja, wenn Sie die Diagnosetools auf den Desktops nicht benötigen.  |
| Vorabruf/SuperFetch               | Speichert spezifische Informationen zu ausgeführten Anwendungen, damit diese schneller gestartet werden. Diese Funktion wurde in Windows XP eingeführt. | Sie ist immer eingeschaltet, sofern Sie sie nicht deaktivieren. | Mittel<br>Führt regelmäßige Updates an den Layout- und Datenbankinformationen sowie einzelnen Dateien für den Vorabruf durch, die bei Bedarf generiert werden.   | Mittel                                  | Ja, wenn die Startzeiten für Anwendungen auch nach dem Deaktivieren dieser Funktion akzeptabel sind.  |

| Dienst oder Task                                    | Beschreibung  | Standardhäufigkeit oder -start                         | Auswirkung auf Linked-Clone-Betriebssystemfestplatten   | Auswirkung auf E/A-Vorgänge pro Sekunde | Dienst oder Task deaktivieren?  |
|---|---|--|---|---|---|
| Sicherung der Windows-Registrierung (RegIdleBackup) | Führt eine automatische Sicherung der Windows-Registrierung durch, wenn das System sich im Leerlauf befindet. | Alle 10 Tage um 12:00 Uhr                              | Mittel.<br>Bei jeder Ausführung dieses Tasks werden Sicherungsdateien der Registrierung erstellt.   | Mittel.                                 | Ja.<br>Es besteht keine Notwendigkeit zur Sicherung der Windows-Registrierung. Zum Wiederherstellen von Registrierungsdaten können Sie eine View Composer-Aktualisierung durchführen.     |
| Systemwiederherstellung                             | Stellt das Windows-System in einem vorherigen, fehlerfreien Zustand wieder her.                               | Beim Start von Windows und anschließend einmal täglich | Gering bis mittel.<br>Erfasst immer dann einen Systemwiederherstellungspunkt, wenn das System dies als erforderlich betrachtet. Wenn sich der verknüpfte Klon im Leerlauf befindet, ist der so entstehende Overhead gering. | Keine nennenswerte Auswirkung           | Ja<br>Trotz geringer Auswirkung ist dieser Task überflüssig, wenn Sie Betriebssystemfestplatten mithilfe von View Composer in den Zustand ihrer ursprünglichen Snapshots zurückversetzen. |

| Dienst oder Task                                   | Beschreibung  | Standardhäufigkeit oder -start   | Auswirkung auf Linked-Clone-Betriebssystemfestplatten  | Auswirkung auf E/A-Vorgänge pro Sekunde | Dienst oder Task deaktivieren?   |
|--|---|--|--|---|--|
| Windows Defender                                   | Stellt Anti-Spyware-Funktionen bereit.  | Beim Start von Windows. Führt einmal täglich eine Schnellprüfung durch. Vor jedem Scan wird auf Updates geprüft. | Mittel bis hoch. Führt Definitions-Updates, geplante Scans und Scans aus, die bei Bedarf gestartet werden.   | Mittel bis hoch.                        | Ja, wenn eine andere Anti-Spyware-Software installiert ist.  |
| Microsoft-Feeds-Synchronisierung (msfeedssync.exe) | Führt eine regelmäßige Aktualisierung der RSS-Feeds in Windows Internet Explorer-Webbrowsern durch. Dieser Task aktualisiert RSS-Feeds, für die eine automatische RSS-Feed-Synchronisierung aktiviert wurde. Der Prozess erscheint nur im Windows Task Manager, wenn Internet Explorer ausgeführt wird. | Einmal täglich   | Mittel. Wirkt sich auf das Wachstum von Betriebssystemfestplatten aus, wenn keine persistenten Festplatten konfiguriert sind. Sind persistente Festplatten konfiguriert, gelten die Auswirkungen für die persistenten Festplatten. | Mittel                                  | Ja, wenn Ihre Benutzer keine automatischen RSS-Feed-Aktualisierungen auf ihren Desktops benötigen. |

## Deaktivieren der geplanten Datenträgerdefragmentierung auf übergeordneten virtuellen Windows 7- und Windows 8-Maschinen

Bevor Sie verknüpfte Klone erstellen, müssen Sie die geplante Datenträgerdefragmentierung auf übergeordneten virtuellen Windows 7- und Windows 8-Maschinen deaktivieren. Windows 7 und Windows 8 planen standardmäßig eine wöchentliche Datenträgerdefragmentierung. Wiederholte Defragmentierungsvorgänge können die Linked-Clone-Betriebssystemfestplatten erheblich anwachsen lassen und verbessern den Festplattenzugriff auf verknüpfte Klone nur unwesentlich.

Wenn Sie einen Linked-Clone-Pool aus der übergeordneten virtuellen Maschine erstellen, nutzen die verknüpften Klone die Replikatfestplatte gemeinsam. Nachfolgende Defragmentierungsvorgänge wirken sich nicht auf die Replikatfestplatte aus, da diese schreibgeschützt ist. Stattdessen werden durch die Defragmentierung die Betriebssystemfestplatten der Klone vergrößert.

Als empfohlene Vorgehensweise sollten Sie die übergeordnete virtuelle Maschine einmalig defragmentieren, bevor Sie einen Snapshot erstellen und den Pool erstellen. Die verknüpften Klone profitieren von der Defragmentierung, da sie die optimierte schreibgeschützte Replikatfestplatte gemeinsam nutzen.



## Voraussetzungen

- Stellen Sie sicher, dass die auf den verknüpften Klonen bereitzustellenden Anwendungen auf der virtuellen Maschine installiert sind.
- Vergewissern Sie sich, dass View Agent mit View Composer Agent auf der virtuellen Maschine installiert ist.

## Verfahren

- 1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **Konsole öffnen**.
- 2 Melden Sie sich am Windows 7- oder Windows 8-Gastbetriebssystem als Administrator an.
- 3 Klicken Sie auf **Start** und geben Sie im Feld **Programme/Dateien durchsuchen** den Befehl **defrag** ein.
- 4 Klicken Sie im Programmfenster auf **Defragmentierung**.
- 5 Klicken Sie im Dialogfeld **Defragmentierung** auf **Datenträger defragmentieren**.  
  
Die Datenträgerdefragmentierung konsolidiert defragmentierte Dateien auf der Festplatte der virtuellen Maschine.
- 6 Klicken Sie im Dialogfeld **Defragmentierung** auf **Zeitplan konfigurieren**.
- 7 Deaktivieren Sie die Option **Nach Zeitplan ausführen (empfohlen)** und klicken Sie auf **OK**.

Es werden keine Defragmentierungsvorgänge auf virtuellen Linked-Clone-Maschinen durchgeführt, die über diese übergeordnete virtuelle Maschine erstellt werden.

## Deaktivieren des Windows Update-Dienstes auf virtuellen Windows 7- und Windows 8-Maschinen

Durch eine Deaktivierung des Windows Update-Dienstes können Sie die Anzahl der Dateierstellungen und der Schreibvorgänge verringern, die beim Herunterladen und Installieren von Updates auftreten. Auf diese Weise können Sie das Wachstum verknüpfter Klone und die Anzahl der E/A-Vorgänge pro Sekunde auf verknüpften Klonen und vollständigen virtuellen Maschinen verringern.

Deaktivieren Sie den Windows Update-Dienst, wenn Sie Linked-Clone-Desktops aktualisieren und neu zusammenstellen. Bei einer Aktualisierung werden die Betriebssystemfestplatten in den Zustand ihrer ursprünglichen Snapshots zurückversetzt und automatische Windows-Updates werden gelöscht. Bei einer Neuzusammenstellung werden die Betriebssystemfestplatten unter Verwendung eines neuen Snapshots erneut erstellt. Da dieser neue Snapshot die Windows-Updates möglicherweise bereits umfasst, sind automatische Windows-Updates überflüssig.

Deaktivieren Sie den Windows Update-Dienst nicht, wenn Sie Windows-Updates nicht über Neuzusammenstellungen auf den verknüpften Klonen installieren.

## Voraussetzungen

Stellen Sie sicher, dass die neuesten Windows-Updates heruntergeladen und auf der virtuellen Maschine installiert wurden.

## Verfahren

- 1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **Konsole öffnen**.
- 2 Melden Sie sich am Windows 7- oder Windows 8-Gastbetriebssystem als Administrator an.
- 3 Klicken Sie auf **Start > Systemsteuerung > System und Sicherheit > Automatische Updates ein- oder ausschalten**.
- 4 Wählen Sie im Menü **Wichtige Updates** die Option **Nie auf Updates überprüfen**.
- 5 Deaktivieren Sie die Option **Empfohlene Updates auf die gleiche Weise wie wichtige Updates bereitstellen**.
- 6 Deaktivieren Sie die Option **Allen Benutzern das Installieren von Updates auf diesem Computer ermöglichen** und klicken Sie auf **OK**.

## Deaktivieren des Diagnoserichtliniendienstes auf virtuellen Windows 7- und Windows 8-Maschinen

Durch das Deaktivieren des Windows-Diagnoserichtliniendienstes kann die Anzahl der Systemschreibvorgänge minimiert und das Wachstum von Linked-Clone-Computern verringert werden.

Deaktivieren Sie den Windows-Diagnoserichtliniendienst nicht, wenn Ihre Benutzer die Diagnosetools auf ihren Desktops benötigen.

## Verfahren

- 1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **Konsole öffnen**.
- 2 Melden Sie sich am Windows 7- oder Windows 8-Gastbetriebssystem als Administrator an.
- 3 Klicken Sie auf **Start > Systemsteuerung > System und Sicherheit > Verwaltung**.
- 4 Wählen Sie **Dienste** und klicken Sie auf **Öffnen**.
- 5 Doppelklicken Sie auf **Diagnoserichtliniendienst**.
- 6 Klicken Sie im Dialogfeld „Eigenschaften von Diagnoserichtliniendienst (Lokaler Computer)“ auf **Beenden**.
- 7 Wählen Sie im Menü „Starttyp“ die Option **Deaktiviert**.
- 8 Klicken Sie auf **OK**.

## Deaktivieren der Vorabruf- und SuperFetch-Funktionen auf virtuellen Windows 7- und Windows 8-Maschinen

Durch das Deaktivieren der Vorabruf- und SuperFetch-Funktionen in Windows können Sie das Generieren von Vorabrufdateien und den Overhead vermeiden, der mit Vorabruf- und SuperFetch-Vorgängen verbunden ist. Auf diese Weise kann das Wachstum von Linked-Clone-Maschinen verringert und die Anzahl der E/A-Vorgänge pro Sekunde auf vollständigen virtuellen Maschinen und verknüpften Klonen minimiert werden.

Zum Deaktivieren der Vorabruf- und SuperFetch-Funktionen müssen Sie einen Windows-Registrierungsschlüssel bearbeiten und den Vorabrufdienst auf der virtuellen Maschine deaktivieren.

### Voraussetzungen

Informationen zur Verwendung des Windows-Registrierungs-Editors unter Windows 7 und Windows 8 finden Sie auf der Microsoft TechNet-Website.

### Verfahren

- 1 Starten Sie den Windows-Registrierungs-Editor auf der lokalen virtuellen Windows 7- oder Windows 8-Maschine.
- 2 Navigieren Sie zum Registrierungsschlüssel **PrefetchParameters**.  
Der Registrierungsschlüssel befindet sich im folgenden Pfad: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters.
- 3 Legen Sie die Werte für **EnablePrefetcher** und **EnableSuperfetch** auf **0** fest.
- 4 Klicken Sie auf **Start > Systemsteuerung > System und Sicherheit > Verwaltung**.
- 5 Wählen Sie **Dienste** und klicken Sie auf **Öffnen**.
- 6 Doppelklicken Sie auf den Dienst **Superfetch**.
- 7 Klicken Sie im Dialogfeld „Eigenschaften von SuperFetch (Lokaler Computer)“ auf **Beenden**.
- 8 Wählen Sie im Menü „Starttyp“ die Option **Deaktiviert**.
- 9 Klicken Sie auf **OK**.

## Deaktivieren der Sicherung der Windows-Registrierung auf virtuellen Windows 7- und Windows 8-Maschinen

Durch das Deaktivieren der Sicherung der Windows-Registrierung, RegIdleBackup, kann die Anzahl der Systemschreibvorgänge minimiert und das Wachstum von Linked-Clone-Maschinen verringert werden.

### Verfahren

- 1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **Konsole öffnen**.
- 2 Melden Sie sich am Windows 7- oder Windows 8-Gastbetriebssystem als Administrator an.
- 3 Klicken Sie auf **Start > Systemsteuerung > System und Sicherheit > Verwaltung**.

- 4 Wählen Sie **Aufgabenplanung** und klicken Sie auf **Öffnen**.
- 5 Erweitern Sie im linken Bereich **Aufgabenplanungsbibliothek, Microsoft, Windows**.
- 6 Doppelklicken Sie auf **Registrierung** und wählen Sie **RegIdleBackup**.
- 7 Klicken Sie im Fensterbereich „Aktionen“ auf **Deaktivieren**.

## Deaktivieren der Systemwiederherstellung auf virtuellen Windows 7- und Windows 8-Maschinen

Sie benötigen die Windows-Funktion zur Systemwiederherstellung nicht, wenn Sie Linked-Clone-Betriebssystemfestplatten mithilfe der View Composer-Aktualisierung in den Zustand ihrer ursprünglichen Snapshots zurückversetzen.

Wenn sich das Betriebssystem im Leerlauf befindet, hat die Systemwiederherstellung keine sichtbare Auswirkung auf das Wachstum von Betriebssystemfestplatten. Wenn sich das Betriebssystem jedoch in Verwendung befindet, generiert die Systemwiederherstellung Wiederherstellungspunkte basierend auf der Systemverwendung. Dies kann erhebliche Auswirkungen auf das Wachstum von Betriebssystemfestplatten haben.

Die Funktion der Windows-Systemwiederherstellung entspricht der einer View Composer-Aktualisierung.

Als empfohlene Vorgehensweise können Sie die Windows-Systemwiederherstellung deaktivieren und ein unnötiges Wachstum Ihrer verknüpften Klone vermeiden.

Wenn Sie keine Aktualisierungen verwenden, wägen Sie ab, ob die Systemwiederherstellung in Ihrer View-Umgebung aktiviert bleiben sollte.

### Verfahren

- 1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **Konsole öffnen**.
- 2 Melden Sie sich am Windows 7- oder Windows 8-Gastbetriebssystem als Administrator an.
- 3 Klicken Sie auf **Start > Systemsteuerung > System und Sicherheit > Verwaltung**.
- 4 Wählen Sie **Aufgabenplanung** und klicken Sie auf **Öffnen**.
- 5 Erweitern Sie im linken Bereich **Aufgabenplanungsbibliothek, Microsoft, Windows**.
- 6 Doppelklicken Sie auf **SystemRestore** und wählen Sie **SR**.
- 7 Klicken Sie im Fensterbereich „Aktionen“ auf **Deaktivieren**.

## Deaktivieren von Windows Defender auf virtuellen Windows 7- und Windows 8-Maschinen

Microsoft Windows Defender kann zu einem Wachstum von Linked-Clone-Betriebssystemfestplatten beitragen und die Anzahl an E/A-Vorgängen pro Sekunde auf verknüpften Klonen und vollständigen virtuellen Maschinen erhöhen. Deaktivieren Sie Windows Defender, wenn Sie eine andere Anti-Spyware-Software auf der virtuellen Maschine installiert haben.

Wenn Windows Defender die einzige installierte Anti-Spyware-Software auf der virtuellen Maschine ist, sollten Sie Windows Defender möglicherweise auf den Desktops in Ihrer Umgebung aktiviert lassen.

#### Verfahren

- 1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **Konsole öffnen**.
- 2 Melden Sie sich am Windows 7- oder Windows 8-Gastbetriebssystem als Administrator an.
- 3 Klicken Sie auf **Start** und geben Sie im Feld „Programme/Dateien durchsuchen“ den Befehl **Windows Defender** ein.
- 4 Klicken Sie auf **Tools > Optionen > Administrator**.
- 5 Deaktivieren Sie die Option **Dieses Programm verwenden** und klicken Sie auf **Speichern**.

## Deaktivieren der Microsoft-Feeds-Synchronisierung auf virtuellen Windows 7- und Windows 8-Maschinen

Windows Internet Explorer verwendet die Microsoft-Feeds-Synchronisierung, um RSS-Feeds in den Webbrowsern der Benutzer zu aktualisieren. Dieser Task kann zu einem Wachstum der verknüpften Klone beitragen. Deaktivieren Sie diesen Task, wenn Ihre Benutzer keine automatische Aktualisierung der RSS-Feeds in ihren Browsern benötigen.

Die Microsoft-Feeds-Synchronisierung kann zu einem Wachstum der Betriebssystemfestplatten führen, wenn keine persistenten Festplatten konfiguriert sind. Sind persistente Festplatten konfiguriert, gelten die Auswirkungen für die persistenten Festplatten. In dieser Situation sollten Sie dennoch die Microsoft-Feeds-Synchronisierung deaktivieren, um das Wachstum persistenter Festplatten zu kontrollieren.

#### Verfahren

- 1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **Konsole öffnen**.
- 2 Melden Sie sich am Windows 7- oder Windows 8-Gastbetriebssystem als Administrator an.
- 3 Klicken Sie auf **Start > Systemsteuerung > Netzwerk und Internet > Internetoptionen**.
- 4 Klicken Sie auf die Registerkarte **Inhalt**.
- 5 Klicken Sie unter **Feeds und Web Slices** auf **Einstellungen**.
- 6 Deaktivieren Sie die Option **Feeds und Web Slices automatisch auf Aktualisierungen prüfen** und klicken Sie auf **OK**.
- 7 Klicken Sie im Dialogfeld **Interneteigenschaften** auf **OK**.

## Vorbereiten virtueller Maschinen für View Composer

Sie müssen zum Bereitstellen eines Linked-Clone-Desktop-Pools eine übergeordnete virtuelle Maschine vorbereiten, die die Anforderungen des View Composer-Dienstes erfüllt.

- **Vorbereiten einer übergeordneten virtuellen Maschine**

Für den View Composer-Dienst ist eine übergeordnete virtuelle Maschine erforderlich, mit der Sie ein Basis-Image zum Erstellen und Verwalten von Linked-Clone-Desktop-Pools generieren.

- **Aktivieren von Windows auf virtuellen Linked-Clone-Computern**

Um sicherzustellen, dass View Composer Windows 8-, Windows 7- und Windows Vista-Betriebssysteme auf Linked-Clone-Computern ordnungsgemäß aktiviert, müssen Sie die Microsoft-Volumenaktivierung auf der übergeordneten virtuellen Maschine verwenden. Für die Volumenaktivierungstechnologie ist ein Volumenlizenzschlüssel erforderlich.

- **Deaktivieren des Windows-Ruhezustands in der übergeordneten virtuellen Maschine**

Die Option für den Windows-Ruhezustand erstellt eine umfangreiche Systemdatei, welche die Linked-Clone-Betriebssystemfestplatten vergrößern kann, die aus der übergeordneten virtuellen Maschine erstellt werden. Durch das Deaktivieren des Ruhezustands wird die Größe verknüpfter Klone verringert.

- **Konfigurieren einer übergeordneten virtuellen Maschine zur Verwendung des lokalen Speichers**

Wenn Sie eine übergeordnete virtuelle Maschine für View Composer vorbereiten, können Sie die übergeordnete virtuelle Maschine sowie die verknüpften Klone so konfigurieren, dass Auslagerungsdateien der virtuellen Maschine im lokalen Datenspeicher gespeichert werden. Bei dieser optionalen Strategie können Sie die Vorteile des lokalen Speichers nutzen.

- **Protokollieren der Auslagerungsdateigröße für die übergeordnete virtuelle Maschine**

Wenn Sie einen Linked-Clone-Pool erstellen, können Sie Auslagerungsdateien und temporäre Dateien des Gastbetriebssystems an eine separate Festplatte umleiten. Sie müssen diese Festplatte so konfigurieren, dass sie größer ist als die Auslagerungsdatei im Gastbetriebssystem.

- **Erhöhen des Zeitüberschreitungslimits für QuickPrep-Anpassungsskripts**

View Composer beendet ein nach der Synchronisierung ausgeführtes QuickPrep-Skript oder ein Abschaltskript, wenn dessen Ausführung länger als 20 Sekunden dauert. Sie können das Zeitüberschreitungslimit für diese Skripts erhöhen, indem Sie den Wert `ExecScriptTimeout` in der Windows-Registrierung auf der übergeordneten virtuellen Maschine ändern.

## Vorbereiten einer übergeordneten virtuellen Maschine

Für den View Composer-Dienst ist eine übergeordnete virtuelle Maschine erforderlich, mit der Sie ein Basis-Image zum Erstellen und Verwalten von Linked-Clone-Desktop-Pools generieren.

### Voraussetzungen

- Stellen Sie sicher, dass Sie eine virtuelle Maschine zur Verwendung für bereitgestellte Remote-Desktops vorbereitet haben. Siehe [Erstellen virtueller Maschinen für die Remote-Desktop-Bereitstellung](#).

Eine übergeordnete virtuelle Maschine, die Sie für View Composer verwenden, muss entweder zu derselben Active Directory-Domäne wie die Domäne gehören, mit der sich die Linked-Clone-Maschinen verbinden, oder sie muss Mitglied der lokalen ARBEITSGRUPPE sein.

---

**Wichtig** Um in View 4.5 oder einer höheren Version unterstützte Funktionen wie z. B. das Umleiten löschtbarer Dateien auf eine separate Festplatte und das Anpassen von Linked-Clone-Maschinen mit Sysprep nutzen zu können, müssen Sie die Maschinen anhand einer übergeordneten virtuellen Maschine bereitstellen, auf der View Agent 4.5 oder höher installiert ist.

Sie können View Composer nicht zur Bereitstellung von Computern verwenden, auf denen die Windows Vista Ultimate Edition oder Windows XP Professional SP1 ausgeführt wird.

---

- Stellen Sie sicher, dass die virtuelle Maschine nicht von einem verknüpften Klon für View Composer konvertiert wurde. Eine virtuelle Maschine, die von einem verknüpften Klon konvertiert wurde, verfügt über die kloneigenen Informationen zu interner Festplatte und Status. Eine übergeordnete virtuelle Maschine kann nicht über Statusinformationen verfügen.

---

**Wichtig** Verknüpfte Klone und virtuelle Maschinen, die aus verknüpften Klonen konvertiert wurden, werden nicht als übergeordnete virtuelle Maschinen unterstützt.

---

- Wenn auf der übergeordneten virtuellen Maschine Windows XP und Active Directory unter Windows Server 2008 ausgeführt wird, wenden Sie ein Update-Patch auf die virtuelle Windows XP-Maschine an. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 944043 unter der folgenden Adresse: <http://support.microsoft.com/kb/944043/en-us>.

Wenn Sie das Windows Server 2008-RODC-Compatibility Pack für Windows XP nicht installieren, können über diese übergeordnete virtuelle Maschine bereitgestellte verknüpfte Klone nicht zur Domäne hinzugefügt werden.

- Wenn Sie View Agent auf der übergeordneten virtuellen Maschine installieren, wählen Sie die Option **View Composer Agent** aus. Siehe [Installieren von View Agent auf einer virtuellen Maschine](#).

Um View Agent in einer großen Umgebung zu aktualisieren, können Sie standardmäßige Windows-Aktualisierungsmethoden wie Altiris, SMS, LanDesk, BMC oder eine andere Software für die Systemverwaltung verwenden. Sie können zum Aktualisieren von View Agent auch den Vorgang der Neuzusammenstellung verwenden.

---

**Hinweis** Das Anmeldekonto für den VMware View Composer-Gastagentserver-Dienst in einer übergeordneten virtuellen Maschine darf nicht geändert werden. Standardmäßig handelt es sich hierbei um das lokale Systemkonto. Wenn Sie dieses Konto ändern, können die von der übergeordneten Maschine erstellten verknüpften Klone nicht gestartet werden.

---

- Zur Bereitstellung von Windows 8-, Windows 7- oder Windows Vista-Maschinen konfigurieren Sie einen Volumenlizenzschlüssel und aktivieren Sie das Betriebssystem der übergeordneten virtuellen Maschine mit der Volumenaktivierung. Siehe [Aktivieren von Windows auf virtuellen Linked-Clone-Computern](#).

- Wenn auf der übergeordneten virtuellen Maschine Windows 7 oder Windows 8 ausgeführt wird, müssen Sie sicherstellen, dass die empfohlenen Vorgehensweisen zur Optimierung des Betriebssystems ausgeführt wurden. Siehe [Optimieren von Windows 7 und Windows 8 für virtuelle Maschinen mit verknüpftem Klon](#).
- Machen Sie sich mit der Vorgehensweise zum Deaktivieren der Suche nach Windows-Updates für Gerätetreiber vertraut. Weitere Informationen finden Sie im Microsoft Technet-Artikel „Disable Searching Windows Update for Device Drivers“ unter [http://technet.microsoft.com/en-us/library/cc730606\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx).

## Verfahren

- ◆ Entfernen Sie die DHCP-Lease auf der übergeordneten virtuellen Maschine, um das Kopieren einer geleasteten IP-Adresse zu den verknüpften Klonen im Pool zu vermeiden.
  - a Öffnen Sie auf der übergeordneten virtuellen Maschine eine Eingabeaufforderung.
  - b Geben Sie den Befehl **ipconfig /release** ein.

- ◆ Stellen Sie sicher, dass die Systemfestplatte ein einzelnes Volume umfasst.

Sie können keine verknüpften Klone von einer übergeordneten virtuellen Maschine bereitstellen, die mehr als ein Volume umfasst. Mit View Composer-Dienst werden mehrere Laufwerkpartitionen nicht unterstützt. Es werden mehrere virtuelle Festplatten unterstützt.

---

**Hinweis** Wenn die übergeordnete virtuelle Maschine mehrere virtuelle Festplatten enthält, wenn Sie einen Desktop-Pool erstellen, wählen Sie keinen Laufwerksbuchstaben für die persistente View Composer-Festplatte oder Festplatte mit löschbaren Daten aus, die bereits auf der übergeordneten virtuellen Maschine besteht oder mit einem Laufwerksbuchstaben in Konflikt steht, der für ein Netzlaufwerk verwendet wird.

---

- ◆ Überprüfen Sie, dass die virtuelle Maschine keine unabhängige Festplatte enthält.

Eine unabhängige Festplatte wird ausgeschlossen, wenn Sie einen Snapshot der virtuellen Maschine erstellen. Verknüpfte Klone, die von der virtuellen Maschine erstellt oder neu zusammengesetzt werden, enthalten die unabhängige Festplatte nicht.
- ◆ Wenn Sie planen, bei der Erstellung von Linked-Clone-Maschinen Festplatten mit löschbaren Daten zu konfigurieren, entfernen Sie standardmäßige Benutzer-TEMP- und TMP-Variablen von der übergeordneten virtuellen Maschine.

Sie können die Datei `pagefile.sys` auch entfernen, um zu verhindern, dass die Datei auf allen verknüpften Klonen dupliziert wird. Wenn Sie die Datei `pagefile.sys` auf der übergeordneten virtuellen Maschine lassen, wird eine schreibgeschützte Version der Datei von den verknüpften Klonen geerbt, während eine zweite Version der Datei auf der Festplatte mit löschbaren Daten verwendet wird.
- ◆ Deaktivieren Sie die Option für den Ruhezustand, um die Größe der Linked-Clone-Betriebssystemfestplatten zu verringern, die aus der übergeordneten virtuellen Maschine erstellt werden.



- ◆ Deaktivieren Sie das Durchsuchen der Windows Update-Website nach Gerätetreibern, bevor Sie einen Snapshot der übergeordneten virtuellen Maschine erstellen.

Diese Windows-Funktion kann bei der Anpassung von Linked-Clone-Maschinen zu Konflikten führen. Bei der Anpassung der einzelnen verknüpften Klone sucht Windows möglicherweise im Internet nach den besten Treibern für den jeweiligen Klon, sodass wiederholt Suchvorgänge ausgeführt werden und es zu Verzögerungen bei der Anpassung kommt.

- ◆ Deaktivieren Sie in vSphere Client die vApp-Optionseinstellung auf der übergeordneten virtuellen Maschine.
- ◆ Deaktivieren Sie auf Maschinen mit Windows 8.1 und Windows Server 2008 R2 die geplante Wartungsaufgabe, die Festplattenspeicherplatz durch Entfernen nicht verwendeter Funktionen wiederherstellt.

Beispiel: `Schtasks.exe /change /disable /tn "\\Microsoft\\Windows\\AppxDeploymentClient\\Pre-staged app cleanup"`

Wenn Sie sie nicht deaktivieren, kann diese Wartungsaufgabe das Sysprep-Anpassungsskript entfernen, nachdem die verknüpften Klone erstellt wurden. Dies würde dazu führen, dass nachfolgende Neuzusammenstellungen mit Zeitüberschreitungsfehlern beim Anpassungsvorgang fehlschlagen.

Sie können einen Linked-Clone-Pool von einer übergeordneten virtuellen Maschine bereitstellen.

### Nächste Schritte

Verwenden Sie vSphere Client oder vSphere Web Client, um einen Snapshot der übergeordneten virtuellen Maschine im ausgeschalteten Zustand zu erstellen. Dieser Snapshot wird als Baselinekonfiguration für den ersten Satz an Linked-Clone-Maschinen verwendet, die an die übergeordnete virtuelle Maschine gekoppelt sind.

---

**Wichtig** Bevor Sie einen Snapshot erstellen, müssen Sie die übergeordnete virtuelle Maschine vollständig herunterfahren. Verwenden Sie hierzu den Befehl **Herunterfahren** im Gastbetriebssystem.

---

## Aktivieren von Windows auf virtuellen Linked-Clone-Computern

Um sicherzustellen, dass View Composer Windows 8-, Windows 7- und Windows Vista-Betriebssysteme auf Linked-Clone-Computern ordnungsgemäß aktiviert, müssen Sie die Microsoft-Volumenaktivierung auf der übergeordneten virtuellen Maschine verwenden. Für die Volumenaktivierungstechnologie ist ein Volumenlizenzschlüssel erforderlich.

Zur Aktivierung von Windows 8, Windows 7 oder Windows Vista mit Volumenaktivierung müssen Sie den Schlüsselverwaltungsdienst (Key Management Service, KMS) verwenden, für den ein KMS-Lizenzschlüssel erforderlich ist. Wenden Sie sich an Ihren Microsoft-Händler, um einen Volumenlizenzschlüssel zu erhalten und die Volumenaktivierung zu konfigurieren.

---

**Hinweis** View Composer bietet keine Unterstützung für die MAK-Lizenzierung (Multiple Activation Key).

---

Bevor Sie mit View Composer Linked-Clone-Computer erstellen können, müssen Sie die Volumenaktivierung verwenden, um das Betriebssystem auf der übergeordneten virtuellen Maschine zu aktivieren.

---

**Hinweis** Bei Windows XP-Computer mit Volumenlizenzen ist keine Aktivierung notwendig.

---

Bei der Erstellung eines Linked-Clone-Computers und bei jeder Neuzusammenstellung des verknüpften Klons verwendet View Composer Agent den KMS-Server der übergeordneten virtuellen Maschine, um das Betriebssystem auf dem verknüpften Klon zu aktivieren.

Das View Composer QuickPrep-Tool führt zur Aktivierung die folgenden Schritte aus:

- 1 Aufruf eines Skripts, um den aktuellen Lizenzstatus auf der virtuellen Linked-Clone-Maschine zu entfernen
- 2 Neustart des Gastbetriebssystems
- 3 Aufruf eines Skripts, das mithilfe der KMS-Lizenzierung das Betriebssystem auf dem Klon aktiviert.

Die Aktivierung wird bei jeder Ausführung von QuickPrep auf einem verknüpften Klon durchgeführt.

View Composer verwendet für die KMS-Lizenzierung den KMS-Server, der für die Aktivierung der übergeordneten virtuellen Maschine konfiguriert ist. Der KMS-Server behandelt einen aktivierten verknüpften Klon als einen Computer mit einer neu ausgegebenen Lizenz.

## Deaktivieren des Windows-Ruhezustands in der übergeordneten virtuellen Maschine

Die Option für den Windows-Ruhezustand erstellt eine umfangreiche Systemdatei, welche die Linked-Clone-Betriebssystemfestplatten vergrößern kann, die aus der übergeordneten virtuellen Maschine erstellt werden. Durch das Deaktivieren des Ruhezustands wird die Größe verknüpfter Klone verringert.

Die Option für den Windows-Ruhezustand erstellt eine versteckte Systemdatei, `Hiberfil.sys`. Windows verwendet diese Datei, um eine Kopie des Systemarbeitspeichers auf der Festplatte zu speichern, wenn die Funktion für den hybriden Standbymodus aktiviert ist. Wenn Sie einen Linked-Clone-Pool erstellen, wird die Datei auf der Betriebssystemfestplatte für jeden verknüpften Klon erstellt.

Auf virtuellen Windows 7- oder Windows 8-Maschinen kann diese Datei bis zu 10 GB groß sein.

---

**Vorsicht** Wenn Sie den Ruhezustand deaktivieren, funktioniert die Einstellung für den hybriden Standbymodus nicht. Benutzer können Daten verlieren, wenn die Einstellung für den hybriden Standbymodus eingeschaltet ist und es zu einem Stromausfall kommt.

---

### Voraussetzungen

Machen Sie sich mit der Funktion für den Windows-Ruhezustand vertraut. Informationen finden Sie auf der Website des Microsoft-Supports. Informationen zum Deaktivieren des Ruhezustands unter Windows 8, Windows 7 oder Windows Vista finden Sie auf der Microsoft-Supportwebsite. Suchen Sie nach der Vorgehensweise für das Deaktivieren und erneute Aktivieren des Ruhezustands auf einem Computer, auf dem Windows ausgeführt wird.

## Verfahren

- 1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **Konsole öffnen**.
- 2 Melden Sie sich am Windows-Gastbetriebssystem als Administrator an.
- 3 Deaktivieren Sie die Option für den Ruhezustand.

| Betriebssystem                          | Aktion   |
|---|--|
| Windows 8, Windows 7 oder Windows Vista | <ol style="list-style-type: none"> <li>a Klicken Sie auf <b>Start</b> und geben Sie im Feld <b>Suche starten</b> den Befehl <b>cmd</b> ein.</li> <li>b Klicken Sie in den Suchergebnissen mit der rechten Maustaste auf <b>Eingabeaufforderung</b> und klicken Sie auf <b>Als Administrator ausführen</b>.</li> <li>c Klicken Sie an der Eingabeaufforderung der Benutzerkontensteuerung auf <b>Weiter</b>.</li> <li>d Geben Sie an der Eingabeaufforderung <b>powercfg.exe /hibernate off</b> ein und drücken Sie die Eingabetaste.</li> <li>e Geben Sie <b>exit</b> ein und drücken Sie die Eingabetaste.</li> </ol> |
| Windows XP                              | <ol style="list-style-type: none"> <li>a Klicken Sie auf <b>Start &gt; Ausführen</b>.</li> <li>b Geben Sie <b>cmd</b> ein und klicken Sie auf <b>OK</b>.</li> <li>c Geben Sie an der Eingabeaufforderung <b>powercfg.exe /hibernate off</b> ein und drücken Sie die Eingabetaste.</li> <li>d Geben Sie <b>exit</b> ein und drücken Sie die Eingabetaste.</li> </ol>  |

- 4 Melden Sie sich vom Gastbetriebssystem ab.

Wenn Sie aus der übergeordneten virtuellen Maschine eine Linked-Clone-Maschine erstellt haben, wird die Datei Hiberfil.sys nicht auf den Linked-Clone-Betriebssystemfestplatten erstellt.

## Konfigurieren einer übergeordneten virtuellen Maschine zur Verwendung des lokalen Speichers

Wenn Sie eine übergeordnete virtuelle Maschine für View Composer vorbereiten, können Sie die übergeordnete virtuelle Maschine sowie die verknüpften Klone so konfigurieren, dass Auslagerungsdateien der virtuellen Maschine im lokalen Datenspeicher gespeichert werden. Bei dieser optionalen Strategie können Sie die Vorteile des lokalen Speichers nutzen.

Bei dieser Vorgehensweise können Sie den lokalen Speicher für die Auslagerungsdateien der virtuellen Maschine und nicht die Auslagerungsdateien und temporären Dateien im Gastbetriebssystem konfigurieren. Wenn Sie einen Linked-Clone-Pool erstellen, können Sie Auslagerungsdateien und temporäre Dateien des Gastbetriebssystems zu einer separaten Festplatte umleiten. Siehe [Arbeitsblatt zum Erstellen eines Linked-Clone-Desktop-Pools](#).

### Voraussetzungen

Bereiten Sie die übergeordnete virtuelle Maschine vor, damit die Anforderungen des View Composer-Dienstes erfüllt werden. Siehe [Vorbereiten einer übergeordneten virtuellen Maschine](#).

## Verfahren

- 1 Konfigurieren Sie einen Auslagerungsdatei-Datenspeicher auf dem ESXi-Host oder -Cluster, auf dem Sie den Linked-Clone-Pool bereitstellen möchten.
- 2 Wenn Sie die übergeordnete virtuelle Maschine in vCenter Server erstellen, speichern Sie die Auslagerungsdateien der virtuellen Maschine im Auslagerungsdatei-Datenspeicher auf dem lokalen ESXi-Host oder -Cluster:
  - a Wählen Sie in vSphere Client die übergeordnete virtuelle Maschine aus.
  - b Klicken Sie auf **Einstellungen bearbeiten** und anschließend auf die Registerkarte **Optionen**.
  - c Klicken Sie auf **Speicherort der Auslagerungsdatei** und auf **Im Auslagerungsdatei-Datenspeicher des Hosts speichern**.

Weitere Anweisungen finden Sie in der VMware vSphere-Dokumentation.

Wenn Sie einen Pool aus dieser übergeordneten virtuellen Maschine bereitstellen, verwenden die verknüpften Klone den Auslagerungsdatei-Datenspeicher des lokalen ESXi-Hosts.

## Protokollieren der Auslagerungsdateigröße für die übergeordnete virtuelle Maschine

Wenn Sie einen Linked-Clone-Pool erstellen, können Sie Auslagerungsdateien und temporäre Dateien des Gastbetriebssystems an eine separate Festplatte umleiten. Sie müssen diese Festplatte so konfigurieren, dass sie größer ist als die Auslagerungsdatei im Gastbetriebssystem.

Wenn ein verknüpfter Klon, der mit einer separaten Festplatte für die löschbaren Dateien konfiguriert ist, ausgeschaltet wird, ersetzt View die temporäre Festplatte mit einer Kopie der ursprünglichen temporären Festplatte, die View Composer mit dem Linked-Clone-Pool erstellt hat. Diese Funktion kann das Wachstum verknüpfter Klone verlangsamen. Diese Funktion kann jedoch nur verwendet werden, wenn die Größe der Festplatte mit löschbaren Dateien ausreicht, um die Auslagerungsdateien des Gastbetriebssystems aufzunehmen.

Bevor Sie die Festplatte für löschbare Dateien konfigurieren können, müssen Sie die maximale Auslagerungsdateigröße in der übergeordneten virtuellen Maschine kennen. Die Auslagerungsdatei der verknüpften Klone weist dieselbe Größe auf wie die Auslagerungsdatei der übergeordneten virtuellen Maschine, aus der die verknüpften Klone erstellt wurden.

Um zu verhindern, dass die Datei auf allen verknüpften Klonen dupliziert wird, sollten Sie die Datei `pagefile.sys` vor dem Erstellen eines Snapshots aus der übergeordneten virtuellen Maschine entfernen. Siehe [Vorbereiten einer übergeordneten virtuellen Maschine](#).

---

**Hinweis** Diese Funktion ist nicht mit der Konfiguration von lokalem Speicher für die Auslagerungsdateien der virtuellen Maschine identisch. Siehe [Konfigurieren einer übergeordneten virtuellen Maschine zur Verwendung des lokalen Speichers](#).

---

## Verfahren

- 1 Klicken Sie in vSphere Client mit der rechten Maustaste auf die übergeordnete virtuelle Maschine und klicken Sie dann auf **Konsole öffnen**.

- 2 Wählen Sie **Start > Einstellungen > Systemsteuerung > System**.
- 3 Klicken Sie auf die Registerkarte **Erweitert**.
- 4 Klicken Sie im Fensterbereich „Leistung“ auf **Einstellungen**.
- 5 Klicken Sie auf die Registerkarte **Erweitert**.
- 6 Klicken Sie im Fensterbereich „Virtueller Arbeitsspeicher“ auf **Ändern**.  
Die Seite „Virtueller Arbeitsspeicher“ wird angezeigt.
- 7 Legen Sie für die Auslagerungsdateigröße einen höheren Wert fest als für den Arbeitsspeicher, der der virtuellen Maschine zugewiesen ist.

---

**Wichtig** Wenn die Einstellung **Maximale Größe (MB)** kleiner ist als die Arbeitsspeichergröße der virtuellen Maschine, geben Sie einen höheren Wert ein und speichern Sie den neuen Wert.

---

- 8 Notieren Sie sich die Einstellung **Maximale Größe (MB)**, die im Fensterbereich „Auslagerungsdateigröße für ausgewähltes Laufwerk“ konfiguriert ist.

#### Nächste Schritte

Wenn Sie einen Linked-Clone-Pool über diese übergeordnete virtuelle Maschine konfigurieren, konfigurieren Sie eine Festplatte für löschbare Dateien, die größer ist als die Auslagerungsdateigröße.

## Erhöhen des Zeitüberschreitungslimits für QuickPrep-Anpassungsskripts

View Composer beendet ein nach der Synchronisierung ausgeführtes QuickPrep-Skript oder ein Abschaltskript, wenn dessen Ausführung länger als 20 Sekunden dauert. Sie können das Zeitüberschreitungslimit für diese Skripts erhöhen, indem Sie den Wert ExecScriptTimeout in der Windows-Registrierung auf der übergeordneten virtuellen Maschine ändern.

Das höhere Zeitüberschreitungslimit wird auf verknüpfte Klone übertragen, die aus der übergeordneten virtuellen Maschine erstellt werden. QuickPrep-Anpassungsskripte können auf den verknüpften Klonen für die von Ihnen angegebene Zeit ausgeführt werden.

Alternativ dazu können Sie mit Ihrem Anpassungsskript ein weiteres Skript oder einen Prozess starten, durch das bzw. den die Aufgabe mit langer Laufzeit durchgeführt wird.

---

**Hinweis** Die meisten QuickPrep-Anpassungsskripts werden innerhalb des Limits von 20 Sekunden ausgeführt. Testen Sie Ihre Skripts, bevor Sie das Limit erhöhen.

---

#### Voraussetzungen

- Installieren Sie View Agent mit der Option **View Composer Agent** auf der übergeordneten virtuellen Maschine.
- Stellen Sie sicher, dass die übergeordnete virtuelle Maschine für die Erstellung eines Linked-Clone-Pools vorbereitet ist. Siehe [Vorbereiten einer übergeordneten virtuellen Maschine](#).

## Verfahren

- 1 Starten Sie auf der übergeordneten virtuellen Maschine den Windows-Registrierungs-Editor.
  - a Wählen Sie **Start > Eingabeaufforderung**.
  - b Geben Sie an der Eingabeaufforderung den Befehl **regedit** ein.
- 2 Suchen Sie in der Windows-Registrierung den Registrierungsschlüssel vmware-viewcomposer-ga.  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\vmware-viewcomposer-ga
- 3 Klicken Sie auf **Bearbeiten** und bearbeiten Sie den Wert in der Registrierung.

```
Value Name: ExecScriptTimeout  
Value Type: REG_DWORD  
Value unit: milliseconds
```

Der Standardwert lautet 20000 Millisekunden.

Der Zeitüberschreitungswert wird erhöht. Sie müssen Windows nicht neu starten, damit dieser Wert wirksam wird.

## Nächste Schritte

Erstellen Sie einen Snapshot der übergeordneten virtuellen Maschine sowie einen Linked-Clone-Pool.

# Erstellen von Vorlagen virtueller Maschinen

Sie müssen eine Vorlage virtueller Maschinen erstellen, bevor Sie einen automatisierten Pool mit vollständigen virtuellen Maschinen erstellen können.

Eine Vorlage einer virtuellen Maschine ist eine Masterkopie einer virtuellen Maschine, die zum Erstellen und Bereitstellen neuer virtueller Maschinen verwendet werden kann. Eine Vorlage umfasst im Allgemeinen ein installiertes Gastbetriebssystem und einen Satz an Anwendungen.

Sie erstellen Vorlagen virtueller Maschinen in vSphere Client. Sie können eine Vorlage einer virtuellen Maschine von einer zuvor konfigurierten virtuellen Maschine erstellen oder eine zuvor konfigurierte virtuelle Maschine zu einer Vorlage einer virtuellen Maschine umwandeln.

Weitere Informationen zum Verwenden von vSphere Client, um Vorlagen virtueller Maschinen zu erstellen, finden Sie im Handbuch *vSphere Basic System Administration*. Weitere Informationen zum Erstellen von automatisierten Pools finden Sie unter [Automatisierte Pools mit vollständigen virtuellen Maschinen](#).

---

**Hinweis** Anhand einer Vorlage für eine virtuelle Maschine erstellen Sie keinen Linked-Clone-Pool.

---

# Erstellen von Anpassungsspezifikationen

Anpassungsspezifikationen sind optional, können jedoch die Bereitstellung von automatisierten Desktop-Pools erheblich beschleunigen. Möglich wird dies durch die Vorgabe von Konfigurationsinformationen für allgemeine Eigenschaften, beispielsweise Lizenzierung, Domänenanbindung und DHCP-Einstellungen.

Mit Anpassungsspezifikationen können Sie Remote-Desktops anpassen, wenn sie in View Administrator erstellt werden. Sie können mit dem Assistenten für Anpassungsspezifikationen in vSphere Client neue Anpassungsspezifikationen erstellen. Sie können den Assistenten für Anpassungsspezifikationen auch verwenden, um die vorhandene benutzerdefinierte Datei `sysprep.ini` zu importieren.

Informationen zur Verwendung des Assistenten für Anpassungsspezifikationen finden Sie im Dokument *Verwaltung virtueller vSphere-Maschinen*.

Stellen Sie die Richtigkeit der Anpassungsspezifikationen sicher, bevor Sie sie in View Administrator verwenden. In vSphere Client führen Sie die Bereitstellung und Anpassung einer virtuellen Maschine anhand Ihrer Vorlage mithilfe von Anpassungsspezifikationen durch. Führen Sie vollständige Tests der virtuellen Maschine durch (einschließlich DHCP und Authentifizierung), bevor Sie Remote-Desktops erstellen.

---

**Hinweis** Um Anpassungsspezifikationen auf Desktop-Pools anzuwenden, die Windows XP verwenden, müssen Sie die Microsoft Sysprep-Tools auf Ihrer vCenter Server-Maschine installieren.

Sie müssen keine Sysprep-Tools in vCenter Server für Desktop-Pools installieren, die Windows 8, Windows 7 oder Vista verwenden. Sysprep-Tools sind in diesen Betriebssystemen integriert.

---

Wenn Sie eine Sysprep-Anpassungsspezifikation verwenden, um einen Windows 8- oder Windows 7-Desktop zu einer Domäne hinzuzufügen, müssen Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der Active Directory-Domäne verwenden. Es ist nicht möglich, den NetBIOS-Namen der Active Directory-Domäne zu verwenden.

# Erstellen automatisierter Desktop-Pools mit vollständigen virtuellen Maschinen

# 4

Erstellen Sie mithilfe eines automatisierten Desktop-Pools, der vollständige virtuelle Maschinen enthält, eine Vorlage virtueller Maschinen. View verwendet die Vorlage, um virtuelle Maschinen für jeden Desktop zu erstellen. Optional können Sie Anpassungsspezifikationen erstellen, um automatisierte Pool-Bereitstellungen zu beschleunigen.

Dieses Kapitel enthält die folgenden Themen:

- [Automatisierte Pools mit vollständigen virtuellen Maschinen](#)
- [Arbeitsblatt zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen](#)
- [Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen](#)
- [Desktop-Einstellungen für automatisierte Pools mit vollständigen virtuellen Maschinen](#)

## Automatisierte Pools mit vollständigen virtuellen Maschinen

Zur Erstellung eines automatisierten Desktop-Pools stellt View Computer dynamisch basierend auf Einstellungen bereit, die Sie auf den Pool anwenden. View verwendet eine Vorlage virtueller Maschinen als Basis des Pools. View erstellt über die Vorlage eine neue virtuelle Maschine in vCenter Server für jeden Desktop.

## Arbeitsblatt zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen

Bei der Erstellung eines automatisierten Desktop-Pools fordert der View Administrator-Assistent zum Hinzufügen von Desktop-Pools Sie zum Konfigurieren bestimmter Optionen auf. Mithilfe dieses Arbeitsblatts können Sie Ihre Konfigurationsoptionen vorbereiten, bevor Sie den Pool erstellen.

Sie können dieses Arbeitsblatt drucken und die Werte notieren, die Sie bei Ausführung des Assistenten **Desktop-Pool hinzufügen** angeben möchten.

Informationen zum Erstellen eines Linked-Clone-Pools finden Sie unter [Pools von Linked-Clone-Desktops](#).



**Tabelle 4-1. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen**

| Option                            | Beschreibung  | Wert |
|-----------------------------------|---|------|
| Benutzerzuweisung                 | <p>Wählen Sie die Art der Benutzerzuweisung:</p> <ul style="list-style-type: none"> <li>■ In einem Pool mit dedizierter Zuweisung wird jeder Benutzer einem Computer zugewiesen. Benutzer erhalten bei jeder Anmeldung beim Pool dieselbe Maschine.</li> <li>■ In einem Pool mit dynamischer Zuweisung erhalten die Benutzer bei jeder Anmeldung einen anderen Computer.</li> </ul> <p>Weitere Informationen finden Sie unter <a href="#">Benutzerzuweisung in Desktop-Pools</a>.</p> |      |
| Automatische Zuweisung aktivieren | <p>In einem Pool mit dedizierter Zuweisung wird ein Computer einem Benutzer zugewiesen, wenn der Benutzer sich erstmals am Pool anmeldet. Sie können den Benutzern ihre Computer auch explizit zuweisen.</p> <p>Wenn Sie die automatische Zuweisung nicht aktivieren, müssen Sie jedem Benutzer explizit einen Computer zuweisen.</p> <p>Sie können Maschinen manuell zuweisen, selbst wenn die automatische Zuweisung aktiviert ist.</p>   |      |
| vCenter Server                    | Wählen Sie die vCenter Server-Instanz aus, welche die virtuellen Maschinen im Pool verwaltet.   |      |
| Desktop-Pool-ID                   | <p>Der eindeutige Name, der den Pool in View Administrator identifiziert.</p> <p>Wenn mehrere vCenter Server-Instanzen in Ihrer Umgebung ausgeführt werden, stellen Sie sicher, dass keine weitere vCenter Server-Instanz dieselbe Pool-ID verwendet.</p> <p>A View Connection Server configuration can be a standalone View Connection Server instance or a pod of replicated instances that share a common View LDAP configuration.</p>   |      |
| Anzeigenname                      | Der Pool-Name, der Benutzern bei ihrer Anmeldung über ein Client-Gerät angezeigt wird. Wenn Sie keinen Anzeigenamen angeben, wird den Benutzern die Pool-ID angezeigt.  |      |

| Option                              | Beschreibung   | Wert |
|-------------------------------------|--|------|
| Zugriffsgruppe                      | <p>Wählen Sie eine Zugriffsgruppe aus, in der der Pool abgelegt wird, oder belassen Sie den Pool in der standardmäßigen Stammzugriffsgruppe.</p> <p>Wenn Sie eine Zugriffsgruppe verwenden, können Sie die Verwaltung des Pools an einen Administrator mit einer bestimmten Rolle delegieren. Weitere Informationen finden Sie im Kapitel zur rollenbasierten Verwaltungsdelegation im Dokument <i>Verwaltung von View</i>.</p> <hr/> <p><b>Hinweis</b> Zugriffsgruppen unterscheiden sich von vCenter Server-Ordern, in denen virtuelle Desktop-Maschinen gespeichert werden. Sie wählen einen vCenter Server-Ordner zusammen mit anderen vCenter Server-Einstellungen an einer späteren Stelle im Assistenten aus.</p> |      |
| Computer nach Abmeldung löschen     | <p>Wenn Sie die dynamische Benutzerzuweisung auswählen, legen Sie fest, ob Maschinen nach der Benutzerabmeldung gelöscht werden.</p> <hr/> <p><b>Hinweis</b> Diese Option wird auf der Seite mit den Desktop-Pool-Einstellungen festgelegt.</p>  |      |
| Desktop-Pool-Einstellungen          | <p>Einstellungen, die den Desktop-Status, den Betriebsstatus bei Nichtnutzung einer virtuellen Maschine, das Anzeigeprotokoll, die Adobe Flash-Qualität usw. festlegen.</p> <p>Eine Beschreibung finden Sie unter <a href="#">Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen</a>.</p> <p>Eine Liste der Einstellungen für automatisierte Pools finden Sie unter <a href="#">Desktop-Einstellungen für automatisierte Pools mit vollständigen virtuellen Maschinen</a>.</p> <p>Weitere Informationen über Betriebsrichtlinien und automatisierte Pools finden Sie unter <a href="#">Einstellen von Betriebsrichtlinien für Desktop-Pools</a>.</p>   |      |
| Bereitstellung bei Fehler abbrechen | <p>Sie können View lenken, um die Bereitstellung anzuhalten oder mit der Bereitstellung virtueller Maschinen in einem Desktop-Pool fortzufahren, nachdem ein Fehler während der Bereitstellung einer virtuellen Maschine aufgetreten ist. Wenn Sie die ausgewählte Einstellung belassen, können Sie eine Wiederholung des Bereitstellungsfehlers auf mehreren virtuellen Maschinen verhindern.</p>   |      |
| Benennung virtueller Maschinen      | <p>Geben Sie an, ob die Computer bereitgestellt werden sollen, indem eine Liste der Computernamen manuell festgelegt bzw. ein Benennungsmuster und die Gesamtanzahl der Computer angegeben wird.</p> <p>Weitere Informationen finden Sie unter <a href="#">Manuelles Benennen von Computern oder Bereitstellen eines Benennungsmusters</a>.</p>  |      |

| Option  | Beschreibung   | Wert |
|---|--|------|
| Namen manuell angeben                         | Wenn Sie Namen manuell angeben, bereiten Sie eine Liste vor, in der die Computernamen aufgeführt sind. Optional können Sie auch die verknüpften Benutzernamen angeben.   |      |
| Benennungsmuster                              | <p>Wenn Sie diese Benennungsmethode verwenden, stellen Sie das Muster bereit.</p> <p>Das angegebene Muster wird als Präfix in allen Computernamen festgelegt, gefolgt von einer eindeutigen Zahl zur Identifizierung der einzelnen Computer an.</p> <p>Weitere Informationen finden Sie unter <a href="#">Verwenden eines Benennungsmusters für automatisierte Desktop-Pools</a>.</p>  |      |
| Maximale Anzahl an Maschinen                  | <p>Wenn Sie ein Benennungsmuster verwenden, geben Sie die Gesamtzahl an Computern im Pool an.</p> <p>Außerdem können Sie bei der ersten Erstellung des Pools eine Mindestzahl an bereitzustellenden Computern angeben.</p>   |      |
| Anzahl der (eingeschalteten) Reservemaschinen | <p>Wenn Sie Namen manuell angeben oder ein Benennungsmuster verwenden, geben Sie eine Anzahl an Computern an, um sie für neue Benutzer verfügbar und eingeschaltet zu lassen. Weitere Informationen finden Sie unter <a href="#">Manuelles Benennen von Computern oder Bereitstellen eines Benennungsmusters</a>.</p> <p>Wenn Sie Namen manuell festlegen, heißt diese Option <b>Anzahl an ständig eingeschalteten nicht zugewiesenen Computern</b>.</p> |      |
| Minimale Anzahl an Maschinen                  | <p>Wenn Sie ein Benennungsmuster verwenden und Maschinen nach Bedarf bereitstellen, geben Sie eine Mindestanzahl an Maschinen im Pool an.</p> <p>Die minimale Anzahl an Maschinen wird erstellt, wenn Sie den Pool erstellen.</p> <p>Wenn Sie Maschinen nach Bedarf bereitstellen, werden zusätzliche Maschinen erstellt, wenn sich Benutzer zum ersten Mal mit dem Pool verbinden oder wenn Sie Benutzern Maschinen zuweisen.</p>                       |      |
| vSphere Virtual SAN verwenden                 | Geben Sie an, ob Virtual SAN verwendet werden soll, sofern verfügbar. Bei Virtual SAN handelt es sich um eine softwaredefinierte Speicherebene, die die lokalen physischen Speicherfestplatten virtualisiert, die auf einem Cluster der ESXi-Hosts verfügbar sind. Weitere Informationen finden Sie unter <a href="#">Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung</a> .                                       |      |
| Vorlage                                       | Wählen Sie die Vorlage für virtuelle Maschinen aus, die zum Erstellen des Pools verwendet werden soll.   |      |

| Option  | Beschreibung  | Wert |
|---|---|------|
| vCenter Server folder (vCenter Server-Ordner) | Wählen Sie den Ordner in vCenter Server aus, in dem der Desktop-Pool gespeichert wird.  |      |
| Host or cluster (Host oder Cluster)           | Wählen Sie den ESXi-Host oder -Cluster aus, in dem die virtuellen Maschinen ausgeführt werden.<br>In vSphere 5.1 oder höher können Sie einen Cluster mit bis zu 32 ESXi-Hosts auswählen.  |      |
| Resource pool (Ressourcen-Pool)               | Wählen Sie den vCenter Server-Ressourcen-Pool aus, in dem der Desktop-Pool gespeichert ist.   |      |
| Datenspeicher                                 | Wählen Sie einen oder mehrere Datenspeicher zur Speicherung des Desktop-Pools aus.<br>Für Cluster können Sie freigegebene oder lokal gespeicherte Datenspeicher verwenden.<br><br><b>Hinweis</b> Wenn Sie Virtual SAN verwenden, wählen Sie nur einen Datenspeicher aus.  |      |
| View-Speicherbeschleunigung verwenden         | Bestimmt, ob ESXi-Hosts Festplattendaten von virtuellen Maschinen im Cache speichern. Die View-Speicherbeschleunigung kann die Leistung verbessern und die Notwendigkeit von extra Speicher-E/A-Bandbreite verringern, um Startüberlastungen und Antiviren-E/A-Überlastungen zu verwalten.<br><br>Diese Funktion wird unter vSphere 5.0 und höher unterstützt.<br>Diese Funktion ist standardmäßig aktiviert.<br>Weitere Informationen finden Sie unter <a href="#">Konfigurieren der View-Speicherbeschleunigung für Desktop-Pools</a> . |      |
| Guest customization (Gastanpassung)           | Wählen Sie eine Anpassungsspezifikation (SYSPREP) aus der Liste aus, um die Lizenzierung, die Domänenbindung, DHCP-Einstellungen und andere Eigenschaften auf den Maschinen zu konfigurieren.<br><br>Alternativ können Sie die Maschinen manuell anpassen, nachdem sie erstellt wurden.   |      |

## Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen

Sie können einen automatisierten Desktop-Pool basierend auf einer von Ihnen ausgewählten Vorlage für virtuelle Maschinen erstellen. View stellt die Desktops dynamisch bereit und erstellt so für jeden Desktop in vCenter Server eine neue virtuelle Maschine.

Informationen zum Erstellen eines Linked-Clone-Pools finden Sie unter [Pools von Linked-Clone-Desktops](#).

## Voraussetzungen

- Bereiten Sie eine Vorlage zu einer virtuellen Maschine vor, die View zur Erstellung der Maschinen verwendet. View Agent muss in der Vorlage installiert sein. Siehe [Kapitel 3 Erstellen und Vorbereiten virtueller Maschinen](#).
- Wenn Sie eine Anpassungsspezifikation verwenden möchten, müssen Sie die Richtigkeit der Spezifikationen sicherstellen. In vSphere Client führen Sie die Bereitstellung und Anpassung einer virtuellen Maschine anhand Ihrer Vorlage mithilfe von Anpassungsspezifikationen durch. Führen Sie vollständige Tests der virtuellen Maschine durch, einschließlich DHCP und Authentifizierung.
- Stellen Sie sicher, dass Sie auf dem virtuellen ESXi-Switch, der für die virtuellen als Remote-Desktops eingesetzten Maschinen verwendet wird, über eine ausreichende Anzahl an Ports verfügen. Der Standardwert reicht möglicherweise nicht aus, wenn Sie große Desktop-Pools erstellen. Die Anzahl der Ports für den virtuellen Switch auf dem ESXi-Host muss der Anzahl der virtuellen Maschinen multipliziert mit der Anzahl der virtuellen Netzwerkkarten pro virtueller Maschine entsprechen (oder diese übersteigen).
- Sammeln Sie die Konfigurationsinformationen, die Sie zum Erstellen des Pools bereitstellen müssen. Siehe [Arbeitsblatt zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen](#).
- Entscheiden Sie, wie die Betriebseinstellungen, das Anzeigeprotokoll, die Adobe Flash-Qualität und andere Einstellungen konfiguriert werden sollen. Siehe [Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen](#).
- 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.

## Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie **Automatisierter Desktop-Pool** aus.
- 4 Wählen Sie auf der Seite **vCenter Server** die Option **Vollständige virtuelle Maschinen**.
- 5 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

Verwenden Sie die Konfigurationsinformationen, die Sie im Arbeitsblatt zusammengetragen haben. Sie können jederzeit auf eine beliebige Assistentenseite zurückwechseln, die Sie bereits ausgefüllt haben, indem Sie im Navigationsbereich auf den Seitennamen klicken.

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

## Nächste Schritte

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe [Hinzufügen von Berechtigungen zu einem Desktop- oder Anwendungspool](#).

# Desktop-Einstellungen für automatisierte Pools mit vollständigen virtuellen Maschinen

Bei der Konfiguration automatisierter Pools mit vollständigen virtuellen Maschinen müssen Sie Desktop-Pool-Einstellungen angeben. Für Pools mit dedizierten Benutzerzuweisungen und dynamischen Benutzerzuweisungen gelten unterschiedliche Einstellungen.

**Tabelle 4-2. Einstellungen für automatisierte Pools mit vollständigen virtuellen Maschinen** werden die Einstellungen aufgeführt, die für automatisierte Pools mit dedizierten Zuweisungen und dynamischen Zuweisungen gelten.

Beschreibungen der einzelnen Desktop-Einstellungen finden Sie unter [Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen](#).

**Tabelle 4-2. Einstellungen für automatisierte Pools mit vollständigen virtuellen Maschinen**

| Einstellung   | Automatisierter Pool, dedizierte Zuweisung | Automatisierter Pool, dynamische Zuweisung |
|---|--|--|
| Status  | Ja   | Ja   |
| Einschränkungen für Verbindungsserver   | Ja   | Ja   |
| Betriebsrichtlinie für Remote-Computer  | Ja   | Ja   |
| Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden) | Ja   | Ja   |
| Benutzern das Zurücksetzen ihrer Computer gestatten                               | Ja   | Ja   |
| Mehrere Sitzungen pro Benutzer zulassen   |  | Ja   |
| Computer nach Abmeldung löschen   |  | Ja   |
| Standardanzeigeprotokoll  | Ja   | Ja   |
| Benutzern die Wahl des Protokolls erlauben  | Ja   | Ja   |
| 3D-Renderer   | Ja   | Ja   |
| Max number of monitors (Maximale Anzahl an Monitoren)                             | Ja   | Ja   |
| Max resolution of any one monitor (Max. Auflösung eines Monitors)                 | Ja   | Ja   |
| Adobe Flash quality (Adobe Flash-Qualität)  | Ja   | Ja   |
| Adobe Flash throttling (Adobe Flash-Drosselung)                                   | Ja   | Ja   |

| <b>Einstellung</b>                         | <b>Automatisierter Pool, dedizierte Zuweisung</b> | <b>Automatisierter Pool, dynamische Zuweisung</b> |
|--|---|---|
| Globale Mirage-Einstellungen überschreiben | Ja  | Ja  |
| Mirage-Serverkonfiguration                 | Ja  | Ja  |

# Erstellen von Linked-Clone-Desktop-Pools

# 5

Mit einem Desktop-Pool mit verknüpften Klonen erstellt View einen Desktop-Pool basierend auf einer übergeordneten virtuellen Maschine, die Sie auswählen. Der View Composer-Dienst erstellt dynamisch für jeden Desktop eine neue virtuelle Linked-Clone-Maschine in vCenter Server.

Dieses Kapitel enthält die folgenden Themen:

- [Pools von Linked-Clone-Desktops](#)
- [Arbeitsblatt zum Erstellen eines Linked-Clone-Desktop-Pools](#)
- [Erstellen eines Linked-Clone-Desktop-Pools](#)
- [Desktop-Pool-Einstellungen für Linked-Clone-Desktop-Pools](#)
- [View Composer-Unterstützung für Linked-Clone-SIDs und Drittanbieteranwendungen](#)
- [Linked-Clone-Maschinen während View Composer-Vorgängen bereitgestellt und einsatzbereit halten](#)
- [Verwenden vorhandener Active Directory-Computerkonten für verknüpfte Klone](#)

## Pools von Linked-Clone-Desktops

Zum Erstellen eines Pools von Linked-Clone-Desktops generiert View Composer virtuelle Linked-Clone-Maschinen aus einem Snapshot einer übergeordneten virtuellen Maschine. View stellt die Linked-Clone-Desktops dynamisch basierend auf den Einstellungen bereit, die Sie auf den Pool anwenden.

Da Linked-Clone-Desktops ein Basis-Image der Systemfestplatte gemeinsam nutzen, benötigen sie weniger Speicher als vollständige virtuelle Maschinen.

## Arbeitsblatt zum Erstellen eines Linked-Clone-Desktop-Pools

Bei der Erstellung eines Linked-Clone-Desktop-Pools fordert der View Administrator-Assistent **Desktop-Pool hinzufügen** Sie zum Konfigurieren bestimmter Optionen auf. Mithilfe dieses Arbeitsblatts können Sie Ihre Konfigurationsoptionen vorbereiten, bevor Sie den Pool erstellen.

Sie können dieses Arbeitsblatt drucken und die Werte notieren, die Sie bei Ausführung des Assistenten **Desktop-Pool hinzufügen** angeben möchten.



Bevor Sie einen Linked-Clone-Pool erstellen, müssen Sie mithilfe von vCenter Server einen Snapshot der übergeordneten virtuellen Maschine erstellen, die Sie für den Pool vorbereiten. Vor dem Erstellen des Snapshots müssen Sie die übergeordnete virtuelle Maschine herunterfahren. View Composer verwendet den Snapshot als Basis-Image, von dem die Klone erstellt werden.

**Hinweis** Sie können aus einer Vorlage für virtuelle Maschinen keinen Linked-Clone-Pool erstellen.

**Tabelle 5-1. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines Linked-Clone-Desktop-Pools**

| Option                            | Beschreibung  | Wert |
|-----------------------------------|---|------|
| Benutzerzuweisung                 | <p>Wählen Sie die Art der Benutzerzuweisung:</p> <ul style="list-style-type: none"> <li>■ In einem Pool mit dedizierter Zuweisung wird jeder Benutzer einem Computer zugewiesen. Benutzer erhalten bei jeder Anmeldung denselben Computer.</li> <li>■ In einem Pool mit dynamischer Zuweisung erhalten die Benutzer bei jeder Anmeldung einen anderen Computer.</li> </ul> <p>Weitere Informationen finden Sie unter <a href="#">Benutzerzuweisung in Desktop-Pools</a>.</p>                |      |
| Automatische Zuweisung aktivieren | <p>In einem Pool mit dedizierter Zuweisung wird ein Computer einem Benutzer zugewiesen, wenn der Benutzer sich erstmals beim Pool anmeldet. Sie können den Benutzern ihre Computer auch explizit zuweisen.</p> <p>Wenn Sie die automatische Zuweisung nicht aktivieren, müssen Sie jedem Benutzer explizit einen Computer zuweisen.</p>   |      |
| vCenter Server                    | Wählen Sie die vCenter Server-Instanz aus, welche die virtuellen Maschinen im Pool verwaltet.   |      |
| Desktop-Pool-ID                   | <p>Der eindeutige Name, der den Pool in View Administrator identifiziert.</p> <p>Wenn mehrere View-Verbindungsserver-Konfigurationen in Ihrer Umgebung ausgeführt werden, stellen Sie sicher, dass keine weitere View-Verbindungsserver-Konfiguration dieselbe Pool-ID verwendet.</p> <p>Eine View-Verbindungsserver-Konfiguration kann eine eigenständige View-Verbindungsserver-Instanz oder ein Pod replizierter Instanzen sein, die eine gemeinsame View LDAP-Konfiguration nutzen.</p> |      |
| Anzeigename                       | Der Pool-Name, der Benutzern bei ihrer Anmeldung über ein Client-Gerät angezeigt wird. Wenn Sie keinen Anzeigenamen angeben, wird den Benutzern die Pool-ID angezeigt.  |      |

| Option   | Beschreibung  | Wert |
|--|---|------|
| Zugriffsgruppe   | <p>Wählen Sie eine Zugriffsgruppe aus, in der der Pool abgelegt wird, oder belassen Sie den Pool in der standardmäßigen Stammzugriffsgruppe.</p> <p>Wenn Sie eine Zugriffsgruppe verwenden, können Sie die Verwaltung des Pools an einen Administrator mit einer bestimmten Rolle delegieren. Weitere Informationen finden Sie im Kapitel zur rollenbasierten Verwaltungsdelegation im Dokument <i>Verwaltung von View</i>.</p> <hr/> <p><b>Hinweis</b> Zugriffsgruppen unterscheiden sich von vCenter Server-Ordern, die virtuelle Maschinen speichern, die als Desktops verwendet werden. Sie wählen einen vCenter Server-Ordner zusammen mit anderen vCenter Server-Einstellungen an einer späteren Stelle im Assistenten aus.</p> |      |
| Computer bei Abmeldung löschen oder aktualisieren          | <p>Wenn Sie die dynamische Benutzerzuweisung auswählen, legen Sie fest, ob Computer nach der Benutzerabmeldung aktualisiert, gelöscht oder unverändert beibehalten werden.</p> <hr/> <p><b>Hinweis</b> Diese Option wird auf der Seite mit den Desktop-Pool-Einstellungen festgelegt.</p>   |      |
| Desktop-Pool-Einstellungen                                 | <p>Einstellungen, die den Computerstatus, den Betriebsstatus bei Nichtnutzung einer virtuellen Maschine, das Anzeigeprotokoll, die Adobe Flash-Qualität usw. festlegen.</p> <p>Eine Beschreibung finden Sie unter <a href="#">Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen</a>.</p> <p>Eine Liste der Einstellungen für Linked-Clone-Pools finden Sie unter <a href="#">Desktop-Pool-Einstellungen für Linked-Clone-Desktop-Pools</a>.</p> <p>Weitere Informationen über Betriebsrichtlinien und automatisierte Pools finden Sie unter <a href="#">Einstellen von Betriebsrichtlinien für Desktop-Pools</a>.</p>  |      |
| Bereitstellung bei Fehler abbrechen                        | <p>Sie können View lenken, um die Bereitstellung anzuhalten oder mit der Bereitstellung virtueller Maschinen in einem Desktop-Pool fortzufahren, nachdem ein Fehler während der Bereitstellung einer virtuellen Maschine aufgetreten ist. Wenn Sie die ausgewählte Einstellung belassen, können Sie eine Wiederholung des Bereitstellungsfehlers auf mehreren virtuellen Maschinen verhindern.</p>  |      |
| Virtual machine naming<br>(Benennung virtueller Maschinen) | <p>Geben Sie an, ob die Computer bereitgestellt werden sollen, indem eine Liste der Computernamen manuell festgelegt bzw. ein Benennungsmuster und die Gesamtanzahl der Computer angegeben wird.</p> <p>Weitere Informationen finden Sie unter <a href="#">Manuelles Benennen von Computern oder Bereitstellen eines Benennungsmusters</a>.</p>   |      |

| Option   | Beschreibung  | Wert |
|--|---|------|
| Namen manuell angeben  | Wenn Sie Namen manuell angeben, bereiten Sie eine Liste vor, in der die Computernamen aufgeführt sind. Optional können Sie auch die verknüpften Benutzernamen angeben.  |      |
| Naming pattern<br>(Benennungsmuster)   | Wenn Sie diese Benennungsmethode verwenden, stellen Sie das Muster bereit.<br><br>Das angegebene Muster wird als Präfix in allen Computernamen festgelegt, gefolgt von einer eindeutigen Zahl zur Identifizierung der einzelnen Computer an.<br><br>Weitere Informationen finden Sie unter <a href="#">Verwenden eines Benennungsmusters für automatisierte Desktop-Pools</a> .   |      |
| Maximale Anzahl an Computern   | Wenn Sie ein Benennungsmuster verwenden, geben Sie die Gesamtzahl an Computern im Pool an.<br><br>Außerdem können Sie bei der ersten Erstellung des Pools eine Mindestzahl an bereitzustellenden Computern angeben.   |      |
| Anzahl der (eingeschalteten) Reservemaschinen  | Wenn Sie Namen manuell angeben oder ein Benennungsmuster verwenden, geben Sie eine Anzahl an Computern an, um sie für neue Benutzer verfügbar und eingeschaltet zu lassen. Weitere Informationen finden Sie unter <a href="#">Manuelles Benennen von Computern oder Bereitstellen eines Benennungsmusters</a> .<br><br>Wenn Sie Namen manuell festlegen, heißt diese Option <b>Anzahl an ständig eingeschalteten nicht zugewiesenen Computern</b> .   |      |
| Minimale Anzahl von bereiten (bereitgestellten) Computern während der View Composer-Wartungsvorgänge | Wenn Sie die Namen manuell angeben oder ein Benennungsmuster verwenden, geben Sie die Mindestanzahl von Computern an, die bereit und bereitgestellt sind, während die View Composer-Vorgänge stattfinden.<br><br>Mit dieser Einstellung können Sie Computer bereitgestellt und bereit halten, um Verbindungsanforderungen von Benutzern anzunehmen, während View Composer die Computer im Pool aktualisiert, neu zusammenstellt oder neu verteilt.<br><br>Dieser Wert muss kleiner als der Wert für <b>Mindestanzahl an Computern</b> sein, den Sie angeben, wenn Sie Computer nach Bedarf bereitstellen.<br><br>Siehe <a href="#">Linked-Clone-Maschinen während View Composer-Vorgängen bereitgestellt und einsatzbereit halten</a> . |      |

| Option   | Beschreibung   | Wert |
|--|--|------|
| Computer bei Bedarf bereitstellen<br>oder<br>Alle Computer im Voraus bereitstellen | <p>Wenn Sie ein Benennungsmuster verwenden, geben Sie an, ob alle Computer bereitgestellt werden sollen, wenn der Pool erstellt wird, oder ob die Computer nach Bedarf bereitgestellt werden.</p> <ul style="list-style-type: none"> <li>■ <b>Alle Computer im Voraus bereitstellen.</b> Wenn der Pool erstellt wird, stellt das System die Anzahl an Computern bereit, die Sie unter <b>Maximale Anzahl an Computern</b> angeben.</li> <li>■ <b>Computer bei Bedarf bereitstellen.</b> Wenn der Pool erstellt wird, erstellt das System die Anzahl an Computern bereit, die Sie unter <b>Mindestanzahl an Computern</b> angeben. Es werden zusätzliche Computer erstellt, wenn sich Benutzer zum ersten Mal mit dem Pool verbinden oder wenn Sie Benutzern Computer zuweisen.</li> </ul>  |      |
| Mindestanzahl an Computern   | <p>Wenn Sie ein Benennungsmuster verwenden und Desktops nach Bedarf bereitstellen, geben Sie eine Mindestanzahl an Computern im Pool an.</p> <p>Das System erstellt die Mindestanzahl an Computern bei der Erstellung des Pools. Die Anzahl bleibt auch dann beibehalten, wenn andere Einstellungen wie <b>Computer bei Abmeldung löschen oder aktualisieren</b> zum Löschen von Computern führen.</p>   |      |
| Windows-Profil auf persistente Festplatten umleiten                                | <p>Wenn Sie dedizierte Benutzerzuweisungen auswählen, legen Sie fest, ob Windows-Benutzerprofildaten auf einer separaten persistenten View Composer-Festplatte oder auf derselben Festplatte wie die Betriebssystemdaten abgelegt werden.</p> <p>Separate persistente Festplatten ermöglichen Ihnen das Beibehalten von Benutzerdaten und -einstellungen. View Composer-Aktualisierungen, -Neuzusammenstellungen und Neuverteilungen wirken sich nicht auf persistente Festplatten aus. Sie können eine persistente Festplatte von einem verknüpften Klon trennen und den virtuellen Linked-Clone-Computer von der getrennten Festplatte neu erstellen. Wenn beispielsweise ein Computer oder Pool gelöscht wird, können Sie die persistente Festplatte trennen und den Desktop neu erstellen, wobei die ursprünglichen Benutzerdaten und Einstellungen erhalten bleiben.</p> <p>Wenn Sie das Windows-Profil auf der Betriebssystemfestplatte speichern, werden Benutzerdaten und -einstellungen während der Vorgänge zur Aktualisierung, Neuzusammenstellung oder Neuverteilung entfernt.</p> |      |

| Option  | Beschreibung  | Wert |
|---|---|------|
| Disk size and drive letter for persistent disk (Festplattengröße und Laufwerksbuchstabe für persistente Festplatte) | <p>Wenn Sie Profildaten auf einer separaten persistenten View Composer-Festplatte speichern, geben Sie die Festplattengröße in Megabyte und den Laufwerksbuchstaben an.</p> <hr/> <p><b>Hinweis</b> Wählen Sie keinen Laufwerksbuchstaben aus, der bereits auf der übergeordneten virtuellen Maschine vorhanden ist oder der einen Konflikt mit einem Laufwerksbuchstaben verursacht, der für ein im Netzwerk bereitgestelltes Laufwerk verwendet wird.</p>   |      |
| Umleitung löschrbarer Dateien   | <p>Wählen Sie aus, ob die Auslagerungsdateien und temporären Dateien des Gastbetriebssystems auf eine separate, nicht persistente Festplatte umgeleitet werden sollen. Geben Sie in diesem Fall die Festplattengröße in Megabyte an.</p> <p>Wenn mit dieser Konfiguration ein verknüpfter Klon ausgeschaltet wird, wird die Festplatte für löschrbare Dateien durch eine Kopie der ursprünglichen Festplatte ersetzt, die mit dem Linked-Clone-Pool erstellt wurde. Verknüpfte Klone können an Größe zunehmen, wenn Benutzer mit ihren Desktops interagieren. Das Umleiten löschrbarer Dateien kann Speicherplatz einsparen und so das Wachstum von verknüpften Klonen verlangsamen.</p>  |      |
| Disk size and drive letter for disposable disk (Festplattengröße und Laufwerksbuchstabe für löschrbare Festplatte)  | <p>Wenn Sie löschrbare Dateien auf eine nichtpersistente Festplatte umleiten, geben Sie die Festplattengröße in Megabyte und den Laufwerksbuchstaben an.</p> <p>Die Festplattengröße sollte die Auslagerungsdateigröße des Gastbetriebssystems übersteigen. Informationen zum Ermitteln der Auslagerungsdateigröße finden Sie unter <a href="#">Protokollieren der Auslagerungsdateigröße für die übergeordnete virtuelle Maschine</a>.</p> <p>Wenn Sie die Größe der Festplatte für löschrbare Dateien konfigurieren, sollten Sie berücksichtigen, dass die tatsächliche Größe einer formatierten Festplattenpartition leicht unter dem Wert liegt, den Sie in View Administrator angeben.</p> <p>Sie können einen Laufwerksbuchstaben für die Festplatte mit den löschrbaren Dateien auswählen. Der Standardwert <b>Auto</b> weist View an, den Laufwerksbuchstaben zuzuweisen.</p> <hr/> <p><b>Hinweis</b> Wählen Sie keinen Laufwerksbuchstaben aus, der bereits auf der übergeordneten virtuellen Maschine vorhanden ist oder der einen Konflikt mit einem Laufwerksbuchstaben verursacht, der für ein im Netzwerk bereitgestelltes Laufwerk verwendet wird.</p> |      |

| Option   | Beschreibung   | Wert |
|--|--|------|
| vSphere Virtual SAN verwenden  | Legen Sie fest, ob VMware Virtual SAN verwendet werden soll (falls verfügbar). Bei Virtual SAN handelt es sich um eine softwaredefinierte Speicherebene, die die lokalen physischen Speicherfestplatten virtualisiert, die auf einem Cluster der ESXi-Hosts verfügbar sind. Weitere Informationen finden Sie unter <a href="#">Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung</a> .  |      |
| Separate Datenspeicher für persistente und Betriebssystemfestplatten auswählen | (Nur verfügbar, wenn Sie Virtual SAN nicht verwenden) Wenn Sie Benutzerprofile auf separate persistente Festplatten umleiten, können Sie die persistenten und die Betriebssystemfestplatten in verschiedenen Datenspeichern speichern.   |      |
| Separate Datenspeicher für Replikat- und Betriebssystemfestplatten auswählen   | <p>(Nur verfügbar, wenn Sie Virtual SAN nicht verwenden) Sie können die Festplatte des Replikats- (Master-)VM in einem Hochleistungsdatenspeicher und die verknüpften Klone in separaten Datenspeichern ablegen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Speichern von View Composer-Replikaten und verknüpften Klonen in separaten Datenspeichern</a>.</p> <p>Wenn Sie Replikat- und Betriebssystemfestplatten in separaten Datenspeichern ablegen, können keine nativen NFS-Snapshots verwendet werden. Natives Klonen auf einem NAS-Gerät kann nur dann stattfinden, wenn die Replikat- und Betriebssystemfestplatten auf denselben Datenspeichern abgelegt sind.</p> |      |
| Übergeordnete VM   | <p>Wählen Sie die übergeordnete virtuelle Maschine für den Pool aus.</p> <hr/> <p><b>Hinweis</b> Sie können View Composer nicht zur Bereitstellung von Computern verwenden, auf denen die Windows Vista Ultimate Edition oder Windows XP Professional SP1 ausgeführt wird.</p>   |      |
| Snapshot (Standard-Image)  | <p>Wählen Sie den Snapshot der übergeordneten virtuellen Maschine aus, die als das Basis-Image für den Pool eingesetzt werden soll.</p> <p>Löschen Sie den Snapshot und die übergeordnete Maschine von vCenter Server nicht, es sei denn, das Standard-Image wird von keinen verknüpften Klonen im Pool genutzt und es werden keine verknüpften Klone mehr von diesem Standard-Image erstellt. Das System benötigt die übergeordnete virtuelle Maschine und den Snapshot, um gemäß den Poolrichtlinien neue verknüpfte Klone im Pool bereitzustellen. Die übergeordnete virtuelle Maschine und der Snapshot sind auch für View Composer-Wartungsvorgänge erforderlich.</p>                 |      |

| Option                     | Beschreibung   | Wert |
|----------------------------|--|------|
| Speicherort des VM-Ordners | Wählen Sie den Ordner in vCenter Server aus, in dem der Desktop-Pool gespeichert wird.   |      |
| Host oder Cluster          | <p>Wählen Sie den ESXi-Host oder -Cluster aus, in dem die virtuellen Desktop-Maschinen ausgeführt werden.</p> <p>In vSphere 5.1 oder höher können Sie einen Cluster mit bis zu 32 ESXi-Hosts auswählen, wenn die Replikate in Datenspeichern der Version VMFS5 oder höher bzw. in NFS-Datenspeichern gespeichert werden. Wenn Sie Replikate in einem Datenspeicher einer früheren VMFS-Version als VMFS5 speichern, kann ein Cluster über maximal acht Hosts verfügen.</p> <p>In vSphere 5.0 können Sie einen Cluster mit mehr als acht ESXi-Hosts auswählen, wenn die Replikate auf NFS-Datenspeichern gespeichert werden. Wenn Sie Repliken auf VMFS-Datenspeichern speichern, kann ein Cluster höchstens acht Hosts besitzen. Siehe <a href="#">Konfigurieren von Desktop-Pools auf Clustern mit mehr als acht Hosts</a>.</p> |      |
| Ressourcen-Pool            | Wählen Sie den vCenter Server-Ressourcen-Pool aus, in dem der Desktop-Pool gespeichert ist.  |      |

| Option                  | Beschreibung   | Wert |
|-------------------------|--|------|
| Datenspeicher           | <p>Wählen Sie einen oder mehrere Datenspeicher zur Speicherung des Desktop-Pools aus.</p> <p>Eine Tabelle auf der Seite <b>Datenspeicher verknüpfter Klone auswählen</b> im Assistenten „Desktop-Pools hinzufügen“ liefert allgemeine Richtlinien zur Ermittlung der Speicheranforderungen für den Pool. Anhand dieser Richtlinien können Sie ermitteln, welche Datenspeicher über ausreichend Kapazität zum Speichern der Linked-Clone-Festplatten verfügen. Weitere Informationen finden Sie unter <a href="#">Speichergößen für Linked-Clone-Desktop-Pools</a>.</p> <p>Sie können freigegebene oder lokale Datenspeicher für einen einzelnen ESXi-Host oder für ESXi-Cluster verwenden. Wenn Sie lokale Datenspeicher in einem ESXi-Cluster verwenden, müssen Sie die Beschränkungen durch die vSphere-Infrastruktur für Ihre Desktop-Bereitstellung berücksichtigen. Siehe <a href="#">Speichern von verknüpften Klonen auf lokalen Datenspeichern</a>.</p> <p>In vSphere 5.1 oder höher kann ein Cluster über mehr als acht ESXi-Hosts verfügen, wenn die Replikate in VMFS-Datenspeichern der Version VMFS5 oder höher bzw. in NFS-Datenspeichern gespeichert werden. In vSphere 5.0 kann ein Cluster nur dann über mehr als acht ESXi-Hosts verfügen, wenn die Replikate in NFS-Datenspeichern gespeichert werden. Siehe <a href="#">Konfigurieren von Desktop-Pools auf Clustern mit mehr als acht Hosts</a>.</p> <p>Weitere Informationen zu den Festplatten, die für verknüpfte Klone erstellt werden, finden Sie unter <a href="#">Datenfestplatten von verknüpften Klonen</a>.</p> <hr/> <p><b>Hinweis</b> Wenn Sie Virtual SAN verwenden, wählen Sie nur einen Datenspeicher aus.</p> |      |
| Speichermehrfachvergabe | <p>Legen Sie den Grad der Speichermehrfachvergabe fest, mit dem verknüpfte Klone in den einzelnen Datenspeichern erstellt werden.</p> <p>Mit steigendem Wert passen mehr verknüpfte Klone in den Datenspeicher, und es wird weniger Speicherplatz für das Anwachsen der einzelnen Klone reserviert. Ein hohes Maß an Speichermehrfachvergabe ermöglicht Ihnen die Erstellung verknüpfter Klone, deren logische Gesamtgröße die physische Speichergrenze des Datenspeichers übertrifft. Weitere Informationen finden Sie unter <a href="#">Festlegen des Werts für die Speichermehrfachvergabe für virtuelle Linked-Clone-Computer</a>.</p> <hr/> <p><b>Hinweis</b> Diese Einstellung bleibt wirkungslos, wenn Virtual SAN verwendet wird.</p>  |      |



| Option                                      | Beschreibung   | Wert |
|---|--|------|
| View-Speicherbeschleunigung verwenden       | <p>Legen Sie fest, ob die View-Speicherbeschleunigung verwendet werden soll, die es ESXi-Hosts erlaubt, gemeinsame Festplattendaten von virtuellen Maschinen zwischenspeichern. Die View-Speicherbeschleunigung kann die Leistung verbessern und die Notwendigkeit von extra Speicher-E/A-Bandbreite verringern, um Startüberlastungen und Antiviren-E/A-Überlastungen zu verwalten.</p> <p>Diese Funktion wird unter vSphere 5.0 und höher unterstützt.</p> <p>Diese Funktion ist standardmäßig aktiviert.</p> <p>Weitere Informationen finden Sie unter <a href="#">Konfigurieren der View-Speicherbeschleunigung für Desktop-Pools</a>.</p>   |      |
| Systemeigene NFS-Snapshots (VAAI) verwenden | <p>(Nur verfügbar, wenn Sie Virtual SAN nicht verwenden) Wenn Ihre Bereitstellung NAS-Geräte umfasst, die die vStorage APIs for Array Integration (VAAI) unterstützen, können Sie die Native Snapshot-Technologie zum Klonen virtueller Maschinen verwenden.</p> <p>Sie können diese Funktion nur dann verwenden, wenn Sie Datenspeicher auswählen, die sich auf NAS-Geräten befinden, die über VAAI systemeigene Klonvorgänge unterstützen.</p> <p>Sie können diese Funktion nicht verwenden, wenn Sie Replikate und Betriebssystemfestplatten in separaten Datenspeichern speichern. Sie können diese Funktion nicht auf virtuellen Maschinen mit speicherplatzsparenden Festplatten verwenden. VAAI wird auf Maschinen mit der virtuellen Hardwareversion 9 oder höher nicht unterstützt, da die Betriebssystemfestplatten immer speicherplatzsparend sind, sogar wenn Sie den Vorgang zur Rückgewinnung von Speicherplatz deaktivieren.</p> <p>Diese Funktion wird unter vSphere 5.0 und höher unterstützt.</p> <p>Weitere Informationen finden Sie unter <a href="#">Verwenden der View Composer Array Integration mit systemeigener NFS-Snapshot-Technologie (VAAI)</a>.</p> |      |

| Option  | Beschreibung  | Wert |
|---|---|------|
| VM-Datenträgerplatz zurückgewinnen  | <p>(Nur verfügbar, wenn Sie Virtual SAN nicht verwenden) Legen Sie fest, ob Sie ESXi-Hosts erlauben möchten, ungenutzten Datenträgerplatz auf verknüpften Klonen zurückzugewinnen, die im platzsparenden Diskformat erstellt wurden. Die Funktion zur Rückgewinnung von Datenträgerplatz verringert den insgesamt für Linked-Clone-Desktops erforderlichen Speicherplatz.</p> <p>Diese Funktion wird unter vSphere 5.1 und höher unterstützt. Die virtuellen Linked-Clone-Maschinen müssen die virtuelle Hardwareversion 9 oder höher aufweisen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Rückgewinnung von Festplattenspeicherplatz auf virtuellen Linked-Clone-Maschinen</a>.</p>  |      |
| Zurückgewinnung initiieren, wenn der nicht belegte Speicherplatz auf VM größer ist als: | <p>(Nur verfügbar, wenn Sie Virtual SAN nicht verwenden) Geben Sie die Mindestmenge ungenutzten Speicherplatzes in Gigabyte ein, der sich auf einer Linked-Clone-Betriebssystemfestplatte ansammeln muss, damit die Speicherplatzrückgewinnung ausgelöst wird. Wenn der ungenutzte Festplattenspeicherplatz diesen Grenzwert überschreitet, initiiert View den Vorgang, der den ESXi-Host anweist, Speicherplatz auf der Betriebssystemfestplatte zurückzugewinnen.</p> <p>Dieser Wert wird pro virtueller Maschine gemessen. Der ungenutzte Speicherplatz muss den angegebenen Grenzwert auf einer virtuellen Maschine überschreiten, bevor View den Vorgang zur Rückgewinnung von Datenträgerplatz auf der Maschine startet.</p> <p>Beispiel: 2 GB.</p> <p>Der Standardwert ist 1 GB.</p> |      |
| Ausfallzeiten   | <p>Konfigurieren Sie Tage und Uhrzeiten, während derer die Neugenerierung der View-Speicherbeschleunigung und die Rückgewinnung von Datenträgerplatz virtueller Maschinen nicht stattfinden.</p> <p>Um sicherzustellen, dass ESXi-Ressourcen bei Bedarf für im Vordergrund ausgeführte Aufgaben verwendet werden, können Sie festlegen, dass ESXi-Hosts diese Aufgaben an bestimmten Tagen in bestimmten Zeiträumen nicht ausführen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Festlegen von Ausfallzeiten für ESXi-Vorgänge auf View-VMs</a>.</p>  |      |

| Option   | Beschreibung  | Wert |
|--|---|------|
| Domäne   | <p>Wählen Sie die Active Directory-Domäne und den Benutzernamen aus.</p> <p>View Composer benötigt zum Erstellen eines Linked-Clone-Pools spezielle Benutzerberechtigungen. Das Domänen- und das Benutzerkonto werden von QuickPrep oder Sysprep zum Anpassen der Linked-Clone-Computer eingesetzt.</p> <p>Sie geben diesen Benutzer an, wenn Sie View Composer-Einstellungen für vCenter Server konfigurieren. Sie können mehrere Domänen und Benutzer angeben, wenn Sie die View Composer-Einstellungen konfigurieren. Wenn Sie den Assistenten <b>Desktop-Pool hinzufügen</b> zum Erstellen eines Pools verwenden, müssen Sie eine Domäne und einen Benutzer aus der Liste auswählen.</p> <p>Weitere Informationen zum Konfigurieren von View Composer finden Sie im Dokument „Verwaltung von View“.</p>   |      |
| AD-Container   | <p>Stellen Sie den RDN (Relative Distinguished Name) des Active Directory-Containers bereit.</p> <p>Beispiel: <b>CN=Computers</b></p> <p>Bei der Ausführung des Assistenten <b>Desktop-Pool hinzufügen</b> können Sie die Active Directory-Struktur nach dem Container durchsuchen.</p>   |      |
| Wiederverwendung bereits bestehender Computerkonten zulassen | <p>Wählen Sie diese Option, um vorhandene Computerkonten in Active Directory für verknüpfte Klone zu verwenden, die von View Composer bereitgestellt werden. Mit dieser Option können Sie die Computerkonten steuern, die in Active Directory erstellt werden.</p> <p>Wenn ein verknüpfter Klon bereitgestellt wird, sofern der Name eines vorhandenen AD-Computerkontos dem Namen des Linked-Clone-Computers entspricht, verwendet View Composer das vorhandene Computerkonto. Anderenfalls wird ein neues Computerkonto erstellt.</p> <p>Die vorhandenen Computerkonten müssen sich im Active Directory-Container befinden, den Sie über die Einstellung <b>Active Directory-Container</b> angeben.</p> <p>Wenn diese Option deaktiviert ist, wird ein neues AD-Computerkonto erstellt, sofern View Composer einen verknüpften Klon bereitstellt. Diese Option ist standardmäßig deaktiviert.</p> <p>Weitere Informationen finden Sie unter <a href="#">Verwenden vorhandener Active Directory-Computerkonten für verknüpfte Klone</a>.</p> |      |

| Option   | Beschreibung  | Wert |
|--|---|------|
| Use QuickPrep or a customization specification (Sysprep) (QuickPrep oder eine Anpassungsspezifikation (Sysprep) verwenden) | <p>Geben Sie an, ob Sie QuickPrep verwenden oder eine Anpassungsspezifikation (Sysprep) auswählen möchten, damit die Lizenzierung, Domänenbindung, DHCP-Einstellungen und andere Eigenschaften auf den Computern konfiguriert wird.</p> <p>Sysprep wird nur unter vSphere 4.1 oder höher für verknüpfte Klone unterstützt.</p> <p>Nachdem Sie mithilfe von QuickPrep oder Sysprep einen Pool erstellt haben, können Sie bei einer späteren Erstellung oder Neuzusammenstellung von Computern im Pool nicht die Anpassungsmethode ändern.</p> <p>Weitere Informationen finden Sie unter <a href="#">Wählen von QuickPrep oder Sysprep zum Anpassen von Linked-Clone-Maschinen</a>.</p> |      |
| Power-off script (Ausschaltskript)   | <p>QuickPrep kann ein Anpassungsskript auf Linked-Clone-Computern ausführen, bevor diese ausgeschaltet werden.</p> <p>Stellen Sie den Pfad zum Skript auf der übergeordneten virtuellen Maschine und den Skriptparametern bereit.</p>   |      |
| Nach Synchronisierung ausgeführtes Skript  | <p>QuickPrep kann ein Anpassungsskript auf Linked-Clone-Computern ausführen, nachdem diese erstellt, neu zusammengestellt und aktualisiert wurden.</p> <p>Stellen Sie den Pfad zum Skript auf der übergeordneten virtuellen Maschine und den Skriptparametern bereit.</p>   |      |

## Erstellen eines Linked-Clone-Desktop-Pools

Sie können einen automatisierten Linked-Clone-Desktop-Pool basierend auf einer von Ihnen ausgewählten übergeordneten virtuellen Maschine erstellen. Der View Composer-Dienst erstellt dynamisch für jeden Desktop eine neue virtuelle Linked-Clone-Maschine in vCenter Server.

Informationen zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen finden Sie unter [Automatisierte Pools mit vollständigen virtuellen Maschinen](#).

### Voraussetzungen

- Stellen Sie sicher, dass der View Composer-Dienst entweder auf demselben Host wie vCenter Server oder auf einem separaten Host installiert und eine View Composer-Datenbank konfiguriert ist. Weitere Informationen finden Sie im Dokument *Installation von View*.
- Stellen Sie sicher, dass View Composer-Einstellungen für vCenter Server in View Administrator konfiguriert sind. Weitere Informationen finden Sie im Dokument *Verwaltung von View*.

- Stellen Sie sicher, dass Sie auf dem virtuellen ESXi-Switch, der für die virtuellen als Remote-Desktops eingesetzten Maschinen verwendet wird, über eine ausreichende Anzahl an Ports verfügen. Der Standardwert reicht möglicherweise nicht aus, wenn Sie große Desktop-Pools erstellen. Die Anzahl der Ports für den virtuellen Switch auf dem ESXi-Host muss der Anzahl der virtuellen Maschinen multipliziert mit der Anzahl der virtuellen Netzwerkkarten pro virtueller Maschine entsprechen (oder diese übersteigen).
- Stellen Sie sicher, dass Sie eine übergeordnete virtuelle Maschine vorbereitet haben. View Agent muss auf der übergeordneten virtuellen Maschine installiert sein. Siehe [Kapitel 3 Erstellen und Vorbereiten virtueller Maschinen](#).
- Erstellen Sie einen Snapshot der übergeordneten virtuellen Maschine in vCenter Server. Vor dem Erstellen des Snapshots müssen Sie die übergeordnete virtuelle Maschine herunterfahren. View Composer verwendet den Snapshot als Basis-Image, von dem die Klone erstellt werden.

---

**Hinweis** Sie können aus einer Vorlage für virtuelle Maschinen keinen Linked-Clone-Pool erstellen.

---

- Sammeln Sie die Konfigurationsinformationen, die Sie zum Erstellen des Pools bereitstellen müssen. Siehe [Arbeitsblatt zum Erstellen eines Linked-Clone-Desktop-Pools](#).
- Entscheiden Sie, wie die Betriebseinstellungen, das Anzeigeprotokoll, die Adobe Flash-Qualität und andere Einstellungen konfiguriert werden sollen. Siehe [Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen](#).
- 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.

---

**Wichtig** Während der Erstellung eines Linked-Clone-Pools sollten Sie die übergeordnete virtuelle Maschine in vCenter Server nicht ändern. Konvertieren Sie beispielsweise nicht die übergeordnete virtuelle Maschine in eine Vorlage. Für den View Composer-Dienst muss die übergeordnete virtuelle Maschine während der Pool-Erstellung in einem statischen, unveränderten Zustand bleiben.

---

## Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie **Automatisierter Desktop-Pool** aus.
- 4 Wählen Sie auf der Seite **vCenter Server** die Option **Verknüpfte View Composer-Klone**.
- 5 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

Verwenden Sie die Konfigurationsinformationen, die Sie im Arbeitsblatt zusammengetragen haben. Sie können jederzeit auf eine beliebige Assistentenseite zurückwechseln, die Sie bereits ausgefüllt haben, indem Sie im Navigationsbereich auf den Seitennamen klicken.

Sie müssen auf der Seite **vCenter-Einstellungen** auf **Durchsuchen** klicken und nacheinander alle vCenter Server-Einstellungen auswählen. Es ist nicht möglich, eine vCenter Server-Einstellung zu überspringen:

- a Übergeordnete VM
- b Snapshot
- c Speicherort des VM-Ordners
- d Host oder Cluster
- e Ressourcen-Pool
- f Datenspeicher

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

Die verknüpften Klone werden möglicherweise während ihrer Bereitstellung mehrmals neu gestartet. Wenn sich ein verknüpfter Klon in einem Fehlerstatus befindet, versucht der automatische Wiederherstellungsmechanismus von View, den verknüpften Klon einzuschalten oder auszuschalten und neu zu starten. Wenn wiederholte Wiederherstellungsversuche fehlschlagen, wird der verknüpfte Klon gelöscht.

View Composer erstellt außerdem eine Replik-VM, die als das Master-Image für die Bereitstellung der verknüpften Klone dient. Um den Speicherplatzbedarf zu reduzieren, wird das Replikat als Thin-Festplatte erstellt. Werden alle virtuelle Maschinen neu zusammengestellt oder gelöscht und sind keine Klone mit dem Replikat verknüpft, wird die Replik-VM von vCenter Server gelöscht.

Wenn Sie das Replikat nicht in einem separaten Datenspeicher speichern, erstellt View Composer ein Replikat in jedem Datenspeicher, in dem verknüpfte Klone erstellt werden.

Wenn Sie das Replikat in einem separaten Datenspeicher speichern, wird ein Replikat für den gesamten Pool erstellt, selbst wenn verknüpfte Klone in mehreren Datenspeichern erstellt werden.

### Nächste Schritte

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe [Hinzufügen von Berechtigungen zu einem Desktop- oder Anwendungspool](#).

## Desktop-Pool-Einstellungen für Linked-Clone-Desktop-Pools

Bei der Konfiguration automatisierter Pools mit verknüpften Klonen, die über View Composer erstellt wurden, müssen Sie Computer- und Desktop-Pool-Einstellungen angeben. Für Pools mit dedizierten Benutzerzuweisungen und dynamischen Benutzerzuweisungen gelten unterschiedliche Einstellungen.

[Tabelle 5-2. Einstellungen für automatisierte Linked-Clone-Desktop-Pools](#) werden die Einstellungen aufgeführt, die für Linked-Clone-Pools mit dedizierten Zuweisungen und dynamischen Zuweisungen gelten.

Beschreibungen der einzelnen Einstellungen finden Sie unter [Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen](#)

**Tabelle 5-2. Einstellungen für automatisierte Linked-Clone-Desktop-Pools**

| <b>Einstellung</b>  | <b>Linked-Clone-Pool, dedizierte Zuweisung</b> | <b>Linked-Clone-Pool, dynamische Zuweisung</b> |
|---|--|--|
| Status  | Ja   | Ja   |
| Einschränkungen für Verbindungsserver   | Ja   | Ja   |
| Betriebsrichtlinie für Remote-Computer  | Ja   | Ja   |
| Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)   | Ja   | Ja   |
| Benutzern das Zurücksetzen ihrer Computer gestatten                                 | Ja   | Ja   |
| Mehrere Sitzungen pro Benutzer zulassen   |  | Ja   |
| Computer bei Abmeldung löschen oder aktualisieren                                   |  | Ja   |
| Refresh OS disk after logoff (Betriebssystemfestplatte nach Abmelden aktualisieren) | Ja   |  |
| Standardanzeigeprotokoll  | Ja   | Ja   |
| Benutzern die Wahl des Protokolls erlauben  | Ja   | Ja   |
| 3D-Renderer   | Ja   | Ja   |
| Max number of monitors (Maximale Anzahl an Monitoren)                               | Ja   | Ja   |
| Max resolution of any one monitor (Max. Auflösung eines Monitors)                   | Ja   | Ja   |
| Adobe Flash quality (Adobe Flash-Qualität)  | Ja   | Ja   |
| Adobe Flash throttling (Adobe Flash-Drosselung)                                     | Ja   | Ja   |
| Globale Mirage-Einstellungen überschreiben  | Ja   | Ja   |
| Mirage-Serverkonfiguration  | Ja   | Ja   |

## View Composer-Unterstützung für Linked-Clone-SIDs und Drittanbieteranwendungen

View Composer kann in einigen Situationen lokale Computer-SIDs für virtuelle Linked-Clone-Maschinen generieren und beibehalten. View Composer kann GUIDs von Drittanbieteranwendungen abhängig davon beibehalten, wie diese GUIDs von den Anwendungen generiert werden.

Um zu verstehen, wie View Composer-Vorgänge sich auf SIDs und Anwendungs-GUIDs auswirken, müssen Sie wissen, wie Linked-Clone-Maschinen erstellt und bereitgestellt werden:

- 1 View Composer erstellt einen verknüpften Klon anhand dieser Schritte:
  - a Erstellung des Replikats, indem der übergeordnete VM-Snapshot geklont wird.
  - b Erstellung des verknüpften Klons, der als übergeordnete Festplatte das Replikat referenziert.
- 2 View Composer und View passen den verknüpften Klon mit QuickPrep bzw. einer Sysprep-Anpassungsspezifikation an, je nachdem, welches Anpassungstool Sie beim Erstellen des Pools auswählen.

- Wenn Sie Sysprep wählen, wird für jeden Klon eine eindeutige SID generiert.
- Wenn Sie QuickPrep einsetzen, wird keine neue SID generiert. Die SID der übergeordneten virtuellen Maschine wird auf allen bereitgestellten Linked-Clone-Maschinen im Pool repliziert.
- Einige Anwendungen generieren während der Anpassung eine GUID.

- 3 View erstellt einen Snapshot des verknüpften Klons.

Der Snapshot enthält die eindeutige SID, die über Sysprep generiert wurde, bzw. die gemeinsame SID, die über QuickPrep generiert wurde.

- 4 View schaltet die Maschine entsprechend den von Ihnen beim Erstellen des Pools ausgewählten Einstellungen ein.

Einige Anwendungen generieren eine GUID, wenn die Maschine erstmals eingeschaltet wird.

Einen Vergleich zwischen der QuickPrep- und der Sysprep-Anpassung finden Sie unter [Wählen von QuickPrep oder Sysprep zum Anpassen von Linked-Clone-Maschinen](#).

Wenn Sie den verknüpften Klon aktualisieren, verwendet View Composer den Snapshot zum Wiederherstellen des Klons in seinem anfänglichen Zustand. Die SID wird beibehalten.

Wenn Sie QuickPrep verwenden und den verknüpften Klon erneut zusammenstellen, bleibt die SID der übergeordneten virtuellen Maschine im verknüpften Klon erhalten, sofern Sie dieselbe übergeordnete virtuelle Maschine für die Neuzusammenstellung auswählen. Wenn Sie für die Neuzusammenstellung eine andere übergeordnete virtuelle Maschine auswählen, wird die SID der neuen übergeordneten Maschine auf dem Klon repliziert.

Wenn Sie Sysprep wählen, wird für den Klon immer eine neue SID generiert. Weitere Informationen finden Sie unter [Neuzusammenstellung von mit Sysprep angepassten verknüpften Klonen](#).

[Tabelle 5-3. View Composer-Vorgänge, Linked-Clone-SIDs und Anwendungs-GUIDs](#) zeigt die Auswirkungen von View Composer-Vorgängen auf Linked-Clone-SIDs und die GUIDs von Drittanbieteranwendungen.



**Tabelle 5-3. View Composer-Vorgänge, Linked-Clone-SIDs und Anwendungs-GUIDs**

| Unterstützung für SIDs oder GUIDs               | Klonerstellung  | Aktualisieren  | Neu zusammenstellen   |
|---|---|--|---|
| Sysprep: Eindeutige SIDs für verknüpfte Klone   | Bei der Sysprep-Anpassung werden eindeutige SIDs für verknüpfte Klone generiert.  | Eindeutige SIDs bleiben erhalten.  | Eindeutige SIDs bleiben nicht erhalten.   |
| QuickPrep: Gemeinsame SIDs für verknüpfte Klone | Bei der QuickPrep-Anpassung wird für alle Klone in einem Pool eine gemeinsame SID generiert.  | Gemeinsame SID wird beibehalten.   | Gemeinsame SID wird beibehalten.  |
| GUIDs von Drittanbieteranwendungen              | Jede Anwendung verhält sich anders.<br><br><b>Hinweis</b> Sysprep und QuickPrep besitzen dieselben Auswirkungen auf den Erhalt von GUIDs. | Die GUID bleibt erhalten, wenn eine Anwendung die GUID vor der Erstellung des anfänglichen Snapshots generiert.<br><br>Die GUID bleibt nicht erhalten, wenn eine Anwendung die GUID erst nach Erstellung des anfänglichen Snapshots generiert. | Bei Neuzusammenstellungen bleibt eine Anwendungs-GUID nur dann erhalten, wenn die Anwendung die GUID auf das Laufwerk schreibt, das als persistente View Composer-Festplatte angegeben wurde. |

## Wählen von QuickPrep oder Sysprep zum Anpassen von Linked-Clone-Maschinen

QuickPrep und Microsoft Sysprep bieten verschiedene Ansätze zum Anpassen von Linked-Clone-Maschinen. QuickPrep wurde für eine effiziente Zusammenarbeit mit View Composer konzipiert. Microsoft Sysprep stellt Standard-Tools zur Anpassung bereit.

Bei der Erstellung von Linked-Clone-Maschinen müssen Sie die einzelnen virtuellen Maschinen so bearbeiten, dass sie als eindeutige Computer im Netzwerk verwendet werden können. View und View Composer bieten zwei Methoden zur Personalisierung von Linked-Clone-Maschinen.

[Tabelle 5-4. Vergleichen von QuickPrep und Microsoft Sysprep](#) vergleicht QuickPrep mit Anpassungsspezifikationen, die mit Microsoft Sysprep erstellt werden.

**Tabelle 5-4. Vergleichen von QuickPrep und Microsoft Sysprep**

| QuickPrep  | Anpassungsspezifikation (Sysprep)   |
|--|---|
| Für die Zusammenarbeit mit View Composer ausgelegt.<br>Weitere Informationen finden Sie unter <a href="#">Anpassen von Linked-Clone-Maschinen mit QuickPrep</a> .        | Kann mit den Standard-Tools von Microsoft Sysprep erstellt werden.                    |
| Verwendet dieselbe Sicherheits-ID (SID) für lokale Computer für alle verknüpften Klone im Pool.  | Generiert eine eindeutige SID für lokale Computer für jeden verknüpften Klon im Pool. |
| Kann zusätzliche Anpassungsskripts ausführen, bevor verknüpfte Klone ausgeschaltet und nachdem verknüpfte Klone erstellt, aktualisiert oder neu zusammengestellt werden. | Kann bei der ersten Anmeldung des Benutzers ein zusätzliches Skript ausführen.        |

| QuickPrep   | Anpassungsspezifikation (Sysprep)   |
|---|---|
| Nimmt den Linked-Clone-Computer in die Active Directory-Domäne auf.   | Nimmt den Linked-Clone-Computer in die Active Directory-Domäne auf.<br><br>Die Domänen- und Administratorinformationen in der Sysprep-Anpassungsspezifikation werden nicht verwendet. Die virtuelle Maschine wird anhand der Gastanpassungsinformationen der Domäne hinzugefügt, die Sie in View Administrator beim Erstellen des Pools eingeben. |
| Für jeden verknüpften Klon wird dem Active Directory-Domänenkonto eine eindeutige ID hinzugefügt.           | Für jeden verknüpften Klon wird dem Active Directory-Domänenkonto eine eindeutige ID hinzugefügt.   |
| Generiert keine neue SID nach dem Aktualisieren verknüpfter Klone. Die gemeinsame SID bleibt erhalten.      | Generiert eine neue SID, sobald die einzelnen verknüpften Klone angepasst werden. Erhält die eindeutigen SIDs während eines Aktualisierungsvorgangs, jedoch nicht während einer Neuzusammenstellung oder Neuverteilung.   |
| Generiert keine neue SID nach dem Neuzusammenstellen verknüpfter Klone. Die gemeinsame SID bleibt erhalten. | Wird nach der Neuzusammenstellung verknüpfter Klone erneut ausgeführt und generiert neue SIDs für die virtuellen Maschinen. Weitere Informationen finden Sie unter <a href="#">Neuzusammenstellung von mit Sysprep angepassten verknüpften Klonen</a> .   |
| Wird schneller als Sysprep ausgeführt.  | Kann längere Zeit benötigen als QuickPrep.  |

Nach der Anpassung eines Linked-Clone-Pools mit QuickPrep oder Sysprep können Sie nicht zur anderen Anpassungsmethode wechseln, wenn Sie Maschinen im Pool erstellen oder neu zusammenstellen.

## Anpassen von Linked-Clone-Maschinen mit QuickPrep

Sie können die durch eine übergeordnete virtuelle Maschine erstellten Linked-Clone-Maschinen über das System-Tool QuickPrep personalisieren. View Composer führt QuickPrep aus, sobald eine Linked-Clone-Maschine erstellt oder neu zusammengestellt wird.

QuickPrep passt eine Linked-Clone-Maschine auf verschiedene Weise an:

- Zuweisen eines Namens für den Computer, den Sie bei der Erstellung des Linked-Clone-Pools angeben.
- Erstellen eines Computerkontos in Active Directory und Aufnehmen des Computers in die geeignete Domäne.
- Bereitstellen der persistenten View Composer-Festplatte. Das Windows-Benutzerprofil wird auf diese Festplatte umgeleitet.
- Umleiten von temporären und Auslagerungsdateien auf eine separate Festplatte.

Für diese Schritte müssen die verknüpften Klone möglicherweise einmal oder mehrmals neu gestartet werden.

QuickPrep verwendet die KMS-Volumenlizenzschlüssel zum Aktivieren von Linked-Clone-Maschinen unter Windows 8, Windows 7 und Windows Vista. Details finden Sie im Dokument „Verwaltung von View“.

Sie können Ihre eigenen Skripts zur weiteren Anpassung der verknüpften Klone erstellen. QuickPrep kann zwei Typen von Skripts zu vordefinierten Zeitpunkten ausführen:

- Nach der Erstellung oder Neuzusammenstellung verknüpfter Klone
- Unmittelbar vor dem Ausschalten verknüpfter Klone

Richtlinien und Regeln für die Verwendung von QuickPrep-Anpassungsskripts finden Sie unter [Ausführen von QuickPrep-Anpassungsskripts](#).

---

**Hinweis** View Composer erfordert Anmeldedaten von Domänenbenutzern, um Linked-Clone-Maschinen in eine Active Directory-Domäne aufzunehmen. Details finden Sie im Dokument *Verwaltung von View*.

---

## Ausführen von QuickPrep-Anpassungsskripts

Mit dem QuickPrep-Tool können Sie Skripts zur Anpassung der in einem Pool enthaltenen Linked-Clone-Computer erstellen. Sie können QuickPrep so konfigurieren, dass Anpassungsskripts zu zwei vordefinierten Zeitpunkten ausgeführt werden.

### Wann werden QuickPrep-Skripts ausgeführt?

Das nach der Synchronisierung ausgeführte Skript wird nach der Erstellung, Neuzusammenstellung oder Neuverteilung von verknüpften Klonen eingesetzt, wenn sich die Klone im Status **Bereit** befinden. Das Abschaltskript wird ausgeführt, bevor verknüpfte Klone ausgeschaltet werden. Die Skripts werden in den Gastbetriebssystemen der verknüpften Klone ausgeführt.

### Wie werden QuickPrep-Skripts ausgeführt?

Der QuickPrep-Prozess verwendet die Windows-API `CreateProcess` zum Ausführen von Skripts. Ihr Skript kann einen beliebigen Prozess starten, der mit der `CreateProcess`-API erstellt werden kann. Beispielsweise arbeiten `cmd`, `vbscript`, `exe` und Batch-Dateiprozesse mit der API zusammen.

Bei Ausführung des Skripts übergibt QuickPrep den für das Skript angegebenen Pfad als zweiten Parameter an die `CreateProcess`-API und legt den ersten Parameter auf `NULL` fest.

Wenn der Skriptpfad beispielsweise `C:\MeinSkript.cmd` lautet, erscheint der Pfad in der View Composer-Protokolldatei als zweiter Parameter in der Funktion:  
`CreateProcess(NULL,C:\MeinSkript.cmd,...)`.

### Bereitstellen von Pfaden für QuickPrep-Skripts

Sie stellen den QuickPrep-Anpassungsskripts Pfade bereit, wenn Sie einen Linked-Clone-Computer-Pool erstellen oder die Gastanpassungseinstellungen für einen Pool bearbeiten. Die Skripts müssen auf der übergeordneten virtuellen Maschine gespeichert sein. Sie können keinen UNC-Pfad zu einer Netzwerkfreigabe verwenden.

Wenn Sie eine Skriptsprache verwenden, die zur Skriptausführung einen Interpreter erfordert, muss der Skriptpfad mit der Interpreter-Binärdatei beginnen.

Wenn Sie beispielsweise den Pfad `C:\script\myvb.vbs` als QuickPrep-Anpassungsskript angeben, kann View Composer Agent das Skript nicht ausführen. Sie müssen einen Pfad angeben, der mit der Interpreter-Binärdatei beginnt:

```
C:\windows\system32\cscript.exe c:\script\myvb.vbs
```

---

**Wichtig** Schützen Sie QuickPrep-Anpassungsskripts vor dem Zugang durch normale Benutzer. Platzieren Sie die Skripts in einem sicheren Ordner.

---

### Zeitüberschreitungslimits für QuickPrep-Skripts

View Composer beendet ein nach der Synchronisierung ausgeführtes Skript oder ein Abschaltskript, wenn dessen Ausführung länger als 20 Sekunden dauert. Wenn Ihr Skript länger als 20 Sekunden ausgeführt wird, können Sie das Limit für die Zeitüberschreitung erhöhen. Weitere Informationen finden Sie unter [Erhöhen des Zeitüberschreitungslimits für QuickPrep-Anpassungsskripts](#).

Alternativ dazu können Sie mit Ihrem Skript ein weiteres Skript oder einen Prozess starten, durch das bzw. den die Aufgabe mit langer Laufzeit durchgeführt wird.

### Konto für die Ausführung von QuickPrep-Skripts

QuickPrep führt die Skripts mit dem Konto aus, das zur Ausführung des VMware View Composer Gastagentserver-Dienstes konfiguriert ist. Standardmäßig handelt es sich hier um das Konto `LocalSystem`.

Ändern Sie dieses Anmeldekonto nicht. Wenn Sie das Konto ändern, können die verknüpften Klone nicht starten.

### Berechtigungen für den QuickPrep-Prozess

Aus Sicherheitsgründen werden bestimmte Berechtigungen für das Windows-Betriebssystem aus dem View Composer Guest Agent-Prozess entfernt, der die QuickPrep-Anpassungsskripts aufruft.

Ein QuickPrep-Anpassungsskript kann keine Aktion ausführen, die eine Berechtigung benötigt, die aus dem View Composer Guest Agent-Prozess entfernt wurde.

Die folgenden Berechtigungen werden aus dem Prozess entfernt, der QuickPrep-Skripts aufruft:

```
SeCreateTokenPrivilege
SeTakeOwnershipPrivilege
SeSecurityPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeSystemtimePrivilege
SeUndockPrivilege
SeManageVolumePrivilege
SeLockMemoryPrivilege
SeIncreaseBasePriorityPrivilege
SeCreatePermanentPrivilege
SeDebugPrivilege
SeAuditPrivilege
```

### Protokolle zu QuickPrep-Skripts

View Composer-Protokolle enthalten Informationen zur Ausführung von QuickPrep-Skripts. Das Protokoll zeichnet den Start und das Ende der Skriptausführung auf und protokolliert Ausgabe- oder Fehlermeldungen. Das Protokoll befindet sich im Windows-Verzeichnis `Temp`:

C:\Windows\Temp\vmware-viewcomposer-ga-new.log

## Neuzusammenstellung von mit Sysprep angepassten verknüpften Klonen

Wenn Sie eine mit Sysprep angepasste Linked-Clone-Maschine neu zusammenstellen, führt View die Sysprep-Anpassungsspezifikation erneut aus, nachdem die Betriebssystemfestplatte neu zusammengestellt wurde. Durch diesen Vorgang wird eine neue SID für die virtuelle Linked-Clone-Maschine generiert.

Wird eine neue SID generiert, fungiert der neu zusammengestellte verknüpfte Klon als neuer Computer im Netzwerk. Einige Softwareprogramme wie Tools zur Systemverwaltung verwenden die SID zum Identifizieren der von ihnen verwalteten Computer. Diese Programme können die virtuelle Linked-Clone-Maschine möglicherweise nicht identifizieren oder finden.

Wenn auf der Systemfestplatte außerdem eine Drittanbietersoftware installiert ist, werden die GUIDs für die jeweilige Software nach der Neuzusammenstellung möglicherweise durch die Anpassungsspezifikation neu generiert.

Durch eine Neuzusammenstellung wird der verknüpfte Klon in seinen ursprünglichen Zustand vor der ersten Ausführung der Anpassungsspezifikation zurückversetzt. In diesem Zustand besitzt der verknüpfte Klon keine lokale Computer-SID oder die GUID einer auf dem Systemlaufwerk installierten Drittanbietersoftware. View muss die Sysprep-Anpassungsspezifikation ausführen, nachdem der verknüpfte Klon neu zusammengestellt wird.

## Linked-Clone-Maschinen während View Composer-Vorgängen bereitgestellt und einsatzbereit halten

Wenn Ihre Benutzer jederzeit auf Remote-Desktops zugreifen können müssen, müssen Sie eine bestimmte Anzahl Maschinen bereitgestellt und einsatzbereit belassen. Nur so können diese auch dann Verbindungsanforderungen von Ihren Benutzern akzeptieren, während View Composer-Wartungsvorgänge stattfinden. Sie können eine Mindestanzahl bereitgestellter, einsatzbereiter Maschinen einstellen, während View Composer die virtuellen Linked-Clone-Maschinen in einem Pool aktualisiert, neu zusammenstellt oder neu verteilt.

Wenn Sie eine **Mindestanzahl von einsatzbereiten (bereitgestellten) Maschinen während der View Composer-Wartungsvorgänge** angeben, stellt View sicher, dass die angegebene Anzahl Maschinen bereitgestellt und einsatzbereit bleibt, während View Composer den Vorgang durchläuft. Sie können die Mindestanzahl einsatzbereiter Maschinen angeben, wenn Sie einen Linked-Clone-Pool erstellen oder bearbeiten.

Für diese Einstellung gelten folgende Richtlinien:

- Wenn Sie ein Benennungsmuster für die Bereitstellung von Maschinen verwenden und Maschinen nach Bedarf bereitstellen, stellen Sie die Anzahl einsatzbereiter Maschinen während der View Composer-Vorgänge auf einen kleineren Wert ein als die angegebene **Mindestanzahl an**

**Maschinen.** Bei einer kleineren Mindestanzahl könnte Ihr Pool insgesamt weniger Maschinen enthalten als die Mindestanzahl, die Sie während der View Composer-Vorgänge bereitgestellt und einsatzbereit halten möchten. In diesem Fall könnten die View Composer-Wartungsvorgänge nicht stattfinden.

- Wenn Sie Maschinen manuell bereitstellen, indem Sie eine Liste von Maschinennamen angeben, verringern Sie die gesamte Pool-Größe nicht auf eine geringere Anzahl als die Mindestanzahl einsatzbereiter Maschinen (durch Entfernen von Maschinennamen). In diesem Fall könnten die View Composer-Wartungsvorgänge nicht stattfinden.
- Wenn Sie eine große Mindestanzahl einsatzbereiter Maschinen im Verhältnis zur Pool-Größe einstellen, könnte das Abschließen der View Composer-Wartungsvorgänge längere Zeit beanspruchen. Während View die Mindestanzahl an einsatzbereiten Maschinen während eines Wartungsvorgangs beibehält, könnte der Vorgang das Limit paralleler Vorgänge nicht erreichen, das in der Einstellung **Maximale parallele View Composer-Wartungsvorgänge** festgelegt ist.

Wenn ein Pool beispielsweise 20 Maschinen umfasst und die Mindestanzahl einsatzbereiter Maschinen 15 lautet, kann View Composer auf maximal fünf Maschinen gleichzeitig arbeiten. Wenn das Limit für parallele View Composer-Wartungsvorgänge 12 beträgt, wird das Limit paralleler Vorgänge nie erreicht.

- Der Begriff „einsatzbereit“ bezieht sich auf den Status der virtuellen Linked-Clone-Maschine, nicht auf den Maschinenstatus, der in View Administrator angezeigt wird. Eine virtuelle Maschine ist bereit, wenn sie bereitgestellt ist und eingeschaltet werden kann. Der Maschinenstatus reflektiert den von View verwalteten Zustand der Maschine. Eine Maschine kann beispielsweise den Status Verbunden, Nicht verbunden, Agent nicht erreichbar, Wird gelöscht usw. haben.

## Verwenden vorhandener Active Directory-Computerkonten für verknüpfte Klone

Wenn Sie einen Desktop-Pool erstellen oder bearbeiten, können Sie View Composer konfigurieren, um vorhandene Computerkonten in Active Directory für neu bereitgestellte verknüpfte Klone zu verwenden.

View Composer generiert standardmäßig ein neues Active Directory-Computerkonto für jeden verknüpften Klon, den es bereitstellt. Mit der Option **Wiederverwendung bereits bestehender Computerkonten zulassen** können Sie die Computerkonten steuern, die in Active Directory erstellt werden, indem Sie sicherstellen, dass View Composer vorhandene AD-Computerkonten verwendet.

Wenn diese Option während der Bereitstellung eines verknüpften Klons aktiviert ist, überprüft View Composer, ob ein vorhandener AD-Computerkontoname dem Namen der Maschine mit verknüpftem Klon entspricht. Gibt es eine Übereinstimmung, verwendet View Composer das vorhandene AD-Computerkonto. Findet View Composer keinen übereinstimmenden AD-Computerkontonamen, generiert View Composer ein neues AD-Computerkonto für den verknüpften Klon.

Sie können die Option **Wiederverwendung bereits bestehender Computerkonten zulassen** einstellen, wenn Sie einen neuen Desktop-Pool erstellen oder einen vorhandenen Pool bearbeiten. Wenn Sie einen Pool bearbeiten und diese Option einstellen, wirkt sich die Einstellung auf Maschinen mit verknüpftem Klon aus, die künftig bereitgestellt werden. Schon bereitgestellte verknüpfte Klone sind nicht betroffen.

Wenn Sie die Option **Wiederverwendung bereits bestehender Computerkonten zulassen** einstellen, können Sie die Active Directory-Berechtigungen beschränken, die dem View Composer-Benutzerkonto, das den Desktop-Pool generiert, zugewiesen werden. Nur die folgenden Active Directory-Berechtigungen sind erforderlich:

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

Sie können die Active Directory-Berechtigungen nur einschränken, wenn Sie sicher sind, dass allen Maschinen, die bereitgestellt werden sollen, bereits bestehende Computerkonten in Active Directory zugewiesen sind. Wenn kein übereinstimmender Name gefunden wird, generiert View Composer ein neues Active Directory-Computerkonto. Zum Erstellen neuer Computerkonten sind zusätzliche Berechtigungen wie „Computerobjekte erstellen“ erforderlich. Eine vollständige Liste der für das View Composer-Benutzerkonto erforderlichen Berechtigungen finden Sie im Dokument *Verwaltung von View*.

Diese Option kann nicht deaktiviert werden, wenn View Composer derzeit mindestens ein vorhandenes AD-Computerkonto verwendet.

### Voraussetzungen

Stellen Sie sicher, dass sich die vorhandenen Computerkonten im Active Directory-Container befinden, den Sie über die Einstellung **Active Directory-Container** angeben. Wenn sich die vorhandenen Konten in einem anderen Container befinden, schlägt die Bereitstellung für verknüpfte Klone mit diesen Kontonamen fehl und in einer Fehlermeldung wird angegeben, dass die vorhandenen Computerkonten bereits in Active Directory vorhanden sind.

Wenn Sie z. B. die Option **Wiederverwendung bereits bestehender Computerkonten zulassen** auswählen, für **Active Directory-Container** den Standardwert angeben (**CN=Computers**) und sich die vorhandenen Computerkonten in **OU=mydesktops** befinden, schlägt die Bereitstellung für diese Konten fehl.

### Verfahren

- 1 Erstellen Sie in Active Directory die Computerkonten, die für die Maschinen mit verknüpftem Klon verwendet werden sollen.

Beispiel: machine1, machine2, machine3

Die Computerkontonamen müssen fortlaufende Ganzzahlen aufweisen, damit sie den Namen entsprechen, die während der Maschinenbereitstellung in View generiert werden.

- 2 Erstellen Sie in View Administrator einen Pool mit dem Assistenten „Desktop-Pool hinzufügen“ oder bearbeiten Sie den Pool im Bearbeitungsdialogfeld.
- 3 Wählen Sie auf der Seite oder Registerkarte Bereitstellungseinstellungen die Option **Benennungsmuster verwenden**.

- 4 Geben Sie in das Textfeld **Benennungsmuster** einen Maschinennamen ein, der dem Active Directory-Computerkontonamen entspricht.

Beispiel: machine

View hängt eindeutige Nummern an das Muster an, um für jede Maschine einen eindeutigen Namen zu schaffen.

Beispiel: machine1, machine2, machine3

- 5 Wählen Sie auf der Seite oder Registerkarte Gastanpassung die Option **Wiederverwendung bereits bestehender Computerkonten zulassen**.



# Erstellen von manuellen Desktop-Pools

# 6

In einem manuellen Desktop-Pool handelt es sich bei jedem Remote-Desktop, auf den ein Endbenutzer zugreift, um einen separaten Computer. Wenn Sie einen manuellen Desktop-Pool erstellen, wählen Sie vorhandene Computer aus. Sie können einen Pool erstellen, der nur einen einzigen Desktop enthält, indem Sie einen manuellen Desktop-Pool erstellen und einen einzelnen Computer auswählen.

Dieses Kapitel enthält die folgenden Themen:

- [Manuelle Desktop-Pools](#)
- [Arbeitsblatt zum Erstellen eines manuellen Desktop-Pools](#)
- [Erstellen eines manuellen Desktop-Pools](#)
- [Erstellen eines manuellen Pools mit einem Computer](#)
- [Desktop-Pool-Einstellungen für manuelle Pools](#)

## Manuelle Desktop-Pools

Zum Erstellen eines manuellen Desktop-Pools stellt View Desktops von vorhandenen Maschinen bereit. Für jeden Desktop im Pool wählen Sie eine separate Maschine aus.

View kann mehrere Arten von Maschinen in manuellen Pools verwenden:

- Mit vCenter Server verwaltete virtuelle Maschinen
- Virtuelle Maschinen, die auf einer anderen Virtualisierungsplattform als vCenter Server ausgeführt werden
- Physische Computer

## Arbeitsblatt zum Erstellen eines manuellen Desktop-Pools

Bei der Erstellung eines manuellen Desktop-Pools fordert der View Administrator-Assistent **Desktop-Pool hinzufügen** Sie zum Konfigurieren bestimmter Optionen auf. Mithilfe dieses Arbeitsblatts können Sie Ihre Konfigurationsoptionen vorbereiten, bevor Sie den Pool erstellen.

Sie können dieses Arbeitsblatt drucken und die Werte notieren, die Sie bei Ausführung des Assistenten **Desktop-Pool hinzufügen** angeben möchten.

**Hinweis** In einem manuellen Pool müssen Sie jeden Computer so vorbereiten, dass er Remote-Desktop-Zugriff bereitstellt. View Agent muss auf jedem Computer installiert sein und ausgeführt werden.

**Tabelle 6-1. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines manuellen Desktop-Pools**

| Option            | Beschreibung  | Wert |
|-------------------|---|------|
| Benutzerzuweisung | <p>Wählen Sie die Art der Benutzerzuweisung:</p> <ul style="list-style-type: none"><li>■ In einem Pool mit dedizierter Zuweisung wird jeder Benutzer einem Computer zugewiesen. Benutzer erhalten bei jeder Anmeldung denselben Computer.</li><li>■ In einem Pool mit dynamischer Zuweisung erhalten die Benutzer bei jeder Anmeldung einen anderen Computer.</li></ul> <p>Weitere Informationen finden Sie unter <a href="#">Benutzerzuweisung in Desktop-Pools</a>.</p> |      |
| vCenter Server    | <p>Der vCenter Server, der den Computer verwaltet.</p> <p>Diese Option wird nur angezeigt, wenn es sich bei den Computern um virtuelle Maschinen handelt, die von vCenter Server verwaltet werden.</p>  |      |

| Option                     | Beschreibung  | Wert |
|----------------------------|---|------|
| Computerquelle             | <p>Die virtuellen Maschinen oder physischen Computer, die Sie im Desktop-Pool verwenden möchten.</p> <ol style="list-style-type: none"> <li>1 Entscheiden Sie, welchen Typ des Computers Sie verwenden möchten. Sie können entweder virtuelle Maschinen einsetzen, die von vCenter Server verwaltet werden, oder nicht verwaltete virtuelle Maschinen und physische Computer.</li> <li>2 Bereiten Sie eine Liste mit virtuellen vCenter Server-Maschinen oder nicht verwalteten virtuellen Maschinen und physischen Computern vor, die Sie in den Desktop-Pool aufnehmen möchten.</li> <li>3 Installieren Sie View Agent auf jedem Computer, den Sie im Desktop-Pool einbeziehen möchten.</li> </ol> <p>Um PCoIP mit Computern zu verwenden, bei denen es sich um nicht verwaltete virtuelle Maschinen oder physische Computer handelt, müssen Sie Teradici-Hardware einsetzen.</p> <hr/> <p><b>Hinweis</b> Wenn Sie Windows Server 2008 R2-Desktops in View Administrator aktivieren, zeigt View Administrator alle verfügbaren Windows Server 2008 R2-Computer, einschließlich Computer, auf denen View-Verbindungsserver und andere View Server installiert sind, als mögliche Computerquellen an.</p> <p>Sie können Computer nicht für den Desktop-Pool auswählen, wenn die View Server-Software auf den Computern installiert ist. Die View Agent-Software darf nicht auf derselben virtuellen Maschine oder demselben physischen Computer wie eine andere View-Softwarekomponente vorliegen, View-Verbindungsserver, Sicherheitsserver, View Composer oder Horizon Client eingeschlossen.</p> |      |
| Desktop-Pool-ID            | <p>Der Pool-Name, der Benutzern bei der Anmeldung angezeigt wird und der den Pool in View Administrator identifiziert.</p> <p>Wenn mehrere vCenter Server-Instanzen in Ihrer Umgebung ausgeführt werden, stellen Sie sicher, dass keine weitere vCenter Server-Instanz dieselbe Pool-ID verwendet.</p>  |      |
| Desktop-Pool-Einstellungen | <p>Einstellungen, die den Computerstatus, den Betriebsstatus bei Nichtnutzung einer virtuellen Maschine, das Anzeigeprotokoll, die Adobe Flash-Qualität usw. festlegen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen</a>.</p> <p>Eine Liste der Einstellungen für manuelle Pools finden Sie unter <a href="#">Desktop-Pool-Einstellungen für manuelle Pools</a>.</p>  |      |

## Erstellen eines manuellen Desktop-Pools

Sie können einen manuellen Desktop-Pool erstellen, der Desktops aus vorhandenen virtuellen Maschinen oder physischen Computern bereitstellt. Sie müssen die Computer auswählen, die in den Desktop-Pool einbezogen werden.

Für manuelle Pools mit virtuellen Maschinen, die über vCenter Server verwaltet werden, schaltet View eine Reservemaschine ein, damit die Benutzer sich verbinden können. Die Reservemaschine wird unabhängig davon eingeschaltet, welche Betriebsrichtlinie in Kraft ist.

### Voraussetzungen

- Bereiten Sie die Computer für das Bereitstellen von Zugriff auf einen Remote-Desktop vor. In einem manuellen Pool müssen Sie jeden Computer einzeln vorbereiten. View Agent muss auf jedem Computer installiert sein und ausgeführt werden.

Informationen zum Vorbereiten einer von vCenter Server verwalteten virtuellen Maschine finden Sie unter [Kapitel 3 Erstellen und Vorbereiten virtueller Maschinen](#).

Informationen zum Vorbereiten nicht verwalteter virtueller Maschinen und physischer Computer finden Sie unter [Kapitel 2 Vorbereiten nicht verwalteter Maschinen](#).

- Sammeln Sie die Konfigurationsinformationen, die Sie zum Erstellen des Pools bereitstellen müssen. Siehe [Arbeitsblatt zum Erstellen eines manuellen Desktop-Pools](#).
- Entscheiden Sie, wie die Betriebseinstellungen, das Anzeigeprotokoll, die Adobe Flash-Qualität und andere Einstellungen konfiguriert werden sollen. Siehe [Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen](#).

### Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie **Manueller Desktop-Pool** aus.
- 4 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

Verwenden Sie die Konfigurationsinformationen, die Sie im Arbeitsblatt zusammengetragen haben. Sie können jederzeit auf eine beliebige Assistentenseite zurückwechseln, die Sie bereits ausgefüllt haben, indem Sie im Navigationsbereich auf den Seitennamen klicken.

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

### Nächste Schritte

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe [Hinzufügen von Berechtigungen zu einem Desktop- oder Anwendungspool](#).

## Erstellen eines manuellen Pools mit einem Computer

Sie können einen Pool mit einem einzigen Computer erstellen, wenn Benutzer einen eindeutigen dedizierten Desktop benötigen oder wenn mehrere Benutzer zu unterschiedlichen Zeiten auf eine kostspielige Anwendung mit einer einzelnen Hostlizenz zugreifen müssen.

Sie können einen einzelnen Computer in einem eigenen Pool bereitstellen, indem Sie einen manuellen Desktop-Pool erstellen und einen einzelnen Computer auswählen.

Um einen physischen Computer zu simulieren, der von mehreren Benutzern gemeinsam verwendet werden kann, geben Sie eine dynamische Zuweisung für die Benutzer an, die zum Zugriff auf den Pool berechtigt sind.

Unabhängig davon, ob Sie einen Pool mit einem einzelnen Computer mit einer dynamischen oder dedizierten Zuweisung konfigurieren, werden Betriebsvorgänge von der Sitzungsverwaltung initiiert. Die virtuelle Maschine wird eingeschaltet, wenn ein Benutzer den Desktop anfordert, und ausgeschaltet oder angehalten, wenn der Benutzer sich abmeldet.

Wenn Sie die Richtlinie **Computer müssen immer eingeschaltet sein** konfigurieren, bleibt die virtuelle Maschine immer eingeschaltet. Wenn der Benutzer die virtuelle Maschine herunterfährt, wird sie sofort neu gestartet.

### Voraussetzungen

- Bereiten Sie den Computer darauf vor, Remote-Desktop-Zugriff zu bieten. View Agent muss auf dem Computer installiert sein und ausgeführt werden.

Informationen zum Vorbereiten einer von vCenter Server verwalteten virtuellen Maschine finden Sie unter [Kapitel 3 Erstellen und Vorbereiten virtueller Maschinen](#).

Informationen zum Vorbereiten einer nicht verwalteten virtuellen Maschine oder eines nicht verwalteten physischen Computers finden Sie unter [Kapitel 2 Vorbereiten nicht verwalteter Maschinen](#).

- Sammeln Sie die Konfigurationsinformationen, die Sie zum Erstellen des manuellen Pools bereitstellen müssen. Siehe [Arbeitsblatt zum Erstellen eines manuellen Desktop-Pools](#).
- Entscheiden Sie, wie die Betriebseinstellungen, das Anzeigeprotokoll, die Adobe Flash-Qualität und andere Einstellungen konfiguriert werden sollen. Siehe [Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen](#).

### Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie **Manueller Desktop-Pool** aus.

#### 4 Wählen Sie die Art der Benutzerzuweisung.

| Option           | Beschreibung   |
|------------------|--|
| <b>Dediziert</b> | Der Computer ist einem Benutzer zugewiesen. Nur dieser Benutzer kann sich am Desktop anmelden.   |
| <b>Dynamisch</b> | Der Computer wird von allen Benutzern gemeinsam genutzt, die über Berechtigungen für den Pool verfügen. Jeder berechtigte Benutzer kann sich am Desktop anmelden, sofern zurzeit kein anderer Benutzer angemeldet ist. |

#### 5 Wählen Sie auf der Seite „Computerquelle“ den Computer aus, der in den Desktop-Pool aufgenommen werden soll.

#### 6 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

Verwenden Sie die Konfigurationsinformationen, die Sie im Arbeitsblatt zusammengetragen haben. Sie können jederzeit auf eine beliebige Assistentenseite zurückwechseln, die Sie bereits ausgefüllt haben, indem Sie im Navigationsbereich auf den Seitennamen klicken.

In View Administrator können Sie anzeigen, welcher Computer den Pool hinzugefügt wird, indem Sie **Katalog > Desktop-Pools** auswählen.

#### Nächste Schritte

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe [Hinzufügen von Berechtigungen zu einem Desktop- oder Anwendungspool](#).

## Desktop-Pool-Einstellungen für manuelle Pools

Beim Konfigurieren manueller Desktop-Pools müssen Sie Maschinen- und Pool-Einstellungen angeben. Nicht alle Einstellungen gelten für alle Typen manueller Pools.

[Tabelle 6-2. Einstellungen für manuelle Desktop-Pools](#) werden die Einstellungen aufgeführt, die für mit diesen Eigenschaften konfigurierte manuelle Desktop-Pools gelten:

- Dedizierte Benutzerzuweisungen
- Dynamische Benutzerzuweisungen
- Verwaltete Maschinen (virtuelle Maschinen mit vCenter Server)
- Nicht verwaltete Maschinen

Diese Einstellungen gelten auch für einen manuellen Pool mit einer einzigen Maschine.

Beschreibungen der einzelnen Desktop-Einstellungen finden Sie unter [Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen](#).

**Tabelle 6-2. Einstellungen für manuelle Desktop-Pools**

| <b>Einstellung</b>  | <b>Manueller verwalteter Pool, dedizierte Zuweisung</b> | <b>Manueller verwalteter Pool, dynamische Zuweisung</b> | <b>Manueller nicht verwalteter Pool, dedizierte Zuweisung</b>  | <b>Manueller nicht verwalteter Pool, dynamische Zuweisung</b>  |
|---|---|---|--|--|
| Status  | Ja  | Ja  | Ja   | Ja   |
| Einschränkungen für Verbindungsserver   | Ja  | Ja  | Ja   | Ja   |
| Betriebsrichtlinie für Remote-Computer  | Ja  | Ja  |  |  |
| Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden) | Ja  | Ja  | Ja   | Ja   |
| Benutzern das Zurücksetzen ihrer Computer gestatten                               | Ja  | Ja  |  |  |
| Mehrere Sitzungen pro Benutzer zulassen   |   | Ja  |  | Ja   |
| Standardanzeigeprotokoll  | Ja  | Ja  | Ja<br>Um PCoIP mit einer Maschine zu verwenden, die nicht von vCenter Server verwaltet wird, müssen Sie Teradici-Hardware auf der Maschine installieren. | Ja<br>Um PCoIP mit einer Maschine zu verwenden, die nicht von vCenter Server verwaltet wird, müssen Sie Teradici-Hardware auf der Maschine installieren. |
| Benutzern die Wahl des Protokolls erlauben  | Ja  | Ja  | Ja   | Ja   |
| 3D-Renderer   | Ja  | Ja  |  |  |
| Max number of monitors (Maximale Anzahl an Monitoren)                             | Ja  | Ja  |  |  |
| Max resolution of any one monitor (Max. Auflösung eines Monitors)                 | Ja  | Ja  |  |  |

| <b>Einstellung</b>                              | <b>Manueller verwalteter Pool, dedizierte Zuweisung</b> | <b>Manueller verwalteter Pool, dynamische Zuweisung</b> | <b>Manueller nicht verwalteter Pool, dedizierte Zuweisung</b> | <b>Manueller nicht verwalteter Pool, dynamische Zuweisung</b> |
|---|---|---|---|---|
| Adobe Flash quality (Adobe Flash-Qualität)      | Ja  | Ja  | Ja  | Ja  |
| Adobe Flash throttling (Adobe Flash-Drosselung) | Ja  | Ja  | Ja  | Ja  |
| Globale Mirage-Einstellungen überschreiben      | Ja  | Ja  | Ja  | Ja  |
| Mirage-Serverkonfiguration                      | Ja  | Ja  | Ja  | Ja  |



# Einrichten von Remote-Desktop-Dienste-Hosts

# 7

Hosts mit Microsoft Remote Desktop Services (RDS) stellen Desktop-Sitzungen und Anwendungen bereit, auf die Benutzer von Clientgeräten aus zugreifen können. Falls Sie vorhaben, RDS-Desktop-Pools oder Anwendungspools zu erstellen, müssen Sie zunächst RDS-Hosts einrichten.

Dieses Kapitel enthält die folgenden Themen:

- [RDS-Hosts](#)
- [Installieren von „Remotedesktopdienste“ auf Windows Server 2008 R2](#)
- [Installieren von Remotedesktopdiensten auf Windows Server 2012 oder Windows Server 2012 R2](#)
- [Installieren von „Desktopdarstellung“ auf Windows Server 2008 R2](#)
- [Installieren von „Desktopdarstellung“ auf Windows Server 2012 oder Windows Server 2012 R2](#)
- [Einschränken von Benutzern auf eine einzelne Sitzung](#)
- [Installation von View Agent auf einem Remote-Desktop-Dienste-Host](#)
- [Aktivieren der Zeitzone-Umleitung für RDS-Desktop- und Anwendungssitzungen](#)
- [Aktivieren des Windows-Basisdesigns für Anwendungen](#)
- [Konfigurieren der Gruppenrichtlinie zum Ausführen von Start Runonce.exe](#)
- [RDS-Host-Performance-Optionen](#)

## RDS-Hosts

Ein RDS-Host ist ein Server-Computer, der Anwendungen und Desktop-Sitzungen für den Remote-Zugriff hostet. Ein RDS-Host kann eine virtuelle Maschine oder ein physischer Server sein.

In View ist ein RDS-Host ein Server, der die Rolle Microsoft-Remote-Desktop-Dienste innehat, bei dem der Microsoft Remote-Desktop-Sitzungshost-Dienst aktiviert und View Agent installiert ist. Remote-Desktop-Dienste waren vorher unter dem Namen Terminaldienste bekannt. Der Remote-Desktop-Sitzungshost-Dienst ermöglicht es einem Server, Anwendungen und Remote-Desktop-Sitzungen zu hosten. Bei installiertem View Agent auf einem RDS-Host können Benutzer unter Verwendung des Anzeigeprotokolls PCoIP eine Verbindung zu Anwendungen und Desktop-Sitzungen herstellen. PCoIP bietet eine optimierte Benutzererfahrung für die Bereitstellung von Remote-Inhalten, einschließlich Bildern, Audio und Video.

Die Leistung eines RDS-Hosts hängt von vielen Faktoren ab. Informationen zur Feineinstellung der Leistung unterschiedlicher Versionen von Windows Server finden Sie unter <http://msdn.microsoft.com/library/windows/hardware/gg463392.aspx>.

View unterstützt maximal eine Desktop-Sitzung und eine Anwendungssitzung pro Benutzer auf einem RDS-Host.

Wenn Benutzer gleichzeitig Druckaufträge von RDS-Desktops oder -Anwendungen senden, die sich auf demselben RDS-Host befinden, verarbeitet der ThinPrint-Server auf dem RDS-Host die Druckaufträge seriell und nicht parallel. Dies führt bei einigen Benutzern zu Verzögerungen. Beachten Sie, dass der Druckserver nicht die Fertigstellung eines Druckauftrags abwartet, bevor er den nächsten verarbeitet. Druckaufträge, die an verschiedene Drucker gesendet werden, werden parallel ausgeführt.

Wenn ein Benutzer eine Anwendung und einen RDS-Desktop startet und sich beide auf demselben RDS-Host befinden, teilen sie dasselbe Benutzerprofil. Wenn ein Benutzer eine Anwendung vom Desktop aus startet, können Konflikte auftreten, wenn beide Anwendungen versuchen, auf dieselben Teile des Benutzerprofils zuzugreifen bzw. diese zu ändern. Eine der beiden Anwendungen wird möglicherweise nicht mehr ordnungsgemäß ausgeführt.

Die Einrichtung von Anwendungen oder RDS-Desktops für den Remotezugriff beinhaltet folgende Aufgaben:

- 1 Richten Sie RDS-Hosts ein.
- 2 Erstellen Sie eine Farm. Siehe [Kapitel 8 Erstellen von Farmen](#).
- 3 Erstellen Sie einen Anwendungspool oder einen RDS-Desktop-Pool. Siehe [Kapitel 9 Erstellen von Anwendungspools](#) oder [Kapitel 10 Erstellen von RDS-Desktop-Pools](#).
- 4 Berechtigen von Benutzern und Gruppen. Siehe [Kapitel 12 Berechtigen von Benutzern und Gruppen](#).
- 5 (Optional) Aktivieren der Zeitzonenumleitung für RDS-Desktop- und Anwendungssitzungen. Siehe [Aktivieren der Zeitzone-Umleitung für RDS-Desktop- und Anwendungssitzungen](#).

---

**Vorsicht** Wenn ein Benutzer eine Anwendung wie beispielsweise einen Webbrowser startet, kann er Zugriff auf die lokalen Laufwerke auf dem RDS-Host erlangen, der die Anwendung hostet. Dies kann geschehen, wenn die Anwendung Funktionen bereitstellt, durch die Windows Explorer aufgerufen wird. Um diese Art von Zugriff auf den RDS-Host zu verhindern, folgen Sie der Vorgehensweise, die unter <http://support.microsoft.com/kb/179221> beschrieben ist, um zu verhindern, dass eine Anwendung Windows Explorer ausführt.

Da die unter <http://support.microsoft.com/kb/179221> beschriebene Vorgehensweise Auswirkungen sowohl auf Desktop- als auch auf Anwendungssitzungen hat, empfiehlt es sich, keine RDS-Desktop-Pools und Anwendungspools auf derselben Farm zu erstellen, wenn Sie vorhaben, der Vorgehensweise im Microsoft KB-Artikel zu folgen, so dass Desktop-Sitzungen nicht betroffen sind.

---

## Installieren von Anwendungen

Wenn Sie vorhaben, Anwendungspools zu erstellen, müssen die Anwendungen auf den RDS-Hosts installiert werden. Falls View automatisch die Liste der installierten Anwendungen anzeigen soll, müssen Sie die Anwendungen so installieren, dass sie allen Benutzern über das **Start**-Menü zur Verfügung stehen. Sie können eine Anwendung jederzeit installieren, bevor Sie den Anwendungspool erstellen. Wenn Sie vorhaben, eine Anwendung manuell anzugeben, können Sie die Anwendung jederzeit installieren, entweder vor oder nach der Erstellung eines Anwendungspools.

---

**Wichtig** Wenn Sie eine Anwendung installieren, müssen Sie sie auf allen RDS-Hosts in einer Farm und am selben Speicherort auf jedem RDS-Host installieren. Andernfalls wird eine Systemzustandswarnung auf dem View Administrator-Dashboard angezeigt. In einer solchen Situation tritt beim Erstellen eines Anwendungspools bei Benutzern ein Fehler auf, wenn sie versuchen, die Anwendung auszuführen.

---

Wenn Sie einen Anwendungspool erstellen, zeigt View im **Start**-Menü auf allen RDS-Hosts in einer Farm automatisch die Anwendungen an, die allen Benutzern statt nur einzelnen Benutzern zur Verfügung stehen. Sie können beliebige Anwendungen aus dieser Liste auswählen. Zusätzlich können Sie eine Anwendung, die nicht allen Benutzern über das **Start**-Menü zur Verfügung steht, manuell angeben. Bezüglich der Anzahl der Anwendungen, die Sie auf einem RDS-Host installieren können, gibt es keine Einschränkung.

## Installieren von „Remotedesktopdienste“ auf Windows Server 2008 R2

„Remotedesktopdienste“ (RDS) bezeichnet eine der Rollen, die ein Windows Server übernehmen kann. Sie müssen diese Rolle installieren, um einen RDS-Host einzurichten, auf dem Windows Server 2008 R2 ausgeführt wird.

### Voraussetzungen

- Stellen Sie sicher, dass der RDS-Host Windows Server 2008 R2 Service Pack 1 (SP1) ausführt.
- Überprüfen Sie, ob der RDS-Host Teil der Active Directory-Domäne für die View-Bereitstellung ist.
- Installieren Sie das Microsoft Hotfixrollup, das auf <http://support.microsoft.com/kb/2775511> dokumentiert ist.

### Verfahren

- 1 Melden Sie sich beim RDS-Host als Administrator an.
- 2 Starten Sie Server Manager.
- 3 Wählen Sie in der Navigationsstruktur **Rollen** aus.
- 4 Klicken Sie auf **Rollen hinzufügen**, um den Assistenten **Rolle hinzufügen** zu starten.
- 5 Wählen Sie die Rolle **Remotedesktopdienste**.
- 6 Wählen Sie auf der Seite „Rollen-Dienste auswählen“ die Option **Remote-Desktop-Sitzungshost**.

- 7 Wählen Sie auf der Seite zur Angabe der Authentifizierungsmethode entweder **Authentifizierung auf Netzwerkebene erforderlich** oder **Authentifizierung auf Netzwerkebene nicht erforderlich**, je nachdem, was zutrifft.
- 8 Wählen Sie auf der Seite zur Konfiguration der Clienterfahrung die Funktionen, die Sie Benutzern bereitstellen möchten.
- 9 Folgen Sie den Anweisungen und schließen Sie die Installation ab.

#### Nächste Schritte

Wenn Sie beabsichtigen, HTML Access oder Scannerumleitung zu verwenden, müssen Sie die Funktion „Desktopdarstellung“ installieren. Die Schritte zur Installation von „Desktopdarstellung“ unterscheiden sich je nachdem, ob die Installation auf Windows Server 2008 R2 oder auf Windows Server 2012 bzw. Windows Server 2012 R2 erfolgt.

Beschränken Sie Benutzer auf eine einzelne Desktop-Sitzung. Siehe [Einschränken von Benutzern auf eine einzelne Sitzung](#).

## Installieren von Remotedesktopdiensten auf Windows Server 2012 oder Windows Server 2012 R2

Remotedesktopdienste ist eine der Rollen, die ein Windows Server 2012 oder 2012 R2 übernehmen kann. Sie müssen diese Rolle installieren, um einen RDS-Host einzurichten.

#### Voraussetzungen

- Stellen Sie sicher, dass auf dem RDS-Host Windows Server 2012 oder Windows Server 2012 R2 ausgeführt wird.
- Überprüfen Sie, ob der RDS-Host Teil der Active Directory-Domäne für die View-Bereitstellung ist.

#### Verfahren

- 1 Melden Sie sich beim RDS-Host als Administrator an.
- 2 Starten Sie Server Manager.
- 3 Wählen Sie **Rollen und Funktionen hinzufügen**.
- 4 Wählen Sie auf der Seite „Installationstyp auswählen“ **Rollenbasierter oder funktionsbasierter Installationstyp** aus.
- 5 Wählen Sie auf der Seite „Zielserver auswählen“ einen Server aus.
- 6 Wählen Sie auf der Seite „Serverrollen auswählen“ die Option **Remotedesktopdienste**.
- 7 Bestätigen Sie auf der Seite „Funktionen auswählen“ die Standardeinstellungen.
- 8 Wählen Sie auf der Seite „Rollen-Dienste auswählen“ die Option **Remote-Desktop-Sitzungshost**.
- 9 Folgen Sie den Anweisungen und schließen Sie die Installation ab.

## Nächste Schritte

Wenn Sie beabsichtigen, HTML Access oder Scannerumleitung zu verwenden, müssen Sie die Funktion „Desktopdarstellung“ installieren. Die Schritte zur Installation von „Desktopdarstellung“ unterscheiden sich je nachdem, ob die Installation auf Windows Server 2008 R2 oder auf Windows Server 2012 bzw. Windows Server 2012 R2 erfolgt.

Beschränken Sie Benutzer auf eine einzelne Desktop-Sitzung. Siehe [Einschränken von Benutzern auf eine einzelne Sitzung](#).

## Installieren von „Desktopdarstellung“ auf Windows Server 2008 R2

Für RDS-Desktops und -Anwendungen und für VDI-Desktops, die auf Einzelbenutzer-VMs mit Windows Server bereitgestellt werden, erfordert die Scannerumleitung, dass Sie die Funktion „Desktopdarstellung“ auf den RDS-Hosts und den Einzelbenutzer-VMs installieren.

### Verfahren

- 1 Melden Sie sich als Administrator an.
- 2 Starten Sie Server Manager.
- 3 Klicken Sie auf **Features**.
- 4 Klicken Sie auf **Features hinzufügen**.
- 5 Aktivieren Sie auf der Seite „Features auswählen“ das Kontrollkästchen **Desktopdarstellung**.
- 6 Lesen Sie die Informationen zu anderen Funktionen, die die Funktion „Desktopdarstellung“ benötigt, und klicken Sie auf **Erforderliche Features hinzufügen**.
- 7 Folgen Sie den Anweisungen und schließen Sie die Installation ab.

## Installieren von „Desktopdarstellung“ auf Windows Server 2012 oder Windows Server 2012 R2

Für RDS-Desktops und -Anwendungen und für VDI-Desktops, die auf Einzelbenutzer-VMs mit Windows Server bereitgestellt werden, erfordert die Scannerumleitung, dass Sie die Funktion „Desktopdarstellung“ auf den RDS-Hosts und den Einzelbenutzer-VMs installieren.

### Verfahren

- 1 Melden Sie sich als Administrator an.
- 2 Starten Sie Server Manager.
- 3 Wählen Sie **Rollen und Funktionen hinzufügen**.
- 4 Wählen Sie auf der Seite „Installationstyp auswählen“ **Rollenbasierter oder funktionsbasierter Installationstyp** aus.

- 5 Wählen Sie auf der Seite „Zielserver auswählen“ einen Server aus.
- 6 Übernehmen Sie auf der Seite „Serverrollen auswählen“ die Standardauswahl und klicken Sie auf **Weiter**.
- 7 Wählen Sie auf der Seite „Funktionen auswählen“ unter **Benutzeroberflächen und Infrastruktur** die Option **Desktopdarstellung** aus.
- 8 Folgen Sie den Anweisungen und schließen Sie die Installation ab.

## Einschränken von Benutzern auf eine einzelne Sitzung

View unterstützt maximal eine Desktop-Sitzung und eine Anwendungssitzung pro Benutzer auf einem RDS-Host. Sie müssen den RDS-Host konfigurieren, um Benutzer auf eine einzelne Sitzung zu beschränken.

### Voraussetzungen

- Installieren Sie die Remote-Desktop-Dienste-Rolle wie in [Installieren von „Remotedesktopdienste“ auf Windows Server 2008 R2](#) bzw. [Installieren von Remotedesktopdiensten auf Windows Server 2012 oder Windows Server 2012 R2](#) beschrieben.

### Verfahren

- 1 Klicken Sie auf **Start > Verwaltung > Remote-Desktop-Dienste > Hostkonfiguration von Remote-Desktop-Sitzungen**.
- 2 Doppelklicken Sie Fensterbereich „Einstellungen bearbeiten“ unter „Allgemein“ auf **Jeden Benutzer auf eine einzelne Sitzung beschränken**.
- 3 Wählen Sie im Dialogfeld „Eigenschaften“ auf der Registerkarte „Allgemein“ **Jeden Benutzer auf eine einzelne Sitzung beschränken** und klicken Sie auf **OK**.

### Nächste Schritte

Installieren Sie View Agent auf dem RDS-Host. Siehe [Installation von View Agent auf einem Remote-Desktop-Dienste-Host](#).

## Installation von View Agent auf einem Remote-Desktop-Dienste-Host

View Agent kommuniziert mit dem View-Verbindungsserver und unterstützt das PCoIP-Anzeigeprotokoll. Sie müssen View Agent auf einem RDS-Host installieren.

### Voraussetzungen

- Installieren Sie die Remote-Desktop-Dienste-Rolle wie in [Installieren von „Remotedesktopdienste“ auf Windows Server 2008 R2](#) bzw. [Installieren von Remotedesktopdiensten auf Windows Server 2012 oder Windows Server 2012 R2](#) beschrieben.

- Beschränken Sie Benutzer auf eine einzelne Desktop-Sitzung. Siehe [Einschränken von Benutzern auf eine einzelne Sitzung](#).
- Machen Sie sich mit den benutzerdefinierten Setup-Optionen für View Agent vertraut. Siehe [Benutzerdefinierte Setup-Optionen für View Agent für einen RDS-Host](#).
- Laden Sie die View Agent-Installationsdatei von der VMware-Produktseite unter <http://www.vmware.com/products/> herunter.

## Verfahren

- 1 Melden Sie sich als Administrator an.
- 2 Zum Starten des View Agent-Installationsprogramms doppelklicken Sie auf die Installationsdatei.  
Der Dateiname des Installationsprogramms lautet VMware-viewagent-x86\_64-y.y.y-xxxxxx.exe, wobei y.y.y die Versionsnummer und xxxxxx die Buildnummer ist.
- 3 Wählen Sie Ihre benutzerdefinierten Setup-Optionen.
- 4 Geben Sie im Textfeld **Server** den Hostnamen oder die IP-Adresse eines View-Verbindungsserverhosts ein.

Während der Installation registriert das Installationsprogramm den RDS-Host bei dieser View-Verbindungsserver-Instanz. Nach der Registrierung können die angegebene View-Verbindungsserver-Instanz sowie alle zusätzlichen Instanzen in derselben View-Verbindungsserver-Gruppe mit dem RDS-Host kommunizieren.

- 5 Wählen Sie eine Authentifizierungsmethode zur Registrierung des RDS-Hosts für die View-Verbindungsserver-Instanz aus.

| Option   | Beschreibung  |
|--|---|
| <b>Authentifizierung als aktuell angemeldeter Benutzer</b> | Die Textfelder <b>Benutzername</b> und <b>Kennwort</b> sind deaktiviert und die Anmeldung bei der View-Verbindungsserver-Instanz erfolgt anhand der aktuellen Anmeldeinformationen. |
| <b>Angeben von Administratoranmeldeinformationen</b>       | In die Textfelder <b>Benutzername</b> und <b>Kennwort</b> müssen der Benutzername und das Kennwort eines View-Verbindungsserver-Administrators eingegeben werden.                   |

Beim Benutzerkonto muss es sich um einen Domänenbenutzer mit Zugang zu View LDAP auf der View-Verbindungsserver-Instanz handeln. Ein lokales Benutzerkonto funktioniert nicht.

- 6 Folgen Sie den Anweisungen und schließen Sie die Installation ab.

## Nächste Schritte

Erstellen Sie eine Farm. Siehe [Kapitel 8 Erstellen von Farmen](#).

## Benutzerdefinierte Setup-Optionen für View Agent für einen RDS-Host

Wenn Sie View Agent auf einem RDS-Host installieren, können Sie benutzerdefinierte Setup-Optionen auswählen. Zusätzlich installiert View Agent bestimmte Funktionen automatisch auf allen Gastbetriebssystemen, auf denen sie unterstützt werden. Diese Funktionen sind nicht optional.

**Tabelle 7-1. Benutzerdefinierte Setup-Optionen von View Agent für einen RDS-Host**

| Option                           | Beschreibung  |
|----------------------------------|---|
| vCenter Operations Manager-Agent | Ermöglicht das Zusammenwirken von View und vCenter Operations Manager for Horizon.  |
| Scannerumleitung                 | <p>Leitet Scangeräte um, die mit dem Clientsystem verbunden sind, sodass diese auf dem RDS-Desktop oder in einer RDS-Anwendung verwendet werden können.</p> <p>Sie müssen die Funktion „Desktopdarstellung“ im Windows Server-Betriebssystem auf den RDS-Hosts installieren, damit diese Option im View Agent-Installationsprogramm zur Verfügung steht.</p> <p>Diese Setup-Option wird standardmäßig nicht auf Windows Server-Gastbetriebssystemen installiert. Um sie zu installieren, müssen Sie die Option auswählen.</p> <p>Die Scannerumleitung ist in den Versionen Horizon 6.0.2 und höher verfügbar.</p> |

**Tabelle 7-2. View Agent-Funktionen, die automatisch auf einem RDS-Host installiert werden**

| Option      | Beschreibung   |
|-------------|--|
| PCoIP-Agent | <p>Ermöglicht es Benutzern, eine Verbindung zu Anwendungen und RDS-Desktops unter Zuhilfenahme des PCoIP-Anzeigeprotokolls herzustellen.</p> <p>Sie müssen diese Komponente installieren, wenn Sie vorhaben, Anwendungspools zu erstellen, da Benutzer nur eine Verbindung zu Anwendungen über PCoIP herstellen können.</p>                                      |
| Unity Touch | Ermöglicht es Tablet- und Smartphone-Benutzern, mit Windows-Anwendungen zu interagieren, die auf dem Remote-Desktop ausgeführt werden. Benutzer können Windows-Anwendungen und -Dateien durchsuchen und öffnen, bevorzugte Anwendungen und Dateien auswählen und zwischen laufenden Anwendungen umschalten, ohne das Startmenü oder die Taskleiste zu verwenden. |
| PSG Agent   | Installiert das PCoIP Secure Gateway auf RDS-Hosts, um das PCoIP-Anzeigeprotokoll für Desktop- und Anwendungssitzungen zu implementieren, die auf RDS-Hosts ausgeführt werden.   |
| VMwareRDS   | Bietet die VMware-Implementierung der Remotedesktopdienste-Funktion (RDS).   |

Weitere Funktionen, die auf RDS-Hosts unterstützt werden, finden Sie unter „Funktionsunterstützungsmatrix für View Agent“ im Dokument *Planung der View-Architektur*.



## Aktivieren der Zeitzonen-Umleitung für RDS-Desktop- und Anwendungssitzungen

Falls ein RDS-Host sich in einer Zeitzone befindet und ein Benutzer sich in einer anderen Zeitzone befindet, wenn der Benutzer eine Verbindung mit einem RDS-Desktop herstellt, zeigt der Desktop die Zeitzone an, die sich in der Zeitzone des RDS-Hosts befindet. Sie können die Gruppenrichtlinieneinstellung „Zeitzonen-Umleitung“ aktivieren, um sicherzustellen, dass der RDS-Desktop die Zeit in der lokalen Zeitzone anzeigt. Die Richtlinieneinstellung gilt auch für Anwendungssitzungen.

### Voraussetzungen

- Stellen Sie sicher, dass die Funktion „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server verfügbar ist.  
  
Die Schritte zum Öffnen der Verwaltungskonsolle für Gruppenrichtlinien unterscheiden sich in den Versionen Windows 2012, Windows 2008 und Windows 2003 Active Directory. Siehe [Erstellen von GPOs für View-Gruppenrichtlinien](#).
- Stellen Sie sicher, dass die ADMX-Dateien von View-Remotedesktopdiensten zu Active Directory hinzugefügt werden. Siehe [Hinzufügen der ADMX-Dateien der Remote-Desktop-Dienste zu Active Directory](#).
- Machen Sie sich mit den Gruppenrichtlinieneinstellungen vertraut. Siehe [Einstellungen zur Umleitung von RDS-Geräten und Ressourcen](#).

### Verfahren

- 1 Öffnen Sie auf dem Active Directory-Server die Verwaltungskonsolle für Gruppenrichtlinien.
- 2 Erweitern Sie Ihre Domäne und die **Gruppenrichtlinienobjekte**.
- 3 Klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **Bearbeiten** aus.
- 4 Navigieren Sie im Gruppenrichtlinienverwaltungs-Editor zu **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > RDSH-Dienste anzeigen > Remote-Desktop-Sitzungshost > Umleitung von Geräten und Ressourcen**.
- 5 Aktivieren Sie die Einstellung **Zeitzonen-Umleitung** zulassen.

## Aktivieren des Windows-Basisdesigns für Anwendungen

Wenn ein Benutzer zuvor noch nie eine Verbindung zu einem Desktop auf einem RDS-Host hergestellt hat und nun eine auf diesem RDS-Host gehostete Anwendung startet, wird das Windows-Basisdesign nicht auf die Anwendung angewendet, auch wenn eine GPO-Einstellung zum Laden des Aero-Designs konfiguriert wurde. View unterstützt nicht das Aero-Design, aber das Windows-Basisdesign. Damit das Windows-Basisdesign auf die Anwendung angewendet wird, müssen Sie eine weitere GPO-Einstellung konfigurieren.

## Voraussetzungen

- Stellen Sie sicher, dass die Funktion „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server verfügbar ist.

Die Schritte zum Öffnen der Verwaltungskonsole für Gruppenrichtlinien unterscheiden sich in den Versionen Windows 2012, Windows 2008 und Windows 2003 Active Directory. Siehe [Erstellen von GPOs für View-Gruppenrichtlinien](#).

## Verfahren

- 1 Öffnen Sie auf dem Active Directory-Server die Verwaltungskonsole für Gruppenrichtlinien.
- 2 Erweitern Sie Ihre Domäne und die **Gruppenrichtlinienobjekte**.
- 3 Klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **Bearbeiten** aus.
- 4 Navigieren Sie im Gruppenrichtlinienverwaltungs-Editor zu **Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > Systemsteuerung > Personalisierung**.
- 5 Aktivieren Sie die Einstellung **Bestimmten visuellen Stil oder Windows – klassisch erzwingen** und geben Sie für den Pfad zum visuellen Stil `%windir%\Ressourcen\Themen\Aero\ aero.msstyles` an.

# Konfigurieren der Gruppenrichtlinie zum Ausführen von Start Runonce.exe

Anwendungen, die auf der Datei Explorer.exe basieren, werden in einer Anwendungssitzung möglicherweise nicht ausgeführt. Konfigurieren Sie eine GPO-Einstellung für den Start von runonce.exe, um dieses Problem zu vermeiden.

## Voraussetzungen

- Stellen Sie sicher, dass die Funktion „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server verfügbar ist.

Die Schritte zum Öffnen der Verwaltungskonsole für Gruppenrichtlinien unterscheiden sich in den Versionen Windows 2012, Windows 2008 und Windows 2003 Active Directory. Siehe [Erstellen von GPOs für View-Gruppenrichtlinien](#).

## Verfahren

- 1 Öffnen Sie auf dem Active Directory-Server die Verwaltungskonsole für Gruppenrichtlinien.
- 2 Erweitern Sie Ihre Domäne und die **Gruppenrichtlinienobjekte**.
- 3 Klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **Bearbeiten** aus.
- 4 Navigieren Sie im Gruppenrichtlinienverwaltungs-Editor zu **Benutzerkonfiguration > Richtlinien > Windows-Einstellungen > Anmelde- bzw. Abmeldeskripts**.

- 5 Doppelklicken Sie auf **Anmeldung** und klicken Sie anschließend auf **Hinzufügen**.
- 6 Geben Sie in das Feld „Skriptname“ **runonce.exe** ein.
- 7 Geben Sie in das Feld „Skriptparameter“ **/AlternateShellStartup** ein.

## RDS-Host-Performance-Optionen

Sie können Windows durch Festlegen von Performance-Optionen entweder für Vordergrundprogramme oder für Hintergrunddienste optimieren. Standardmäßig deaktiviert View bestimmte Performance-Optionen für RDS-Hosts für alle unterstützten Versionen von Windows Server.

Die folgende Tabelle zeigt die Performance-Optionen, die von View deaktiviert werden.

**Tabelle 7-3. Von View deaktivierte Performance-Optionen**

| Von View deaktivierte Performance-Optionen                        |
|---|
| Fenster beim Minimieren und Maximieren animieren                  |
| Schatten unter Mauszeiger anzeigen                                |
| Schatten unter Fenstern anzeigen                                  |
| Schlagschatten für Symbolbeschriftungen auf dem Desktop verwenden |
| Fensterinhalte beim Ziehen anzeigen                               |

Die fünf Performance-Optionen, die von View deaktiviert werden, entsprechen vier View-Einstellungen in der Registrierung. Die folgende Tabelle zeigt die View-Einstellungen und ihre standardmäßigen Registrierungswerte. Die Registrierungswerte befinden sich alle im Registrierungsunterschlüssel `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration`. Sie können die Performance-Optionen erneut aktivieren, indem Sie einen oder mehrere View-Registrierungswerte auf **false** setzen.

**Tabelle 7-4. View-Einstellungen für Windows-Performance-Optionen**

| View-Einstellung                         | Registrierungswert     |
|--|------------------------|
| Mauszeigerschatten deaktivieren          | DisableMouseShadows    |
| Vollständiges Fensterziehen deaktivieren | DisableFullWindowDrag  |
| Schatten der Listenansicht deaktivieren  | DisableListViewShadow  |
| Fensteranimation deaktivieren            | DisableWindowAnimation |

# Erstellen von Farmen

Eine Farm ist eine Gruppe von RDS-Hosts, die Benutzern einen gemeinsamen Satz von Anwendungen oder RDS-Desktops bereitstellt.

Dieses Kapitel enthält die folgenden Themen:

- [Farmen](#)
- [Arbeitsblatt zum Erstellen einer Farm](#)
- [Erstellen einer Farm](#)

## Farmen

Farmen vereinfachen die Verwaltung von RDS-Hosts, RDS-Desktops und Anwendungen in einem Unternehmen. Sie können Farmen erstellen, die Benutzergruppen dienen, die unterschiedlich groß sind oder unterschiedliche Desktop- oder Anwendungsanforderungen haben.

Wenn Sie einen Anwendungspool oder einen RDS-Desktop-Pool erstellen, müssen Sie genau eine Farm angeben. Die RDS-Hosts in einer Farm können RDS-Desktops, Anwendungen oder beides hosten. Eine Farm kann maximal einen RDS-Desktop-Pool, aber mehrere Anwendungspools unterstützen. Eine Farm kann beide Pooltypen gleichzeitig unterstützen.

Farmen bieten folgende Vorteile:

- **Lastausgleich**  
Standardmäßig gleicht View die Lasten der RDS-Desktop-Sitzungen und der Anwendungssitzungen über alle RDS-Hosts in der Farm hinweg aus.
- **Redundanz**  
Falls ein RDS-Host in einer Farm offline geht, stellen die anderen RDS-Hosts in der Farm weiterhin Anwendungen und Desktops für Benutzer bereit.
- **Skalierbarkeit**  
Eine Farm kann eine variable Anzahl von RDS-Hosts haben. Sie können Farmen mit unterschiedlichen Anzahlen von RDS-Hosts erstellen, die Benutzergruppen unterschiedlicher Größe dienen.

Farmen haben folgende Eigenschaften:

- Ein View-Pod kann maximal 200 Farmen haben.

- Eine Farm darf maximal 200 RDS-Hosts haben.
- Die RDS-Hosts in einer Farm können eine beliebige unterstützte Version von Windows Server ausführen. Siehe hierzu „Systemanforderungen für Gastbetriebssysteme“ im Dokument *Installation von View*.

**Wichtig** Microsoft empfiehlt die separate Konfiguration von Roaming-Profilen für Benutzer für jede Farm. Die Profile sollten nicht zwischen Farmen oder physischen Desktops von Benutzern ausgetauscht werden, da es zur Beschädigung von Profilen und Datenverlust kommen kann, wenn ein Benutzer gleichzeitig bei zwei Maschinen, die dasselbe Profile geladen haben, angemeldet ist.

## Arbeitsblatt zum Erstellen einer Farm

Beim Erstellen einer Farm fordert der Assistent **Farm hinzufügen** Sie zum Konfigurieren von bestimmten Optionen auf.

Sie können dieses Arbeitsblatt drucken und die Werte notieren, die Sie bei Ausführung des Assistenten **Farm hinzufügen** angeben möchten.

**Tabelle 8-1. Arbeitsblatt: Konfigurationsoptionen zum Erstellen einer Farm**

| Option                   | Beschreibung  | Wert hier eingeben |
|--------------------------|---|--------------------|
| ID                       | Der eindeutige Name, der die Farm in View Administrator identifiziert.  |                    |
| Beschreibung             | Beschreibung dieser Farm.   |                    |
| Zugriffsgruppe           | Zugriffsgruppe, in der alle Pools in dieser Farm platziert werden sollen.<br>Wenn Sie eine Zugriffsgruppe verwenden, können Sie die Verwaltung des Pools an einen Administrator mit einer bestimmten Rolle delegieren. Weitere Informationen finden Sie im Kapitel zur rollenbasierten Verwaltungsdelegation im Dokument <i>Verwaltung von View</i> .   |                    |
| Standardanzeigeprotokoll | Wählen Sie <b>PCoIP</b> oder <b>RDP</b> aus. Diese Einstellung gilt nur für Desktop-Pools. Beim Anzeigeprotokoll für Anwendungspools handelt es sich immer um <b>PCoIP</b> . Wenn Sie <b>RDP</b> auswählen und diese Farm für das Hosten von Anwendungspools verwenden möchten, müssen Sie die Option <b>Benutzern die Wahl des Protokolls erlauben</b> auf <b>Ja</b> festlegen. Die Standardeinstellung ist <b>PCoIP</b> . |                    |

| Option  | Beschreibung  | Wert hier eingeben |
|---|---|--------------------|
| Benutzern die Wahl des Protokolls erlauben              | Wählen Sie <b>Ja</b> oder <b>Nein</b> aus. Diese Option gilt nur für RDS-Desktop-Pools. Wenn Sie <b>Ja</b> auswählen, ermöglichen Sie es Benutzern, das Anzeigeprotokoll auszuwählen, wenn sie eine Verbindung zu einem RDS-Desktop über Horizon Client herstellen. Die Standardeinstellung ist <b>Ja</b> .   |                    |
| Zeitüberschreitung bei leerer Sitzung (nur Anwendungen) | Legt die Zeit fest, in der eine leere Anwendungssitzung geöffnet bleibt. Eine Anwendungssitzung ist leer, wenn alle Anwendungen, die in der Sitzung ausgeführt werden, geschlossen wurden. Benutzer können Anwendungen schneller öffnen, wenn die Sitzung geöffnet ist. Sie können Systemressourcen speichern, wenn Sie leere Anwendungssitzungen trennen oder abmelden. Wählen Sie <b>Nie</b> aus oder legen Sie die Anzahl der Minuten als Wert für die Zeitüberschreitung fest. Die Standardeinstellung ist <b>Nach 1 Minute</b> . |                    |
| Bei einer Zeitüberschreitung                            | Legt fest, ob eine leere Anwendungssitzung getrennt oder abgemeldet wurde, nachdem das Limit der <b>Zeitüberschreitung bei leerer Sitzung</b> erreicht wurde. Wählen Sie <b>Trennen</b> oder <b>Abmelden</b> aus. Eine abgemeldete Sitzung gibt Ressourcen frei. Das Öffnen einer Anwendung dauert jedoch länger. Die Standardeinstellung ist <b>Trennen</b> .  |                    |
| Getrennte Sitzung abmelden                              | Bestimmt, wann eine getrennte Sitzung abgemeldet wird. Diese Einstellung gilt sowohl für den Desktop als auch für die Anwendungssitzungen. Wählen Sie <b>Nie</b> , <b>Sofort</b> oder <b>Nach ... Minuten</b> aus. Wählen Sie <b>Sofort</b> oder <b>Nach ... Minuten</b> mit Bedacht aus. Wenn eine getrennte Sitzung abgemeldet wird, geht die Sitzung verloren. Die Standardeinstellung ist <b>Nie</b> .  |                    |

## Erstellen einer Farm

Sie erstellen eine Farm im Rahmen des Prozesses, bei dem Sie Benutzern Zugriff auf Anwendungen oder RDS-Desktops gewähren.

## Voraussetzungen

- Richten Sie die RDS-Hosts ein, die zu der Farm gehören. Siehe [Kapitel 7 Einrichten von Remote-Desktop-Dienste-Hosts](#).
- Vergewissern Sie sich, dass alle RDS-Hosts den Status „Verfügbar“ haben. Wählen Sie in View Administrator **View-Konfiguration > Registrierte Computer** und überprüfen Sie auf der Registerkarte „RDS-Hosts“ den Status jedes RDS-Hosts.
- Sammeln Sie die Konfigurationsinformationen, die Sie zum Erstellen der Farm bereitstellen müssen. Siehe [Arbeitsblatt zum Erstellen einer Farm](#).

## Verfahren

- 1 Klicken Sie in View Administrator auf **Ressourcen > Farmen**.
- 2 Klicken Sie auf **Hinzufügen**, um die Konfigurationsinformationen einzugeben, die Sie im Arbeitsblatt zusammengetragen haben.
- 3 Geben Sie Einstellungen für die Farm an und klicken Sie auf **Weiter**.
- 4 Wählen Sie die RDS-Hosts aus, die zu der Farm hinzugefügt werden sollen, und klicken Sie auf **Weiter**.
- 5 Klicken Sie auf **Fertig stellen**.

In View Administrator können Sie nun die Farm anzeigen, indem Sie auf **Ressourcen > Farmen** klicken.

## Nächste Schritte

Erstellen Sie einen Anwendungspool oder einen RDS-Desktop-Pool. Siehe [Kapitel 9 Erstellen von Anwendungspools](#) oder [Kapitel 10 Erstellen von RDS-Desktop-Pools](#).

# Erstellen von Anwendungspools

Bei einer Aufgabe, die Sie ausführen, um Benutzern Remote-Zugriff auf eine Anwendung zu gewähren, handelt es sich um das Erstellen eines Anwendungspools. Benutzer, die für einen Anwendungspool berechtigt sind, können über eine Vielzahl von Client-Geräten remote auf die Anwendung zugreifen.

Dieses Kapitel enthält die folgenden Themen:

- [Anwendungspools](#)
- [Arbeitsblatt zum manuellen Erstellen eines Anwendungspools](#)
- [Erstellen eines Anwendungspools](#)

## Anwendungspools

Bei Anwendungspools können Sie eine einzige Anwendung für viele Benutzer bereitstellen. Die Anwendung wird auf einer Farm mit RDS-Hosts ausgeführt.

Wenn Sie einen Anwendungspool erstellen, stellen Sie eine Anwendung im Datacenter bereit, auf die Benutzer von überall im Netzwerk aus zugreifen können. Eine Einführung in Anwendungspools finden Sie unter [Farmen, RDS-Hosts und Desktop- und Anwendungspools](#).

Ein Anwendungspool hat eine einzelne Anwendung und ist einer einzigen Farm zugewiesen. Um Fehler zu vermeiden, müssen Sie die Anwendung auf allen RDS-Hosts in der Farm installieren.

Wenn Sie einen Anwendungspool erstellen, zeigt View automatisch die Anwendungen an, die allen Benutzern zur Verfügung stehen, anstatt einzelnen Benutzern aus dem **Start**-Menü auf allen RDS-Hosts in der Farm. Sie können eine oder mehrere Anwendungen aus der Liste auswählen. Wenn Sie mehrere Anwendungen aus der Liste auswählen, wird ein separater Anwendungspool für jede Anwendung erstellt. Sie können auch manuell eine Anwendung angeben, die nicht auf der Liste aufgeführt ist. Wenn eine Anwendung, die Sie manuell angeben möchten, nicht bereits installiert ist, zeigt View eine Warnmeldung an.

Wenn Sie einen Anwendungspool erstellen, können Sie die Zugriffsgruppe, in der der Pool platziert werden soll, nicht angeben. Bei Anwendungspools und RDS-Desktop-Pools geben Sie die Zugriffsgruppe an, wenn Sie eine Farm erstellen.



# Arbeitsblatt zum manuellen Erstellen eines Anwendungspools

Wenn Sie einen Anwendungspool erstellen und manuell eine Anwendung angeben, fordert Sie der Assistent zum **Hinzufügen von Anwendungspools** zur Angabe von Informationen über die Anwendung auf. Die Anwendung muss zu diesem Zweck noch nicht auf einem RDS-Host installiert sein.

Wenn Sie eine Anwendung manuell angeben, können Sie dieses Arbeitsblatt ausdrucken und die Eigenschaften der betreffenden Anwendung notieren.

**Tabelle 9-1. Arbeitsblatt: Anwendungseigenschaften für das manuelle Erstellen eines Anwendungspools**

| Eigenschaft     | Beschreibung  | Wert hier eingeben |
|-----------------|---|--------------------|
| ID              | Eindeutiger Name, der den Pool in View Administrator identifiziert. Dieses Feld ist erforderlich.   |                    |
| Anzeigename     | Poolname, der Benutzern angezeigt wird, wenn sie sich bei Horizon Client anmelden. Wenn Sie keinen Anzeigenamen angeben, entspricht der angezeigte Name der ID. |                    |
| Version         | Version der Anwendung.  |                    |
| Veröffentlicher | Veröffentlicher der Anwendung.  |                    |
| Pfad            | Vollständiger Pfadname der Anwendung. Beispiel: C:\Programme\app1.exe. Dieses Feld ist erforderlich.  |                    |
| Startordner     | Vollständiger Pfadname des Startverzeichnisses der Anwendung.   |                    |
| Parameter       | Parameter zur Weitergabe an die Anwendung, wenn diese gestartet wird. Beispielsweise können Sie <code>-username user1 -loglevel 3</code> angeben.               |                    |
| Beschreibung    | Beschreibung dieses Anwendungspools.  |                    |

## Erstellen eines Anwendungspools

Erstellen Sie ein Anwendungspool als Teil des Prozesses, um Benutzern Zugriff auf eine Anwendung zu gewähren, die auf RDS-Hosts ausgeführt wird.

### Voraussetzungen

- Richten Sie RDS-Hosts ein. Siehe [Kapitel 7 Einrichten von Remote-Desktop-Dienste-Hosts](#).
- Erstellen Sie eine Farm, die die RDS-Hosts enthält. Siehe [Kapitel 8 Erstellen von Farmen](#).
- Wenn Sie das Anwendungspool manuell hinzufügen möchten, sammeln Sie Informationen über die Anwendung. Siehe [Arbeitsblatt zum manuellen Erstellen eines Anwendungspools](#).

## Verfahren

- 1 Klicken Sie in View Administrator auf **Katalog > Anwendungspools**.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

Wenn Sie einen Anwendungspool manuell hinzufügen möchten, verwenden Sie die im Arbeitsblatt gesammelten Konfigurationsinformationen. Wenn Sie Anwendungen aus der Liste auswählen, die View Administrator anzeigt, können Sie mehrere Anwendungen auswählen. Ein separater Pool wird für jede Anwendung erstellt.

In View Administrator können Sie nun das Anwendungspool anzeigen, indem Sie auf **Katalog > Anwendungspools** klicken.

## Nächste Schritte

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe [Kapitel 12 Berechtigen von Benutzern und Gruppen](#).

Stellen Sie sicher, dass Ihre Endbenutzer über Zugang zu Horizon Client 3.0 oder höher verfügen. Dies ist für die Unterstützung von RDS-Anwendungen notwendig.

# Erstellen von RDS-Desktop-Pools

10

Bei einer Aufgabe, die Sie ausführen, um Benutzern Remote-Zugriff auf sitzungsbasierte Desktops zu gewähren, handelt es sich um das Erstellen eines Remote-Desktop-Dienste-Desktop-Pools. Ein RDS-Desktop-Pool enthält Eigenschaften, die einigen bestimmten Anforderungen einer Remote-Desktop-Bereitstellung entsprechen können.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zu RDS-Desktop-Pools](#)
- [Erstellen eines RDS-Desktop-Pools](#)
- [Desktop-Pool-Einstellungen für RDS-Desktop-Pools](#)
- [Konfigurieren der Adobe Flash-Drosselung mit Internet Explorer für RDS-Desktop-Pools](#)

## Grundlegendes zu RDS-Desktop-Pools

Der RDS-Desktop-Pool ist einer von drei Desktop-Pool-Typen, die Sie erstellen können. Dieser Pool-Typ wurde in früheren View-Versionen als Microsoft-Terminaldienste-Pool bezeichnet.

Ein RDS-Desktop-Pool und ein RDS-Desktop haben die folgenden Eigenschaften:

- Ein RDS-Desktop-Pool ist einer Farm, d. h. einer Gruppe von RDS-Hosts, zugeordnet. Jeder RDS-Host ist ein Windows-Server, der als Host für mehrere RDS-Desktops verwendet werden kann.
- Ein RDS-Desktop basiert auf einer Sitzung an einen RDS-Host. Im Gegensatz dazu basiert ein Desktop in einem automatisierten Desktop-Pool auf einer virtuellen Maschine und ein Desktop in einem manuellen Desktop-Pool auf einer virtuellen Maschine oder einem physischen Computer.
- Ein RDS-Desktop unterstützt die RDP-, PCoIP- und HTML Access-Anzeigeprotokolle. Informationen zum Aktivieren von HTML Access finden Sie unter „Ermöglichen des Zugriffs auf Desktops von RDS-Hosts in HTML Access“ im Kapitel „Konfigurieren von HTML Access für Endbenutzer“ im Dokument *Verwendung von HTML Access*, das Ihnen über [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html) zur Verfügung steht.
- Ein RDS-Desktop-Pool wird nur auf Windows Server-Betriebssystemen unterstützt, die ihrerseits die RDS-Rolle unterstützen und von View unterstützt werden. Siehe hierzu „Systemanforderungen für Gastbetriebssysteme“ im Dokument *Installation von View*.

- View ermöglicht einen Lastausgleich zwischen den RDS-Hosts einer Farm, indem Verbindungsanfragen an den RDS-Host geleitet werden, auf dem die geringste Anzahl aktiver Sitzungen vorliegt.
- Da ein RDS-Desktop-Pool sitzungsbasierte Desktops bereitstellt, unterstützt er keine Vorgänge, die spezifisch für einen Linked-Clone-Desktop-Pool sind, z. B. Aktualisierungen, Neuzusammenstellungen und Neuverteilungsvorgänge.
- Wenn es sich bei einem RDS-Host um eine virtuelle Maschine handelt, die von vCenter Server verwaltet wird, können Sie Snapshots als Basis-Images verwenden. Sie können vCenter Server zur Verwaltung der Snapshots einsetzen. Die Verwendung von Snapshots auf virtuellen RDS-Hostmaschinen ist für View transparent.
- View Persona Management wird von RDS-Desktops nicht unterstützt.
- Die Funktion für das Kopieren und Einfügen ist standardmäßig für HTML Access deaktiviert. Informationen zum Aktivieren der Funktion finden Sie unter „Gruppenrichtlinieneinstellungen für HTML Access“ im Kapitel „Konfigurieren von HTML Access für Endbenutzer“ im Dokument *Verwendung von HTML Access*, das Ihnen über [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html) zur Verfügung steht.

## Erstellen eines RDS-Desktop-Pools

Sie können einen RDS-Desktop-Pool als Teil des Vorgangs erstellen, um Benutzern Zugriff auf RDS-Desktops zu gewähren.

### Voraussetzungen

- Richten Sie RDS-Hosts ein. Siehe [Kapitel 7 Einrichten von Remote-Desktop-Dienste-Hosts](#).
- Erstellen Sie eine Farm, die die RDS-Hosts enthält. Siehe [Kapitel 8 Erstellen von Farmen](#).
- Entscheiden Sie, wie die Pool-Einstellungen konfiguriert werden sollen. Siehe [Desktop-Pool-Einstellungen für RDS-Desktop-Pools](#).

### Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie **RDS-Desktop-Pool** aus.
- 4 Geben Sie eine Pool-ID, einen Anzeigenamen und eine Beschreibung an.

Die Pool-ID ist der eindeutige Name, der den Pool in View Administrator identifiziert. Der Anzeigename ist der Name des RDS-Desktop-Pools, den Benutzer angezeigt bekommen, wenn sie sich bei Horizon Client anmelden. Wenn Sie keinen Anzeigenamen angeben, wird stattdessen die Pool-ID angezeigt.

- 5 Wählen Sie Pool-Einstellungen aus.
- 6 Wählen Sie eine Farm für diesen Pool aus oder erstellen Sie eine.

In View Administrator können Sie nun den RDS-Desktop-Pool anzeigen, indem Sie **Katalog > Desktop-Pools** auswählen.

### Nächste Schritte

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe [Hinzufügen von Berechtigungen zu einem Desktop- oder Anwendungspool](#).

Stellen Sie sicher, dass Ihre Endbenutzer Zugriff auf Horizon Client 3.0 oder höher haben. Diese Versionen sind für die Unterstützung von RDS-Desktop-Pools erforderlich.

## Desktop-Pool-Einstellungen für RDS-Desktop-Pools

Sie können bestimmte Pool-Einstellungen angeben, wenn Sie einen RDS-Desktop-Pool erstellen. Nicht alle Pool-Einstellungen gelten für alle Typen von Desktop-Pools.

Beschreibungen aller Pool-Einstellungen finden Sie unter [Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen](#). Die folgenden Pool-Einstellungen gelten für einen RDS-Desktop-Pool.

**Tabelle 10-1. Einstellungen für einen RDS-Desktop-Pool**

| Einstellung                                     | Standardwert  |
|---|---------------|
| Status  | Aktiviert     |
| Einschränkungen für Verbindungsserver           | Keine         |
| Adobe Flash quality (Adobe Flash-Qualität)      | Nicht steuern |
| Adobe Flash throttling (Adobe Flash-Drosselung) | Deaktiviert   |

## Konfigurieren der Adobe Flash-Drosselung mit Internet Explorer für RDS-Desktop-Pools

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 Benutzer-Desktop 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.

# Bereitstellen von Desktop-Pools

Bei der Erstellung eines Desktop-Pools legen Sie mithilfe von Konfigurationsoptionen fest, wie der Pool verwaltet wird und wie Benutzer mit den Desktops interagieren.

Diese Bereitstellungsaufgaben gelten für Desktop-Pools, die auf Maschinen für Einzelbenutzer bereitgestellt werden. Sie gelten nicht für RDS-Desktop-Pools. Die Adobe Flash-Qualitäts- und -Drosselungseinstellungen gelten jedoch für alle Typen von Desktop-Pools, einschließlich RDS.

Dieses Kapitel enthält die folgenden Themen:

- [Benutzerzuweisung in Desktop-Pools](#)
- [Manuelles Benennen von Computern oder Bereitstellen eines Benennungsmusters](#)
- [Manuelles Anpassen von Maschinen](#)
- [Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen](#)
- [Adobe Flash-Qualität und -Drosselung](#)
- [Einstellen von Betriebsrichtlinien für Desktop-Pools](#)
- [Konfigurieren von 3D-Rendern auf Windows 7- oder neueren Desktops](#)
- [Verhindern vom Zugriff auf View-Desktops durch RDP](#)
- [Bereitstellen großer Desktop-Pools](#)

## Benutzerzuweisung in Desktop-Pools

Sie können einen Desktop-Pool so konfigurieren, dass die Computer im Pool den Benutzern dediziert oder dynamisch zugewiesen werden. Sie müssen eine Benutzerzuweisung für automatisierte Pools, die vollständige virtuelle Maschinen enthalten, für automatisierte Linked-Clone-Pools und für manuelle Pools auswählen.

Bei einer dedizierten Zuweisung weist View jedem berechtigten Benutzer einen Computer im Pool zu. Wenn ein Benutzer sich mit einem Pool verbindet, meldet sich der Benutzer immer an demselben Computer an. Die Benutzereinstellungen und -daten werden zwischen den Sitzungen gespeichert. Kein anderer Benutzer im Pool kann auf den Computer zugreifen.

Bei einer dynamischen Zuweisung weist View Computer im Pool den berechtigten Benutzern dynamisch zu. Benutzer verbinden sich bei jeder Anmeldung mit einem anderen Computer. Wenn der Benutzer sich abmeldet, wird der Computer wieder dem Pool zurückgegeben.

Sie können Computer mit dynamischer Zuweisung so konfigurieren, dass sie bei der Benutzerabmeldung gelöscht werden. Durch den automatischen Löschvorgang können Sie immer nur die benötigte Anzahl virtueller Maschinen beibehalten. Der automatische Löschvorgang ist nur in automatisierten Pools möglich, die Sie mit einem Computer-Benennungsmuster und einer Gesamtzahl an Computern bereitstellen.

Durch Computer mit dynamischer Zuweisung können Sie die Kosten für die Softwarelizenzierung senken.

## Manuelles Benennen von Computern oder Bereitstellen eines Benennungsmusters

Sie können die Computer in einem automatisierten Pool bereitstellen, indem Sie manuell eine Liste von Computernamen angeben oder ein Benennungsmuster sowie die Anzahl der Computer festlegen, die im Pool enthalten sein sollen. Diese beiden Ansätze bieten unterschiedliche Vorteile.

Wenn Sie Computer durch Angabe einer Liste benennen, können Sie das Namensschema Ihres Unternehmens verwenden und jeden Computernamen mit einem Benutzer verknüpfen.

Wenn Sie ein Benennungsmuster bereitstellen, kann View Computer dynamisch nach Bedarf der Benutzer erstellen und zuweisen.

Sie müssen eine dieser Benennungsmethoden zur Bereitstellung automatisierter Pools anwenden, die vollständige virtuelle Maschinen oder verknüpfte Klone enthalten.

**Tabelle 11-1. Manuelles Benennen von Computern oder Bereitstellen eines Musters für die Computer-Benennung** werden die beiden Benennungsmethoden verglichen. Ferner wird gezeigt, wie die jeweilige Methode sich auf die Erstellung und Verwaltung eines Desktop-Pools auswirkt.

**Tabelle 11-1. Manuelles Benennen von Computern oder Bereitstellen eines Musters für die Computer-Benennung**

| Funktion      | Bereitstellen eines Musters für die Computer-Benennung   | Manuelles Benennen von Computern  |
|---------------|--|---|
| Computernamen | View generiert Computernamen.<br>Sie stellen ein Benennungsmuster bereit.<br>View fügt eine eindeutige Zahl hinzu, welche die einzelnen Computer identifiziert.<br>Weitere Informationen finden Sie unter <a href="#">Verwenden eines Benennungsmusters für automatisierte Desktop-Pools</a> . | Sie geben eine Liste von Computernamen an.<br><br>In einem Pool mit dedizierter Zuweisung können Sie Benutzer und Computer einander zuordnen, indem Sie die Benutzernamen mit den Computernamen aufführen.<br><br>Weitere Informationen finden Sie unter <a href="#">Angaben einer Liste von Maschinennamen</a> . |
| Pool-Größe    | Sie geben eine maximale Anzahl an Computern an.  | Ihre Liste mit Computernamen legt die Anzahl an Computern fest.   |

| Funktion                                | Bereitstellen eines Musters für die Computer-Benennung  | Manuelles Benennen von Computern  |
|---|---|---|
| Hinzufügen von Computern zum Pool       | Sie können die maximale Pool-Größe erhöhen.   | Sie können der Liste Computernamen hinzufügen.<br><br>Weitere Informationen finden Sie unter <a href="#">Hinzufügen von Computern zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde</a> .   |
| Bereitstellung nach Bedarf              | Verfügbar.<br><br>View erstellt die angegebene Mindestanzahl und Anzahl an Reservecomputern dynamisch und stellt sie bereit, wenn sich Benutzer anmelden oder Sie Computer zu Benutzern zuweisen.<br><br>View kann bei Erstellung des Pools auch alle Computer erstellen und bereitstellen.   | Nicht verfügbar.<br><br>Bei Erstellung des Pools erstellt View alle in der Liste angegebenen Computer und stellt diese bereit.  |
| Anfängliche Anpassung                   | Verfügbar.<br><br>Bei der Bereitstellung eines Computers kann View eine von Ihnen ausgewählte Anpassungsspezifikation ausführen.  | Verfügbar.<br><br>Bei der Bereitstellung eines Computers kann View eine von Ihnen ausgewählte Anpassungsspezifikation ausführen.  |
| Manuelle Anpassung dedizierter Computer | Zur Anpassung von Computern und zur Zurückgabe des Desktop-Zugriffs an die Benutzer müssen Sie den Besitz der einzelnen Computer entfernen und neu zuweisen. Abhängig davon, ob Sie Computer bei der ersten Anmeldung zuweisen, müssen Sie diese Schritte möglicherweise zweimal durchführen. Sie können Computer nicht im Wartungsmodus starten. Nach Erstellung des Pools können Sie die Computer manuell in den Wartungsmodus versetzen. | Sie können Computer anpassen und testen, ohne den Besitz neu zuzuweisen.<br><br>Bei der Erstellung des Pools können Sie alle Computer im Wartungsmodus starten, um Benutzer am Zugriff zu hindern. Sie können die Computer anpassen und den Wartungsmodus beenden, um Benutzern den Zugriff wieder zu ermöglichen.<br><br>Weitere Informationen finden Sie unter <a href="#">Manuelles Anpassen von Maschinen</a> . |
| Dynamische oder feste Pool-Größe        | Dynamisch.<br><br>Wenn Sie in einem Pool mit dedizierter Zuweisung eine Benutzerzuweisung von einem Computer entfernen, wird der Computer wieder dem Pool verfügbarer Computer hinzugefügt.<br><br>Wenn Sie in einem Pool mit dynamischer Zuweisung die automatische Löschung von Computern bei Abmeldung wählen, kann sich die Pool-Größe je nach Anzahl aktiver Benutzersitzungen vergrößern oder verkleinern.                            | Fest.<br><br>Der Pool enthält die Anzahl an Computern, die Sie in der Liste mit Computernamen bereitgestellt haben.<br><br>Sie können die Einstellung <b>Desktop bei Abmeldung löschen</b> nicht festlegen, wenn Sie Computer manuell benennen.   |



| Funktion          | Bereitstellen eines Musters für die Computer-Benennung  | Manuelles Benennen von Computern  |
|-------------------|---|---|
| Reservecomputer   | <p>Sie können eine Anzahl an Reservecomputern angeben, die View für neue Benutzer eingeschaltet lässt.</p> <p>View erstellt neue Computer zur Beibehaltung der angegebenen Anzahl. View beendet die Erstellung von Reservecomputern bei Erreichen der maximalen Pool-Größe.</p> <p>View lässt die Reservecomputer auch dann eingeschaltet, wenn die Betriebsrichtlinie für den Pool auf <b>Ausschalten</b> oder <b>Anhalten</b> festgelegt ist oder wenn Sie keine Betriebsrichtlinie einstellen.</p> | <p>Sie können eine Anzahl an Reservecomputern angeben, die View für neue Benutzer eingeschaltet lässt.</p> <p>View erstellt keine neuen Reservecomputer zur Beibehaltung der angegebenen Anzahl.</p> <p>View lässt die Reservecomputer auch dann eingeschaltet, wenn die Betriebsrichtlinie für den Pool auf <b>Ausschalten</b> oder <b>Anhalten</b> festgelegt ist oder wenn Sie keine Betriebsrichtlinie einstellen.</p>                                  |
| Benutzerzuweisung | <p>Sie können für Pools mit dedizierter Zuweisung und für Pools mit dynamischer Zuweisung ein Benennungsmuster verwenden.</p>   | <p>Sie können für Pools mit dedizierter Zuweisung und für Pools mit dynamischer Zuweisung Computernamen angeben.</p> <p><b>Hinweis</b> 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.</p> |

## Angeben einer Liste von Maschinennamen

Sie können einen automatisierten Desktop-Pool durch die manuelle Angabe einer Liste mit Maschinennamen bereitstellen. Durch diese Benennungsmethode können Sie die Namenskonventionen Ihres Unternehmens verwenden, um die Maschinen in einem Pool zu identifizieren.

Wenn Sie Maschinennamen explizit angeben, werden den Benutzern bekannte Namen basierend auf der Organisation ihres Unternehmens angezeigt, wenn sie sich an ihren Remote-Desktops anmelden.

Folgen Sie bei der manuellen Benennung von Maschinen diesen 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 Maschinen angegeben. 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 alle Maschinennamen eindeutig sind. Sie können nicht die Namen vorhandener virtueller Maschinen in vCenter Server verwenden.

### Verfahren

- 1 Erstellen Sie eine Textdatei mit der Liste der Maschinennamen.

Wenn Sie einen Desktop-Pool mit nur wenigen Maschinen erstellen möchten, können Sie die Maschinennamen direkt im Assistenten zum Hinzufügen von Desktop-Pools eingeben. Sie müssen keine separate Textdatei erstellen.

- 2 Starten Sie in View Administrator den Assistenten zum Hinzufügen von Desktop-Pools, um mit der Erstellung eines automatisierten Desktop-Pools zu beginnen.

- 3 Wählen Sie auf der Seite mit den Bereitstellungseinstellungen die Option **Namen manuell angeben**, und klicken Sie auf **Namen eingeben**.

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

Der Assistent zum Eingeben von Maschinennamen zeigt die Desktop-Liste an und weist mit einem roten ! auf Validierungsfehler hin.

- 5 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**.

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

- 7 (Optional) Wählen Sie **Maschinen im Wartungsmodus starten**.

Durch diese Option können Sie die Maschinen anpassen, bevor Benutzer sich anmelden und sie verwenden können.

- 8 Folgen Sie den Anweisungen des Assistenten, um die Erstellung des Desktop-Pools abzuschließen.

View erstellt eine Maschine für jeden Namen in der Liste. Wenn ein Eintrag eine Maschine und einen Benutzernamen umfasst, weist View die Maschine dem jeweiligen Benutzer zu.

Nach der Erstellung des Desktop-Pools können Sie Maschinen hinzufügen, indem Sie eine weitere Listendatei mit zusätzlichen Maschinennamen und Benutzern importieren. Information dazu finden Sie unter „Hinzufügen von Maschinen zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde“ im Dokument *Verwaltung von View*.

## Verwenden eines Benennungsmusters für automatisierte Desktop-Pools

Sie können die Computer in einem Pool bereitstellen, indem Sie ein Benennungsmuster und die Gesamtzahl an Computern bereitstellen, die im Pool enthalten sein sollen. Standardmäßig verwendet View Manager Ihr Muster als Präfix in allen Computernamen und hängt eine eindeutige Zahl zur Identifizierung der einzelnen Computer an.

### Länge des Benennungsmusters in einem Computernamen

Für Computernamen gilt eine Begrenzung auf 15 Zeichen, einschließlich des Benennungsmusters und der automatisch generierten Zahl.

**Tabelle 11-2. Maximale Länge des Benennungsmusters in einem Computernamen**

| Festgelegte Anzahl an Computern im Pool | Maximale Präfixlänge |
|---|----------------------|
| 1-99                                    | 13 Zeichen           |
| 100-999                                 | 12 Zeichen           |
| 1,000 oder mehr                         | 11 Zeichen           |

Namen mit Token fester Länge besitzen unterschiedliche Längenbeschränkungen. Siehe [Länge des Benennungsmusters bei Verwendung eines Tokens fester Länge](#).

### Verwenden eines Tokens in einem Computernamen

Mithilfe eines Tokens können Sie die automatisch generierte Zahl an einer beliebigen anderen Stelle im Namen platzieren. Geben Sie beim Eingeben des Pool-Namens **n**, eingeschlossen von geschweiften Klammern, ein, um das Token zu bezeichnen.

Beispiel: **amber-{n}-desktop**

Wenn View Manager einen Computer erstellt, ersetzt View **{n}** durch eine eindeutige Zahl.

Sie können ein Token fester Länge generieren, indem Sie **{n:fixed=Anzahl der Stellen}** eingeben.

View ersetzt das Token durch Zahlen mit der angegebenen Anzahl an Stellen.

Wenn Sie beispielsweise **amber-{n:fixed=3}** eingeben, ersetzt View **{n:fixed=3}** durch eine dreistellige Zahl und erstellt folgende Computernamen: **amber-001**, **amber-002**, **amber-003** usw.

## Länge des Benennungsmusters bei Verwendung eines Tokens fester Länge

Namen mit Token fester Länge sind auf 15 Zeichen beschränkt, einschließlich Ihres Benennungsmusters und der Anzahl an Stellen im Token.

**Tabelle 11-3. Maximale Länge des Benennungsmusters bei Verwendung eines Tokens fester Länge**

| Token fester Länge | Maximale Länge des Benennungsmusters |
|--------------------|--------------------------------------|
| {n:fixed=1}        | 14 Zeichen                           |
| {n:fixed=2}        | 13 Zeichen                           |
| {n:fixed=3}        | 12 Zeichen                           |

## Beispiel für die Maschinenbenennung

Dieses Beispiel zeigt die Erstellung zweier automatisierter Desktop-Pools, die dieselben Maschinennamen, jedoch unterschiedliche Zahlensätze verwenden. Die in diesem Beispiel verwendeten Strategien führen zum Erreichen eines bestimmten Benutzerziels und demonstrieren die Flexibilität der Methoden zur Maschinenbenennung.

Das Ziel besteht darin, zwei Pools mit derselben Namenskonvention wie VDIABC-XX zu erstellen, wobei XX für eine Zahl steht. Jeder Pool enthält einen anderen Satz aufeinander folgender Zahlen. Beispielsweise enthält der erste Pool die Maschinen VDIABC-01 bis VDIABC-10. Der zweite Pool enthält die Maschinen VDIABC-11 bis VDIABC-20.

Sie können beide Maschinenbenennungsmethoden einsetzen, um dieses Ziel zu erreichen.

- Um einmal feststehende Sätze von Maschinen zu erstellen, geben Sie die Maschinennamen manuell an.
- Um Maschinen dynamisch bei der ersten Benutzeranmeldung zu erstellen, stellen Sie ein Benennungsmuster bereit, und verwenden Sie ein Token zum Festlegen der aufeinanderfolgenden Zahlen.

## Manuelles Angeben der Namen

- 1 Bereiten Sie für den ersten Pool eine Textdatei vor, die eine Liste der Maschinennamen von VDIABC-01 bis VDIABC-10 enthält.
- 2 Erstellen Sie den Pool in View Administrator, und geben Sie die Maschinennamen manuell an.
- 3 Klicken Sie auf **Namen eingeben** und kopieren Sie Ihre Liste in das Listenfeld **Computernamen eingeben**.
- 4 Wiederholen Sie diese Schritte für den zweiten Pool, und verwenden Sie dabei die Namen VDIABC-11 bis VDIABC-20.

Weitere Anleitungen finden Sie unter [Angeben einer Liste von Maschinennamen](#).

Nach der Erstellung der Pools können Sie jedem Pool weitere Maschinen hinzufügen. Beispielsweise können Sie dem ersten Pool die Maschinen VDIABC-21 bis VDIABC-30, und dem zweiten Pool die Maschinen VDIABC-31 bis VDIABC-40 hinzufügen. Siehe [Hinzufügen von Computern zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde](#).

## Bereitstellen eines Benennungsmusters mit einem Token

- 1 Erstellen Sie den ersten Pool in View Administrator, und verwenden Sie ein Benennungsmuster zum Bereitstellen der Maschinennamen.
- 2 Geben Sie im Textfeld für das Benennungsmuster **VDIABC-0{n}** ein.
- 3 Begrenzen Sie die maximale Pool-Größe auf 9.
- 4 Wiederholen Sie diese Schritte für den zweiten Pool, geben Sie jedoch im Textfeld für das Benennungsmuster **VDIABC-1{n}** ein.

Der erste Pool enthält die Maschinen VDIABC-01 bis VDIABC-09. Der zweite Pool enthält die Maschinen VDIABC-11 bis VDIABC-19.

Alternativ dazu können Sie die Pools so konfigurieren, dass sie jeweils bis zu 99 Maschinen enthalten können, indem Sie ein Token fester Länge mit 2 Stellen verwenden:

- Geben Sie für den ersten Pool **VDIABC-0{n:fixed=2}** ein.
- Geben Sie für den zweiten Pool **VDIABC-1{n:fixed=2}** ein.

Begrenzen Sie die maximale Größe beider Pools auf 99. Durch diese Konfiguration werden Maschinen nach einem Benennungsmuster erstellt, bei dem die Maschinennamen auf eine sequenzielle, dreistellige Zahl enden.

Erster Pool:

```
VDIABC-001
VDIABC-002
VDIABC-003
```

Zweiter Pool:

```
VDIABC-101
VDIABC-102
VDIABC-103
```

Weitere Informationen zu Benennungsmustern und Token finden Sie unter [Verwenden eines Benennungsmusters für automatisierte Desktop-Pools](#).

## 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.

## Manuelles Anpassen von Maschinen

Nach der Erstellung eines automatisierten Pools können Sie bestimmte Maschinen anpassen, ohne den Besitz neu zuzuweisen. Durch das Starten der Maschinen im Wartungsmodus können Sie die Maschinen ändern und testen, bevor Sie sie den zugewiesenen Benutzern freigeben oder allen berechtigten Benutzern im Pool zur Verfügung stellen.

### Anpassen von Maschinen im Wartungsmodus

Der Wartungsmodus hindert Benutzer am Zugriff auf ihre Desktops. Wenn Sie Maschinen im Wartungsmodus starten, versetzt View jede Maschine bei ihrer Erstellung in den Wartungsmodus.

In einem Pool mit dedizierter Zuweisung können Sie den Wartungsmodus zum Anmelden bei einer Maschine verwenden, ohne den Besitz erneut Ihrem eigenen Administratorkonto zuzuweisen. Nach der Anpassung müssen Sie den Besitz nicht wieder an den Benutzer zurückgeben, der der Maschine zugewiesen ist.

In einem Pool mit dynamischer Zuweisung können Sie Maschinen im Wartungsmodus testen, bevor Benutzern die Anmeldung erlaubt wird.

Um dieselbe Anpassung auf allen Maschinen in einem automatisierten Pool durchzuführen, passen Sie die virtuelle Maschine an, die Sie als Vorlage oder übergeordnetes Element vorbereiten. View stellt Ihre Anpassung für alle Maschinen bereit. Bei der Erstellung des Pools können Sie auch eine Sysprep-Anpassungsspezifikation zum Konfigurieren aller Maschinen mit Lizenzierung, Domänenanbindung, DHCP-Einstellungen und anderen Computereigenschaften verwenden.

---

**Hinweis** Maschinen können im Wartungsmodus gestartet werden, sofern Sie die Maschinennamen für den Pool manuell angeben. Wenn Sie zur Benennung der Maschinen ein Benennungsmuster verwenden, ist dies nicht möglich.

---

## Anpassen einzelner Maschinen

Sie können nach der Erstellung eines Pools einzelne Maschinen anpassen, indem Sie die Maschinen im Wartungsmodus starten.

### Verfahren

- 1 Erstellen Sie zunächst in View Administrator einen automatisierten Desktop-Pool, indem Sie den Assistenten zum Hinzufügen von Desktop-Pools starten.
- 2 Wählen Sie auf der Seite mit den Bereitstellungseinstellungen die Option **Namen manuell angeben**.
- 3 Wählen Sie **Maschinen im Wartungsmodus starten** aus.
- 4 Schließen Sie den Assistenten zum Hinzufügen von Desktop-Pools ab, um den Desktop-Pool zu erstellen.
- 5 Melden Sie sich in vCenter Server bei den einzelnen virtuellen Maschinen an, passen Sie sie an, und testen Sie sie.

Sie können die Computer manuell oder über eine Windows-Standardsoftware zur Systemverwaltung anpassen, beispielsweise Altiris, SMS, LanDesk oder BMC.

- 6 Wählen Sie in View Administrator den Desktop-Pool aus.
- 7 Wählen Sie mithilfe des Filtertools bestimmte Computer aus, die Sie für Ihre Benutzer freigeben möchten.
- 8 Klicken Sie auf **Weitere Befehle > Wartungsmodus beenden**.

### Nächste Schritte

Benachrichtigen Sie Ihre Benutzer darüber, dass sie sich an ihren Desktops anmelden können.

## Desktop-Pool-Einstellungen für alle Desktop-Pool-Typen

Bei der Konfiguration von automatisierten Pools mit vollständigen virtuellen Maschinen, Linked-Clone-Desktop-Pools, manuellen Desktop-Pools und RDS-Desktop-Pools müssen Sie Computer- und Desktop-Pool-Einstellungen angeben. Nicht alle Einstellungen gelten für alle Typen von Desktop-Pools.



**Tabelle 11-4. Beschreibungen der Desktop-Pool-Einstellungen**

| <b>Einstellung</b>                                  | <b>Optionen</b>   |
|---|---|
| Status  | <ul style="list-style-type: none"> <li>■ <b>Aktiviert.</b> Nach seiner Erstellung wird der Desktop-Pool aktiviert und kann sofort verwendet werden.</li> <li>■ <b>Deaktiviert.</b> Nach seiner Erstellung ist der Desktop-Pool deaktiviert und nicht verfügbar und die Bereitstellung für den Pool ist unterbrochen. Diese Einstellung ist geeignet, wenn Sie nach der Bereitstellung noch verschiedene Aufgaben ausführen möchten, z.B. ein Testing oder eine grundlegende Wartung.</li> </ul> <p>In diesem Status stehen Remote-Desktops nicht zur Verfügung.</p>   |
| Einschränkungen für Verbindungsserver               | <ul style="list-style-type: none"> <li>■ <b>Keine.</b> Der Desktop-Pool ist für jede View-Verbindungsserver-Instanz zugänglich.</li> <li>■ <b>Mit Kennzeichen.</b> Wählen Sie mindestens ein View-Verbindungsserver-Kennzeichen aus, um den Zugriff auf den Desktop-Pool nur für View-Verbindungsserver-Instanzen zuzulassen, die über diese Kennzeichen verfügen. Sie können die Kontrollkästchen verwenden, um mehrere Kennzeichen auszuwählen.</li> </ul> <p>Wenn Sie den Zugriff auf Ihre Desktops über Workspace ermöglichen möchten und Einschränkungen für View-Verbindungsserver konfigurieren, werden im Workspace App Portal möglicherweise Desktops angezeigt, obwohl für diese Desktops Einschränkungen gelten. Workspace-Benutzer können diese Desktops nicht starten.</p>   |
| Betriebsrichtlinie für Remote-Computer              | <p>Legt fest, wie eine virtuelle Maschine sich beim Abmelden eines Benutzers vom verknüpften Desktop verhält.</p> <p>Beschreibungen der Betriebsrichtlinienoptionen finden Sie unter <a href="#">Betriebsrichtlinien für Desktop-Pools</a>.</p> <p>Weitere Informationen über die Auswirkungen von Betriebsrichtlinien auf automatisierte Pools finden Sie unter <a href="#">Einstellen von Betriebsrichtlinien für Desktop-Pools</a>.</p>  |
| Nach Verbindungstrennung automatisch abmelden       | <ul style="list-style-type: none"> <li>■ <b>Sofort.</b> Benutzer werden sofort nach der Verbindungstrennung abgemeldet.</li> <li>■ <b>Nie.</b> Benutzer werden nie abgemeldet.</li> <li>■ <b>Nach.</b> Zeitspanne, nach der Benutzer abgemeldet werden, wenn sie die Verbindung trennen. Geben Sie die Dauer in Minuten ein.</li> </ul> <p>Die Abmeldezeit gilt für zukünftige Verbindungstrennungen. Wenn eine Desktop-Sitzung bereits getrennt war, als Sie die Abmeldezeit festlegten, startet die Abmeldedauer für diesen Benutzer, wenn Sie die Abmeldezeit festlegen, und nicht zu dem Zeitpunkt, als die Trennung ursprünglich stattfand. Wenn Sie hierfür beispielsweise fünf Minuten festlegen und eine Sitzung vor 10 Minuten getrennt wurde, meldet View diese Sitzung fünf Minuten nach dem Festlegen des Werts ab.</p> |
| Benutzern das Zurücksetzen ihrer Computer gestatten | Ermöglicht Benutzern das Zurücksetzen ihrer eigenen Desktops ohne Unterstützung des Administrators.   |
| Mehrere Sitzungen pro Benutzer zulassen             | Ermöglicht Benutzern das Herstellen gleichzeitiger Verbindungen mit mehreren Desktops im Pool.  |
| Computer nach Abmeldung löschen                     | <p>Geben Sie an, ob vollständige virtuelle Maschinen mit dynamischer Zuweisung gelöscht werden sollen.</p> <ul style="list-style-type: none"> <li>■ <b>Nein.</b> Virtuelle Maschinen verbleiben nach der Abmeldung des Benutzers im Desktop-Pool.</li> <li>■ <b>Ja.</b> Virtuelle Maschinen werden ausgeschaltet und gelöscht, sobald Benutzer sich abmelden.</li> </ul>  |

| Einstellung  | Optionen  |              |  |                      |   |
|--|---|--------------|--|----------------------|---|
| Computer bei Abmeldung löschen oder aktualisieren    | <p>Geben Sie an, ob virtuelle Linked-Clone-Maschinen mit dynamischer Zuordnung gelöscht, aktualisiert oder unverändert belassen werden sollen.</p> <ul style="list-style-type: none"> <li>■ <b>Nie.</b> Virtuelle Maschinen verbleiben nach der Abmeldung des Benutzers im Desktop-Pool und werden nicht aktualisiert.</li> <li>■ <b>Sofort löschen.</b> Virtuelle Maschinen werden ausgeschaltet und gelöscht, sobald Benutzer sich abmelden. Wenn sich Benutzer abmelden, werden virtuelle Maschinen sofort in den Zustand <b>Wird gelöscht</b> versetzt.</li> <li>■ <b>Sofort aktualisieren.</b> Virtuelle Maschinen werden bei Benutzerabmeldung sofort aktualisiert. Wenn sich Benutzer abmelden, werden virtuelle Maschinen sofort in den Wartungsmodus versetzt, damit andere Benutzer sich zu Beginn des Aktualisierungsvorgangs nicht anmelden können.</li> </ul>  |              |  |                      |   |
| Betriebssystemfestplatte nach Abmelden aktualisieren | <p>Geben Sie an, ob und wann die Betriebssystemfestplatten für virtuelle Linked-Clone-Maschinen mit dedizierter Zuweisung aktualisiert werden sollen.</p> <ul style="list-style-type: none"> <li>■ <b>Nie.</b> Die Betriebssystemfestplatte wird nie aktualisiert.</li> <li>■ <b>Immer.</b> Die Betriebssystemfestplatte wird bei jeder Abmeldung des Benutzers aktualisiert.</li> <li>■ <b>Alle.</b> Die Betriebssystemfestplatte wird in regelmäßigen Intervallen aus einer bestimmten Anzahl an Tagen aktualisiert. Geben Sie die Anzahl der Tage ein.</li> </ul> <p>Die Anzahl der Tage wird von der letzten Aktualisierung oder von der erstmaligen Bereitstellung an berechnet, sofern noch keine Aktualisierung vorgenommen wurde. Wird der Wert z. B. mit <b>3</b> Tagen angegeben und es sind drei Tage seit der letzten Aktualisierung vergangen, wird der Computer aktualisiert, nachdem sich der Benutzer abgemeldet hat.</p> <ul style="list-style-type: none"> <li>■ <b>Bei.</b> Die Betriebssystemfestplatte wird aktualisiert, wenn die aktuelle Größe einen bestimmten Prozentsatz der maximal zulässigen Größe erreicht. Die maximale Größe der Betriebssystemfestplatte eines vernetzten Klangs entspricht der Größe der Betriebssystemfestplatte des Replikats. Geben Sie den Prozentsatz ein, bei dem der Aktualisierungsvorgang stattfinden soll.</li> </ul> <p>Mit der Option <b>Bei</b> wird die Größe der Linked-Clone-Betriebssystemfestplatte im Datenspeicher mit der maximal zulässigen Größe verglichen. Der Prozentsatz der Festplattennutzung stellt nicht die Festplattennutzung dar, die möglicherweise im Gastbetriebssystem des Computers angezeigt wird.</p> <p>Wenn Sie die Betriebssystemfestplatten in einem Linked-Clone-Pool mit dedizierter Zuweisung aktualisieren, bleiben die persistenten View Composer-Festplatten unberührt.</p> |              |  |                      |   |
| Standardanzeigeprotokoll                             | <p>Wählen Sie das Anzeigeprotokoll, das der View-Verbindungsserver zur Kommunikation mit Clients verwenden soll.</p> <table> <tr> <td><b>PCoIP</b></td><td>Die Standardoption, sofern sie unterstützt wird. PCoIP wird als Anzeigeprotokoll für virtuelle und physische Maschinen mit Teradici-Hardware unterstützt. PCoIP ermöglicht ein optimales PC-Erlebnis bei der Bereitstellung von Bildern sowie Audio- und Videoinhalten für eine große Anzahl an Benutzern im LAN oder im gesamten WAN.</td></tr> <tr> <td><b>Microsoft RDP</b></td><td>Microsoft Remotedesktopverbindung (Remote Desktop Connection, RDC) verwendet für die Übertragung von Daten RDP. RDP ist ein Mehrkanalprotokoll, das einem Benutzer die Remote-Verbindung mit einem Computer ermöglicht.</td></tr> </table>  | <b>PCoIP</b> | Die Standardoption, sofern sie unterstützt wird. PCoIP wird als Anzeigeprotokoll für virtuelle und physische Maschinen mit Teradici-Hardware unterstützt. PCoIP ermöglicht ein optimales PC-Erlebnis bei der Bereitstellung von Bildern sowie Audio- und Videoinhalten für eine große Anzahl an Benutzern im LAN oder im gesamten WAN. | <b>Microsoft RDP</b> | Microsoft Remotedesktopverbindung (Remote Desktop Connection, RDC) verwendet für die Übertragung von Daten RDP. RDP ist ein Mehrkanalprotokoll, das einem Benutzer die Remote-Verbindung mit einem Computer ermöglicht. |
| <b>PCoIP</b>   | Die Standardoption, sofern sie unterstützt wird. PCoIP wird als Anzeigeprotokoll für virtuelle und physische Maschinen mit Teradici-Hardware unterstützt. PCoIP ermöglicht ein optimales PC-Erlebnis bei der Bereitstellung von Bildern sowie Audio- und Videoinhalten für eine große Anzahl an Benutzern im LAN oder im gesamten WAN.  |              |  |                      |   |
| <b>Microsoft RDP</b>                                 | Microsoft Remotedesktopverbindung (Remote Desktop Connection, RDC) verwendet für die Übertragung von Daten RDP. RDP ist ein Mehrkanalprotokoll, das einem Benutzer die Remote-Verbindung mit einem Computer ermöglicht.   |              |  |                      |   |
| Benutzern die Wahl des Protokolls erlauben           | Erlauben Sie Benutzern das Außerkraftsetzen des Standardanzeigeprotokolls für ihre Desktops über Horizon Client.  |              |  |                      |   |

| Einstellung                   | Optionen  |
|-------------------------------|---|
| 3D-Renderer                   | <p>Sie können wählen, ob 3D-Grafikrendern aktiviert werden soll, wenn Ihr Pool Windows 7- oder neuere Desktops enthält. Sie können den <b>3D-Renderer</b> so konfigurieren, dass Software- oder Hardware-Rendern verwendet wird, basierend auf den physischen GPU-Grafikkarten, die auf ESXi 5.1 oder neueren Hosts installiert sind.</p> <p>Zum Aktivieren dieser Funktion müssen Sie PCoIP als Protokoll auswählen und die Einstellung <b>Benutzern die Wahl des Protokolls erlauben</b> deaktivieren (wählen Sie <b>Nein</b>).</p> <p>Bei den hardwarebasierten Optionen für den <b>3D-Renderer</b> können Benutzer Grafikanwendungen für Entwurf, Modellierung und Multimedia nutzen. Mit der Softwareoption <b>3D-Renderer</b> können die Benutzer Grafikverbesserungen von weniger anspruchsvollen Anwendungen wie AERO, Microsoft Office und Google Earth nutzen. Weitere Informationen zu den Systemanforderungen finden Sie unter <a href="#">Konfigurieren von 3D-Rendern auf Windows 7- oder neueren Desktops</a>.</p> <p>Wenn Ihre View-Bereitstellung nicht mit vSphere 5.0 oder höher ausgeführt wird, ist diese Einstellung nicht verfügbar und in View Administrator nicht aktiv.</p> <p>Wenn Sie diese Funktion auswählen, können Sie die Größe des VRAM konfigurieren, der den Computern im Pool zugeordnet wird. Sie können höchstens zwei Monitore für Ihre Computer auswählen, die als Remote-Desktops verwendet werden. Die <b>Maximale Auflösung jedes Monitors</b> beträgt 1920 x 1200 Pixel. Dieser Wert kann nicht konfiguriert werden.</p> <hr/> <p><b>Hinweis</b> Wenn Sie diese Einstellung konfigurieren oder bearbeiten, müssen Sie vorhandene virtuelle Maschinen ausschalten. Zudem müssen Sie sicherstellen, dass die Computer in vCenter Server erneut konfiguriert werden und die Computer einschalten, damit die neue Einstellung übernommen wird. Durch einen Neustart einer virtuellen Maschine wird diese neue Einstellung nicht übernommen.</p> <hr/> <p>Weitere Informationen finden Sie unter <a href="#">Konfigurieren von 3D-Rendern auf Windows 7- oder neueren Desktops</a>, <a href="#">3D-Render-Optionen</a> und <a href="#">Empfohlene Vorgehensweise für das Konfigurieren des 3D-Renderns</a>.</p> |
| Maximale Anzahl an Monitoren  | <p>Wenn Sie PCoIP als Anzeigeprotokoll verwenden, können Sie die <b>Maximale Anzahl an Monitoren</b> auswählen, auf denen Benutzer den Desktop anzeigen können.</p> <p>Wenn die Einstellung <b>3D-Renderer</b> nicht ausgewählt ist, wirkt sich die Einstellung <b>Maximale Anzahl an Monitoren</b> auf die Größe des VRAM aus, das den Computern im Pool zugeordnet ist. Wenn Sie die Monitoranzahl erhöhen, wird in den verknüpften ESXi-Hosts mehr Arbeitsspeicher belegt.</p> <p>Wenn die Einstellung <b>3D-Renderer</b> ausgewählt ist, können Sie höchstens zwei Monitore auswählen.</p> <hr/> <p><b>Hinweis</b> Sie müssen die vorhandenen virtuellen Maschinen aus- und wieder einschalten, damit diese Einstellung übernommen wird. Durch einen Neustart einer virtuellen Maschine wird diese Einstellung nicht übernommen.</p>  |
| Max. Auflösung eines Monitors | <p>Wenn Sie PCoIP als Anzeigeprotokoll verwenden und dabei die Einstellung <b>3D-Renderer</b> nicht auswählen, sollten Sie die <b>Maximale Auflösung jedes Monitors</b> angeben.</p> <p>Wenn die Einstellung <b>3D-Renderer</b> nicht ausgewählt ist, wirkt sich die Einstellung <b>Maximale Auflösung eines Monitors</b> auf die Größe des VRAM aus, das den Computern im Pool zugeordnet ist. Wenn Sie die Auflösung erhöhen, wird in den verknüpften ESXi-Hosts mehr Arbeitsspeicher belegt.</p> <p>Wenn die Einstellung <b>3D-Renderer</b> ausgewählt ist, können Sie die <b>Maximale Auflösung eines Monitors</b> nicht ändern. Die Auflösung wird auf 1920x1200 Pixel festgesetzt.</p> <hr/> <p><b>Hinweis</b> Sie müssen die vorhandenen virtuellen Maschinen aus- und wieder einschalten, damit diese Einstellung übernommen wird. Durch einen Neustart einer virtuellen Maschine wird diese Einstellung nicht übernommen.</p>  |

| Einstellung                                | Optionen  |
|--|---|
| HTML Access                                | <p>Wählen Sie <b>Aktiviert</b> aus, um Benutzern zu erlauben, eine Verbindung zu Remote-Desktops in ihren Webbrowsern herzustellen.</p> <p>Wenn sich ein Benutzer bei der VMware Horizon-Webportalseite oder beim Workspace App Portal anmeldet und einen Remote-Desktop auswählt, erlaubt der HTML Access Agent dem Benutzer, über HTTPS eine Verbindung zum Desktop herzustellen. Der Desktop wird im Browser des Benutzers angezeigt. Andere Anzeigeprotokolle wie PCoIP oder RDP werden nicht verwendet. Die Horizon Client-Software braucht nicht auf den Client-Geräten installiert zu sein.</p> <p>Um den HTML Access zu verwenden, müssen Sie das HTML Access in Ihrer View-Bereitstellung installieren. Weitere Informationen finden Sie in <i>Verwendung von HTML Access</i>, verfügbar unter <a href="https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html">https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html</a>.</p> <p>Um HTML Access mit Workspace zu verwenden, müssen Sie den View-Verbindungsserver mit einem SAML-Authentifizierungsserver kombinieren, wie im Dokument <i>Verwaltung von View</i> beschrieben. Workspace muss installiert und für die Verwendung mit dem View-Verbindungsserver konfiguriert sein.</p> |
| Adobe Flash-Qualität                       | <p>Legt die Qualität der Adobe Flash-Inhalte fest, die auf Webseiten angezeigt werden.</p> <ul style="list-style-type: none"> <li>■ <b>Nicht steuern.</b> Die Qualität wird durch die Webseiteneinstellungen bestimmt.</li> <li>■ <b>Niedrig.</b> Mit dieser Einstellung werden die höchsten Bandbreiteeinsparungen erzielt. Wenn keine Qualitätsstufe angegeben ist, verwendet das System die Standardeinstellung Niedrig.</li> <li>■ <b>Mittel.</b> Mit dieser Einstellung werden mittlere Bandbreiteeinsparungen erzielt.</li> <li>■ <b>Hoch.</b> Mit dieser Einstellung werden die geringsten Bandbreiteeinsparungen erzielt.</li> </ul> <p>Weitere Informationen finden Sie unter <a href="#">Adobe Flash-Qualität und -Drosselung</a>.</p>  |
| Adobe Flash-Drosselung                     | <p>Legt die Frame-Rate von Adobe Flash-Filmen fest. Wenn Sie diese Einstellung aktivieren, können Sie die Anzahl der pro Sekunde angezeigten Frames verringern oder steigern, indem Sie eine aggressive Stufe auswählen.</p> <ul style="list-style-type: none"> <li>■ <b>Deaktiviert.</b> Es erfolgt keine Drosselung. Das Zeitgeberintervall bleibt unverändert.</li> <li>■ <b>Konservativ.</b> Das Zeitgeberintervall lautet 100 Millisekunden. Diese Einstellung führt zur geringsten Anzahl an verworfenen Frames.</li> <li>■ <b>Mittel.</b> Das Zeitgeberintervall lautet 500 Millisekunden.</li> <li>■ <b>Aggressiv.</b> Das Zeitgeberintervall lautet 2500 Millisekunden. Diese Einstellung führt zur höchsten Anzahl an verworfenen Frames.</li> </ul> <p>Weitere Informationen finden Sie unter <a href="#">Adobe Flash-Qualität und -Drosselung</a>.</p>  |
| Globale Mirage-Einstellungen überschreiben | <p>Um denselben Mirage-Server für alle Desktop-Pools anzugeben, verwenden Sie die globale View-Konfigurationseinstellung anstelle dieser poolspezifischen Einstellung.</p>  |
| Mirage-Serverkonfiguration                 | <p>Ermöglicht Ihnen, die URL eines Mirage-Servers anzugeben, und zwar in dem Format <b>mirage://Servername:Port</b> bzw. <b>mirages://Servername:port</b>. <i>Servername</i> ist hier der vollqualifizierte Domänenname. Wenn Sie die Portnummer nicht angeben, wird die standardmäßige Portnummer 8000 verwendet.</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 <a href="https://www.vmware.com/support/pubs/mirage_pubs.html">https://www.vmware.com/support/pubs/mirage_pubs.html</a>.</p>   |

## 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 11-5. Adobe Flash-Qualitätseinstellungen** zeigt die verfügbaren Einstellungen für die Adobe Flash-Anzeigequalität.

**Tabelle 11-5. Adobe Flash-Qualitätseinstellungen**

| Qualitätseinstellung | Beschreibung  |
|----------------------|---|
| <b>Nicht steuern</b> | Die Qualität wird durch die Webseiteneinstellungen bestimmt.                |
| <b>Niedrig</b>       | Mit dieser Einstellung werden die höchsten Bandbreiteinsparungen erzielt.   |
| <b>Mittel</b>        | Mit dieser Einstellung werden mittlere Bandbreiteinsparungen erzielt.       |
| <b>Hoch</b>          | 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 11-6. Adobe Flash-Drosselungseinstellungen** zeigt die verfügbaren Einstellungen für die Adobe Flash-Drosselung.

**Tabelle 11-6. Adobe Flash-Drosselungseinstellungen**

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

Die Audiogeschwindigkeit bleibt unabhängig von der gewählten Drosselungseinstellung konstant.

## Einstellen von Betriebsrichtlinien für Desktop-Pools

Sie können eine Betriebsrichtlinie für die virtuellen Maschinen in einem Desktop-Pool konfigurieren, wenn die virtuellen Maschinen über vCenter Server verwaltet werden.

Über Betriebsrichtlinien wird gesteuert, wie eine virtuelle Maschine sich verhält, wenn der damit verknüpfte Desktop nicht verwendet wird. Ein Desktop wird als nicht verwendet betrachtet, bevor ein Benutzer sich anmeldet und nachdem ein Benutzer die Verbindung trennt oder sich abmeldet. Betriebsrichtlinien steuern außerdem, wie sich eine virtuelle Maschine nach Abschluss von Verwaltungsaufgaben wie der Aktualisierung, Neuzusammenstellung und Neuverteilung verhält.

Sie konfigurieren Betriebsrichtlinien, wenn Sie Desktop-Pools in View Administrator erstellen oder bearbeiten.

**Hinweis** Für Desktop-Pools mit nicht verwalteten Maschinen können Sie keine Betriebsrichtlinien konfigurieren.

## Betriebsrichtlinien für Desktop-Pools

Über Betriebsrichtlinien wird gesteuert, wie eine virtuelle Maschine sich verhält, wenn der damit verknüpfte Remote-Desktop nicht verwendet wird.

Sie legen Betriebsrichtlinien fest, wenn Sie einen Desktop-Pool erstellen oder bearbeiten. In [Tabelle 11-7. Betriebsrichtlinien](#) werden die verfügbaren Betriebsrichtlinien beschrieben.

**Tabelle 11-7. Betriebsrichtlinien**

| Betriebsrichtlinie                              | Beschreibung   |
|---|--|
| <b>Keine Betriebsaktion vornehmen</b>           | <p>View wendet nach der Abmeldung des Benutzers keine Betriebsrichtlinie an. Diese Einstellung hat zwei Konsequenzen.</p> <ul style="list-style-type: none"> <li>■ View ändert nach der Abmeldung eines Benutzers den Betriebsstatus der virtuellen Maschine nicht.</li> </ul> <p>Wenn ein Benutzer die virtuelle Maschine beispielsweise herunterfährt, bleibt die virtuelle Maschine ausgeschaltet. Wenn ein Benutzer sich abmeldet, ohne die virtuelle Maschine herunterzufahren, bleibt die virtuelle Maschine eingeschaltet. Wenn sich ein Benutzer erneut mit dem Desktop verbindet, wird die virtuelle Maschine neu gestartet, wenn sie zuvor ausgeschaltet war.</p> <ul style="list-style-type: none"> <li>■ View setzt keinen Betriebsstatus durch, nachdem eine Verwaltungsaufgabe abgeschlossen wurde.</li> </ul> <p>Beispielsweise kann ein Benutzer sich abmelden, ohne die virtuelle Maschine herunterzufahren. Die virtuelle Maschine bleibt eingeschaltet. Wenn eine geplante Neuzusammenstellung stattfindet, wird die virtuelle Maschine ausgeschaltet. Nach Abschluss der Neuzusammenstellung unternimmt View keine Schritte zum Ändern des Betriebsstatus der virtuellen Maschine. Sie bleibt ausgeschaltet.</p> |
| <b>Computer müssen immer eingeschaltet sein</b> | <p>Die virtuelle Maschine bleibt auch dann eingeschaltet, wenn sie nicht verwendet wird. Wenn ein Benutzer die virtuelle Maschine herunterfährt, wird sie sofort neu gestartet. Die virtuelle Maschine wird außerdem nach Abschluss einer Verwaltungsaufgabe wie z.B. einer Aktualisierung, Neuzusammenstellung oder Neuverteilung neu gestartet.</p> <p>Wählen Sie <b>Computer müssen immer eingeschaltet sein</b>, wenn Sie Batch-Prozesse oder Systemverwaltungs-Tools ausführen, welche zu bestimmten Zeiten auf die virtuellen Maschinen zugreifen müssen.</p>  |

| Betriebsrichtlinie | Beschreibung  |
|--------------------|---|
| <b>Anhalten</b>    | <p>Die virtuelle Maschine wird angehalten, wenn sich ein Benutzer abmeldet, jedoch nicht, wenn ein Benutzer die Verbindung trennt.</p> <p>Sie können die Computer in einem dedizierten Pool auch so konfigurieren, dass sie angehalten werden, wenn ein Benutzer die Verbindung trennt, ohne sich abzumelden. Um diese Richtlinie zu konfigurieren, müssen Sie ein Attribut in View LDAP festlegen. Siehe <a href="#">Konfigurieren von speziellen Maschinen zum Anhalten nach Trennung der Verbindung durch Benutzer</a>.</p> <p>Wenn mehrere angehaltene virtuelle Maschinen fortgesetzt werden, treten beim Einschalten einiger virtueller Maschinen möglicherweise Verzögerungen auf. Ob Verzögerungen auftreten, hängt von der Hardware des ESXi-Hosts und der Anzahl der virtuellen Maschinen ab, die auf einem ESXi-Host konfiguriert sind. Benutzer, die sich über Horizon Client mit ihren Desktops verbinden, werden möglicherweise vorübergehend in einer Meldung darüber informiert, dass die Desktops nicht verfügbar sind. Die Benutzer können sich erneut verbinden, um auf ihre Desktops zuzugreifen.</p> |
| <b>Ausschalten</b> | <p>Die virtuelle Maschine wird heruntergefahren, wenn sich ein Benutzer abmeldet, jedoch nicht, wenn ein Benutzer die Verbindung trennt.</p>  |

**Hinweis** Wenn Sie einen Computer zu einem manuellen Pool hinzufügen, schaltet View den Computer ein, um sicherzustellen, dass er vollständig konfiguriert ist. Dies geschieht selbst dann, wenn Sie die Betriebsrichtlinie **Ausschalten** oder **Keine Betriebsaktion vornehmen** auswählen. Sobald der View Agent konfiguriert ist, wird er als bereit markiert, und es gelten die normalen Betriebsverwaltungseinstellungen für den Pool.

Für manuelle Pools mit Computern, die über vCenter Server verwaltet werden, schaltet View einen Reservecomputer ein, damit die Benutzer sich verbinden können. Der Reservecomputer wird unabhängig davon eingeschaltet, welche Betriebsrichtlinie in Kraft ist.

**Tabelle 11-8. Zeitpunkt der Anwendung der Betriebsrichtlinie durch View** beschreibt, wann View die konfigurierte Betriebsrichtlinie anwendet.

**Tabelle 11-8. Zeitpunkt der Anwendung der Betriebsrichtlinie durch View**

| Typ des Desktop-Pools   | Anwendung der Betriebsrichtlinie   |
|---|--|
| Manueller Pool mit einem Computer (über vCenter Server verwaltete virtuelle Maschine) | <p>Betriebsvorgänge werden durch die Sitzungsverwaltung initiiert. Die virtuelle Maschine wird eingeschaltet, wenn ein Benutzer den Desktop anfordert, und ausgeschaltet oder angehalten, wenn der Benutzer sich abmeldet.</p> <p><b>Hinweis</b> Die Richtlinie <b>Computer müssen immer eingeschaltet sein</b> wird immer angewendet, unabhängig davon, ob der Pool mit einem einzigen Computer eine dynamische oder dedizierte Zuweisung verwendet und ob der Computer zugewiesen oder nicht zugewiesen ist.</p> |
| Automatisierter Pool mit dedizierter Zuweisung  | <p>Wird nur auf nicht zugewiesene Computer angewendet.</p> <p>Auf zugewiesenen Computern werden Betriebsvorgänge von der Sitzungsverwaltung initiiert. Virtuelle Maschinen werden eingeschaltet, wenn ein Benutzer einen zugewiesenen Computer anfordert, und ausgeschaltet oder angehalten, wenn der Benutzer sich abmeldet.</p> <p><b>Hinweis</b> Die Richtlinie <b>Computer müssen immer eingeschaltet sein</b> gilt für zugewiesene und nicht zugewiesene Computer.</p>  |
| Automatisierter Pool mit dynamischer Zuweisung  | <p>Wird angewendet, wenn ein Computer nicht verwendet wird und nachdem ein Benutzer sich abgemeldet hat.</p> <p>Wenn Sie die Betriebsrichtlinie <b>Ausschalten</b> oder <b>Anhalten</b> für einen Desktop-Pool mit dynamischer Zuweisung konfigurieren, stellen Sie <b>Nach Verbindungstrennung automatisch abmelden</b> auf <b>Sofort</b>, um verworfene oder verwaiste Sitzungen zu verhindern.</p>  |
| Manueller Pool mit dedizierter Zuweisung  | <p>Wird nur auf nicht zugewiesene Computer angewendet.</p> <p>Auf zugewiesenen Computern werden Betriebsvorgänge von der Sitzungsverwaltung initiiert. Virtuelle Maschinen werden eingeschaltet, wenn ein Benutzer einen zugewiesenen Computer anfordert, und ausgeschaltet oder angehalten, wenn der Benutzer sich abmeldet.</p> <p><b>Hinweis</b> Die Richtlinie <b>Computer müssen immer eingeschaltet sein</b> gilt für zugewiesene und nicht zugewiesene Computer.</p>  |
| Manueller Pool mit dynamischer Zuweisung  | <p>Wird angewendet, wenn ein Computer nicht verwendet wird und nachdem ein Benutzer sich abgemeldet hat.</p> <p>Wenn Sie die Betriebsrichtlinie <b>Ausschalten</b> oder <b>Anhalten</b> für einen Desktop-Pool mit dynamischer Zuweisung konfigurieren, stellen Sie <b>Nach Verbindungstrennung automatisch abmelden</b> auf <b>Sofort</b>, um verworfene oder verwaiste Sitzungen zu verhindern.</p>  |

Wie View die konfigurierte Betriebsrichtlinie auf automatisierte Pools anwendet, hängt davon ab, ob ein Computer verfügbar ist. Weitere Informationen finden Sie unter [Auswirkungen von Betriebsrichtlinien auf automatisierte Desktop-Pools](#).



## Konfigurieren von speziellen Maschinen zum Anhalten nach Trennung der Verbindung durch Benutzer

Die Betriebsrichtlinie **Anhalten** bewirkt, dass virtuelle Maschinen angehalten werden, wenn sich ein Benutzer abmeldet, aber nicht wenn ein Benutzer die Verbindung trennt. Sie können Maschinen in einem dedizierten Pool auch so konfigurieren, dass sie angehalten werden, wenn ein Benutzer die Verbindung zu einem Desktop trennt, ohne sich abzumelden. Die Verwendung der Anhaltefunktion bei der Trennung der Verbindung durch Benutzer hilft dabei, Ressourcen zu sparen.

Um die Funktion zu aktivieren, dass bei Trennen der Verbindung spezielle Maschinen angehalten werden, muss ein Attribut in View LDAP gesetzt werden.

### Verfahren

- 1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem View-Verbindungsserver-Host.
- 2 Wählen Sie im Konsolenbaum **Verbinden mit**.
- 3 Geben Sie im Feld **Domäne oder Server auswählen bzw. eintippen** den Servernamen als **localhost:389** ein.
- 4 Klicken Sie unter **Verbindungspunkt** auf **Definierten Namen oder Namenskontext auswählen bzw. eintippen**, geben Sie den definierten Namen als **DC=vdi,DC=vmware,DC=int** ein und klicken Sie auf **OK**.

Das Hauptfenster des ADAM ADSI-Editors wird angezeigt.

- 5 Erweitern Sie die ADAM ADSI-Baumstruktur und erweitern Sie **OU=Properties**.
- 6 Wählen Sie **OU=Global** und wählen Sie **CN=Common** im rechten Fensterbereich.
- 7 Wählen Sie **Aktion > Eigenschaften** und fügen Sie unter dem Attribut **pae-NameValuePair** den neuen Eintrag **suspendOnDisconnect=1** hinzu.
- 8 Starten Sie den VMware Horizon View-Verbindungsserver-Dienst oder View-Verbindungsserver neu.

## Auswirkungen von Betriebsrichtlinien auf automatisierte Desktop-Pools

Wie View die konfigurierte Betriebsrichtlinie auf automatisierte Pools anwendet, hängt davon ab, ob eine Maschine verfügbar ist.

Eine Maschine in einem automatisierten Pool wird als verfügbar betrachtet, wenn sie den folgenden Kriterien entspricht:

- Desktop ist aktiv
- Desktop enthält keine Benutzersitzung
- Desktop ist keinem Benutzer zugewiesen

Der auf der Maschine ausgeführte View Agent-Dienst bestätigt View-Verbindungsserver die Verfügbarkeit der Maschine.

Bei der Konfiguration eines automatisierten Pools können Sie die Mindest- und die Höchstzahl an bereitzustellenden virtuellen Maschinen sowie die Anzahl an Reservemaschinen angeben, die zu jedem Zeitpunkt eingeschaltet bleiben und zur Verfügung stehen müssen.

## Beispiele für Betriebsrichtlinien für automatisierte Pools mit dynamischer Zuweisung

Wenn Sie einen automatisierten Pool mit dynamischer Zuweisung konfigurieren, können Sie festlegen, dass eine bestimmte Anzahl an Maschinen zu jedem Zeitpunkt zur Verfügung stehen muss. Die verfügbaren Reservemaschinen sind unabhängig von der Betriebsrichtlinieneinstellung jederzeit eingeschaltet.

### Betriebsrichtlinie – Beispiel 1

[Tabelle 11-9. Desktop-Pool-Einstellungen für einen automatisierten Pool mit dynamischer Zuweisung – Beispiel 1](#) beschreibt den automatisierten Pool mit dynamischer Zuweisung in diesem Beispiel. Der Pool verwendet ein Maschinenbenennungsmuster, um die Maschinen bereitzustellen und zu benennen.

**Tabelle 11-9. Desktop-Pool-Einstellungen für einen automatisierten Pool mit dynamischer Zuweisung – Beispiel 1**

| Desktop-Pool-Einstellung                   | Wert        |
|--|-------------|
| Anzahl an Computern (Minimum)              | 10          |
| Anzahl an Computern (Maximum)              | 20          |
| Anzahl an eingeschalteten Reservemaschinen | 2           |
| Betriebsrichtlinie für Remote-Computer     | Ausschalten |

Bei Bereitstellung dieses Desktop-Pools werden zehn Maschinen erstellt, zwei Maschinen werden eingeschaltet und stehen sofort zur Verfügung, und acht Maschinen sind ausgeschaltet.

Für jeden neuen Benutzer, der sich mit dem Pool verbindet, wird eine Maschine eingeschaltet, um die Anzahl an verfügbaren Reservemaschinen zu erhalten. Wenn mehr als acht Benutzer verbunden sind, werden weitere Maschinen bis zur Höchstzahl von 20 erstellt, um die Anzahl an Reservemaschinen beizubehalten. Nach Erreichen der Höchstzahl bleiben die Maschinen der ersten zwei Benutzer, die ihre Verbindung trennen, eingeschaltet, um die Anzahl an Reservemaschinen zu erhalten. Die Maschinen aller nachfolgenden Benutzer werden der Betriebsrichtlinie entsprechend ausgeschaltet.

### Betriebsrichtlinie – Beispiel 2

[Tabelle 11-10. Desktop-Pool-Einstellungen für einen automatisierten Pool mit dynamischer Zuweisung – Beispiel 2](#) beschreibt den automatisierten Pool mit dynamischer Zuweisung in diesem Beispiel. Der Pool verwendet ein Maschinenbenennungsmuster, um die Maschinen bereitzustellen und zu benennen.

**Tabelle 11-10. Desktop-Pool-Einstellungen für einen automatisierten Pool mit dynamischer Zuweisung – Beispiel 2**

| Desktop-Pool-Einstellung                   | Wert        |
|--|-------------|
| Anzahl an Computern (Minimum)              | 5           |
| Anzahl an Computern (Maximum)              | 5           |
| Anzahl an eingeschalteten Reservemaschinen | 2           |
| Betriebsrichtlinie für Remote-Computer     | Ausschalten |

Bei Bereitstellung dieses Desktop-Pools werden fünf Maschinen erstellt, zwei Maschinen werden eingeschaltet und stehen sofort zur Verfügung, und drei Maschinen sind ausgeschaltet.

Wird eine vierte Maschine in diesem Pool ausgeschaltet, wird eine der vorhandenen Maschinen eingeschaltet. Es wird keine weitere Maschine eingeschaltet, weil die Höchstzahl an Maschinen bereits erreicht ist.

## Beispiel für Betriebsrichtlinien für automatisierte Pools mit dedizierter Zuweisung

Im Gegensatz zu einer eingeschalteten Maschine in einem automatisierten Pool mit dynamischer Zuweisung steht eine eingeschaltete Maschine in einem automatisierten Pool mit dedizierter Zuweisung nicht unbedingt zur Verfügung. Sie ist nur dann verfügbar, wenn die Maschine keinem Benutzer zugewiesen ist.

[Tabelle 11-11. Desktop-Pool-Einstellungen für einen automatisierten Pool mit dedizierter Zuweisung – Beispiel](#) beschreibt den automatisierten Pool mit dedizierter Zuweisung in diesem Beispiel.

**Tabelle 11-11. Desktop-Pool-Einstellungen für einen automatisierten Pool mit dedizierter Zuweisung – Beispiel**

| Desktop-Pool-Einstellung                   | Wert                                     |
|--|--|
| Anzahl an Computern (Minimum)              | 3  |
| Anzahl an Computern (Maximum)              | 5  |
| Anzahl an eingeschalteten Reservemaschinen | 2  |
| Betriebsrichtlinie für Remote-Computer     | Computer müssen immer eingeschaltet sein |

Wird dieser Desktop-Pool bereitgestellt, werden drei Maschinen erstellt und eingeschaltet. Wenn die Maschinen in vCenter Server ausgeschaltet werden, werden sie gemäß der Betriebsrichtlinie sofort wieder eingeschaltet.

Nachdem ein Benutzer sich mit einer Maschine im Pool verbunden hat, wird die Maschine dem entsprechenden Benutzer dauerhaft zugewiesen. Nachdem der Benutzer die Verbindung zur Maschine getrennt hat, steht die Maschine keinem anderen Benutzer mehr zur Verfügung. Die Richtlinie **Computer müssen immer eingeschaltet sein** gilt jedoch weiterhin. Wird die zugewiesene Maschine in vCenter Server ausgeschaltet, wird sie sofort wieder eingeschaltet.

Wenn ein anderer Benutzer eine Verbindung herstellt, wird eine zweite Maschine zugewiesen. Da die Anzahl an Reservemaschinen unter die Mindestgrenze fällt, sobald sich der zweite Benutzer verbindet, wird eine weitere Maschine erstellt und eingeschaltet. Bei jeder Zuweisung eines neuen Benutzers wird eine weitere Maschine erstellt und eingeschaltet, bis die Höchstzahl an Maschinen erreicht ist.

## Verhindern von Betriebsrichtlinienkonflikten

Wenn Sie eine Betriebsrichtlinie mithilfe von View Administrator konfigurieren, müssen Sie diese mit den Energieoptionen in der Systemsteuerung auf dem Gastbetriebssystem vergleichen, um Betriebsrichtlinienkonflikte zu vermeiden.

Eine virtuelle Maschine ist möglicherweise vorübergehend nicht verfügbar, wenn die für den Computer konfigurierte Betriebsrichtlinie nicht zu den Energieoptionen kompatibel ist, die für das Gastbetriebssystem konfiguriert wurden. Wenn sich weitere Computer in demselben Pool befinden, können auch diese betroffen sein.

Die folgende Konfiguration ist ein Beispiel für einen Betriebsrichtlinienkonflikt:

- In View Administrator ist die Betriebsrichtlinie **Anhalten** für die virtuelle Maschine konfiguriert. Durch diese Richtlinie wird die virtuelle Maschine angehalten, wenn sie nicht verwendet wird.
- In den Energieoptionen in der Systemsteuerung des Gastbetriebssystems ist die Option **Put the Energiesparmodus nach** auf drei Minuten festgelegt.

Bei dieser Konfiguration können sowohl View-Verbindungsserver als auch das Gastbetriebssystem die virtuelle Maschine anhalten. Durch die Energieoption des Gastbetriebssystems ist die virtuelle Maschine möglicherweise nicht verfügbar, während View-Verbindungsserver erwartet, dass sie eingeschaltet ist.

## Konfigurieren von 3D-Rendern auf Windows 7- oder neueren Desktops

Wenn Sie einen Windows 7- oder neueren Desktop-Pool erstellen, können Sie 3D-Grafikrendern für Ihre Desktops konfigurieren. Desktops können Virtual Shared Graphics Acceleration (vSGA) und Virtual Dedicated Graphics Acceleration (vDGA) nutzen – vSphere-Funktionen, die auf ESXi-Hosts installierte physische Grafikkarten nutzen und die Ressourcen der GPU (Graphics Processing Unit) zwischen den virtuellen Maschinen verwalten.

Wenn Sie die hardwarebasierten Optionen für den **3D-Renderer** verwenden, können Benutzer 3D-Anwendungen für Entwurf, Modellierung und Multimedia nutzen, die üblicherweise eine gute Performance der GPU-Hardware erfordern. Die Einstellung **3D-Renderer** bietet auch eine Softwareoption, die Grafikverbesserungen liefert, die weniger anspruchsvolle Anwendungen wie Windows AERO, Microsoft Office und Google Earth unterstützen können.

## Anforderungen für das 3D-Rendern

Um Hardware- oder Software-3D-Grafikrendern zu aktivieren, muss Ihre Poolbereitstellung die folgenden Anforderungen erfüllen:

- Die virtuellen Maschinen müssen Windows 7 oder höher sein.

- Der Pool muss PCoIP als Standardanzeigeprotokoll verwenden.
- Den Benutzern darf keine Berechtigung zur Auswahl ihres eigenen Protokolls gewährt werden

Damit hardwarebasiertes 3D-Rendern unterstützt wird, muss der Pool die folgenden zusätzlichen Anforderungen erfüllen:

- Um vSGA zu verwenden, müssen die virtuellen Maschinen auf Hosts mit ESXi 5.1 oder höher ausgeführt und von vCenter Server 5.1-Software oder höher verwaltet werden. Diese Funktion ermöglicht es virtuellen Maschinen, die physischen GPUs auf ESXi-Hosts gemeinsam zu nutzen. Sie können 3D-Anwendungen für Design, Modellierung und Multimedia verwenden.
- Um vDGA zu verwenden, müssen die virtuellen Maschinen auf Hosts mit ESXi 5.5 oder höher ausgeführt werden, die Hardware-Version 9 oder höher aufweisen und von vCenter Server 5.5-Software oder höher verwaltet werden. Diese Funktion stellt eine einzelne physische GPU (Grafikprozessor) auf einem ESXi-Host für eine einzelne virtuelle Maschine ab. Verwenden Sie diese Funktion, wenn Sie hochwertige, hardwarebeschleunigte Workstation-Grafiken benötigen.

Um vDGA zu verwenden, müssen Sie die GPU-Durchschleifung auf den ESXi-Hosts aktivieren und die einzelnen virtuellen Maschinen so konfigurieren, dass sie dedizierte PCI-Geräte verwenden, nachdem der Desktop-Pool in View erstellt wurde. Sie können die übergeordnete virtuelle Maschine oder die Vorlage für vDGA nicht konfigurieren und dann einen Desktop-Pool erstellen, da sich dieselbe physische GPU um jede virtuellen Maschine im Pool kümmern müsste. Informationen zur Grafikkbeschleunigung finden Sie unter „vDGA-Installation“ im [VMware-Whitepaper](#).

Für virtuelle Maschinen mit verknüpftem Klon bleiben die vDGA-Einstellungen nach Aktualisierungen, Neuzusammenstellungen und Neuverteilungsvorgängen erhalten.

- Auf den ESXi-Hosts müssen GPU-Grafikkarten und damit verbundene vSphere Installation Bundles (VIBs) installiert werden. Eine Liste unterstützter GPU-Hardware finden Sie in der „VMware Hardware-Kompatibilitätsliste“ unter <http://www.vmware.com/resources/compatibility/search.php>.
- Windows 7-Maschinen müssen über virtuelle Hardware der Version 8 oder höher verfügen. Windows 8-Maschinen müssen über virtuelle Hardware der Version 9 oder höher verfügen.

Damit softwarebasiertes 3D-Rendern unterstützt wird, muss der Pool die folgenden zusätzlichen Anforderungen erfüllen:

- Die virtuellen Maschinen müssen auf Hosts mit ESXi 5.0 oder höher ausgeführt und von vCenter Server 5.0-Software oder höher verwaltet werden.
- Die Maschinen müssen virtuelle Hardware der Version 8 oder höher verwenden.

Wenn Sie die Einstellung **3D-Renderer** konfigurieren oder bearbeiten, müssen Sie vorhandene virtuelle Maschinen ausschalten, sicherstellen, dass die Maschinen in vCenter Server neu konfiguriert sind, und die Maschinen einschalten, damit die neue Einstellung wirksam wird. Durch einen Neustart einer virtuellen Maschine wird diese neue Einstellung nicht übernommen.

## Konfigurieren des 3D-Renderns

Sie wählen Optionen, die bestimmen, wie View das 3D-Rendern verwaltet. Weitere Informationen finden Sie unter [3D-Render-Optionen](#).

Wenn Sie die Einstellung **3D-Renderer** aktivieren, können Sie die Größe des VRAM konfigurieren, der den virtuellen Maschinen im Pool zugewiesen ist. Dazu bewegen Sie den Schieberegler im Dialogfeld **VRAM für 3D-Gäste konfigurieren**. Die VRAM-Mindestgröße beträgt 64 MB. Für virtuelle Maschinen der Hardwareversion 9 beträgt die standardmäßige VRAM-Größe 96MB und Sie können eine maximale Größe von 512MB konfigurieren. Für virtuelle Maschinen der Hardwareversion 8 beträgt die standardmäßige VRAM-Größe 64 MB und Sie können eine maximale Größe von 128 MB konfigurieren.

Die VRAM-Einstellungen, die Sie in View Administrator konfigurieren, haben Vorrang vor den VRAM-Einstellungen, die für die virtuellen Maschinen in vSphere Client oder vSphere Web Client konfiguriert werden können, es sei denn, Sie wählen die Option **Verwaltung mit Hilfe von vSphere Client**.

Wenn Sie die Einstellung **3D-Renderer** aktivieren, können Sie die Einstellung **Maximale Anzahl an Monitoren** auf einen oder zwei Monitore setzen. Sie können nicht mehr als zwei Monitore auswählen. Weiterhin beträgt die **maximale Auflösung für jeden Monitor** 1920x1200 Pixel.

## 3D-Render-Optionen

Mit den Optionen der Einstellung **3D-Renderer** für Desktop-Pools können Sie das Grafikrendern auf verschiedene Weise konfigurieren.

**Tabelle 11-12. 3D-Render-Optionen für Pools mit vSphere 5.1 oder höher**

| Option                                 | Beschreibung  |
|--|---|
| Verwaltung mithilfe des vSphere-Client | <p>Die im vSphere Web Client (oder vSphere Client in vSphere 5.1) für eine virtuelle Maschine eingestellte Option <b>3D-Renderer</b> bestimmt die Art des stattfindenden 3D-Grafikrenderns. View steuert nicht das 3D-Rendern.</p> <p>Sie können im vSphere Web Client oder im vSphere Client die Optionen <b>Automatisch</b>, <b>Software</b> oder <b>Hardware</b> konfigurieren. Diese Optionen haben dieselbe Auswirkung, wie wenn Sie sie in View Administrator einstellen.</p> <p>Wenn Sie die Option <b>Verwaltung mit Hilfe von vSphere Client</b> auswählen, sind die Einstellungen <b>VRAM für 3D-Gäste konfigurieren</b>, <b>Maximale Anzahl an Monitoren</b> und <b>Maximale Auflösung eines Monitors</b> in View Administrator inaktiv. Sie können diese Einstellungen für eine virtuelle Maschine in vSphere Web Client oder vSphere Client konfigurieren.</p> |
| Automatisch                            | <p>3D-Rendern ist aktiviert. Der ESXi-Host steuert die Art 3D-Renderns, das ausgeführt wird.</p> <p>Der ESXi-Host reserviert beispielsweise die GPU-Hardwareressourcen in der Reihenfolge, in der die virtuellen Maschinen eingeschaltet werden. Sind beim Einschalten einer virtuellen Maschine bereits alle GPU-Hardwareressourcen reserviert, verwendet ESXi den Software-Renderer für diese Maschine.</p> <p>Wenn Sie hardwarebasiertes 3D-Rendern konfigurieren, können Sie die GPU-Ressourcen prüfen, die jeder einzelnen virtuellen Maschine auf einem ESXi-Host zugewiesen sind. Weitere Informationen finden Sie unter <a href="#">Prüfen der GPU-Ressourcen auf einem ESXi-Host</a>.</p>  |
| Software                               | <p>3D-Rendern ist aktiviert. Der ESXi-Host verwendet das Software-3D-Grafikrendern. Wenn auf dem ESXi-Host eine GPU-Grafikkarte installiert ist, wird sie von diesem Pool nicht verwendet.</p> <p>Im Dialogfeld <b>VRAM für 3D-Gäste konfigurieren</b> können Sie mithilfe des Schiebereglers die Menge des reservierten VRAM erhöhen.</p>  |

| Option      | Beschreibung  |
|-------------|---|
| Hardware    | <p>3D-Rendern ist aktiviert. Der ESXi-Host reserviert die GPU-Hardwareressourcen in der Reihenfolge, in der die virtuellen Maschinen eingeschaltet werden.</p> <p>Der ESXi-Host weist einer virtuellen Maschine VRAM auf der Basis des Wertes zu, der im Dialogfeld <b>VRAM für 3D-Gäste konfigurieren</b> eingestellt ist.</p> <hr/> <p><b>Wichtig</b> Wenn Sie die Option <b>Hardware</b> konfigurieren, sollten Sie diese möglichen Einschränkungen berücksichtigen:</p> <ul style="list-style-type: none"> <li>■ Wenn ein Benutzer versucht, eine Verbindung zu einer Maschine herzustellen, wenn alle GPU-Hardwareressourcen reserviert sind, schaltet sich die virtuelle Maschine nicht ein und der Benutzer erhält eine Fehlermeldung.</li> <li>■ Eine Maschine kann nicht von vMotion auf einen ESXi-Host verschoben werden, für den keine GPU-Hardware konfiguriert ist.</li> <li>■ Um vSGA (Virtual Shared Graphics Acceleration) zu verwenden, müssen alle ESXi-Hosts im Cluster in der Version 5.1 oder höher vorliegen. Wenn eine virtuelle Maschine auf einem ESXi 5.0-Host in einem gemischten Cluster erstellt wird, schaltet sich die Maschine nicht ein.</li> <li>■ Um vDGA (Virtual Dedicated Graphics Acceleration) zu verwenden, müssen alle ESXi-Hosts im Cluster in der Version 5.5 oder höher vorliegen, und die virtuellen Maschinen in der Hardware-Version 9 oder höher.</li> </ul> <hr/> <p>Wenn Sie hardwarebasiertes 3D-Rendern konfigurieren, können Sie die GPU-Ressourcen prüfen, die jeder einzelnen virtuellen Maschine auf einem ESXi-Host zugewiesen sind. Weitere Informationen finden Sie unter <a href="#">Prüfen der GPU-Ressourcen auf einem ESXi-Host</a>.</p> |
| Deaktiviert | 3D-Rendern ist inaktiv.   |

Tabelle 11-13. 3D-Render-Optionen für Pools mit vSphere 5.0

| Option      | Beschreibung  |
|-------------|---|
| Aktiviert   | <p>Die Option <b>3D-Renderer</b> ist aktiviert. Der ESXi-Host verwendet das Software-3D-Grafikrendern.</p> <p>Wenn Software-Rendern konfiguriert ist, beträgt die Standard-VRAM-Größe 64 MB, die Mindestgröße. Im Dialogfeld <b>VRAM für 3D-Gäste konfigurieren</b> können Sie mithilfe des Schiebereglers die Menge des reservierten VRAM erhöhen. Beim Software-Rendern weist der ESXi-Host maximal bis zu 128 MB pro virtueller Maschine zu. Wenn Sie eine höhere VRAM-Größe einstellen, wird sie ignoriert.</p> |
| Deaktiviert | 3D-Rendern ist inaktiv.   |

Wenn ein Desktop-Pool auf einer älteren vSphere-Version als 5.0 ausgeführt wird, ist die Einstellung **3D-Renderer** inaktiv und nicht in View Administrator verfügbar.

## Empfohlene Vorgehensweise für das Konfigurieren des 3D-Renderns

Die Optionen für das 3D-Rendern und andere Pool-Einstellungen bieten verschiedene Vor- und Nachteile. Wählen Sie die Option, die zu Ihrer vSphere-Hardwareinfrastruktur und den Anforderungen Ihrer Benutzer für das Grafikrendern am besten passt.

**Hinweis** Dieses Thema gibt einen Überblick über die Steuerelemente, die Sie in View Administrator finden. Weitere Informationen zu den verschiedenen Optionen und Anforderungen in Bezug auf das 3D-Rendern finden Sie im [VMware-Whitepaper](#) zur Grafikbeschleunigung.

Die Option **Automatisch** ist für viele View-Bereitstellungen, die 3D-Rendern erfordern, am besten geeignet. Diese Option stellt sicher, dass manche 3D-Renderarten auch dann erfolgen, wenn GPU-Ressourcen vollständig reserviert sind. Bei einem gemischten Cluster aus ESXi 5.1- und ESXi 5.0-Hosts sorgt diese Option dafür, dass eine virtuelle Maschine erfolgreich eingeschaltet wird, und verwendet 3D-Rendern auch dann, wenn vMotion beispielsweise die virtuelle Maschine auf einen ESXi 5.0-Host verschoben hat.

Der einzige Nachteil der Option **Automatisch** besteht darin, dass Sie nicht leicht erkennen können, ob eine virtuelle Maschine Hardware- oder Software-3D-Rendern verwendet.

Die Option **Hardware** garantiert, dass jede virtuelle Maschine im Pool Hardware-3D-Rendern verwendet, unter der Voraussetzung, dass GPU-Ressourcen auf den ESXi-Hosts verfügbar sind. Diese Option eignet sich ggf. am besten, wenn alle Ihre Benutzer grafikintensive Anwendungen ausführen.

Bei der Option **Hardware** müssen Sie Ihre vSphere-Umgebung streng kontrollieren:

- Für vSGA (Virtual Shared Graphics Acceleration) müssen alle ESXi-Hosts über Version 5.1 oder höher verfügen und GPU-Grafikkarten installiert haben.
- Für vDGA (Virtual Dedicated Graphics Acceleration) müssen alle ESXi-Hosts über Version 5.5 oder höher verfügen und GPU-Grafikkarten installiert haben.

Wenn alle GPU-Ressourcen auf einem ESXi-Host reserviert sind, kann View keine virtuelle Maschine für den nächsten Benutzer einschalten, der versucht, sich bei einem Desktop anzumelden. Sie müssen die Zuordnung von GPU-Ressourcen und die Verwendung von vMotion verwalten, um sicherzustellen, dass für Ihre Desktops Ressourcen verfügbar sind.

Wählen Sie die Option **Verwaltung mit Hilfe von vSphere Client**, um eine gemischte Konfiguration von 3D-Rendering und VRAM-Größen für virtuelle Maschinen in einem Pool zu unterstützen. Sie können im vSphere Web Client einzelne virtuelle Maschinen mit verschiedenen Optionen und VRAM-Werten konfigurieren.

Wählen Sie die Option **Software**, wenn Sie nur über ESXi 5.0-Hosts verfügen, wenn die Hosts mit ESXi 5.1 oder höher nicht über GPU-Grafikkarten verfügen oder wenn Ihre Benutzer nur Anwendungen ausführen, die keine Hardwaregrafikbeschleunigung benötigen, wie beispielsweise AERO und Microsoft Office.

## Konfigurieren von Desktop-Einstellungen zum Verwalten von GPU-Ressourcen

Sie können andere Desktop-Einstellungen konfigurieren, um sicherzustellen, dass keine GPU-Ressourcen verschwendet werden, wenn Benutzer sie nicht aktiv verwenden.

Legen Sie für dynamische Pools eine Sitzungszeitüberschreitung fest, sodass GPU-Ressourcen für andere Benutzer freigegeben werden, wenn ein Benutzer den Desktop nicht verwendet.

Für dedizierte Pools können Sie die Einstellung **Nach Verbindungstrennung automatisch abmelden** auf **Sofort** einstellen und eine Energierichtlinie **Anhalten** festlegen, wenn diese Einstellungen für Ihre Benutzer geeignet sind. Sie sollten diese Einstellungen beispielsweise nicht für einen Pool von Forschern verwenden, die lange laufende Simulationen ausführen.



## Prüfen der GPU-Ressourcen auf einem ESXi-Host

Zur besseren Verwaltung der GPU-Ressourcen, die auf einem ESXi-Host verfügbar sind, können Sie die aktuelle GPU-Ressourcenreservierung untersuchen. Das ESXi-Befehlszeilen-Abfragedienstprogramm `gpuvmm` führt die GPUs auf, die auf einem ESXi-Host installiert sind, und zeigt den GPU-Speicher an, der für jede virtuelle Maschine auf dem Host reserviert ist. Beachten Sie, dass diese GPU-Arbeitsspeicherreservierung nicht mit der VRAM-Größe der virtuellen Maschine identisch ist.

Um das Programm auszuführen, geben Sie `gpuvmm` an der Shell-Eingabeaufforderung des ESXi-Hosts ein. Sie können eine Konsole auf dem Host oder eine SSH-Verbindung verwenden.

Das Dienstprogramm kann beispielsweise folgende Ausgabe anzeigen:

```
~ # gpuvmm
Xserver unix:0, GPU maximum memory 2076672KB
    pid 118561, VM "JB-w7-64-FC3", reserved 131072KB of GPU memory.
    pid 64408, VM "JB-w7-64-FC5", reserved 261120KB of GPU memory.
GPU memory left 1684480KB.
```

## Verhindern vom Zugriff auf View-Desktops durch RDP

In bestimmten View-Umgebungen ist die Verhinderung eines Zugriffs auf View-Desktops durch das RDP-Anzeigeprotokoll eine Priorität. Sie können die Benutzer und Administratoren beim Zugriff auf View-Desktops von der RDP-Verwendung abhalten, indem Sie die Pool-Einstellungen und die Gruppenrichtlinieneinstellungen konfigurieren.

Standardmäßig können Sie RDP verwenden, um eine Verbindung zur virtuellen Maschine von außerhalb von View herzustellen, während ein Benutzer bei einer View-Desktopsitzung angemeldet ist. Die RDP-Verbindung beendet die View-Desktopsitzung und die nicht gespeicherten Daten und Einstellungen des View-Benutzers gehen u. U. verloren. Der View-Benutzer kann sich erst dann am Desktop anmelden, wenn die externe RDP-Verbindung beendet wurde. Deaktivieren Sie die Einstellung `AllowDirectRDP`, um diese Situation zu vermeiden.

---

**Hinweis** Remote-Desktop-Dienste, in Windows XP-Systemen als „Terminaldienste“ bezeichnet, müssen auf der virtuellen Maschine gestartet werden, die Sie zur Erstellung von Pools verwenden, und auf virtuellen Maschinen, die in den Pools bereitgestellt werden. Die Remote-Desktop-Dienste sind erforderlich für die Installation von View Agent, SSO und andere View-Sitzungsverwaltungsvorgänge.

---

### Voraussetzungen

Stellen Sie sicher, dass die Datei „Administrative Vorlage zur View Agent-Konfiguration“ (ADM) in Active Directory installiert ist. Siehe [Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien \(ADM\) für View](#).

## Verfahren

- 1 Wählen Sie PCoIP als das Anzeigeprotokoll, das View-Verbindungsserver zur Kommunikation mit Horizon Client-Geräten verwenden soll.

| Option  | Beschreibung  |
|---|---|
| <b>Erstellung eines Desktop-Pools</b>             | <ol style="list-style-type: none"> <li>a Starten Sie in View Administrator den Assistenten <b>Desktop-Pool hinzufügen</b>.</li> <li>b Wählen Sie auf der Seite für die Desktop-Pool-Einstellungen <b>PCoIP</b> als Standardanzeigeprotokoll aus.</li> </ol>                   |
| <b>Bearbeiten eines bestehenden Desktop-Pools</b> | <ol style="list-style-type: none"> <li>a Wählen Sie in View Administrator den Desktop-Pool aus und klicken Sie auf <b>Bearbeiten</b>.</li> <li>b Wählen Sie auf der Registerkarte <b>Desktop-Pool-Einstellungen</b> <b>PCoIP</b> als Standardanzeigeprotokoll aus.</li> </ol> |

- 2 Wählen Sie für die Einstellung **Benutzern die Wahl des Protokolls erlauben** die Option **Nein**.
- 3 Verhindern Sie, dass sich Geräte, auf denen Horizon Client nicht ausgeführt wird, direkt über RDP mit View-Desktops verbinden, indem Sie die Gruppenrichtlinieneinstellung AllowDirectRDP deaktivieren.
  - a Öffnen Sie auf Ihrem Active Directory-Server die Konsole zur Gruppenrichtlinienverwaltung und wählen Sie **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > VMware View Agent-Konfiguration** aus.
  - b Deaktivieren Sie die Einstellung **Direkte RDP-Verbindung** zulassen.

## Bereitstellen großer Desktop-Pools

Wenn viele Benutzer das gleiche Desktop-Image benötigen, können Sie einen großen automatisierten Pool anhand einer einzigen Vorlage oder übergeordneten virtuellen Maschine erstellen. Indem Sie nur ein Basis-Image und einen Poolnamen verwenden, können Sie vermeiden, dass Maschinen willkürlich in kleinere Gruppen aufgeteilt werden, die separat verwaltet werden müssen. Diese Strategie vereinfacht die View-Bereitstellung und Verwaltungsaufgaben.

Damit große Pools unterstützt werden, können Sie Pools auf ESXi-Clustern erstellen, die bis zu 32 ESXi-Hosts enthalten. Sie können auch einen Pool konfigurieren, der mehrere Netzwerkbezeichnungen verwendet, sodass die IP-Adressen mehrerer Port-Gruppen den virtuellen Maschinen im Pool zur Verfügung stehen.

## Konfigurieren von Desktop-Pools auf Clustern mit mehr als acht Hosts

In vSphere 5.1 und höher können Sie einen Linked-Clone-Desktop-Pool in einem Cluster bereitstellen, der bis zu 32 ESXi-Hosts enthält. Alle ESXi-Hosts im Cluster müssen über die Version 5.1 oder höher verfügen. Die Hosts können VMFS- oder NFS-Datenspeicher verwenden. VMFS-Datenspeicher müssen vom Typ VMFS5 oder neuer sein.

In vSphere 5.0 können Sie verknüpfte Klone in einem Cluster bereitstellen, der mehr als acht ESXi-Hosts umfasst, müssen Replikatfestplatten dabei jedoch in NFS-Datenspeichern speichern. Sie können Replikatfestplatten auf VMFS-Datenspeichern nur mit Clustern speichern, die acht oder weniger Hosts enthalten.

In vSphere 5.0 gelten die folgenden Regeln, wenn Sie einen Linked-Clone-Pool auf einem Cluster konfigurieren, der mehr als acht Hosts enthält:

- Wenn Sie Replikatfestplatten auf denselben Datenspeichern wie die Betriebssystemfestplatten speichern, müssen Sie sowohl die Replikat- als auch die Betriebssystemfestplatten auf NFS-Datenspeichern speichern.
- Wenn Sie Replikatfestplatten auf anderen Datenspeichern als die Betriebssystemfestplatten speichern, müssen die Replikatfestplatten auf NFS-Datenspeichern gespeichert werden. Die Betriebssystemfestplatten können auf NFS- oder VMFS-Datenspeichern gespeichert werden.
- Wenn Sie persistente Festplatten von View Composer auf separaten Datenspeichern speichern, können die persistenten Festplatten auf NFS- oder VMFS-Datenspeichern konfiguriert werden.

In vSphere 4.1 und früheren Versionen können Sie Desktop-Pools nur mit Clustern bereitstellen, die acht oder weniger Hosts enthalten.

## **Zuweisen mehrerer Netzwerkbezeichnungen zu einem Desktop-Pool**

In View 5.2 und höheren Versionen können Sie einen automatisierten Desktop-Pool konfigurieren, der mehrere Netzwerkbezeichnungen verwendet. Sie können mehrere Netzwerkbezeichnungen einem Linked-Clone-Pool oder einem automatisierten Pool zuweisen, der vollständige virtuelle Maschinen enthält.

In früheren Versionen erben virtuelle Maschinen im Pool die Netzwerkbezeichnungen, die von Netzwerkkarten der übergeordneten virtuellen Maschine oder Vorlage verwendet wurden. Eine typische übergeordnete virtuelle Maschine oder Vorlage enthält eine Netzwerkkarte und eine Netzwerkbezeichnung. Eine Netzwerkbezeichnung definiert eine Portgruppe und ein VLAN. Die Netzmaske eines VLANs stellt üblicherweise einen begrenzten Bereich verfügbarer IP-Adressen bereit.

In View 5.2 und höheren Versionen können Sie Netzwerkbezeichnungen zuweisen, die in vCenter Server für alle ESXi-Hosts im Cluster verfügbar sind, in dem der Desktop-Pool bereitgestellt wird. Durch Konfigurieren mehrerer Netzwerkbezeichnungen für den Pool erweitern Sie erheblich die Anzahl der IP-Adressen, die den virtuellen Maschinen im Pool zugewiesen werden können.

Sie müssen View PowerCLI-Cmdlets verwenden, um einem Pool mehrere Netzwerkbezeichnungen zuzuweisen. Sie können diese Aufgabe nicht in View Administrator ausführen.

Einzelheiten zur Verwendung von View PowerCLI zur Durchführung dieser Aufgabe finden Sie unter „Zuweisen mehrerer Netzwerkbezeichnungen zu einem Desktop-Pool“ im Kapitel „Verwenden von View PowerCLI“ im Dokument *Integration von View*.

# Berechtigten von Benutzern und Gruppen

# 12

Sie konfigurieren Berechtigungen, um zu steuern, auf welche Remote-Desktops und -Anwendungen Ihre Benutzer zugreifen können. Mithilfe der Funktion für eingeschränkte Berechtigungen kann der Desktop-Zugriff zudem basierend auf der View-Verbindungsserver-Instanz gesteuert werden, mit der sich die Benutzer bei der Auswahl von Remote-Desktops verbinden.

In einer Cloud-Pod-Architektur-Umgebung erstellen Sie globale Berechtigungen, um Benutzern oder Gruppen den Zugriff auf mehrere Desktops in mehreren Pods eines Pod-Verbunds zu gewähren. Bei Verwendung von globalen Berechtigungen ist es nicht erforderlich, lokale Berechtigungen für Remote-Desktops zu konfigurieren und zu verwalten. Weitere Informationen zu globalen Berechtigungen und zur Einrichtung einer Cloud-Pod-Architekturumgebung finden Sie im Dokument *Verwalten der View-Cloud-Pod-Architektur*.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen von Berechtigungen zu einem Desktop- oder Anwendungspool](#)
- [Entfernen von Berechtigungen für einen Desktop- oder Anwendungspool](#)
- [Überprüfen von Desktop-Pool- und Anwendungspool-Berechtigungen](#)
- [Einschränken des Zugriffs auf Remote-Desktops](#)

## Hinzufügen von Berechtigungen zu einem Desktop- oder Anwendungspool

Bevor Benutzer auf Remote-Desktops oder -Anwendungen zugreifen können, muss ihnen die Berechtigung für die Verwendung eines Desktop- oder Anwendungspools zugewiesen werden.

### Voraussetzungen

Erstellen Sie einen Desktop- oder Anwendungspool.

## Verfahren

- 1 Wählen Sie den Desktop- oder Anwendungspool aus.

| Option  | Aktion  |
|---|---|
| Eine Berechtigung für einen Desktop-Pool hinzufügen   | Wählen Sie in View Administrator <b>Katalog &gt; Desktop-Pools</b> aus und klicken Sie auf den Namen des Desktop-Pools.     |
| Eine Berechtigung für einen Anwendungspool hinzufügen | Wählen Sie in View Administrator <b>Katalog &gt; Anwendungspools</b> aus und klicken Sie auf den Namen des Anwendungspools. |

- 2 Wählen Sie die Option **Berechtigung hinzufügen** aus dem Dropdown-Menü **Berechtigungen** aus.
- 3 Klicken Sie auf **Hinzufügen**, wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf **Suchen**, um basierend auf den angegebenen Suchkriterien nach Benutzern oder Gruppen zu suchen.

**Hinweis** Lokale Domänengruppen werden aus Suchergebnissen für Domänen im gemischten Modus herausgefiltert. Sie können Benutzer in lokalen Gruppen der Domäne nicht berechtigen, wenn Ihre Domäne im gemischten Modus konfiguriert ist.

- 4 Wählen Sie die Benutzer oder Gruppen aus, die für die Desktops oder Anwendungen im Pool berechtigt sein sollen, und klicken Sie auf **OK**.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

## Entfernen von Berechtigungen für einen Desktop- oder Anwendungspool

Sie können Berechtigungen für einen Desktop- oder Anwendungspool entfernen, um den Zugriff auf einen Desktop oder eine Anwendung durch bestimmte Benutzer oder Gruppen zu verhindern.

## Verfahren

- 1 Wählen Sie den Desktop- oder Anwendungspool aus.

| Option  | Beschreibung  |
|---|---|
| Entfernen einer Berechtigung für einen Desktop-Pool   | Wählen Sie in View Administrator <b>Katalog &gt; Desktop-Pools</b> und klicken Sie auf den Namen des Desktop-Pools.     |
| Entfernen einer Berechtigung für einen Anwendungspool | Wählen Sie in View Administrator <b>Katalog &gt; Anwendungspools</b> und klicken Sie auf den Namen des Anwendungspools. |

- 2 Wählen Sie im Dropdown-Menü **Berechtigungen** die Option **Berechtigung entfernen**.
- 3 Wählen Sie den Benutzer oder die Gruppe, deren Berechtigung entfernt werden soll, und klicken Sie auf **Entfernen**.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

# Überprüfen von Desktop-Pool- und Anwendungspool-Berechtigungen

Sie können die Desktop-Pool- und Anwendungspool-Berechtigungen eines Benutzers oder einer Gruppe überprüfen.

## Verfahren

- 1 Wählen Sie in View Administrator **Benutzer und Gruppen** und klicken Sie auf den Benutzer- oder Gruppennamen.
- 2 Klicken Sie auf die Registerkarte **Berechtigungen** und überprüfen Sie die Desktop- und Anwendungspools, für die der betreffende Benutzer oder die betreffende Gruppe eine Berechtigung besitzt.

| Option  | Aktion                                   |
|---|--|
| Desktop-Pools auflisten, für die der Benutzer oder die Gruppe eine Berechtigung besitzt   | Klicken Sie auf <b>Desktop-Pools</b> .   |
| Anwendungspools auflisten, für die der Benutzer oder die Gruppe eine Berechtigung besitzt | Klicken Sie auf <b>Anwendungspools</b> . |

## Einschränken des Zugriffs auf Remote-Desktops

Mithilfe der Funktion für eingeschränkte Berechtigungen kann der Zugriff auf Remote-Desktops basierend auf der View-Verbindungsserver-Instanz eingeschränkt werden, mit der sich die Benutzer bei der Auswahl von Desktops verbinden.

Zum Einschränken von Berechtigungen weisen Sie einer View-Verbindungsserver-Instanz ein oder mehrere Kennzeichen zu. Wenn Sie anschließend einen Desktop-Pool konfigurieren, wählen Sie die Kennzeichen der View-Verbindungsserver-Instanzen aus, auf die der Desktop-Pool zugreifen können soll.

Wenn Benutzer sich an einer so konfigurieren View-Verbindungsserver-Instanz anmelden, können sie nur auf die Desktop-Pools zugreifen, die mindestens ein übereinstimmendes Kennzeichen oder keine Kennzeichen aufweisen.

**Hinweis** Sie können die Einschränkungsfunktion für Berechtigungen nicht konfigurieren, um den Zugriff auf Remoteanwendungen zu beschränken.

### ■ Beispiel für eingeschränkte Berechtigungen

In diesem Beispiel wird eine View-Bereitstellung mit zwei View-Verbindungsserver-Instanzen gezeigt. Die erste Instanz unterstützt interne Benutzer. Die zweite Instanz wird mit einem Sicherheitsserver kombiniert und unterstützt externe Benutzer.

- **Kennzeichenabgleich**

Die Funktion für eingeschränkte Berechtigungen ermittelt anhand des Kennzeichenabgleichs, ob eine View-Verbindungsserver-Instanz auf einen bestimmten Desktop-Pool zugreifen kann.

- **Überlegungen und Einschränkungen bei eingeschränkten Berechtigungen**

Vor der Implementierung von eingeschränkten Berechtigungen müssen bestimmte Überlegungen und Einschränkungen berücksichtigt werden.

- **Zuweisen von Kennzeichen zu einer View-Verbindungsserver-Instanz**

Wenn Sie einer View-Verbindungsserver-Instanz ein Kennzeichen zuweisen, können Benutzer, die sich mit dieser View-Verbindungsserver-Instanz verbinden, lediglich auf Desktop-Pools mit übereinstimmenden oder ohne jegliche Kennzeichen zugreifen.

- **Zuweisen von Kennzeichen zu einem Desktop-Pool**

Wenn Sie einem Desktop-Pool ein Kennzeichen zuweisen, können nur Benutzer, die sich mit einer View-Verbindungsserver-Instanz mit übereinstimmendem Kennzeichen verbinden, auf Desktops in diesem Pool zugreifen.

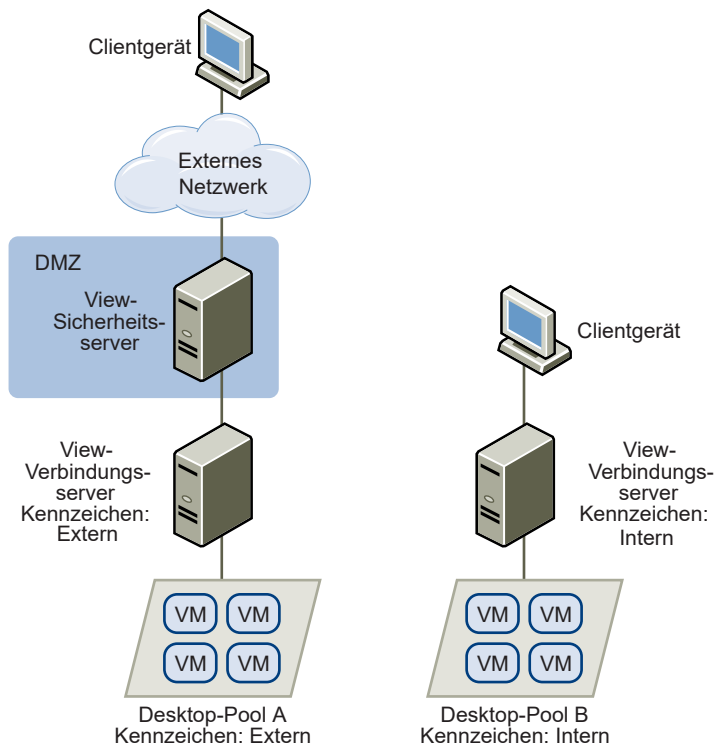
## Beispiel für eingeschränkte Berechtigungen

In diesem Beispiel wird eine View-Bereitstellung mit zwei View-Verbindungsserver-Instanzen gezeigt. Die erste Instanz unterstützt interne Benutzer. Die zweite Instanz wird mit einem Sicherheitsserver kombiniert und unterstützt externe Benutzer.

Um externe Benutzer am Zugriff auf bestimmte Desktops zu hindern, können Sie eingeschränkte Berechtigungen wie folgt einrichten:

- Weisen Sie das Kennzeichen „Intern“ der View-Verbindungsserver-Instanz zu, die die internen Benutzer unterstützt.
- Weisen Sie das Kennzeichen „Extern“ der View-Verbindungsserver-Instanz zu, die mit dem Sicherheitsserver kombiniert wird und die externen Benutzer unterstützt.
- Weisen Sie das Kennzeichen „Intern“ den Desktop-Pools zu, auf die nur interne Benutzer zugreifen dürfen.
- Weisen Sie das Kennzeichen „Extern“ den Desktop-Pools zu, auf die nur externe Benutzer zugreifen dürfen.

Externen Benutzern werden keine als „Intern“ gekennzeichneten Desktop-Pools angezeigt, da sie sich an der als „Extern“ gekennzeichneten View-Verbindungsserver-Instanz anmelden. Ebenso können interne Benutzer keine als „Extern“ gekennzeichneten Desktop-Pools sehen, da sie sich an der als „Intern“ gekennzeichneten View-Verbindungsserver-Instanz anmelden. [Abbildung 12-1. Konfiguration eingeschränkter Berechtigungen](#) zeigt diese Konfiguration.

**Abbildung 12-1. Konfiguration eingeschränkter Berechtigungen**

Außerdem können Sie mithilfe eingeschränkter Berechtigungen den Desktop-Zugriff basierend auf der Benutzerauthentifizierungsmethode steuern, die Sie für eine bestimmte View -Verbindungsserver-Instanz konfigurieren. Sie können beispielsweise bestimmte Desktop-Pools nur Benutzern zur Verfügung stellen, die sich mit einer Smartcard authentifiziert haben.

## Kennzeichenabgleich

Die Funktion für eingeschränkte Berechtigungen ermittelt anhand des Kennzeichenabgleichs, ob eine View-Verbindungsserver-Instanz auf einen bestimmten Desktop-Pool zugreifen kann.

Beim Kennzeichenabgleich wird im Wesentlichen ermittelt, ob eine View-Verbindungsserver-Instanz mit einem bestimmten Kennzeichen auf einen Desktop-Pool zugreifen kann, der dasselbe Kennzeichen aufweist.

Wenn keine Kennzeichen zugewiesen werden, kann sich dies auch darauf auswirken, ob eine View-Verbindungsserver-Instanz auf einen Desktop-Pool zugreifen kann. View-Verbindungsserver-Instanzen ohne Kennzeichen können beispielsweise nur auf Desktop-Pools zugreifen, die ebenfalls nicht über Kennzeichen verfügen.

**Tabelle 12-1. Regeln für den Kennzeichenabgleich** zeigt, wie die Funktion für eingeschränkte Berechtigungen ermittelt, ob ein View-Verbindungsserver auf einen Desktop-Pool zugreifen kann.



**Tabelle 12-1. Regeln für den Kennzeichenabgleich**

| <b>View-Verbindungsserver</b> | <b>Desktop-Pool</b>        | <b>Zugriff zulässig?</b>              |
|-------------------------------|----------------------------|---------------------------------------|
| Keine Kennzeichen             | Keine Kennzeichen          | Ja.                                   |
| Keine Kennzeichen             | Mindestens ein Kennzeichen | Nein                                  |
| Mindestens ein Kennzeichen    | Keine Kennzeichen          | Ja.                                   |
| Mindestens ein Kennzeichen    | Mindestens ein Kennzeichen | Nur bei übereinstimmenden Kennzeichen |

Die Funktion für eingeschränkte Berechtigungen erzwingt nur den Kennzeichenabgleich. Sie müssen Ihre Netzwerktopologie ändern, um für bestimmte Clients die Verbindung über eine bestimmte View-Verbindungsserver-Instanz zu erzwingen.

## Überlegungen und Einschränkungen bei eingeschränkten Berechtigungen

Vor der Implementierung von eingeschränkten Berechtigungen müssen bestimmte Überlegungen und Einschränkungen berücksichtigt werden.

- Einzelne View-Verbindungsserver-Instanzen oder Desktop-Pools können über mehrere Kennzeichen verfügen.
- Mehrere View-Verbindungsserver-Instanzen und Desktop-Pools können über dasselbe Kennzeichen verfügen.
- Auf Desktop-Pools ohne Kennzeichen kann von einer beliebigen View-Verbindungsserver-Instanz zugegriffen werden.
- View-Verbindungsserver-Instanzen ohne Kennzeichen können nur auf Desktop-Pools zugreifen, die ebenfalls nicht über Kennzeichen verfügen.
- Bei Verwendung eines Sicherheitsservers müssen Sie eingeschränkte Berechtigungen für die View-Verbindungsserver-Instanz konfigurieren, mit welcher der Sicherheitsserver kombiniert ist. Eingeschränkte Berechtigungen können nicht auf einem Sicherheitsserver konfiguriert werden.
- Sie können das Kennzeichen einer View-Verbindungsserver-Instanz nicht ändern oder entfernen, wenn dieses Kennzeichen weiterhin einem Desktop-Pool zugewiesen ist und keine anderen View-Verbindungsserver-Instanzen über ein übereinstimmendes Kennzeichen verfügen.
- Eingeschränkte Berechtigungen haben Vorrang vor anderen Desktop-Berechtigungen bzw. -Zuweisungen. Beispiel: Selbst wenn ein Benutzer einem bestimmten Computer zugewiesen ist, kann er nicht auf diesen Computer zugreifen, wenn das Kennzeichen des Desktop-Pools nicht mit dem Kennzeichen der View-Verbindungsserver-Instanz übereinstimmt, mit der sich der Benutzer verbindet.
- Wenn Sie den Zugriff auf Ihre Desktops über Workspace ermöglichen möchten und Einschränkungen für View-Verbindungsserver konfigurieren, werden im Workspace App Portal möglicherweise

Desktops angezeigt, obwohl für diese Desktops Einschränkungen gelten. Wenn ein Workspace-Benutzer versucht, sich bei einem Desktop anzumelden, wird dieser Desktop nicht gestartet, wenn das Kennzeichen des Desktop-Pools nicht mit dem Kennzeichen der View-Verbindungsserver-Instanz übereinstimmt, mit der sich der Benutzer verbindet.

## Zuweisen von Kennzeichen zu einer View-Verbindungsserver-Instanz

Wenn Sie einer View-Verbindungsserver-Instanz ein Kennzeichen zuweisen, können Benutzer, die sich mit dieser View-Verbindungsserver-Instanz verbinden, lediglich auf Desktop-Pools mit übereinstimmenden oder ohne jegliche Kennzeichen zugreifen.

### 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 Geben Sie im Textfeld **Kennzeichen** mindestens ein Kennzeichen ein.  
Trennen Sie mehrere Kennzeichen durch ein Komma oder Semikolon.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

### Nächste Schritte

Weisen Sie Kennzeichen zu Desktop-Pools zu.

## Zuweisen von Kennzeichen zu einem Desktop-Pool

Wenn Sie einem Desktop-Pool ein Kennzeichen zuweisen, können nur Benutzer, die sich mit einer View-Verbindungsserver-Instanz mit übereinstimmendem Kennzeichen verbinden, auf Desktops in diesem Pool zugreifen.

Kennzeichen können beim Hinzufügen oder Bearbeiten eines Desktop-Pools zugewiesen werden.

### Voraussetzungen

Weisen Sie einer oder mehreren View-Verbindungsserver-Instanzen Kennzeichen zu.

### Verfahren

- 1 Wählen Sie in View Administrator **Katalog > Desktop-Pools** aus.
- 2 Wählen Sie den Pool aus, dem Sie ein Kennzeichen zuweisen möchten.

| Option   | Aktion   |
|--|--|
| <b>Zuweisen eines Kennzeichens zu einem neuen Pool</b>       | Klicken Sie auf <b>Hinzufügen</b> , um den Assistenten zum Hinzufügen von Desktop-Pools zu starten und den Pool anzugeben. |
| <b>Zuweisen eines Kennzeichens zu einem vorhandenen Pool</b> | Wählen Sie den Pool aus und klicken Sie auf <b>Bearbeiten</b> .  |

### 3 Wechseln Sie zur Seite „Pool-Einstellungen“.

| Option   | Aktion  |
|--|---|
| <b>Pool-Einstellungen für einen neuen Pool</b>       | Klicken Sie im Assistenten zum Hinzufügen von Desktop-Pools auf <b>Desktop-Pool-Einstellungen</b> . |
| <b>Pool-Einstellungen für einen vorhandenen Pool</b> | Klicken Sie auf die Registerkarte <b>Desktop-Pool-Einstellungen</b> .                               |

### 4 Klicken Sie neben **Einschränkungen für Verbindungsserver** auf **Durchsuchen** und konfigurieren Sie die View-Verbindungsserver-Instanzen, die auf den Desktop-Pool zugreifen können.

| Option   | Aktion   |
|--|--|
| <b>Erteilen von Pool-Zugriff für eine beliebige View-Verbindungsserver-Instanz</b>                     | Wählen Sie <b>Keine Einschränkungen</b> .  |
| <b>Erteilen von Pool-Zugriff nur für entsprechend gekennzeichnete View-Verbindungsserver-Instanzen</b> | Wählen Sie <b>Einschränkungen für diese Tags</b> und wählen Sie mindestens ein Tag aus. Sie können die Kontrollkästchen verwenden, um mehrere Kennzeichen auszuwählen. |

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

# Konfigurieren von Remote-Desktop-Funktionen

# 13

Bestimmte Remote-Desktop-Funktionen, die mit View Agent installiert werden, können in Feature Pack Update-Versionen sowie in Hauptversionen von View aktualisiert werden. Sie können diese Funktionen so konfigurieren, dass die Remote-Desktop-Erfahrung Ihrer Endbenutzer verbessert wird.

Diese Funktionen beinhalten HTML Access, Unity Touch, Flash-URL-Umleitung, Echtzeit-Audio/Video, Windows Media Multimedia-Umleitung (MMR) und USB-Umleitung.

Informationen zu HTML Access finden Sie im Dokument *Verwenden von HTML Access* auf der Dokumentations-Webseite zu VMware Horizon Client.

Informationen zur USB-Umleitung finden Sie unter [Kapitel 14 Verwenden von USB-Geräten mit Remote-Desktops](#).

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren von Unity Touch](#)
- [Konfigurieren der Flash-URL-Umleitung für das Multicast- oder Unicast-Streaming](#)
- [Konfigurieren von Echtzeit-Audio/Video](#)
- [Konfigurieren der Scannerumleitung](#)
- [Verwalten des Zugriffs auf die Multimedia-Umleitung von Windows \(MMR\)](#)

## Konfigurieren von Unity Touch

Mit Unity Touch können Tablet- und Smartphone-Benutzer Windows-Anwendungen und -Dateien bequem durchsuchen, suchen und öffnen, bevorzugte Anwendungen und Dateien auswählen und bequem zwischen ausgeführten Anwendungen wechseln, ohne das Start-Menü oder die Taskleiste zu verwenden. Sie können eine Standardliste der beliebtesten Anwendungen konfigurieren, die in der Unity Touch-Sidebar angezeigt werden.

Sie können die Unity Touch-Funktion nach der Installation deaktivieren bzw. aktivieren, indem Sie die Gruppenrichtlinieneinstellung **Unity Touch aktivieren** konfigurieren. Siehe [ADM-Vorlageneinstellungen für die View Agent-Konfiguration](#).

Die Dokumente zu VMware Horizon Client für iOS- und Android-Geräte enthalten weitere Informationen zu Endbenutzerfunktionen, die über Unity Touch bereitgestellt werden.

## Systemanforderungen für Unity Touch

Die Horizon Client-Software und die mobilen Geräte, auf denen Sie Horizon Client installieren, müssen zur Unterstützung von Unity Touch bestimmte Versionsanforderungen erfüllen.

### View-Desktop

Zur Unterstützung von Unity Touch muss in der virtuellen Maschine, auf die der Endbenutzer zugreift, die folgende Software installiert sein:

- Die Unity Touch-Funktion installieren Sie durch die Installation von View Agent 6.0 oder höher. Siehe [Installieren von View Agent auf einer virtuellen Maschine](#).
- Betriebssysteme: Windows XP SP3 (32 Bit), Windows Vista (32 Bit), Windows 7 (32 Bit oder 64 Bit), Windows 8 (32 Bit oder 64 Bit), Windows 8.1 (32 Bit oder 64 Bit) oder Windows Server 2008 R2

### Horizon Client-Software

Unity Touch wird auf den folgenden Horizon Client-Versionen unterstützt:

- Horizon Client 2.0 für iOS oder höher
- Horizon Client 2.0 für Android oder höher

### Betriebssysteme für mobile Geräte

Unity Touch wird auf den folgenden Betriebssystemen für mobile Geräte unterstützt:

- iOS 5.0 und höher
- Android 3 (Honeycomb), Android 4 (Ice Cream Sandwich) und Android 4.1 und 4.2 (Jelly Bean)

## Konfigurieren von Favoritenanwendungen durch Unity Touch

Mit der Unity Touch-Funktion können Tablet- und Smartphone-Benutzer von einer Unity Touch-Sidebar aus schnell zu einer View-Desktop-Anwendung oder -Datei navigieren. Wenngleich Endbenutzer festlegen können, welche Favoritenanwendungen in der Sidebar angezeigt werden sollen, können Administratoren zur Verbesserung der Benutzerfreundlichkeit eine Standardliste mit Favoritenanwendungen konfigurieren.

Wenn Sie Desktop-Pools mit dynamischer Zuweisung einsetzen, gehen die von den Endbenutzern festgelegten Favoritenanwendungen und -dateien verloren, wenn sie die Verbindung mit einem Desktop trennen. Dies gilt nicht, wenn Sie in Active Directory die Verwendung von Roamingbenutzerprofilen aktivieren.

Die Standardliste der Favoritenanwendungen bleibt erhalten, wenn sich ein Endbenutzer zum ersten Mal mit einem Desktop verbindet, der für Unity Touch aktiviert ist. Wenn der Benutzer jedoch eigene Favoritenanwendungen konfiguriert, wird die Standardliste ignoriert. Die vom Benutzer definierte Liste der Favoritenanwendungen wird im Roamingbenutzerprofil abgelegt und ist verfügbar, wenn sich der Benutzer in einem dynamischen oder dedizierten Pool bei anderen Computern anmeldet.

Wenn Sie eine Standardliste mit Favoritenanwendungen erstellen und mindestens eine der Anwendungen nicht auf dem View-Desktop-Betriebssystem installiert ist oder die Pfade zu diesen Anwendungen nicht im Startmenü gefunden werden, wird die Anwendung nicht in der Favoritenliste angezeigt. Sie können dieses Verhalten dazu nutzen, um eine Master-Standardliste mit Favoritenanwendungen einzurichten, die anschließend auf mehrere virtuelle Maschinen-Images angewendet werden kann, auf denen unterschiedliche Anwendungen installiert sind.

Wenn beispielsweise Microsoft Office und Microsoft Visio auf einer virtuellen Maschine installiert sind und Windows Powershell und VMware vSphere Client auf einer zweiten virtuellen Maschine, können Sie eine Liste erstellen, die alle vier Anwendungen enthält. Es werden nur die installierten Anwendungen als standardmäßige Favoritenanwendungen auf den jeweiligen Desktops angezeigt.

Sie können unterschiedliche Methoden zur Festlegung einer Standardliste mit Favoritenanwendungen einsetzen.

- Fügen Sie der Windows-Registrierung auf den virtuellen Desktop-Maschinen im Desktop-Pool einen Wert hinzu.
- Erstellen Sie ein administratives Installationspaket aus dem View Agent-Installationsprogramm und verteilen Sie das Paket an die virtuellen Maschinen.
- Führen Sie auf den virtuellen Maschinen das View Agent-Installationsprogramm von der Befehlszeile aus.

---

**Hinweis** Für Unity Touch wird davon ausgegangen, dass sich Verknüpfungen für Anwendungen im Programmordner des Menüs **Start** befinden. Wenn sich eine Verknüpfung außerhalb des Programmordners befindet, fügen Sie das Präfix **Programs** in den Verknüpfungspfad ein. Beispiel: Windows Update.lnk befindet sich im Ordner ProgramData\Microsoft\Windows\Start Menu. Zur Veröffentlichung dieser Verknüpfung als standardmäßige Favoritenanwendung fügen Sie dem Verknüpfungspfad das Präfix **Programs** hinzu. Beispiel: "Programs/Windows Update.lnk".

---

### Voraussetzungen

- Stellen Sie sicher, dass View Agent auf der virtuellen Maschine installiert ist.
- Vergewissern Sie sich, dass Sie über Administratorrechte für die virtuelle Maschine verfügen. Für dieses Verfahren müssen Sie möglicherweise eine Registrierungseinstellung bearbeiten.
- Wenn Sie Desktop-Pools mit dynamischer Zuweisung einsetzen, verwenden Sie Active Directory zum Einrichten von Roamingbenutzerprofilen. Folgen Sie den von Microsoft bereitgestellten Anweisungen. Benutzer von Desktop-Pools mit dynamischer Zuweisung sind in der Lage, ihre Liste mit Favoritenanwendungen und -dateien bei jeder Anmeldung anzuzeigen.

## Verfahren

- ◆ (Optional) Erstellen Sie eine Standardliste mit Favoritenanwendungen, indem Sie der Windows-Registrierung einen Wert hinzufügen.

- a Öffnen Sie regedit und navigieren Sie zur Registrierungseinstellung HKLM\Software\VMware, Inc.\VMware Unity.

Navigieren Sie auf einer virtuellen Maschine mit 64 Bit zum Verzeichnis HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity.

- b Erstellen Sie einen Zeichenfolgenwert mit dem Namen FavAppList.
- c Geben Sie die standardmäßigen Favoritenanwendungen an.

Verwenden Sie das folgende Format, um die Verknüpfungspfade zu den Anwendungen im Startmenü anzugeben.

```
path-to-app-1|path-to-app-2|path-to-app-3|...
```

Beispiel:

```
Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010 Language Preferences.lnk
```

- ◆ (Optional) Erstellen Sie eine Standardliste mit Favoritenanwendungen, indem Sie ein administratives Installationspaket aus dem View Agent-Installationsprogramm erstellen.

- a Verwenden Sie an der Befehlszeile das folgende Format, um das administrative Installationspaket zu erstellen.

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""a network share to store the admin install package"" UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the registry""
```

Beispiel:

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-share\viewfeaturepack"" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of Access.lnk|Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|Programs/Google Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|Programs/Skype/Skype.lnk|Programs/WebEx/Productivity Tools/WebEx Settings.lnk|""
```

- b Verteilen Sie das administrative Installationspaket von der Netzwerkfreigabe auf den virtuellen Desktop-Maschinen, indem Sie eine standardmäßige MSI-Bereitstellungsmethode (Microsoft Windows Installer) einsetzen, die in Ihrer Organisation verwendet wird.

- ◆ (Optional) Erstellen Sie eine Standardliste mit Favoritenanwendungen, indem Sie das View Agent-Installationsprogramm an der Befehlszeile einer virtuellen Maschine direkt ausführen.

Verwenden Sie das folgende Format.

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /v"/qn UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the registry""
```

**Hinweis** Der oben gezeigte Befehl kombiniert die Installation des View Agent mit der Festlegung einer Standardliste mit Favoritenanwendungen. Sie müssen den View Agent nicht installieren, bevor Sie diesen Befehl ausführen.

### Nächste Schritte

Wenn Sie diese Aufgabe direkt auf einer virtuellen Maschine ausführen (indem Sie die Windows-Registrierung bearbeiten oder den View Agent über die Befehlszeile installieren), müssen Sie die neu konfigurierte virtuelle Maschine bereitstellen. Sie können einen Snapshot oder eine Vorlage und einen Desktop-Pool erstellen oder Sie stellen einen vorhandenen Pool neu zusammen. Alternativ können Sie eine Active Directory-Gruppenrichtlinie zur Bereitstellung der neuen Konfiguration erstellen.

## Konfigurieren der Flash-URL-Umleitung für das Multicast- oder Unicast-Streaming

Kunden können ab sofort Adobe Media Server und Multicast oder Unicast zur Bereitstellung von Live-Videoereignissen in einer VDI-Umgebung (Virtual Desktop Infrastructure) nutzen. Zur Bereitstellung von Multicast- oder Unicast-Videostreams in einer VDI-Umgebung sollte der Medienstream unter Umgehung der Remote-Desktops direkt von der Medienquelle an die Endpunkte gesendet werden. Die Flash-URL-Umleitung unterstützt diese Funktion, indem die ShockWave-Datei (SWF) abgefangen und vom Remote-Desktop an den Clientendpunkt umgeleitet wird.

Die Flash-Inhalte werden dann mithilfe der lokalen Flash-Medienplayer wiedergegeben.

Durch das direkte Streaming von Flash-Inhalten von Adobe Media Server auf die Clientendpunkte wird die Datenlast auf dem ESXi-Host im Rechenzentrum gesenkt, das zusätzliche Routing über das Rechenzentrum vermieden und die erforderliche Bandbreite zum simultanen Streaming von Flash-Inhalten an mehrere Clientendpunkte verringert.

Die Flash-URL-Umleitung verwendet ein JavaScript, das durch den Webseitenadministrator in eine HTML-Webseite eingebettet wird. Immer dann, wenn ein Benutzer eines Remote-Desktops aus einer Webseite auf den festgelegten URL-Link klickt, fängt das JavaScript die SWF-Datei von der Remote-Desktop-Sitzung ab und leitet sie an den Clientendpunkt um. Der Endpunkt kann anschließend außerhalb der Remote-Desktop-Sitzung einen lokalen Flash Projector öffnen und den Medienstream lokal abspielen.



Zum Konfigurieren der Flash-URL-Umleitung müssen Sie Ihre HTML-Webseite und Ihre Clientgeräte einrichten.

## Verfahren

### 1 Systemanforderungen für die Flash-URL-Umleitung

Zur Unterstützung der Flash-URL-Umleitung muss Ihre View-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

### 2 Sicherstellen, dass die Flash-URL-Umleitung installiert ist

Bevor Sie diese Funktion verwenden, müssen Sie sicherstellen, dass die Flash-URL-Umleitung auf Ihren virtuellen Desktops installiert wurde und ausgeführt wird.

### 3 Einrichten der Webseiten zur Bereitstellung von Multicast- oder Unicast-Streams

Zur Unterstützung der Flash-URL-Umleitung müssen Sie einen JavaScript-Befehl in die MIME HTML-Webseiten (MHTML) einbetten, der Links zu den Multicast- oder Unicast-Streams bereitstellt. Benutzer zeigen diese Webseiten in den Browsern auf ihren Remote-Desktops an, um auf die Video-Streams zuzugreifen.

### 4 Einrichten von Clientgeräten für die Flash-URL-Umleitung

Die Flash-URL-Umleitung leitet die SWF-Datei von Remote-Desktops an Client-Geräte um. Um diesen Clientgeräten die Wiedergabe von Flash-Videos über einen Multicast- oder Unicast-Stream zu ermöglichen, müssen Sie sicherstellen, dass der geeignete Adobe Flash Player auf den Clientgeräten installiert ist. Die Clients müssen außerdem über IP-Konnektivität mit der Medienquelle verfügen.

### 5 Deaktivieren oder Aktivieren der Flash-URL-Umleitung

Die Flash-URL-Umleitung ist aktiviert, wenn Sie eine unbeaufsichtigte Installation von View Agent mit dem Befehlszeilenargument `FlashURLRedirection` durchführen. Sie können die Flash-URL-Umleitung-Funktion auf ausgewählten Remote-Desktops deaktivieren oder erneut aktivieren, indem Sie einen Wert auf einem Windows-Registrierungsschlüssel auf diesen virtuellen Maschinen festlegen.

## Systemanforderungen für die Flash-URL-Umleitung

Zur Unterstützung der Flash-URL-Umleitung muss Ihre View-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

### View-Desktop

- Installieren Sie die Flash-URL-Umleitung, indem Sie das Befehlszeilenargument `FlashURLRedirection` in einer unbeaufsichtigten Installation von View Agent 6.0 oder höher eingeben. Siehe [Eigenschaften für die unbeaufsichtigte Installation von View Agent](#).
- Auf den Desktops muss ein 64-Bit- oder 32-Bit-Betriebssystem mit Windows 7 ausgeführt werden.

- Zu den unterstützten Desktop-Browsern gehören der Internet Explorer 8, 9 und 10, Chrome 29.x sowie Firefox 20.x.

### Flash Media Player und ShockWave Flash (SWF)

Sie müssen einen entsprechenden Flash Media Player wie z. B. Strobe Media Playback in Ihre Website integrieren. Zum Streamen von Multicast-Inhalt können Sie `multicastplayer.swf` oder `StrobeMediaPlayback.swf` in Ihren Webseiten verwenden. Zum Streamen von Live-Unicast-Inhalt müssen Sie `StrobeMediaPlayback.swf` verwenden. Sie können `StrobeMediaPlayback.swf` auch für andere unterstützte Funktionen wie RTMP-Streaming und dynamisches HTTP-Streaming verwenden.

### Horizon Client-Software

Die folgenden Horizon Client-Versionen unterstützen Multicast und Unicast:

- Horizon Client 2.2 für Linux oder höher
- Horizon Client 2.2 für Windows oder höher

Die folgenden Horizon Client-Versionen unterstützen nur Multicast. (Sie bieten keine Unterstützung für Unicast):

- Horizon Client 2.0 oder 2.1 für Linux
- Horizon Client 5.4 für Windows

### Horizon Client-Computer oder Clientzugriffsgerät

- Die Flash-URL-Umleitung wird auf allen Betriebssystemen unterstützt, die Horizon Client für Linux auf x86 Thin Client-Geräten ausführen. Auf ARM-Prozessoren wird diese Funktion nicht unterstützt.
- Die Flash-URL-Umleitung wird auf allen Betriebssystemen unterstützt, auf denen Horizon Client für Windows ausgeführt wird. Weitere Informationen finden Sie im Dokument *Verwendung von VMware Horizon Client für Windows*.
- Auf Windows-Clientgeräten müssen Sie Adobe Flash Player 10.1 oder höher für Internet Explorer installieren.
- Auf Linux Thin Client-Geräten müssen Sie die Dateien „`libexpat.so.0`“ und „`libflashplayer.so`“ installieren. Siehe [Einrichten von Clientgeräten für die Flash-URL-Umleitung](#).

---

**Hinweis** Bei der Flash-URL-Umleitung wird der Multicast- oder Unicast-Stream an Clientgeräte umgeleitet, die sich möglicherweise außerhalb der Unternehmensfirewall befinden. Ihre Clients müssen auf den Adobe Webserver zugreifen können, auf dem die ShockWave Flash-Datei (SWF) zur Initiierung des Multicast- oder Unicast-Streaming gehostet wird. Falls erforderlich, müssen Sie in Ihrer Firewall die geeigneten Ports öffnen, um Clientgeräten den Zugriff auf diesen Server zu ermöglichen.

---

## Sicherstellen, dass die Flash-URL-Umleitung installiert ist

Bevor Sie diese Funktion verwenden, müssen Sie sicherstellen, dass die Flash-URL-Umleitung auf Ihren virtuellen Desktops installiert wurde und ausgeführt wird.

Die Flash-URL-Umleitung muss auf jedem Desktop vorhanden sein, auf dem Sie die Multicast- oder Unicast-Umleitung unterstützen möchten. Anweisungen zur Installation von View Agent finden Sie unter [Eigenschaften für die unbeaufsichtigte Installation von View Agent](#).

### Verfahren

- 1 Starten Sie eine Remote-Desktop-Sitzung, die PCoIP verwendet.
- 2 Öffnen Sie den Task-Manager.
- 3 Stellen Sie sicher, dass der Prozess `ViewMPServer.exe` auf dem Desktop ausgeführt wird.

## Einrichten der Webseiten zur Bereitstellung von Multicast- oder Unicast-Streams

Zur Unterstützung der Flash-URL-Umleitung müssen Sie einen JavaScript-Befehl in die MIME HTML-Webseiten (MHTML) einbetten, der Links zu den Multicast- oder Unicast-Streams bereitstellt. Benutzer zeigen diese Webseiten in den Browsern auf ihren Remote-Desktops an, um auf die Video-Streams zuzugreifen.

Darüber hinaus können Sie die englische Fehlermeldung anpassen, die dem Endbenutzer angezeigt wird, wenn ein Problem bei der Flash-URL-Umleitung auftritt. Führen Sie diesen optionalen Schritt aus, wenn Sie Ihren Endbenutzern eine lokalisierte Fehlermeldung anzeigen möchten. Sie müssen die Konfiguration „`var vmwareScriptErrorMessage`“ zusammen mit dem lokalisierten Text in die MHTML-Webseite einbetten.

### Voraussetzungen

Stellen Sie sicher, dass die Bibliothek `swfobject.js` in die MHTML-Webseite importiert wurde.

### Verfahren

- 1 Betten Sie den JavaScript-Befehl `viewmp.js` in die MHTML-Webseite ein.  
  
Beispiel: `<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`
- 2 (Optional) Passen Sie die Fehlermeldung zur Flash-URL-Umleitung an, die den Endbenutzern gesendet wird.  
  
Beispiel: `"var vmwareScriptErrorMessage= lokalisierte Fehlermeldung"`
- 3 Stellen Sie sicher, dass Sie den JavaScript-Befehl „`viewmp.js`“ einbetten und optional die Fehlermeldung zur Flash-URL-Umleitung anpassen, bevor Sie die ShockWave Flash-Datei (SWF) in die MHTML-Webseite importieren.

Wenn ein Benutzer die Webseite in einem Remote-Desktop anzeigt, löst der JavaScript-Befehl `viewmp.js` den Flash-URL-Umleitungsmechanismus auf dem Remote-Desktop aus, der die SWF-Datei vom Desktop an das hostende Clientgerät umleitet.

## Einrichten von Clientgeräten für die Flash-URL-Umleitung

Die Flash-URL-Umleitung leitet die SWF-Datei von Remote-Desktops an Client-Geräte um. Um diesen Clientgeräten die Wiedergabe von Flash-Videos über einen Multicast- oder Unicast-Stream zu ermöglichen, müssen Sie sicherstellen, dass der geeignete Adobe Flash Player auf den Clientgeräten installiert ist. Die Clients müssen außerdem über IP-Konnektivität mit der Medienquelle verfügen.

**Hinweis** Bei der Flash-URL-Umleitung wird der Multicast- oder Unicast-Stream an Clientgeräte umgeleitet, die sich möglicherweise außerhalb der Unternehmensfirewall befinden. Ihre Clients müssen auf den Adobe Webserver zugreifen können, auf dem die SWF-Datei zur Initiierung des Multicast- oder Unicast-Streaming gehostet wird. Falls erforderlich, müssen Sie in Ihrer Firewall die geeigneten Ports öffnen, um Clientgeräten den Zugriff auf diesen Server zu ermöglichen.

### Verfahren

- ◆ Installieren Sie Adobe Flash Player auf Ihren Clientgeräten.

| Betriebssystem | Aktion   |
|----------------|--|
| Windows        | Installieren Sie Adobe Flash Player 10.1 oder höher für Internet Explorer.   |
| Linux          | <p>a Installieren Sie die Datei „libexpat.so.0“ oder stellen Sie sicher, dass diese Datei bereits installiert ist.</p> <p>Stellen Sie sicher, dass die Datei im Verzeichnis „/usr/lib“ oder „/usr/local/lib“ installiert ist.</p> <p>b Installieren Sie die Datei libflashplayer.so oder stellen Sie sicher, dass diese Datei bereits installiert ist.</p> <p>Vergewissern Sie sich, dass die Datei im geeigneten Flash-Plug-In-Verzeichnis für Ihr Linux-Betriebssystem installiert ist.</p> <p>c Installieren Sie das Programm wget oder stellen Sie sicher, dass die Programmdatei bereits installiert ist.</p> |

## Deaktivieren oder Aktivieren der Flash-URL-Umleitung

Die Flash-URL-Umleitung ist aktiviert, wenn Sie eine unbeaufsichtigte Installation von View Agent mit dem Befehlszeilenargument `FlashURLRedirection` durchführen. Sie können die Flash-URL-Umleitung-Funktion auf ausgewählten Remote-Desktops deaktivieren oder erneut aktivieren, indem Sie einen Wert auf einem Windows-Registrierungsschlüssel auf diesen virtuellen Maschinen festlegen.

### Verfahren

- 1 Starten Sie den Windows-Registrierungs-Editor auf der virtuellen Maschine.

- 2 Navigieren Sie zum Windows-Registrierungsschlüssel, der die Flash-URL-Umleitung steuert.

| Option            | Beschreibung  |
|-------------------|---|
| Windows 7, 64-Bit | HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware ViewMP\enabled = <i>value</i> |
| Windows 7, 32-Bit | HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware ViewMP\enabled = <i>value</i>             |

- 3 Legen Sie den Wert zum Deaktivieren oder Aktivieren der Flash-URL-Umleitung fest.

| Option      | Wert |
|-------------|------|
| Deaktiviert | 0    |
| Aktiviert   | 1    |

Standardmäßig ist der Wert auf 1 festgelegt.

## Konfigurieren von Echtzeit-Audio/Video

Die Echtzeit-Audio/Video-Funktion ermöglicht es View-Benutzern, Skype, Webex, Google Hangouts und andere Anwendungen für Online-Konferenzen auf ihren Remote-Desktops auszuführen. Mit der Echtzeit-Audio/Video-Funktion werden Webcams und Audiogeräte, die lokal an das Clientsystem angeschlossen sind, an den Remote-Desktop umgeleitet. Diese Funktion leitet Video- und Audiodaten mit deutlich weniger Bandbreite an den Desktop um, als mit der USB-Umleitung erreicht werden kann.

Echtzeit-Audio/Video ist mit Standard-Konferenzanwendungen und browserbasierten Videoanwendungen kompatibel und unterstützt standardmäßige Webcams, USB-Audiogeräte und analoge Audioeingänge.

Mit dieser Funktion werden VMware Virtual Webcam und VMware Virtual Microphone auf dem Desktop-Betriebssystem installiert. Die VMware Virtual Webcam verwendet einen Kernel-Webcam-Treiber, der eine bessere Kompatibilität mit browserbasierten Videoanwendungen und anderer Konferenzsoftware von Drittanbietern bietet.

Beim Start einer Konferenz- oder Videoanwendung werden diese virtuellen VMware-Geräte angezeigt und verwendet und sorgen für die Audio/Video-Umleitung von den lokal angeschlossenen Geräten auf dem Client. Die VMware Virtual Webcam und das VMware Virtual Microphone erscheinen auch im Geräte-Manager auf dem Desktop-Betriebssystem.

**Hinweis** Die Echtzeit-Audio/Video-Funktion installiert auch eine frühere Version der VMware Virtual Webcam. Sie sehen in bestimmten Konferenzanwendungen möglicherweise zwei Versionen der VMware Virtual Webcam. Die frühere Version hat die Bezeichnung „VMware Virtual Webcam (legacy)“.

Die Treiber für die Audiogeräte und Webcams müssen auf den Horizon Client-Systemen installiert sein, um die Umleitung zu aktivieren.

## Konfigurationsmöglichkeiten für Echtzeit-Audio/Video

Nachdem Sie View Agent mit Echtzeit-Audio/Video installiert haben, funktioniert diese Funktion auf View-Desktops ohne eine weitere Konfiguration. Die Standardwerte für Webcam-Bildrate und -Bildauflösung werden für die meisten Standardgeräte und -anwendungen empfohlen.

Sie können Gruppenrichtlinieneinstellungen konfigurieren, um diese Standardwerte an bestimmte Anwendungen, Webcams oder Umgebungen anzupassen. Sie können auch eine Richtlinie festlegen, um die Funktion insgesamt zu deaktivieren oder zu aktivieren. Mit einer ADM-Vorlagendatei können Sie Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video in Active Directory oder auf einzelnen Desktops installieren. Siehe [Konfigurieren von Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video](#).

Wenn Benutzer über mehrere integrierte oder an ihre Clientcomputer angeschlossene Webcams und Audioeingabegeräte verfügen, können Sie bevorzugte Webcams und Audioeingabegeräte konfigurieren, die an ihre Desktops umgeleitet werden. Siehe [Auswählen von bevorzugten Webcams und Mikrofonen](#).

---

**Hinweis** Sie können ein bevorzugtes Audiogerät auswählen, es stehen jedoch keine weiteren Optionen für die Audiokonfiguration zur Verfügung.

---

Wenn Webcambilder und Audioeingangsdaten an einen Remote-Desktop umgeleitet werden, können Sie auf dem lokalen Computer nicht auf die Webcam oder die Audiogeräte zugreifen. Ebenso können diese Geräte nicht auf dem Remote-Desktop verwendet werden, wenn auf dem lokalen Computer darauf zugegriffen wird.

Weitere Informationen zu unterstützten Anwendungen finden Sie im VMware KB-Artikel *Richtlinien zur Arbeit mit Echtzeit-Audio/Video mit Drittanbieteranwendungen auf Horizon View-Desktops* unter <http://kb.vmware.com/kb/2053754>.

## Systemanforderungen für Echtzeit-Audio/Video

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

### View-Remote-Desktop

Die Echtzeit-Audio/Video-Funktion installieren Sie durch die Installation von View Agent 6.0 oder höher. Diese Funktion wird von Desktop-Pools unterstützt, die auf virtuellen Einzelbenutzer-Maschinen bereitgestellt werden, aber nicht von RDS-Desktop-Pools. Siehe [Installieren von View Agent auf einer virtuellen Maschine](#).

### Horizon Client-Software

Horizon Client 2.2 für Windows oder höher

Horizon Client 2.2 für Linux oder höher. Für Horizon Client für Linux 3.1 oder eine ältere Version steht diese Funktion nur mit der von Drittanbietern bereitgestellten Horizon Client-Version für Linux zur Verfügung. Für Horizon Client für Linux 3.2 und höher steht diese Funktion auch mit der von VMware verfügbaren Clientversion zur Verfügung.

## Horizon Client-Computer oder Clientzugriffsgerät

Horizon Client 2.3 für Mac OS X oder eine neuere Version

- Alle Betriebssysteme, unter denen Horizon Client für Windows ausgeführt wird.
- Alle Betriebssysteme, unter denen Horizon Client für Linux auf x86-Geräten ausgeführt wird. Auf ARM-Prozessoren wird diese Funktion nicht unterstützt.
- Mac OS X Mountain Lion (10.8) und höher. Auf allen älteren Mac OS X-Betriebssystemen ist diese Funktion deaktiviert.
- Weitere Informationen zu den unterstützten Clientbetriebssystemen finden Sie im Dokument *Verwendung von VMware Horizon Client* für das entsprechende System oder Gerät.
- Auf dem Clientcomputer müssen Treiber für Webcam und Audiogeräte installiert sein, und die Webcam oder das Audiogerät muss betriebsbereit sein. Zur Unterstützung von Echtzeit-Audio/Video ist es nicht erforderlich, die Gerätetreiber auf dem Desktop-Betriebssystem zu installieren, auf dem View Agent installiert ist.

## Anzeigeprotokoll für View

PCoIP

Echtzeit-Audio/Video wird in RDP-Desktop-Sitzungen nicht unterstützt.

## Sicherstellen, dass anstelle der USB-Umleitung Echtzeit-Audio/Video verwendet wird

Echtzeit-Audio/Video unterstützt die Umleitung von Webcam- und Audio-Eingaben für die Verwendung in Konferenzanwendungen. Die Funktion zur USB-Umleitung, die gemeinsam mit View Agent installiert werden kann, unterstützt die Webcam-Umleitung nicht. Wenn Sie Audioeingabegeräte über die USB-Umleitung umleiten, wird der Audio-Stream in Echtzeit-Audio/Video-Sitzungen nicht korrekt mit dem Video synchronisiert und Sie büßen außerdem den Vorteil der verringerten Anforderungen an die Netzwerkbandbreite ein. Mithilfe dieser Schritte können Sie sicherstellen, dass Webcams und Audio-Eingabegeräte über Echtzeit-Audio/Video zu Ihren Desktops umgeleitet werden und nicht über die USB-Umleitung.

Wenn Ihre Desktops mit USB-Umleitung konfiguriert sind, können Endbenutzer ihre lokal verbundenen USB-Geräte verbinden und anzeigen, indem sie in der Menüleiste des Windows-Clients die Option **USB-Gerät verbinden** oder im Mac OS X-Client die Option **Desktop > USB** auswählen. Linux-Clients blockieren standardmäßig die USB-Umleitung von Audio- und Videogeräten und bieten keine USB-Geräte-Optionen für Endbenutzer.

Wenn ein Endbenutzer ein USB-Gerät aus der Liste unter **USB-Gerät verbinden** oder **Desktop > USB** auswählt, kann dieses Gerät nicht mehr für Video- oder Audiokonferenzen verwendet werden. Wenn ein Benutzer beispielsweise einen Skype-Anruf durchführt, wird das Video-Bild möglicherweise nicht angezeigt oder der Audio-Stream ist möglicherweise nur eingeschränkt verfügbar. Wenn ein Endbenutzer während einer Konferenzsitzung ein Gerät auswählt, wird die Webcam- oder Audio-Umleitung unterbrochen.

Um diese Geräte für Endbenutzer auszublenden und potenzielle Störungen zu vermeiden, können Sie Gruppenrichtlinieneinstellungen für die USB-Umleitung konfigurieren. Auf diese Weise können Sie die Anzeige von Webcams und Audioeingabegeräten in VMware Horizon Client deaktivieren.

Sie können insbesondere Filterregeln für die USB-Umleitung für View Agent erstellen und angeben, dass die Gerätefamilien Audio-Eingabe und Video deaktiviert werden. Weitere Informationen zum Festlegen von Gruppenrichtlinien und zum Angeben von Filterregeln für die USB-Umleitung finden Sie unter [Verwenden von Richtlinien zum Steuern der USB-Umleitung](#).

---

**Vorsicht** Wenn Sie keine Filterregeln für die USB-Umleitung einrichten, um die USB-Gerätefamilien zu deaktivieren, informieren Sie Ihre Endbenutzer darüber, dass sie aus der Liste unter **USB-Gerät verbinden** oder **Desktop > USB** in der VMware Horizon Client-Menüleiste keine Webcam- oder Audio-Geräte auswählen können.

---

## Auswählen von bevorzugten Webcams und Mikrofonen

Wenn ein Clientcomputer über mehrere Webcams und Mikrofone verfügt, können Sie eine bevorzugte Webcam und ein Standardmikrofon konfigurieren, die bzw. das über die Echtzeit-Audio/Video-Funktion an den Desktop umgeleitet wird. Diese Geräte können in den lokalen Clientcomputer integriert oder mit diesem verbunden sein.

Auf einem Windows-Clientcomputer wählen Sie eine bevorzugte Webcam aus, indem Sie einen Registrierungsschlüsselwert festlegen. Auf einem Clientcomputer mit Mac OS X können Sie unter Verwendung des Standardwertsystems von Mac OS X eine bevorzugte Webcam oder ein bevorzugtes Mikrofon angeben. Auf einem Linux-Clientcomputer können Sie eine bevorzugte Webcam oder ein Mikrofon angeben, indem Sie eine Konfigurationsdatei bearbeiten. Die Echtzeit-Audio/Video-Funktion leitet die bevorzugte Webcam um, sofern diese verfügbar ist. Falls nicht, verwendet die Echtzeit-Audio/Video-Funktion die erste Webcam, die bei der Systemauflistung bereitgestellt wird.

Zur Auswahl eines Standardmikrofons konfigurieren Sie die Option „Sound“ im Windows-, Mac OS X- oder Linux-Betriebssystem auf dem Clientcomputer.

## Auswählen eines Standardmikrofons auf einem Windows-Clientsystem

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



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

---

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

---

#### Voraussetzungen

- Stellen Sie sicher, dass ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren Remote-Desktop verwenden.

#### Verfahren

- 1 Wenn Sie gerade einen Anruf tätigen, beenden Sie das Gespräch.
- 2 Klicken Sie mit der rechten Maustaste auf das Lautsprechersymbol in der Systemleiste und wählen Sie **Aufnahmegeräte**.  
  
Alternativ können Sie die Option „Sound“ in der Systemsteuerung öffnen und auf die Registerkarte **Aufnahme** klicken.
- 3 Klicken Sie im Dialogfeld **Sound** auf der Registerkarte **Aufnahme** mit der rechten Maustaste auf das Mikrofon, das Sie verwenden möchten.
- 4 Wählen Sie **Als Standardgerät auswählen** und klicken Sie auf **OK**.
- 5 Starten Sie über View-Desktop einen neuen Anruf.

### Auswählen einer bevorzugten Webcam auf einem Windows-Clientsystem

Wenn Sie die Echtzeit-Audio/Video-Funktion einsetzen und auf Ihrem Clientsystem über mehrere Webcams verfügen, wird nur eine davon auf Ihrem View-Desktop verwendet. Zur Festlegung einer bevorzugten Webcam können Sie einen Registrierungsschlüsselwert festlegen.

Die bevorzugte Webcam wird auf dem Remote-Desktop verwendet, sofern sie verfügbar ist. Andernfalls wird eine andere Webcam verwendet.

#### Voraussetzungen

- Stellen Sie sicher, dass auf Ihrem Clientsystem eine USB-Webcam installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren Remote-Desktop verwenden.

#### Verfahren

- 1 Schließen Sie die Webcam an, die Sie verwenden möchten.
- 2 Starten Sie einen Anruf, und stoppen Sie den Anruf.  
  
Auf diese Weise wird eine Protokolldatei erstellt.

- 3 Öffnen Sie die Debug-Protokolldatei mit einem Texteditor.

| Betriebssystem           | Protokolldatei, Speicherort  |
|--------------------------|--|
| Windows XP               | C:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen<br>\Anwendungsdaten\VMware\VDM\Logs\debug-20JJ-MM-TT-XXXXXX.txt |
| Windows 7 oder Windows 8 | C:\Benutzer\%username%\AppData\Local\VMware\VDM\Logs\debug-20JJ-<br>MM-TT-XXXXXX.txt   |

Das Format der Protokolldatei lautet debug-20JJ-MM-TT-XXXXXX.txt, wobei 20JJ für das Jahr, MM für den Monat, TT für den Tag und XXXXXX für eine Nummer steht.

- 4 Durchsuchen Sie die Protokolldatei nach [ViewMMDevRedir] VideoInputBase::LogDevEnum, um die Protokolldateieinträge zu finden, in denen die angeschlossenen Webcams referenziert werden.

Nachfolgend sehen Sie einen Auszug aus der Protokolldatei zur Identifikation der Microsoft Lifecam HD-5000-Webcam:

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum - 2 Device(s) found

[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=0 Name=Integrated Webcam
UserId=vid_1bcf&pid_2b83&mi_00#7&1b2e878b&0&0000 SystemId=\\?\usb#vid_1bcf&pid_2b83&mi_00#

[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=1 Name=Microsoft LifeCam HD-5000
UserId=vid_045e&pid_076d&mi_00#8&11811f49&0&0000 SystemId=\\?\usb#vid_045e&pid_076d&mi_00#
```

- 5 Kopieren Sie die Benutzer-ID der bevorzugten Webcam.

Beispiel: Kopieren Sie vid\_045e&pid\_076d&mi\_00#8&11811f49&0&0000, um die Microsoft LifeCam HD-5000 als Standardwebcam festzulegen.

- 6 Starten Sie den Registrierungs-Editor (regedit.exe) und navigieren Sie zu HKEY\_LOCAL\_MACHINE \SOFTWARE\VMware, Inc.\VMware VDM\RTAV.

- 7 Fügen Sie den ID-Bestandteil der Zeichenfolgen in den REG\_SZ-Wert **srcWCamId** ein.

Beispiel: Fügen Sie vid\_045e&pid\_076d&mi\_00#8&11811f49&0&0000 in **srcWCamId** ein.

- 8 Speichern Sie Ihre Änderungen und beenden Sie die Registrierung.

- 9 Starten Sie einen neuen Anruf.

## Auswählen eines Standardmikrofons auf einem Mac OS X-Clientsystem

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

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

Dieses Verfahren beschreibt die Auswahl eines Mikrofons über die Benutzeroberfläche des Clientsystems. Administratoren können auch über die Mac OS X-Standardwerte ein bevorzugtes Mikrofon konfigurieren. Siehe [Konfigurieren einer bevorzugten Webcam oder eines bevorzugten Mikrofons auf einem Mac OS X-Clientsystem](#).

---

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

---

#### Voraussetzungen

- Stellen Sie sicher, dass ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren Remote-Desktop verwenden.

#### Verfahren

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

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

### Konfigurieren von Echtzeit-Audio/Video auf einem Mac OS X-Client

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

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

#### Syntax zur Konfiguration von Echtzeit-Audio/Video

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

**Tabelle 13-1. Befehlssyntax für die Konfiguration von Echtzeit-Audio/Video**

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

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

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

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

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

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

[Auswählen eines Standardmikrofons auf einem Mac OS X-Clientsystem](#). Wenn Sie keine bevorzugte Webcam konfigurieren, wählt der Remote-Desktop die Webcam anhand der Auflistung aus.

### Voraussetzungen

- Stellen Sie beim Konfigurieren einer bevorzugten USB-Webcam sicher, dass die Webcam auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Stellen Sie beim Konfigurieren eines bevorzugten USB-Mikrofons oder eines sonstigen Mikrofontyps sicher, dass das Mikrofon auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren Remote-Desktop verwenden.

### Verfahren

- 1 Starten Sie auf Ihrem Mac OS X-Clientsystem eine Webcam- oder Mikrofonanwendung, um eine Auflistung der Kamera- oder Audiogeräte in der Echtzeit-Audio/Video-Protokolldatei auszulösen.
  - a Schließen Sie die Webcam oder das Audiogerät an.
  - b Doppelklicken Sie im Ordner **Anwendungen** auf **VMware Horizon View Client** (Horizon Client 3.0) oder **VMware Horizon Client** (Horizon Client 3.1 und höher), um Horizon Client zu starten.
  - c Starten Sie einen Anruf und beenden Sie ihn dann.
- 2 Suchen Sie in der Echtzeit-Audio/Video-Protokolldatei nach Protokolleinträgen für die Webcam oder das Mikrofon.
  - a Öffnen Sie die Echtzeit-Audio/Video-Protokolldatei in einem Text-Editor.

Die Audio-Video-Protokolldatei in Echtzeit heißt ~/Library/Logs/VMware/vmware-RTAV-*pid*.log, wobei *pid* die Prozess-ID der aktuellen Sitzung ist.
  - b Suchen Sie in der Echtzeit-Audio/Video-Protokolldatei nach Einträgen für die angeschlossenen Webcams oder Mikrofone.

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

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

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

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

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

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

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

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

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

Beispiel: `defaults read com.vmware.rtav`

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

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

## Auswählen eines Standardmikrofons auf einem Linux-Clientsystem

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

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

Dieses Verfahren beschreibt die Auswahl eines Standardmikrofons über die Benutzeroberfläche des Clientsystems. Administratoren können auch ein bevorzugtes Mikrofon konfigurieren, indem sie eine Konfigurationsdatei bearbeiten. Siehe [Auswählen einer bevorzugten Webcam oder eines Mikrofons auf einem Linux-Clientsystem](#).

### Voraussetzungen

- Stellen Sie sicher, dass ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren Remote-Desktop verwenden.

### Verfahren

- 1 Wählen Sie auf der Ubuntu-Benutzeroberfläche **System > Preferences > Sound**.

Alternativ können Sie auf das **Sound**-Symbol am rechten Rand der Symbolleiste am oberen Bildschirmrand klicken.

- 2 Klicken Sie im Dialogfeld „Sound Preferences“ auf die Registerkarte **Input**.
- 3 Wählen Sie das bevorzugte Gerät aus und klicken Sie auf **Close**.

## Auswählen einer bevorzugten Webcam oder eines Mikrofons auf einem Linux-Clientsystem

Wenn Sie die Echtzeit-Audio/Video-Funktion einsetzen und auf Ihrem Clientsystem über mehrere Webcams und Mikrofone verfügen, kann nur eine Webcam oder ein Mikrofon auf Ihrem View-Desktop verwendet werden. Um die Webcam- und Mikrofonpräferenz anzugeben, können Sie eine Konfigurationsdatei bearbeiten.

Die bevorzugte Webcam oder das Mikrofon wird auf dem View-Desktop verwendet, sofern sie bzw. es verfügbar ist. Andernfalls wird eine andere Webcam oder ein anderes Mikrofon verwendet.

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

Um die Eigenschaften in der Datei „/etc/vmware/config“ sowie um ein bevorzugtes Gerät festzulegen, müssen Sie die Gerätekennung ermitteln.

- Für Webcams legen Sie die Eigenschaft „rtav.srcWCamId“ auf den Wert der in der Protokolldatei gefundenen Webcam-Beschreibung fest, wie im Folgenden beschrieben.

- Für Audiogeräte legen Sie die Eigenschaft „rtav.srcAudioInId“ auf den Wert des PULSE-Audio-Felds „device.description“ fest.

Durchsuchen Sie die Protokolldatei wie nachfolgend beschrieben, um den Wert dieses Feldes zu ermitteln.

### Voraussetzungen

Führen Sie die entsprechenden Vorabaufgaben durch, je nachdem, ob Sie eine Webcam, ein Mikrofon oder beides auswählen:

- Stellen Sie sicher, dass auf Ihrem Clientsystem eine USB-Webcam installiert und betriebsbereit ist.
- Stellen Sie sicher, dass ein USB-Mikrofon oder ein anderer Mikrofontyp auf Ihrem Clientsystem installiert und betriebsbereit ist.
- Vergewissern Sie sich, dass Sie das PCoIP-Anzeigeprotokoll für Ihren Remote-Desktop verwenden.

### Verfahren

- 1 Starten Sie den Client und eine Webcam- oder Mikrofonanwendung, um eine Auflistung der Kamerageräte oder Audiogeräte im Clientprotokoll auszulösen.
  - a Schließen Sie die Webcam oder das Audiogerät an, die bzw. das Sie verwenden möchten.
  - b Verwenden Sie den Befehl „vmware-view“, um Horizon Client zu starten.
  - c Starten Sie einen Anruf und beenden Sie ihn dann.

Auf diese Weise wird eine Protokolldatei erstellt.



## 2 Suchen Sie nach Protokolleinträgen für die Webcam oder das Mikrofon.

- a Öffnen Sie die Debug-Protokolldatei mit einem Texteditor.

Die Protokolldatei mit Protokollmeldungen zu Audio-Video in Echtzeit befindet sich unter `/tmp/vmware-<username>/vmware-RTAV-<pid>.log`. Das Clientprotokoll befindet sich unter `„/tmp/vmware-<Benutzername>/vmware-view-<pid>.log“`.

- b Durchsuchen Sie die Protokolldatei nach den Einträgen, die auf die angeschlossenen Webcams und Mikrofone verweisen.

Das folgende Beispiel zeigt einen Auszug der Webcam-Auswahl:

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:0819)
UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.5
SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=Microsoft® LifeCam HD-6000 for Notebooks UserId=Microsoft® LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6 SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) -
enumeration data unavailable
```

Das folgende Beispiel zeigt einen Auszug der Audiogeräteauswahl sowie den jeweiligen aktuellen Audiopegel:

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB Headset Analog Mono')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of Microsoft
LifeChat LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
```

Es werden Warnungen angezeigt, wenn einer der Quellaudiopegel für das ausgewählte Gerät nicht die PulseAudio-Kriterien erfüllt, wenn die Quelle nicht auf 100 % (0 dB) gesetzt ist oder wenn das ausgewählte Quellgerät stummgeschaltet wurde. Beispiel:

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0: 67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

- 3 Kopieren Sie die Beschreibung des Geräts und verwenden Sie sie zum Festlegen der entsprechenden Eigenschaft in der Datei „/etc/vmware/config“.

Kopieren Sie beispielsweise bei einer Webcam „Microsoft® LifeCam HD-6000 for Notebooks“, um die Microsoft-Webcam als bevorzugte Webcam festzulegen sowie um die Eigenschaft folgendermaßen anzugeben:

```
rtav.srcWCamId="Microsoft® LifeCam HD-6000 for Notebooks"
```

In diesem Beispiel könnten Sie die Eigenschaft auch auf „rtav.srcWCamId="Microsoft"“ festlegen. Kopieren Sie beispielsweise für ein Audiogerät „Logitech USB Headset Analog Mono“, um das Logitech-Headset als bevorzugtes Audiogerät festzulegen sowie um die Eigenschaft folgendermaßen anzugeben:

```
rtav.srcAudioInId="Logitech USB Headset Analog Mono"
```

- 4 Speichern Sie Ihre Änderungen und schließen Sie die Konfigurationsdatei „/etc/vmware/config“.
- 5 Melden Sie sich von der Desktop-Sitzung ab und starten Sie eine neue Sitzung.

## Konfigurieren von Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video

Sie können Gruppenrichtlinieneinstellungen konfigurieren, die das Verhalten der Echtzeit-Audio/Video-Funktion (Real-Time Audio-Video, RTAV) auf Ihren View-Desktops steuert. Mithilfe dieser Einstellungen wird die maximale Bildrate und -auflösung einer virtuellen Webcam festgelegt. Die Einstellungen ermöglichen es Ihnen, die maximale Bandbreite zu verwalten, die ein Benutzer belegen kann. Über eine zusätzliche Einstellung wird die RTAV-Funktion deaktiviert oder aktiviert.

Sie müssen diese Richtlinieneinstellungen nicht konfigurieren. Die Echtzeit-Audio/Video-Funktion verwendet die Bildrate und -auflösung, die für die Webcam auf den Clientsystemen festgelegt ist. Für die meisten Webcams und Audioanwendungen werden die Standardeinstellungen empfohlen.

Beispiele für die Bandbreitenbelegung durch die Echtzeit-Audio/Video-Funktion finden Sie unter [Bandbreite für Echtzeit-Audio/Video](#).

Diese Richtlinieneinstellungen wirken sich auf Ihre View-Desktops aus, nicht auf die Clientsysteme, an die die physischen Geräte angeschlossen sind. Fügen Sie zum Konfigurieren dieser Einstellungen auf Ihren Desktops die administrative Vorlagendatei (ADM) für die RTAV-Gruppenrichtlinie in Active Directory hinzu.

Informationen zum Konfigurieren von Einstellungen auf Clientsystemen finden Sie im VMware KB-Artikel *Festlegen von Frame-Raten und Auflösung für Echtzeit-Audio/Video auf Horizon View Clients* unter <http://kb.vmware.com/kb/2053644>.

## Hinzufügen der RTAV ADM-Vorlage in Active Directory und Konfigurieren der Einstellungen

Sie können die Richtlinieneinstellungen in der RTAV-ADM-Datei `vdm_agent_rtav.adm` zu Gruppenrichtlinienobjekten (GPOs) in Active Directory hinzufügen und im Gruppenrichtlinienobjekt-Editor die zugehörigen Einstellungen konfigurieren.

### Voraussetzungen

- Prüfen Sie, ob die RTAV-Setuptools auf Ihren Desktops installiert ist. Diese Setuptools wird standardmäßig installiert, kann aber während der Installation abgewählt werden. Die Einstellungen haben keine Auswirkungen, wenn RTAV nicht installiert ist. Siehe [Installieren von View Agent auf einer virtuellen Maschine](#).
- Stellen Sie sicher, dass Active Directory-GPOs für die RTAV-Gruppenrichtlinieneinstellungen erstellt wurden. Die GPOs müssen mit der OU verknüpft werden, die Ihre Desktops enthält. Siehe [Beispiel einer Active Directory-Gruppenrichtlinie](#).
- Vergewissern Sie sich, dass Microsoft Management Console (MMC) und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Machen Sie sich mit den RTAV-Gruppenrichtlinieneinstellungen vertraut. Siehe [Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video](#).

### Verfahren

- 1 Laden Sie die View GPO-Bundle-ZIP-Datei von der Download-Site von VMware Horizon (mit View) unter <http://www.vmware.com/go/downloadview> herunter.  
  
Der Dateiname ist `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip` (x.x.x ist die Version, yyyyyyy die Build-Nummer). Alle ADM- und ADMX-Dateien, die Gruppenrichtlinieneinstellungen für View bereitstellen, sind in dieser Datei verfügbar.
- 2 Extrahieren Sie die Datei `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip` und kopieren Sie die RTAV ADM-Datei `vdm_agent_rtav.adm` auf Ihren Active Directory-Server.
- 3 Bearbeiten Sie auf dem Active Directory-Server das GPO, indem Sie **Start > Verwaltung > Gruppenrichtlinienverwaltung** wählen, mit der rechten Maustaste auf das GPO klicken und **Bearbeiten** auswählen.
- 4 Klicken Sie im Gruppenrichtlinienobjekt-Editor mit der rechten Maustaste auf den Ordner **Computerkonfiguration > Administrative Vorlagen** und wählen Sie **Vorlagen hinzufügen/entfernen**.
- 5 Klicken Sie auf **Hinzufügen**, wechseln Sie zur Datei „`vdm_agent_rtav.adm`“ und klicken Sie auf **Öffnen**.

- 6 Klicken Sie auf **Schließen**, um die Richtlinieneinstellungen in der ADM-Datei auf das GPO anzuwenden.

Die Einstellungen sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Klassische administrative Vorlagen > VMware View Agent-Konfiguration > View RTAV-Konfiguration** enthalten.

- 7 Konfigurieren Sie die RTAV-Gruppenrichtlinieneinstellungen.

## Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video

Mithilfe der Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video (RTAV) werden die maximale Frame-Rate und -Auflösung einer virtuellen Webcam gesteuert. Über eine zusätzliche Einstellung können Sie die RTAV-Funktion deaktivieren oder aktivieren. Diese Richtlinieneinstellungen wirken sich auf Ihre View-Desktops aus, nicht auf die Clientsysteme, an die die physischen Geräte angeschlossen sind.

Wenn Sie die RTAV-Gruppenrichtlinieneinstellungen nicht konfigurieren, verwendet RTAV die Werte, die auf den Clientsystemen festgelegt sind. Die standardmäßige Webcam-Bildrate auf Clientsystemen beträgt 15 Frames pro Sekunde. Die standardmäßige Bildauflösung für die Webcam beträgt 320x240 Pixel.

Die Gruppenrichtlinieneinstellungen **Auflösung - Maximales Bild...** bestimmen die Maximalwerte, die verwendet werden können. Die Frame-Rate und -Auflösung, die auf den Clientsystemen festgelegt sind, sind absolute Werte. Beispiel: Wenn Sie die RTAV-Einstellungen für die maximale Bildauflösung auf 640x480 Pixel konfigurieren, zeigt die Webcam alle Auflösungen an, die auf dem Client auf bis zu 640x480 Pixel festgelegt wurde. Wenn Sie die Bildauflösung auf dem Client auf einen Wert über 640x480 Pixel festlegen, beträgt die Obergrenze der Client-Auflösung 640x480 Pixel.

Nicht alle Konfigurationen können die maximalen Gruppenrichtlinieneinstellungen mit einer Auflösung von 1920x1080 bei 25 Frames pro Sekunde erreichen. Welche maximale Frame-Rate Ihre Konfiguration für eine bestimmte Auflösung erreichen kann, hängt von der Webcam, die noch verwendet wird, von der Clientsystem-Hardware, der virtuellen View Agent-Hardware und der verfügbaren Bandbreite ab.

Die Gruppenrichtlinieneinstellungen **Auflösung - Standard-Image...** bestimmen die standardmäßigen Werte, die verwendet werden, wenn die Auflösungswerte nicht vom Benutzer festgelegt wurden.

| Gruppenrichtlinieneinstellung            | Beschreibung   |
|--|--|
| RTAV deaktivieren                        | <p>Wenn Sie diese Einstellung aktivieren, wird die Echtzeit-Audio/Video-Funktion deaktiviert. Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, wird Echtzeit-Audio/Video aktiviert.</p> <p>Diese Einstellung befindet sich im Ordner <b>View RTAV-Konfiguration</b>.</p>  |
| Maximale Frames pro Sekunde              | <p>Bestimmt die maximale Rate pro Sekunde, in der die Webcam Frames aufnehmen kann. Sie können diese Einstellung verwenden, um die Frame-Rate der Webcam in Netzwerkumgebungen mit einer geringen Bandbreite einzuschränken.</p> <p>Der Minimalwert beträgt ein Frame pro Sekunde. Der Maximalwert beträgt 25 Frames pro Sekunde.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, wird keine maximale Frame-Rate festgelegt. Echtzeit-Audio/Video verwendet die Frame-Rate, die für die Webcam auf dem Clientsystem ausgewählt wurde.</p> <p>Standardmäßig verfügen Webcams über eine Frame-Rate von 15 Frames pro Sekunde. Wenn keine Einstellung auf dem Clientsystem konfiguriert ist und die Einstellung <b>Maximale Bilder pro Sekunde</b> nicht konfiguriert oder deaktiviert ist, erfasst die Webcam 15 Frames pro Sekunde.</p> <p>Diese Einstellung befindet sich im Ordner <b>View RTAV-Konfiguration &gt; Einstellungen zur View RTAV-Webcam</b>.</p> |
| Auflösung - Maximale Bildbreite in Pixel | <p>Bestimmt die maximale Breite von Bildframes in Pixel, die von der Webcam erfasst werden. Durch das Festlegen einer niedrigen, maximalen Bildbreite können Sie die Auflösung von erfassten Frames verringern, die die Erfahrung bei der Bildverarbeitung in Netzwerkumgebungen mit einer geringen Bandbreite verbessern können.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, wird keine maximale Bildbreite festgelegt. RTAV verwendet die Bildbreite, die auf dem Clientsystem festgelegt wurde. Die Standardbreite eines Webcam-Bildes auf einem Clientsystem beträgt 320 Pixel.</p> <p>Die maximale Größe für ein Webcam-Bild beträgt 1920x1080 Pixel. Wenn Sie diese Einstellung mit einem Wert konfigurieren, der 1920 Pixel überschreitet, beträgt die effektive, maximale Bildbreite 1920 Pixel.</p> <p>Diese Einstellung befindet sich im Ordner <b>View RTAV-Konfiguration &gt; Einstellungen zur View RTAV-Webcam</b>.</p>                       |
| Auflösung - Maximale Bildhöhe in Pixel   | <p>Bestimmt die maximale Höhe von Bildframes in Pixel, die von der Webcam erfasst werden. Durch das Festlegen einer niedrigen, maximalen Bildhöhe können Sie die Auflösung von erfassten Frames verringern, die die Erfahrung bei der Bildverarbeitung in Netzwerkumgebungen mit einer geringen Bandbreite verbessern können.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, wird keine maximale Bildhöhe festgelegt. RTAV verwendet die Bildhöhe, die auf dem Clientsystem festgelegt wurde. Die Standardhöhe eines Webcam-Bildes auf einem Clientsystem beträgt 240 Pixel.</p> <p>Die maximale Größe für ein Webcam-Bild beträgt 1920x1080 Pixel. Wenn Sie diese Einstellung mit einem Wert konfigurieren, der 1080 Pixel überschreitet, beträgt die effektive, maximale Bildhöhe 1080 Pixel.</p> <p>Diese Einstellung befindet sich im Ordner <b>View RTAV-Konfiguration &gt; Einstellungen zur View RTAV-Webcam</b>.</p>                                   |

| Gruppenrichtlinieneinstellung                                | Beschreibung  |
|--|---|
| Auflösung - Standardmäßige Breite der Bildauflösung in Pixel | <p>Bestimmt die standardmäßige Auflösungsbreite von Bildframes in Pixel, die von der Webcam erfasst werden. Diese Einstellung wird verwendet, wenn kein Auflösungswert vom Benutzer definiert wird.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, beträgt die standardmäßige Bildbreite 320 Pixel.</p> <p>Der Wert, der von der Richtlinieneinstellung konfiguriert wird, ist nur wirksam, wenn View Agent 6.0 oder höher sowie Horizon Client 3.0 oder höher verwendet werden. Diese Richtlinieneinstellung ist für ältere Versionen von View Agent und Horizon Client nicht wirksam. Zudem beträgt die standardmäßige Bildbreite 320 Pixel.</p> <p>Diese Einstellung befindet sich im Ordner <b>View RTAV-Konfiguration &gt; Einstellungen zur View RTAV-Webcam</b>.</p> |
| Auflösung - Standardmäßige Höhe der Bildauflösung in Pixel   | <p>Bestimmt die standardmäßige Auflösungshöhe von Bildframes in Pixel, die von der Webcam erfasst werden. Diese Einstellung wird verwendet, wenn kein Auflösungswert vom Benutzer definiert wird.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert ist, beträgt die standardmäßige Bildhöhe 240 Pixel.</p> <p>Der Wert, der von der Richtlinieneinstellung konfiguriert wird, ist nur wirksam, wenn View Agent 6.0 oder höher sowie Horizon Client 3.0 oder höher verwendet werden. Diese Richtlinieneinstellung ist für ältere Versionen von View Agent und Horizon Client nicht wirksam. Zudem beträgt die standardmäßige Bildhöhe 240 Pixel.</p> <p>Diese Einstellung befindet sich im Ordner <b>View RTAV-Konfiguration &gt; Einstellungen zur View RTAV-Webcam</b>.</p>       |

## Bandbreite für Echtzeit-Audio/Video

Die Bandbreite für Echtzeit-Audio/Video variiert entsprechend der Webcam-Frame-Rate und -Bildauflösung und der erfassten Bild- und Audiodaten.

Die in [Tabelle 13-2. Beispielhafte Bandbreitenergebnisse für das Senden von Echtzeit-Audio/Video-Daten von Horizon Client an View Agent](#) dargestellten Beispieltests messen die Bandbreite, die die Echtzeit-Audio/Video-Funktion in einer View-Umgebung mit Standard-Webcams und Audioeingabegeräten verwendet. Diese Tests messen die Bandbreite für das Senden von Video- und Audiodaten von Horizon Client an View Agent. Die für das Ausführen einer Desktopsitzung von Horizon Client erforderliche Gesamtbandbreite ist möglicherweise größer als diese Zahlen. Bei diesen Tests erfasst die Webcam Bilder bei 15 Frames pro Sekunde für jede Bildauflösung.

**Tabelle 13-2. Beispielhafte Bandbreitenergebnisse für das Senden von Echtzeit-Audio/Video-Daten von Horizon Client an View Agent**

| Bildauflösung (Breite x Höhe) | Verwendete Bandbreite (KBit/s) |
|-------------------------------|--------------------------------|
| 160 x 120                     | 225                            |
| 320 x 240                     | 320                            |
| 640 x 480                     | 600                            |

## Konfigurieren der Scannerumleitung

Durch Verwenden der Scannerumleitung können View-Benutzer Informationen in ihren Remote-Desktops und -anwendungen mit Scan- und Bildverarbeitungsgeräten scannen, die lokal an ihren Clientcomputern angeschlossen sind. Die Scannerumleitung ist in den Versionen Horizon 6.0.2 und höher verfügbar.

Die Scannerumleitung unterstützt Standard-Scan- und Bildverarbeitungsgeräte, die zu den TWAIN- und WIA-Formaten kompatibel sind.

Nach der Installation von View Agent mithilfe des Scannerumleitungs-Setup funktioniert die Funktion auf Ihren Remote-Desktops und -anwendungen, ohne dass eine weitere Konfiguration erforderlich ist. Sie müssen keine scannerspezifischen Treiber auf Remote-Desktops oder -anwendungen konfigurieren.

Sie können Gruppenrichtlinieneinstellungen konfigurieren, um Standardwerte an bestimmte Scan- und Bildanwendungen oder -umgebungen anzupassen. Sie können auch eine Richtlinie festlegen, um die Funktion insgesamt zu deaktivieren oder zu aktivieren. Mit einer ADM-Vorlagendatei können Sie Gruppenrichtlinieneinstellungen für die Scannerumleitung in Active Directory oder auf einzelnen Desktops installieren. Siehe [Konfigurieren der Gruppenrichtlinieneinstellungen für Scannerumleitung](#).

Wenn Scandaten an einen Remote-Desktop oder eine Remoteanwendung weitergeleitet werden, können Sie nicht auf das Scan- oder Bildverarbeitungsgerät auf dem lokalen Computer zugreifen. Ebenso kann dieses Gerät nicht auf dem Remote-Desktop oder der Remoteanwendung verwendet werden, wenn auf dem lokalen Computer darauf zugegriffen wird.

## Systemanforderungen für Scannerumleitung

Zur Unterstützung der Scannerumleitung muss Ihre View-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen.

### **View-Remote-Desktop oder Remoteanwendung**

Diese Funktion wird für RDS-Desktops, RDS-Anwendungen und VDI-Desktops, die auf virtuellen Maschinen für Einzelbenutzer bereitgestellt werden, unterstützt.

Sie müssen View Agent 6.0.2 oder höher mit aktivierter Setup-Option „Scannerumleitung“ auf übergeordneten virtuellen Maschinen oder virtuellen Vorlagenmaschinen bzw. auf RDS-Hosts installieren.

Auf Windows-Desktop- und Windows-Server-Gastbetriebssystemen ist die Setup-Option „Scannerumleitung“ von View Agent standardmäßig deaktiviert.

Die folgenden Gastbetriebssysteme werden auf Einzelbenutzer-VMs und, sofern angegeben, auf RDS-Hosts unterstützt:

- Windows Vista, 32 Bit
- Windows 7, 32 oder 64 Bit
- Windows 8/8.1, 32 oder 64 Bit
- Windows Server 2008 R2, als Desktop oder RDS-Host konfiguriert

- Windows Server 2012 R2, als RDS-Host konfiguriert

---

**Wichtig** Auf den Windows Server-Gastbetriebssystemen muss die Funktion „Desktopdarstellung“ installiert sein. Dies gilt unabhängig davon, ob sie als Desktops oder RDS-Hosts konfiguriert sind.

---

Es ist nicht erforderlich, die Gerätetreiber für den Scanner auf dem Desktop-Betriebssystem zu installieren, auf dem View Agent installiert ist.

#### Horizon Client-Software

Horizon Client 3.2 für Windows oder höher

#### Horizon Client-Computer oder Clientzugriffsgerät

Unterstützte Betriebssysteme:

- Windows Vista, 32 Bit
- Windows 7, 32 oder 64 Bit
- Windows 8/8.1, 32 oder 64 Bit

Auf dem Clientcomputer müssen Treiber für das Scannergerät installiert sein, und der Scanner muss betriebsbereit sein.

#### Scangerät-Standard

TWAIN oder WIA

#### Anzeigeprotokoll für View

PCoIP

Scannerumleitung wird in RDP-Desktop-Sitzungen nicht unterstützt.

## Bedienung der Scannerumleitung durch den Benutzer

Mithilfe der Scannerumleitung können Benutzer physische Scanner und Bildverarbeitungsgeräte, die mit ihren Clientcomputern verbunden sind, als virtuelle Geräte handhaben, die Scanarbeitsgänge im Kontext ihrer Remote-Desktops und Remote-Anwendungen ausführen können.

Benutzer können ihre virtuellen Scanner auf sehr ähnliche Weise handhaben wie die Scanner, die mit ihren lokalen Clientcomputern verbunden sind.

- Nachdem die Option Scannerumleitung mit View Agent installiert wurde, wird ein Scanner-Taskleistensymbol zum Desktop hinzugefügt. In RDS-Anwendungen wird das Scanner-Taskleistensymbol zum lokalen Clientcomputer umgeleitet.

Es besteht keine Notwendigkeit, das Scanner-Taskleistensymbol zu verwenden. Die Umleitung von Scanvorgängen funktioniert ohne weitere Konfiguration. Sie können das Symbol dazu verwenden, Optionen zu konfigurieren und beispielsweise die Festlegung, welche Geräte zu verwenden sind, wenn mehrere Geräte mit dem Clientcomputer verbunden sind, zu ändern.

- Wenn Sie auf das Scanner-Symbol klicken, wird das Menü „Scannerumleitung für VMware Horizon“ angezeigt. Wenn inkompatible Scanner mit dem Clientcomputer verbunden sind, werden keine Scanner in der Menüliste aufgeführt.



- Scangeräte werden standardmäßig automatisch ausgewählt. Die Auswahl von TWAIN- und WIA-Scannern erfolgt separat. Zu einem gegebenen Zeitpunkt kann jeweils nur ein TWAIN-Scanner und ein WIA-Scanner ausgewählt sein.
- Wenn mehrere lokal verbundene Scanner konfiguriert sind, haben Sie die Möglichkeit, statt des standardmäßig ausgewählten einen anderen Scanner auszuwählen.
- WIA-Scanner werden im Gerätemanager-Menü des Remote-Desktops unter **Bildverarbeitungsgeräte** angezeigt. Der Name für den WIA-Scanner lautet **Virtueller VMware-WIA-Scanner**.
- Im Menü „Scannerumleitung für VMware Horizon“ können Sie auf die Option **Einstellungen** klicken und Optionen wie das Ausblenden von Webcams im Scannerumleitungsmenü und die Vorgehensweise bei der Auswahl des Standardscanners auswählen.

Außerdem können Sie diese Funktionen durch Konfigurieren der Gruppenrichtlinieneinstellungen für die Scannerumleitung in Active Directory steuern. Siehe [Gruppenrichtlinieneinstellungen für Scannerumleitung](#).

- Wenn Sie mit einem TWAIN-Scanner arbeiten, bietet das Menü „Scannerumleitung für VMware Horizon“ des TWAIN-Scanners zusätzliche Optionen für die Auswahl von Bildbereichen, das Scannen in Farbe, Schwarzweiß oder Graustufen und die Auswahl anderer üblicher Funktionen.
- Um das Fenster der TWAIN-Benutzeroberfläche für TWAIN-Scansoftware anzuzeigen, die das Fenster nicht standardmäßig anzeigt, können Sie die Option **Dialogfeld 'Scannereinstellungen' immer einblenden** im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ auswählen.

Beachten Sie, dass die meisten TWAIN-Scansoftware-Produkte das Fenster mit der TWAIN-Benutzeroberfläche standardmäßig anzeigen. Für diese Software wird das Fenster immer angezeigt, unabhängig davon, ob Sie die Option **Dialogfeld 'Scannereinstellungen' immer einblenden** aktivieren oder deaktivieren.

---

**Hinweis** Wenn Sie zwei RDS-Anwendungen ausführen, die auf unterschiedlichen Farmen gehostet werden, zeigt die Taskleiste auf dem Clientcomputer zwei Scannerumleitungssymbole an. In der Regel ist nur ein Scanner mit einem Clientcomputer verbunden. In diesem Fall steuern beide Symbole dasselbe Gerät, und es ist nicht von Belang, welches Symbol Sie auswählen. In einigen Situationen kann es vorkommen, dass zwei RDS-Anwendungen auf unterschiedlichen Farmen ausgeführt werden und zwei Scanner lokal verbunden sind. In diesem Fall müssen Sie jedes Symbol öffnen, um herauszufinden, welches Scannerumleitungsmenü welche RDS-Anwendung steuert.

---

Endbenutzeranleitungen für die Handhabung umgeleiteter Scanner finden Sie im Dokument *Verwenden von VMware Horizon Client für Windows*.

## Konfigurieren der Gruppenrichtlinieneinstellungen für Scannerumleitung

Sie können Gruppenrichtlinieneinstellungen konfigurieren, die das Verhalten der Scannerumleitung auf ihren View-Desktops und -Anwendungen steuern. Mit diesen Richtlinieneinstellungen können Sie die

Optionen, die im Dialogfenster „VMware Horizon Scannerumleitungs-Präferenzen“ auf Desktops und Anwendungen von Benutzern verfügbar sind, zentral aus dem Active Directory steuern.

Sie müssen diese Richtlinieneinstellungen nicht konfigurieren. Die Scannerumleitung funktioniert mit den Standardeinstellungen, die für Scanner auf Remote-Desktops und Clientsystemen konfiguriert sind.

Diese Richtlinieneinstellungen wirken sich auf Ihre Remote-Desktops aus, nicht auf die Clientsysteme, an die die physischen Scanner angeschlossen sind. Fügen Sie zum Konfigurieren dieser Einstellungen auf Ihren Desktops und Anwendungen die administrative Vorlagendatei (ADM) für die Scannerumleitungs-Gruppenrichtlinie in Active Directory hinzu.

## Hinzufügen der ADM-Vorlage für die Scannerumleitung in Active Directory

Sie können die Richtlinieneinstellungen in der Scannerumleitungs-ADM-Datei `vdm_agent_scanner.adm` zu Gruppenrichtlinienobjekten (GPOs) in Active Directory hinzufügen und im Gruppenrichtlinienobjekt-Editor die zugehörigen Einstellungen konfigurieren.

### Voraussetzungen

- Vergewissern Sie sich, dass die Setup-Option für die Scannerumleitung auf Ihren Desktops und RDS-Hosts installiert ist. Die Gruppenrichtlinieneinstellungen haben keine Auswirkungen, wenn die Scannerumleitung nicht installiert ist. Siehe [Installieren von View Agent auf einer virtuellen Maschine](#).
- Stellen Sie sicher, dass Active Directory-GPOs für die Gruppenrichtlinieneinstellungen für die Scannerumleitung erstellt wurden. Die GPOs müssen mit der OU verknüpft werden, die Ihre Desktops und RDS-Hosts enthält. Siehe [Beispiel einer Active Directory-Gruppenrichtlinie](#).
- Vergewissern Sie sich, dass MMC und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.
- Machen Sie sich mit den Gruppenrichtlinieneinstellungen für die Scannerumleitung vertraut. Siehe [Gruppenrichtlinieneinstellungen für Scannerumleitung](#).

### Verfahren

- 1 Laden Sie die View GPO-Bundle-ZIP-Datei von der Download-Site von VMware Horizon (mit View) unter <http://www.vmware.com/go/downloadview> herunter.

Der Dateiname ist `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip` (`x.x.x` ist die Version, `yyyyyyy` die Build-Nummer). Alle ADM- und ADMX-Dateien, die Gruppenrichtlinieneinstellungen für View bereitstellen, sind in dieser Datei verfügbar.

- 2 Extrahieren Sie die Datei `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip` und kopieren Sie die Scannerumleitungs-ADM-Datei `vdm_agent_scanner.adm` auf Ihren Active Directory-Server.
- 3 Bearbeiten Sie auf dem Active Directory-Server das GPO, indem Sie **Start > Verwaltung > Gruppenrichtlinienverwaltung** wählen, mit der rechten Maustaste auf das GPO klicken und **Bearbeiten** auswählen.

- 4 Klicken Sie im Gruppenrichtlinienobjekt-Editor mit der rechten Maustaste auf den Ordner **Computerkonfiguration > Administrative Vorlagen** und wählen Sie **Vorlagen hinzufügen/entfernen**.
- 5 Klicken Sie auf **Hinzufügen**, suchen Sie nach der Datei `vdm_agent_scanner.adm` und klicken Sie auf **Öffnen**.
- 6 Klicken Sie auf **Schließen**, um die Richtlinieneinstellungen in der ADM-Datei auf das GPO anzuwenden.

Die Einstellungen sind im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Klassische administrative Vorlagen > VMware View Agent-Konfiguration > Scannerumleitung** enthalten.

Die meisten Einstellungen werden außerdem zum Ordner **Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > Klassische administrative Vorlagen > VMware View Agent-Konfiguration > Scannerumleitung** hinzugefügt.

- 7 Konfigurieren Sie die Gruppenrichtlinieneinstellungen für Scannerumleitung.

## Gruppenrichtlinieneinstellungen für Scannerumleitung

Die Gruppenrichtlinieneinstellungen für Scannerumleitung steuern die Optionen, die im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ auf Desktops und in Anwendungen für Benutzer verfügbar sind.

Die ADM-Datei für die Scannerumleitung enthält sowohl Richtlinien für die Computerkonfiguration als auch Richtlinien für die Benutzerkonfiguration. Die Richtlinien für die Benutzerkonfiguration ermöglichen es Ihnen, unterschiedliche Konfigurationen für Benutzer von VDI-Desktops, RDS-Desktops und RDS-Anwendungen einzurichten. Unterschiedliche Benutzerkonfigurationsrichtlinien können selbst dann wirksam werden, wenn Desktop-Sitzungen und -Anwendungen von Benutzern auf denselben RDS-Hosts ausgeführt werden.

| Gruppenrichtlinieneinstellung | Beschreibung  |
|-------------------------------|---|
| Funktionalität deaktivieren   | <p>Deaktiviert die Scannerumleitungsfunktion.</p> <p>Diese Einstellung ist nur als Computerkonfigurationsrichtlinie verfügbar.</p> <p>Wenn Sie diese Einstellung aktivieren, können Scanner nicht umgeleitet werden. Sie werden auch nicht im Scanner-Menü auf den Desktops bzw. in den Anwendungen der Benutzer angezeigt.</p> <p>Wenn Sie die Einstellung deaktivieren oder nicht konfigurieren, funktioniert die Scannerumleitung und die Scanner werden im Scanner-Menü angezeigt.</p>  |
| Konfiguration sperren         | <p>Sperrt die Benutzeroberfläche für die Scannerumleitung und verhindert, dass Benutzer Konfigurationsoptionen auf ihren Desktops und in ihren Anwendungen ändern.</p> <p>Diese Einstellung ist nur als Computerkonfigurationsrichtlinie verfügbar.</p> <p>Wenn Sie diese Einstellung aktivieren, können Benutzer die Optionen, die über das Taskleisten-Menü auf ihren Desktops und in ihren Anwendungen verfügbar sind, nicht konfigurieren. Benutzer können zwar das Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ öffnen, doch die Optionen sind inaktiv und ihre Einstellungen können nicht geändert werden.</p> <p>Wenn Sie die Einstellung deaktivieren oder nicht konfigurieren, können Benutzer die Optionen im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ konfigurieren.</p> |

| Gruppenrichtlinieneinstellung | Beschreibung   |
|-------------------------------|--|
| Webcam ausblenden             | <p>Verhindert, dass Webcams im Scannerauswahlmenü im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ angezeigt werden.</p> <p>Diese Einstellung ist sowohl als Computerkonfigurationsrichtlinie als auch als Benutzerkonfigurationsrichtlinie verfügbar.</p> <p>Webcams können standardmäßig zu Desktops und Anwendungen umgeleitet werden. Benutzer können Webcams auswählen und sie als virtuelle Scanner zum Aufnehmen von Bildern verwenden.</p> <p>Wenn Sie diese Einstellung als Computerkonfigurationsrichtlinie aktivieren, werden Webcams für alle Benutzer der betroffenen Computer ausgeblendet. Benutzer können die Option <b>Webcam ausblenden</b> im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ nicht ändern.</p> <p>Wenn Sie diese Einstellung als Benutzerkonfigurationsrichtlinie aktivieren, werden Webcams für alle betroffenen Benutzer ausgeblendet. Benutzer können jedoch die Option <b>Webcam ausblenden</b> im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ ändern.</p> <p>Wenn Sie diese Einstellung sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration aktivieren, hat die Einstellung von <b>Webcam ausblenden</b> in der Computerkonfiguration Vorrang vor der entsprechenden Richtlinieneinstellung in der Benutzerkonfiguration für alle Benutzer der betroffenen Computer.</p> <p>Wenn Sie diese Einstellung deaktivieren oder nicht in beiden Richtlinienkonfigurationen konfigurieren, wird die Einstellung von <b>Webcam ausblenden</b> durch die entsprechende Richtlinieneinstellung (entweder der Benutzerkonfiguration oder der Computerkonfiguration) oder durch Benutzerauswahl im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ bestimmt.</p> |

| Gruppenrichtlinieneinstellung | Beschreibung  |
|-------------------------------|---|
| Standardscanner               | <p>Ermöglicht eine zentrale Verwaltung der automatischen Scannerauswahl.</p> <p>Diese Einstellung ist sowohl als Computerkonfigurationsrichtlinie als auch als Benutzerkonfigurationsrichtlinie verfügbar.</p> <p>Sie können Optionen für die automatische Scannerauswahl separat für TWAIN- und WIA-Scanner auswählen. Sie können zwischen folgenden Optionen für die automatische Scannerauswahl wählen:</p> <ul style="list-style-type: none"> <li>■ <b>Keine.</b> Scanner werden nicht automatisch ausgewählt.</li> <li>■ <b>Automatische Auswahl</b> Der lokal verbundene Scanner wird automatisch ausgewählt.</li> <li>■ <b>Zuletzt verwendet</b> Der zuletzt verwendete Scanner wird automatisch ausgewählt.</li> <li>■ <b>Angegeben</b> Der Scanner, dessen Namen Sie in das Textfeld <b>Angegebener Scanner</b> eingeben, wird ausgewählt.</li> </ul> <p>Wenn Sie diese Einstellung als Computerkonfigurationsrichtlinie aktivieren, bestimmt die Einstellung den Modus der automatischen Scannerauswahl für alle Benutzer der betroffenen Computer. Benutzer können die Option <b>Standardscanner</b> im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ nicht ändern.</p> <p>Wenn Sie diese Einstellung als Benutzerkonfigurationsrichtlinie aktivieren, bestimmt die Einstellung den Modus der automatischen Scannerauswahl für alle betroffenen Benutzer. Benutzer können jedoch die Option <b>Standardscanner</b> im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ ändern.</p> <p>Wenn Sie diese Einstellung sowohl in der Computerkonfiguration als auch in der Benutzerkonfiguration aktivieren, hat der Modus für die automatische Scannerauswahl in der Computerkonfiguration Vorrang vor der entsprechenden Richtlinieneinstellung in der Benutzerkonfiguration für alle Benutzer der betroffenen Computer.</p> <p>Wenn Sie diese Einstellung deaktivieren oder nicht in beiden Richtlinienkonfigurationen konfigurieren, wird der Modus für die automatische Scannerauswahl durch die entsprechende Richtlinieneinstellung (entweder der Benutzerkonfiguration oder der Computerkonfiguration) oder durch Benutzererauswahl im Dialogfeld „Einstellungen für die VMware Horizon-Scannerumleitung“ bestimmt.</p> |

## Verwalten des Zugriffs auf die Multimedia-Umleitung von Windows (MMR)

In Horizon 6.0.2 und höher bietet View die Windows Media-MMR-Funktion für Windows 7- und Windows 8/8.1-Desktops und -Clients sowie die Wyse-MMR-Funktion für Windows XP- und Windows Vista-Desktops.

In Horizon 6.0.1 und älteren Versionen bietet View die Windows 7-MMR-Funktion für Windows 7-Desktops und -Clients sowie die Wyse-MMR-Funktion für Windows XP- und Windows Vista-Desktops.

MMR stellt den Multimedia-Stream direkt auf den Clientcomputern bereit. Mit MMR wird der Multimedia-Stream auf dem Clientsystem verarbeitet, d. h. entschlüsselt. Das Clientsystem gibt die Medieninhalte wieder und lagert so die Anforderung vom ESXi-Host aus.

MMR-Daten werden ohne anwendungsbasierte Verschlüsselung über das Netzwerk gesendet und können je nach umgeleitetem Inhalt vertrauliche Daten enthalten. Um sicherzustellen, dass diese Daten nicht auf dem Netzwerk nachverfolgt werden können, sollten Sie MMR nur auf einem sicheren Netzwerk verwenden.

## Aktivieren von Multimedia-Umleitung in View

Sie können Maßnahmen ergreifen, um sicherzustellen, dass nur Horizon Client-Systeme mit ausreichenden Ressourcen auf MMR zugreifen können, um die lokale Multimedia-Dekodierung zu verarbeiten, und in einem sicheren Netzwerk mit View verbunden sind.

Standardmäßig ist die globale Richtlinie in View Administrator **Multimedia-Umleitung (MMR)** auf **Verweigern** festgelegt.

Für die Verwendung von MMR müssen Sie den Wert explizit auf **Zulassen** festlegen.

Wenn Sie den Zugriff auf MMR steuern möchten, haben Sie die Möglichkeit, die Richtlinie **Multimedia-Umleitung (MMR)** für einzelne Desktop-Pools oder für bestimmte Benutzer global zu aktivieren bzw. zu deaktivieren.

Diese Richtlinie betrifft MMR auf Desktops mit Windows 7 und höher sowie Windows XP und Windows Vista.

Anweisungen zum Festlegen von globalen Richtlinien in View Administrator finden Sie unter [View-Richtlinien](#).

## Systemanforderungen für Windows Media MMR

Zur Unterstützung von Windows Media-Multimedia-Umleitung (MMR) muss Ihre View-Bereitstellung bestimmte Software- und Hardwareanforderungen erfüllen. Windows Media MMR wird mit Horizon 6.0.2 und neueren Versionen bereitgestellt.

Horizon 6.0.1 und ältere Versionen stellen die Windows 7-MMR-Komponente für Windows 7-Desktops und -Clients bereit.

Einen Vergleich der Windows Media-MMR-, Windows 7-MMR- und Wyse-MMR-Komponenten finden Sie unter [Unterstützung der Multimedia-Umleitung auf Desktop-Betriebssystemen](#).

### View-Desktop

- Auf den Desktops muss eines der folgenden Betriebssysteme ausgeführt werden:
  - 64-Bit- oder 32-Bit-Version von Windows 7 Enterprise oder Ultimate
  - 64-Bit- oder 32-Bit-Version von Windows 8/8.1 Professional oder Enterprise
- **3D-Rendering** kann für den Desktop-Pool aktiviert oder deaktiviert werden.
- Benutzer müssen Videos in Windows Media Player 12 oder höher oder in Internet Explorer 8 oder höher wiedergeben.

Um Internet Explorer zu verwenden, müssen Sie den geschützten Modus deaktivieren. Klicken Sie im Dialogfeld „Internetoptionen“ auf die Registerkarte **Sicherheit** und deaktivieren Sie **Geschützten Modus aktivieren**.

**Horizon Client-Software** Horizon Client 3.2 für Windows oder höher

**Horizon Client-Computer oder Clientzugriffsgerät**

- Auf den Clients muss ein Windows 7- oder Windows 8/8.1-Betriebssystem mit 64 Bit oder 32 Bit ausgeführt werden.

**Unterstützte Medienformate**

In Windows Media Player unterstützte Medienformate werden unterstützt. Beispielsweise: M4V; MOV; MP4; WMP; MPEG2-1; MPEG-2; MPEG-4 Part 2; WMV 7, 8 und 9; WMA; AVI; ACE; MP3; WAV.

---

**Hinweis** DRM-geschützter Inhalt wird nicht über Windows Media MMR umgeleitet.

---

**View-Richtlinien**

Legen Sie in View Administrator die Richtlinie **Multimedia-Umleitung (MMR)** auf **Zulassen** fest. Der Standardwert lautet **Verweigern**.

**Backend-Firewall**

Wenn Ihre View-Bereitstellung eine Backend-Firewall zwischen Ihren DMZ-basierten Sicherheitsservern und dem internen Netzwerk enthält, stellen Sie sicher, dass die Backend-Firewall den Datenverkehr zu Port 9427 auf Ihren Desktops zulässt.

## Unterstützung der Multimedia-Umleitung auf Desktop-Betriebssystemen

Mit Horizon 6.0.2 und höher werden die Komponenten für die Multimedia-Umleitung Windows Media-MMR- und Wyse-MMR mit View Agent installiert. Die Wyse MMR-Komponente wird auf Windows XP- und Windows Vista-Desktops ausgeführt.

Mit Horizon 6.0.1 und älteren Versionen werden die Windows 7-MMR- und die Wyse-MMR-Komponente mit View Agent installiert.

Diese MMR-Komponenten unterscheiden sich geringfügig bezüglich ihrer Merkmale und Anforderungen.

**Tabelle 13-3. View Desktop-Betriebssystemunterstützung für die Multimedia-Umleitung**

| View-Version                       | MMR               | Desktop-Betriebssystem                             | Anforderungen virtueller Maschinen   | Unterstützte Medienformate  | Unterstützte Clients  |
|------------------------------------|-------------------|--|--|---|---|
| Horizon 6.0.2 und höher            | Windows Media MMR | Windows 7, Windows 8/8.1                           | <b>3D-Rendering</b> kann aktiviert bzw. deaktiviert werden.<br><br>Windows Media Player 12 oder höher muss installiert sein. Internet Explorer 8 oder höher muss installiert sein, um Videos in Internet Explorer wiedergeben zu können. | In Windows Media Player unterstützte Formate werden unterstützt.<br><br>Beispiel:<br>M4V, MOV, MP4, WMP, MPEG2-1, MPEG-2, MPEG-4 Part 2, WMV 7, 8 und 9, WMA, AVI, ACE, MP3, WAV<br><br><b>Hinweis</b> DRM-geschützter Inhalt wird nicht über Windows Media MMR umgeleitet. | Windows 7, Windows 8/8.1<br><br>Windows Media Player 12 oder höher muss installiert sein. Internet Explorer 8 oder höher muss installiert sein, um Videos in Internet Explorer wiedergeben zu können.                                   |
| Horizon 6.0.1 und ältere Versionen | Win7 MMR          | Windows 7<br>Windows 8/8.1 wird nicht unterstützt. | Die Desktops müssen virtuelle Hardware der Version 8 oder höher verwenden.<br><br>Das <b>3D-Rendering</b> muss aktiviert sein.<br><br>Windows Media Player 12 oder höher muss installiert sein.  | H.264-Komprimierungsstandard für M4V-, MP4- und MOV-Format.<br><br><b>Hinweis</b> Der Audio-Stream wird nicht über Windows 7-MMR umgeleitet. Audiodaten werden vom Remote-Desktop über PCoIP für das Clientsystem bereitgestellt.   | Windows 7, Windows 8<br><br>Die Clients müssen über DVXA-kompatible (DirectX Video Acceleration) Grafikkarten verfügen, die die ausgewählten Videos decodieren können.<br><br>Windows Media Player 12 oder höher muss installiert sein. |
| Horizon 6.0.x und ältere Versionen | Wyse MMR          | Windows XP, Windows Vista                          | Windows Media Player 10 oder höher muss installiert sein.  | Es werden zahlreiche Formate unterstützt.<br><br>Beispiel:<br>MPEG2-1, MPEG2, MPEG-4 Part 2, WMV 7, 8 und 9, WMA, AVI, ACE, MPT3, WAV   | Windows XP, Windows Vista, Windows 7<br><br>Windows Media Player 10 oder höher muss installiert sein.   |

Weitere Informationen zu den MMR-Systemanforderungen für Horizon Client-Geräte finden Sie im Dokument *Verwenden von VMware Horizon Client für Windows*.

## Sicherstellen, dass Clients Windows 7 MMR initiieren können

In Horizon 6.0.1 und früher bietet Horizon Client die Funktion Windows 7 MMR für Desktops und Clients mit Windows 7. Sie können Maßnahmen ergreifen, damit Clients ausreichend Zeit haben, Windows 7 MMR zu initiieren.



Windows 7 MMR verwendet einen Handshake zwischen dem Horizon Client-System und dem Desktop, um Anfragen für die Multimedia-Umleitung (MMR) zu überprüfen. Unter bestimmten Netzwerkbedingungen dauert dieser Handshake zu lange, sodass MMR nicht initiiert wird. Um sicherzustellen, dass Windows 7 MMR initiiert werden kann, können Sie auf dem Desktop einen Windows-Registrierungsschlüssel konfigurieren, um die Zeit zu verlängern, die für die Durchführung der Handshake-Überprüfung zulässig ist.

Der Windows-Registrierungsschlüssel steuert den TTL-Wert (Time to Live) des Handshakes und wird in Millisekunden angegeben. Der Wert hat das REG\_DWORD (hex)-Format. Der Standardwert liegt bei 5000 Millisekunden (5 Sekunden).

Bevor Sie Windows 7 MMR für Ihre View-Benutzer bereitstellen, sollten Sie ein paar Clientsysteme testen, um sicherzustellen, dass die zulässige Standardzeit für die Durchführung des Handshakes für Ihre Umgebung angemessen ist. Wenn für Ihre Netzwerkbedingungen ein längerer Handshake als fünf Sekunden erforderlich ist, erhöhen Sie den TTL-Wert.

### Verfahren

- 1 Starten Sie den Windows-Registrierungs-Editor auf dem Remote-Desktop.
- 2 Navigieren Sie zum Windows-Registrierungsschlüssel, der den MMR-Überprüfungs-Handshake steuert.

| Option            | Beschreibung  |
|-------------------|---|
| Windows 7, 64 Bit | HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware VDPService\handshakeTTL |
| Windows 7, 32 Bit | HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDPService\handshakeTTL             |

- 3 Erhöhen Sie den handshakeTTL-Wert auf eine Zahl größer als 5000.
- 4 Starten Sie den Windows Media Player auf dem Desktop neu, um den aktualisierten Wert anzuwenden.

# Verwenden von USB-Geräten mit Remote-Desktops

# 14

Administratoren können Remote-Desktops so konfigurieren, dass USB-Geräte wie Flash-Laufwerke, Kameras, VoIP-Geräte und Drucker genutzt werden können. Diese Funktion wird USB-Umleitung genannt und unterstützt die Verwendung des RDP- oder des PCoIP-Anzeigeprotokolls. Ein Remote-Desktop unterstützt maximal 32 USB-Geräte.

Bei Verwendung dieser Funktion stehen die meisten USB-Geräte, die an das lokale Clientsystem angeschlossen sind, auf dem Remote-Desktop zur Verfügung. Es ist sogar möglich, von einem Remote-Desktop aus eine Verbindung mit einem iPad herzustellen und diesen zu verwalten. Sie können zum Beispiel Ihr iPad mit dem auf Ihrem Remote-Desktop installierten iTunes-Programm synchronisieren. Auf einigen Clientgeräten, beispielsweise auf Windows- und Mac OS X-Computern, werden die USB-Geräte in einem Menü in Horizon Client aufgelistet. Über das Menü können Sie die Geräte verbinden oder deren Verbindung trennen.

In den meisten Fällen ist es nicht möglich, ein USB-Gerät gleichzeitig auf einem Clientsystem und auf einem Remote-Desktop zu verwenden. Nur wenige Arten von USB-Geräten können vom Remote-Desktop und dem lokalen Computer gemeinsam verwendet werden. Zu diesen Geräten zählen Smartcard-Leser und Eingabegeräte, wie beispielsweise Tastaturen und Zeigegeräte.

Administratoren können angeben, mit welchen Arten von USB-Geräten die Endbenutzer eine Verbindung herstellen dürfen. Für aus mehreren Gerätetypen zusammengesetzte Gerätegruppen, die etwa aus einem Videoeingabegerät und einem Speichergerät bestehen, können Administratoren auf einigen Clientsystemen die Gerätegruppe so aufgliedern, dass ein Gerät (wie etwa das Videoeingabegerät) zulässig ist, das andere Gerät (etwa das Speichergerät) jedoch nicht.

Die USB-Umleitungsfunktion ist in Desktop-Pools verfügbar, die auf einzelnen Benutzer-Computern bereitgestellt werden. Diese Funktion ist nicht in RDS-Desktop-Pools verfügbar.

---

**Hinweis** Die USB-Umleitung ist nur auf einigen Clienttypen verfügbar. Informationen dazu, ob diese Funktion auf einem bestimmten Clienttyp unterstützt wird, finden Sie in der Funktionsunterstützungsmatrix im Dokument „Verwenden von VMware Horizon Client“ für den spezifischen Typ von Desktop- oder mobilem Clientgerät. Besuchen Sie [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html).

---

Dieses Kapitel enthält die folgenden Themen:

- [Einschränkungen in Bezug auf USB-Gerätetypen](#)
- [Überblick über das Einrichten der USB-Umleitung](#)

- [Netzwerkdatenverkehr und USB-Umleitung](#)
- [Automatische Verbindungen mit USB-Geräten](#)
- [Deaktivieren der USB-Umleitung](#)
- [Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs](#)
- [Verwenden von Richtlinien zum Steuern der USB-Umleitung](#)
- [Fehlerbehebung bei Problemen mit der USB-Umleitung](#)

## Einschränkungen in Bezug auf USB-Gerätetypen

Wenngleich View nicht alle Geräte explizit am Arbeiten in einem Remote-Desktop hindert, funktionieren einige Geräte aufgrund von Faktoren wie Netzwerklatenz und Bandbreite besser als andere. Standardmäßig werden einige Geräte durch Filtern oder Sperren automatisch von der Verwendung ausgeschlossen.

In Horizon 6.0.1 können Sie zusammen mit Horizon Client 3.1 oder höher USB 3.0-Geräte auf der Clientmaschine an USB 3.0-Ports anschließen. USB 3.0-Geräte werden nur mit einem einzelnen Stream unterstützt. Da in dieser Version die Unterstützung mehrerer Streams nicht implementiert ist, wurde die Leistung von USB-Geräten nicht verbessert. Manche USB 3.0-Geräte, die für ihren ordnungsgemäßen Gebrauch einen konstant hohen Durchsatz erfordern, funktionieren aufgrund der Netzwerklatenz möglicherweise nicht in einer VDI-Sitzung.

Obwohl keine Unterstützung für frühere Versionen von View Super-Speed-USB-3.0-Geräten besteht, funktionieren USB 3.0-Geräte oft, wenn sie auf der Clientmaschine an einen USB 2.0-Port angeschlossen werden. Es kann jedoch je nach Art des USB-Chipsatzes auf der Hauptplatine des Clientsystems Ausnahmen geben.

Die folgenden Typen von Geräten eignen sich möglicherweise nicht für die USB-Umleitung an einen Remote-Desktop:

- Aufgrund der Bandbreitenanforderungen von Webcams, die in der Regel mehr als 60 MBit/s Bandbreite verbrauchen, werden Webcams nicht über die USB-Umleitung unterstützt. Für Webcams können Sie die Echtzeit-Audio/Video-Funktion verwenden.
- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz. Wenn Sie die Echtzeit-Audio/Video-Funktion verwenden, arbeiten Audioeingabe- und Audioausgabegeräte ordnungsgemäß, und die Verwendung der USB-Umleitung ist für diese Geräte nicht erforderlich.
- Die Leistung einiger USB-Geräte variiert, insbesondere im WAN, abhängig von der Netzwerklatenz und Zuverlässigkeit sehr stark. Beispiel: Eine einzelne USB-Speichergerät-Leseanforderung benötigt drei Round-Trips zwischen dem Client und dem Remote-Desktop. Für Lesen einer vollständigen Datei sind möglicherweise mehrere USB-Lesevorgänge notwendig. Je größer die Latenz, desto mehr Zeit nimmt der Round-Trip in Anspruch.

Die Dateistruktur kann abhängig vom Format sehr groß sein. Große USB-Festplattenlaufwerke können erst nach mehreren Minuten auf dem Desktop angezeigt werden. Das Formatieren eines USB-Geräts als NTFS anstatt FAT unterstützt das Verringern der ursprünglichen Verbindungszeit. Ein unzuverlässiger Netzwerk-Link führt zu Wiederholungen und die Leistung wird weiter reduziert.

Gleichermaßen funktionieren USB-CD/DVD-Leser und -Writer, die eine stabile Bitrate von Daten für den korrekten Abschluss des Brennvorgangs benötigen, sowie Scanner und Fingereingabegeräte wie Signatur-Tablets auf einem latenten Netzwerk wie ein WAN nicht optimal.

- Das Umleiten von USB-Scannern hängt vom Zustand des Netzwerks ab und es kann länger als normal dauern, bis die Scans fertiggestellt sind.

## Überblick über das Einrichten der USB-Umleitung

Um Ihre Bereitstellung so einzurichten, dass Endbenutzer Wechselmedien wie USB-Sticks, Kameras und Headsets anschließen können, müssen Sie bestimmte Komponenten sowohl auf dem Remote-Desktop als auch auf dem Client-Gerät installieren, und Sie müssen überprüfen, ob die globale Einstellung für USB-Geräte in View Administrator aktiviert ist.

Diese Prüfliste beinhaltet sowohl erforderliche als auch optionale Aufgaben zur Einrichtung einer USB-Umleitung in Ihrem Unternehmen.

---

**Hinweis** Die USB -Umleitungsfunktion ist nur auf einigen Clienttypen wie beispielsweise Windows, Mac OS X und von Partnern bereitgestellten Linux-Clients verfügbar. Informationen dazu, ob diese Funktion auf einem bestimmten Clienttyp unterstützt wird, finden Sie in der Unterstützungsmatrix im Dokument „Verwenden von VMware Horizon Client“ für den spezifischen Typ von Clientgerät. Besuchen Sie [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html).

---

- 1 Wenn Sie den View Agent-Installationsassistenten auf der Remote-Desktop-Quelle ausführen, stellen Sie sicher, dass Sie die USB-Umleitungs-Komponente mitinstallieren.

Diese Komponente ist standardmäßig enthalten. VMware empfiehlt, diese Komponente immer mitzuinstallieren. Sie können Gruppenrichtlinieneinstellungen verwenden, um die USB-Umleitung für einige Remote-Desktops und Benutzer zu deaktivieren oder einzuschränken, welche Typen von USB-Geräten umgeleitet werden können.

- 2 Wenn Sie den VMware Horizon Client-Installationsassistenten auf dem Clientsystem ausführen, stellen Sie sicher, dass Sie die USB-Umleitungs-Komponente mitinstallieren.

Diese Komponente ist standardmäßig enthalten.

- 3 Überprüfen Sie, ob der Zugriff auf USB-Geräte von einem Remote-Desktop in View Administrator aktiviert ist.

Wechseln Sie in View Administrator zu **Richtlinien > Globale Richtlinien** und prüfen Sie, ob **USB-Zugriff** auf **Zulassen** steht.

- 4 (Optional) Konfigurieren Sie View Agent-Gruppenrichtlinien, um anzugeben, welche Typen von Geräten umgeleitet werden können.

Siehe [Verwenden von Richtlinien zum Steuern der USB-Umleitung](#).

- 5 (Optional) Konfigurieren Sie ähnliche Einstellungen auf dem Clientgerät.

Sie können auch konfigurieren, ob Geräte automatisch angeschlossen werden sollen, wenn sich Horizon Client mit dem Remote-Desktop verbindet oder wenn der Endbenutzer ein USB-Gerät einsteckt. Die Methode zur Konfigurierung von USB-Einstellungen auf dem Clientgerät hängt vom Typ des Geräts ab. Bei Windows-Client-Endpoints können Sie beispielsweise Gruppenrichtlinien konfigurieren, während Sie bei Mac OS X-Endpoints einen Befehl in der Befehlszeile verwenden. Anleitungen für einen bestimmten Typ von Clientgerät finden Sie im Dokument „Verwenden von VMware Horizon Client“.

- 6 Endbenutzer sollen eine Verbindung zu einem Remote-Desktop herstellen und ihre USB-Geräte in das lokale Clientsystem einstecken.

Wenn der Treiber für das USB-Gerät nicht bereits auf dem Remote-Desktop installiert ist, erkennt das Gastbetriebssystem das USB-Gerät und sucht genauso wie bei einem physischen Windows-Computer nach einem passenden Treiber.

## Netzwerkdatenverkehr und USB-Umleitung

Die USB-Umleitung erfolgt unabhängig vom Anzeigeprotokoll (RDP oder PCoIP) und der USB-Datenverkehr verwendet gewöhnlich den TCP-Port 32111.

Der Netzwerkdatenverkehr zwischen einem Client-System und einem Remote-Desktop kann über verschiedene Routen erfolgen, abhängig davon, ob das Client-System Teil des Unternehmensnetzwerks ist und für welche Sicherheitseinstellungen sich der Administrator entschieden hat.

- 1 Wenn das Client-System Teil des Unternehmensnetzwerks ist, sodass eine direkte Verbindung zwischen dem Client und dem Desktop hergestellt werden kann, verwendet der USB-Datenverkehr den TCP-Port 32111.
- 2 Wenn das Client-System nicht Teil des Unternehmensnetzwerks ist, kann der Client eine Verbindung über einen View-Sicherheitsserver herstellen.

Ein Sicherheitsserver befindet sich in einem Umkreisnetzwerk und fungiert als Proxy-Host für Verbindungen innerhalb Ihres vertrauenswürdigen Netzwerks. Dieses Konzept bietet eine weitere Sicherheitsebene, indem die View-Verbindungsserver-Instanz vor dem öffentlichen Internet abgeschirmt wird und alle ungeschützten Sitzungsanforderungen zwangsweise durch den Sicherheitsserver geleitet werden.

Eine Sicherheitsserverbereitstellung auf Basis eines Umkreisnetzwerks erfordert das Öffnen verschiedener Ports in der Firewall, damit sich Clients mit Sicherheitsservern im Umkreisnetzwerk verbinden können. Sie müssen ferner Ports für die Kommunikation zwischen Sicherheitsservern und den View-Verbindungsserver-Instanzen im internen Netzwerk konfigurieren.

Informationen zu bestimmten Ports finden Sie unter „Firewall-Regeln für Sicherheitsserver im Umkreisnetzwerk“ im *Architektur-Planungshandbuch für View*.

- 3 Wenn das Client-System nicht Teil des Unternehmensnetzwerks ist, können Sie View Administrator zur Aktivierung des sicheren HTTPS-Tunnels verwenden. Der Client baut dann eine zweite HTTPS-

Verbindung mit dem View-Verbindungsserver- oder Sicherheitsserverhost auf, wenn Benutzer sich mit einem Remote-Desktop verbinden. Die Verbindung wird über den HTTPS-Port 443 an den Sicherheitsserver getunnelt, woraufhin die weiterführende Verbindung für den USB-Datenverkehr vom Server zum Remote-Desktop den TCP-Port 32111 verwendet. Die Leistung des USB-Geräts nimmt bei Verwendung dieses Tunnels leicht ab.

---

**Hinweis** Bei der Verwendung eines Zero-Clients wird der USB-Datenverkehr anstatt durch TCP 32111 über einen virtuellen PCoIP-Kanal umgeleitet. Die Daten werden durch das PCoIP Secure Gateway und über den TCP/UDP-Port 4172 gekapselt und verschlüsselt. Wenn Sie ausschließlich Zero-Clients verwenden, ist es nicht erforderlich, den TCP-Port 32111 zu öffnen.

---

## Automatische Verbindungen mit USB-Geräten

Auf einigen Clientsystemen können Administratoren oder Endbenutzer oder beide automatische Verbindungen von USB-Geräten zu einem Remote-Desktop konfigurieren. Automatische Verbindungen können entweder hergestellt werden, sobald ein Benutzer ein USB-Gerät an das Client-System anschließt oder sobald der Client eine Verbindung zum Remote-Desktop herstellt.

Einige Geräte wie beispielsweise Smartphones und Tablets erfordern automatische Verbindungen, da diese Geräte während eines Upgrades neu gestartet und somit vom System getrennt werden. Wenn diese Geräte nicht auf automatische Verbindungswiederherstellung zum Remote-Desktop eingerichtet werden, stellen sie stattdessen während eines Upgrades und nach dem Neustart der Geräte eine Verbindung zum lokalen Clientsystem her.

Die Konfigurationseigenschaften für automatische USB-Verbindungen, die Administratoren auf dem Client einrichten oder die von Endbenutzern mithilfe eines Horizon Client Menüelements festgelegt werden, gelten für alle USB-Geräte, es sei denn, die Geräte sind für den Ausschluss von der USB-Umleitung konfiguriert. Einige Client-Versionen, Webcams und Mikrofone beispielsweise sind standardmäßig von der USB-Umleitung ausgenommen, da diese Geräte besser mit der Echtzeit-Audio/Video-Funktion funktionieren. Es kann vorkommen, dass ein USB-Gerät nicht standardmäßig von der USB-Umleitung ausgenommen ist, aber ein Administrator für dieses Gerät dennoch explizit den Ausschluss von der USB-Umleitung vornehmen muss. Die folgenden USB-Gerätetypen eignen sich nicht für die USB-Umleitung; für sie darf keine automatische Verbindung zu einem Remote-Desktop hergestellt werden:

- **USB-Ethernet-Geräte.** Wenn Sie ein USB-Ethernet-Gerät umleiten, verliert Ihr Client-System möglicherweise die Verbindung zum Netzwerk, wenn es sich bei diesem Gerät um das einzige Ethernet-Gerät handelt.
- **Touchscreen-Geräte.** Wenn Sie ein Touchscreen-Gerät umleiten, empfängt der Remote-Desktop Eingaben vom Touchscreen und nicht von der Tastatur.

Wenn Sie den Remote-Desktop zur automatischen Verbindung von USB-Geräten konfiguriert haben, können Sie Richtlinien konfigurieren, um bestimmte Geräte wie beispielsweise Touchscreen- und Netzwerkgeräte auszuschließen. Weitere Informationen finden Sie unter [Konfigurieren der Filterrichtlinieneinstellungen für USB-Geräte](#).

Bei Windows-Clients gibt es eine Alternative: Anstatt Einstellungen zu verwenden, die eine automatische Verbindung zu allen Geräten herstellen, wovon einige Geräte ausgenommen sind, können Sie eine Konfigurationsdatei auf dem Client bearbeiten, die Horizon Client für das Wiederherstellen einer Verbindung nur von einem oder mehreren bestimmten Geräten zum Remote-Desktop konfiguriert, z. B. Smartphones und Tablets. Die entsprechenden Anweisungen finden Sie unter *Verwenden von VMware Horizon Client für Windows*.

## Deaktivieren der USB-Umleitung

Für einige äußerst sicherheitsrelevante Anwendungen ist es erforderlich, dass die USB-Umleitung deaktiviert wird. Sie können die USB-Umleitung für alle Desktop-Pools, bestimmte Desktop-Pools oder bestimmte Benutzer in einem Desktop-Pool deaktivieren.

Sie können jede der folgenden Strategien Ihrer Situation entsprechend anwenden:

- Bearbeiten Sie in View Administrator die Richtlinie **USB-Zugriff** für einen bestimmten Pool, um den Zugriff entweder zuzulassen oder zu verweigern.
- Nachdem Sie die Richtlinie in View Administrator auf Desktop-Pool-Ebene festgelegt haben, können Sie die Richtlinie für eine bestimmte virtuelle Maschine im Pool überschreiben.
- Wenn Sie View Agent installieren, deaktivieren Sie die Komponente **USB-Umleitung**. VMware empfiehlt diese Strategie nicht, da sie zu einer geringeren Flexibilität führt als bei der Verwendung von Richtlinieneinstellungen.
- Legen Sie die Richtlinie **Alle Geräte ausschließen** ggf. auf der Agenten-Seite oder auf der Client-Seite auf **true** fest.

Wenn Sie für die Richtlinie **Alle Geräte ausschließen** die Option **true** festlegen, verhindert Horizon Client, dass alle USB-Geräte umgeleitet werden. Sie können andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn Sie für diese Richtlinie **false** festlegen, lässt Horizon Client zu, dass alle USB-Geräte umgeleitet werden, mit Ausnahme derer, die durch andere Richtlinieneinstellungen blockiert werden. Sie können die Richtlinie sowohl für View Agent als auch für Horizon Client festlegen. Die folgende Tabelle zeigt an, wie die Richtlinie **Exclude All Devices**, die Sie für View Agent und Horizon Client festlegen können, kombiniert werden kann, damit sich eine effektive Richtlinie für den Clientcomputer ergibt. Standardmäßig können alle USB-Geräte umgeleitet werden, es sei denn, sie wären anderweitig blockiert.

**Tabelle 14-1. Auswirkungen der Kombination von „Exclude All Devices (Alle Geräte ausschließen)“**

| Richtlinie „Exclude All Devices (Alle Geräte ausschließen)“ auf View Agent | Richtlinie „Alle Geräte ausschließen“ auf Horizon Client         | Kombinierte effektive Richtlinie zum Ausschließen aller Geräte |
|--|--|--|
| <b>false</b> oder nicht definiert (alle USB-Geräte einschließen)           | <b>false</b> oder nicht definiert (alle USB-Geräte einschließen) | Include all USB devices (Alle USB-Geräte einschließen)         |
| <b>false</b> (alle USB-Geräte einschließen)                                | <b>true</b> (alle USB-Geräte ausschließen)                       | Exclude all USB devices (Alle USB-Geräte ausschließen)         |
| <b>true</b> (alle USB-Geräte ausschließen)                                 | Beliebig oder nicht definiert                                    | Exclude all USB devices (Alle USB-Geräte ausschließen)         |

Wenn Sie die Richtlinie `Disable Remote Configuration Download` auf **true** setzen, wird der Wert von `Exclude All Devices` auf View Agent nicht an Horizon Client weitergegeben, sondern View Agent und Horizon Client erzwingen den lokalen Wert von `Exclude All Devices`.

Diese Richtlinien sind in der ADM-Vorlagendatei zur Konfiguration von View Agent (`vdm_agent.adm`) enthalten. Weitere Informationen finden Sie unter [USB-Einstellungen in der ADM-Vorlage für die View Agent-Konfiguration](#).

## Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs

Nützliche Protokolldateien für USB befinden sich sowohl auf dem Client-System als auch auf dem Remote-Desktop-Betriebssystem. Verwenden Sie die Protokolldateien an beiden Speicherorten zur Fehlerbehebung. Um Produkt-IDs für bestimmte Geräte zu suchen, verwenden Sie clientseitige Protokolle.

Wenn Sie versuchen, die USB-Geräteteilung oder -filterung zu konfigurieren, oder wenn Sie versuchen, festzustellen, warum ein spezielles Gerät nicht in einem Horizon Client-Menü angezeigt wird, sehen Sie in die Client-Protokolle. Client-Protokolle werden für den USB-Arbitrator und für den Horizon View USB-Dienst erzeugt. Die Anmeldung bei Windows- und Linux-Clients ist standardmäßig aktiviert. Auf Mac OS X-Client ist die Protokollierung standardmäßig deaktiviert. Informationen zur Aktivierung der Protokollierung auf Mac OS X finden Sie unter *Verwenden von VMware Horizon Client für Mac OS X*.

Wenn Sie Richtlinien für das Teilen und Filtern von USB-Geräten konfigurieren, erfordern einige Werte, die Sie festlegen, die VID (Lieferanten-ID) und die PID (Produkt-ID) für das USB-Gerät. Die korrekte VID und PID finden Sie, indem Sie im Internet nach dem Produktnamen plus VID und PID suchen. Alternativ können Sie nach Anschluss des USB-Geräts an das lokale System bei Ausführung von Horizon Client auch in der USB-Protokolldatei nachsehen. Die folgende Tabelle zeigt den Standardspeicherort der Protokolldateien.



**Tabelle 14-2. Protokolldateispeicherorte**

| Client oder Agent                  | Pfad zu Protokolldateien  |
|------------------------------------|---|
| Windows-Client                     | %PROGRAMDATA%\VMware\VDM\logs\debug-*.txt<br>C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log                |
| Windows-Agent (auf Remote-Desktop) | %PROGRAMDATA%\VMware\VDM\logs\debug-*.txt   |
| Mac OS X-Client                    | /var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log<br>/Library/Logs/VMware/vmware-usbarbitrator-xxxx.log |
| Linux-Client                       | (Standardspeicherort) /tmp/vmware-root/vmware-view-usbd-*.log   |

Falls ein Problem mit dem Gerät auftritt, nachdem das Gerät zum Remote-Desktop umgeleitet wurde, prüfen Sie sowohl die client- als auch die agentseitigen Protokolle.

## Verwenden von Richtlinien zum Steuern der USB-Umleitung

Sie können USB-Richtlinien sowohl für den Remote-Desktop (View Agent) als auch für Horizon Client konfigurieren. Diese Richtlinien geben an, ob das Clientgerät USB-Verbundgeräte für die Umleitung in separate Komponenten aufschlüsseln soll oder nicht. Sie können Geräte aufschlüsseln, um die Typen der USB-Geräte einzuschränken, die der Client zur Umleitung zur Verfügung stellt, und damit View Agent verhindert, dass bestimmte USB-Geräte von einem Client-Computer weitergeleitet werden.

Wenn Sie ältere Versionen von View Agent oder Horizon Client installiert haben, sind nicht alle Funktionen der USB-Umleitungsrichtlinien verfügbar. [Tabelle 14-3. Kompatibilität von USB-Richtlinieneinstellungen](#) zeigt, wie View die Richtlinien auf verschiedene Kombinationen von View Agent und Horizon Client anwendet.

**Tabelle 14-3. Kompatibilität von USB-Richtlinieneinstellungen**

| View Agent-Version | Horizon Client-Version | Auswirkungen von USB-Richtlinieneinstellungen auf die USB-Umleitung   |
|--------------------|------------------------|---|
| 5.1 oder höher     | 5.1 oder höher         | USB-Richtlinieneinstellungen gelten sowohl für View Agent als auch für Horizon Client. Sie können in View Agent USB-Richtlinieneinstellungen festlegen, die bestimmen, USB-Geräte nicht an einen Desktop weiterzuleiten. View Agent kann Gerätesplitting- und Filterrichtlinieneinstellungen an Horizon Client senden. Sie können in Horizon Client USB-Richtlinieneinstellungen festlegen, die bestimmen, USB-Geräte nicht von einem Clientcomputer an einen Desktop weiterzuleiten.   |
| 5.1 oder höher     | 5.0.x oder früher      | USB-Richtlinieneinstellungen gelten nur für View Agent. Sie können in View Agent USB-Richtlinieneinstellungen festlegen, die bestimmen, USB-Geräte nicht an einen Desktop weiterzuleiten. Sie können in Horizon Client keine USB-Richtlinieneinstellungen festlegen, die bestimmen, welche USB-Geräte von einem Clientcomputer an einen Desktop weitergeleitet werden können. Horizon Client kann keine Gerätesplitting- und Filterrichtlinieneinstellungen von View Agent empfangen. Vorhandene Registrierungseinstellungen für die USB-Umleitung von Horizon Client bleiben gültig. |

| <b>View Agent-Version</b> | <b>Horizon Client-Version</b> | <b>Auswirkungen von USB-Richtlinieneinstellungen auf die USB-Umleitung</b>   |
|---------------------------|-------------------------------|--|
| 5.0.x oder früher         | 5.1 oder höher                | USB-Richtlinieneinstellungen gelten nur für Horizon Client. Sie können in Horizon Client USB-Richtlinieneinstellungen festlegen, die bestimmen, USB-Geräte nicht von einem Clientcomputer an einen Desktop weiterzuleiten. Sie können in View Agent keine USB-Richtlinieneinstellungen festlegen, die bestimmen, USB-Geräte nicht an einen Desktop weiterzuleiten. View Agent kann keine Gerätesplitting- und Filterrichtlinieneinstellungen an Horizon Client senden. |
| 5.0.x oder früher         | 5.0.x oder früher             | USB-Richtlinieneinstellungen sind nicht anwendbar. Vorhandene Registrierungseinstellungen für die USB-Umleitung von Horizon Client bleiben gültig.   |

Wenn Sie Horizon Client aktualisieren, bleiben alle vorhandenen Registrierungseinstellungen für die USB-Umleitung (z. B. `HardwareIdFilters`) so lange gültig, bis Sie USB-Richtlinien für Horizon Client definieren.

Auf Clientgeräten, die keine clientseitigen USB-Richtlinien unterstützen, können Sie die USB-Richtlinien für View Agent verwenden, um zu steuern, welche USB-Geräte vom Client an einen Desktop weitergeleitet werden dürfen.

## Konfigurieren der Gerätesplittingrichtlinieneinstellungen für Composite USB-Geräte

USB-Verbundgeräte bestehen aus einer Kombination von zwei oder mehr Geräten, so zum Beispiel einem Videoeingabegerät und einem Speichergerät oder einem Mikrofon und einem Mausgerät. Wenn Sie möchten, dass eine oder mehrere Komponenten für die Umleitung zur Verfügung stehen sollen, können Sie das Verbundgerät in seine Komponentenschnittstellen splitten, bestimmte Schnittstellen von der Umleitung ausschließen und andere einschließen.

Sie können eine Richtlinie festlegen, die Verbundgeräte automatisch aufschlüsselt. Wenn das automatische Gerätesplitten bei einem bestimmten Gerät nicht funktioniert oder wenn das automatische Splitten nicht zu den von Ihrer Anwendung gewünschten Ergebnissen führt, können Sie Verbundgeräte manuell aufschlüsseln.

### Automatisches Gerätesplitten

Wenn Sie das automatische Gerätesplitten aktivieren, versucht View die Funktionen oder Geräte in einem Verbundgerät den wirksamen Filterregeln gemäß aufzuschlüsseln. Beispiel: Ein Diktiermikrofon muss möglicherweise automatisch aufgeschlüsselt werden, sodass das Mausgerät für den Client lokal bleibt, der Rest der Geräte wird jedoch an den Remote-Desktop weitergeleitet.

Die folgende Tabelle zeigt, wie der Wert der Einstellung `Autom. Gerätesplitten` zulassen bestimmt, ob der Horizon Client versucht, USB-Verbundgeräte automatisch zu splitten. Standardmäßig ist das automatische Gerätesplitten deaktiviert.

**Tabelle 14-4. Auswirkungen des Kombinierens von Richtlinien zum Deaktivieren des automatischen Splittens**

| Richtlinie zum Zulassen des automatischen Splittens bei View Agent | Richtlinie zum Zulassen des automatischen Gerätesplittens bei Horizon Client | Kombinierte effektive Richtlinie zum Zulassen des automatischen Splittens von Geräten |
|--|--|---|
| Allow – Default Client Setting                                     | <b>false</b> (automatisches Splitten deaktiviert)                            | Automatisches Splitten deaktiviert  |
| Allow – Default Client Setting                                     | <b>true</b> (automatisches Splitten aktiviert)                               | Automatisches Splitten aktiviert  |
| Allow – Default Client Setting                                     | Nicht definiert  | Automatisches Splitten aktiviert  |
| Allow – Override Client Setting                                    | Beliebig oder nicht definiert  | Automatisches Splitten aktiviert  |
| Nicht definiert  | Nicht definiert  | Automatisches Splitten deaktiviert  |

**Hinweis** Diese Richtlinien sind in der ADM-Vorlagendatei zur Konfiguration von View Agent (`vdm_agent.adm`) enthalten. Weitere Informationen finden Sie unter [USB-Einstellungen in der ADM-Vorlage für die View Agent-Konfiguration](#).

Standardmäßig deaktiviert View das automatische Splitten und schließt alle Audioausgabe-, Tastatur-, Maus- oder Smartcard-Komponenten eines USB-Verbundgeräts von der Umleitung aus.

View wendet die Richtlinieneinstellungen zum Gerätesplitten vor den Filterrichtlinieneinstellungen an. Wenn Sie das automatische Splitten aktiviert haben und nicht explizit verhindern, dass ein USB-Verbundgerät gesplittet wird, indem Sie die Anbieter- und die Produkt-IDs angeben, prüft View jede Schnittstelle des USB-Verbundgeräts, um zu entscheiden, welche Schnittstellen gemäß den Filterrichtlinieneinstellungen eingeschlossen oder ausgeschlossen werden sollten. Wenn Sie das automatische Gerätesplitten deaktiviert haben und nicht explizit die Anbieter- oder Produkt-ID eines USB-Verbundgeräts angeben, das Sie splitten möchten, wendet View die Filterrichtlinieneinstellungen auf das gesamte Gerät an.

Wenn Sie das automatische Splitten aktivieren, können Sie die Richtlinie `Vid/Pid-Gerät vom Splitten ausschließen` verwenden, um das Composite USB-Gerät anzugeben, bei dem Sie das Splitten verhindern möchten.

## Manuelles Gerätesplitten

Sie können die Richtlinie `Split Vid/Pid Device` (`Vid/Pid-Gerät splitten`) verwenden, um die Anbieter- und Produkt-ID eines Composite USB-Geräts anzugeben, das Sie splitten möchten. Sie können auch die Schnittstellen der Komponenten eines Composite USB-Geräts angeben, das Sie von der Umleitung ausschließen möchten. View wendet keine Richtlinieneinstellungen auf Komponenten an, die Sie auf diese Weise ausschließen.

**Wichtig** Wenn Sie die Richtlinie `Vid/Pid-Gerät splitten` verwenden, schließt View nicht automatisch die Komponenten ein, die Sie nicht explizit ausgeschlossen haben. Sie müssen eine Filterrichtlinie wie z. B. `Include Vid/Pid Device` (`Vid/Pid-Gerät einschließen`) angeben, um diese Komponenten einzuschließen.

**Tabelle 14-5. Modifizierer für Richtlinieneinstellungen für das Gerätesplitten auf View Agent** zeigt die Modifizierer, die angeben, wie Horizon Client mit einer View Agent-Richtlinie zum Gerätesplitten umgeht, wenn es eine äquivalente Richtlinieneinstellung für das Gerätesplitten für Horizon Client gibt. Diese Modifizierer gelten für alle Richtlinieneinstellungen zum Gerätesplitten.

**Tabelle 14-5. Modifizierer für Richtlinieneinstellungen für das Gerätesplitten auf View Agent**

| Modifizierer                  | Beschreibung   |
|-------------------------------|--|
| <b>m</b> (Zusammenführen)     | Horizon Client wendet die View Agent-Richtlinieneinstellung zum Gerätesplitten zusätzlich zur Horizon Client-Richtlinieneinstellung zum Gerätesplitten an. |
| <b>o</b> (Außer Kraft setzen) | Horizon Client wendet die View Agent-Richtlinieneinstellung zum Gerätesplitten anstatt der Horizon Client-Richtlinieneinstellung zum Gerätesplitten an.    |

**Tabelle 14-6. Beispiele für das Anwenden von Splittenmodifizierern auf die Richtlinieneinstellungen für das Gerätesplitten** zeigt Beispiele dafür, wie Horizon Client die Einstellungen für Gerät nach Anbieter-/Produkt-ID vom Splitten ausschließen verarbeitet, wenn Sie verschiedene Splittenmodifizierer angeben.

**Tabelle 14-6. Beispiele für das Anwenden von Splittenmodifizierern auf die Richtlinieneinstellungen für das Gerätesplitten**

| Gerät nach Anbieter-/Produkt-ID vom Splitten auf View Agent ausschließen | Gerät nach Anbieter-/Produkt-ID vom Splitten auf Horizon Client ausschließen | Gerät nach von Horizon Client verwendeter Anbieter-/Produkt-ID-Richtlinie effektiv vom Splitten ausschließen |
|--|--|--|
| m:vid-XXXX_pid-XXXX  | vid-YYYY_pid-YYYY  | vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY  |
| o:vid-XXXX_pid-XXXX  | vid-YYYY_pid-YYYY  | vid-XXXX_pid-XXXX  |
| m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY                                    | vid-YYYY_pid-YYYY  | vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY  |
| o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY                                    | vid-YYYY_pid-YYYY  | vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY  |

View Agent wendet die Richtlinieneinstellungen zum Splitten von Geräten auf seiner Seite der Verbindung nicht an.

Horizon Client prüft die Richtlinieneinstellungen zum Gerätesplitten in der folgenden Rangfolge.

- Exclude Vid/Pid Device From Split
- Split Vid/Pid Device

Eine Richtlinieneinstellung zum Splitten von Geräten, in der ein Gerät vom Splitten ausgeschlossen wird, hat Vorrang vor jeder Richtlinie, nach der es gesplittet werden dürfte. Wenn Sie Schnittstellen oder Geräte festlegen, die vom Splitten ausgeschlossen werden sollen, schließt Horizon Client die entsprechenden Komponentengeräte von der Verfügbarkeit für die Umleitung aus.

## Beispiele für das Festlegen von Richtlinien zum Splitten von USB-Geräten

Legen Sie Splittingrichtlinien für Desktops fest, um Geräte mit bestimmten Anbieter- und Produkt-IDs vom Umleiten nach dem automatischen Splitten auszuschließen, und geben Sie diese Richtlinien an Clientcomputer weiter:

- Legen Sie die Richtlinie Autom. Gerätesplitten zulassen auf Zulassen - Client-Einstellung außer Kraft setzen für View Agent fest.
- Legen Sie für View Agent die Richtlinie VidPid vom Splitten ausschließen auf **o:vid-xxx\_pid-yyyy** fest, wobei es sich bei xxx und yyyy um die entsprechenden IDs handelt.

Lassen Sie das automatische Gerätesplitten für Desktops zu und geben Sie Richtlinien für das Splitten von festgelegten Geräten auf Clientcomputern an.

- Legen Sie die Richtlinie Autom. Gerätesplitten zulassen auf Zulassen - Client-Einstellung außer Kraft setzen für View Agent fest.
- Legen Sie die Filterrichtlinie Vid/Pid-Gerät einschließen für das Client-Gerät fest, um das bestimmte Gerät einzuschließen, das Sie splitten möchten. Beispiel: **vid-0781\_pid-554c**.
- Legen Sie die Richtlinie Vid/Pid-Gerät splitten beispielsweise auf **vid-0781\_pid-554c(exintf:00;exintf:01)** fest, um ein bestimmtes USB-Verbundgerät zu splitten, sodass die Schnittstellen 00 und 01 von der Umleitung ausgeschlossen werden.

## Konfigurieren der Filterrichtlinieneinstellungen für USB-Geräte

Filterrichtlinieneinstellungen, die Sie für View Agent und Horizon Client konfigurieren können, legen fest, welche USB-Geräte von einem Clientcomputer zu einem Remote-Desktop umgeleitet werden können. Die USB-Gerätefilterung wird oft von Unternehmen verwendet, um die Verwendung von Massenspeichergeräten auf Remote-Desktops zu deaktivieren oder um die Weiterleitung eines bestimmten Gerätetyps wie eines USB-Ethernet-Adapters zu blockieren, der das Client-Gerät mit dem Remote-Desktop verbindet.

Wenn Sie eine Verbindung mit einem Desktop herstellen, lädt Horizon Client die View Agent-USB-Richtlinieneinstellungen herunter und verwendet diese in Verbindung mit den Horizon Client-USB-Richtlinieneinstellungen, um zu bestimmen, welche USB-Geräte Sie vom Clientcomputer umleiten dürfen.

View wendet jegliche Richtlinieneinstellungen zum Gerätesplitten an, bevor die Filterrichtlinieneinstellungen angewendet werden. Wenn Sie ein USB-Verbundgerät gesplittet haben, prüft View jede der Geräteschnittstellen, um zu entscheiden, welche gemäß den Filterrichtlinieneinstellungen ausgeschlossen oder eingeschlossen werden sollte. Wenn Sie kein USB-Verbundgerät gesplittet haben, wendet View die Filterrichtlinieneinstellungen auf das gesamte Gerät an.

Die Richtlinien zum Gerätesplitten sind in der ADM-Vorlagendatei zur Konfiguration von View Agent (`vdm_agent.adm`) enthalten. Weitere Informationen finden Sie unter [USB-Einstellungen in der ADM-Vorlage für die View Agent-Konfiguration](#).

## Interaktion der von Agent erzwungenen USB-Einstellungen

Die folgende Tabelle zeigt die Modifizierer an, die festlegen, wie Horizon Client mit einer View Agent-Filterrichtlinieneinstellung für eine Einstellung umgeht, die vom Agenten erzwungen werden kann, wenn eine äquivalente Filterrichtlinieneinstellung für Horizon Client vorhanden ist.

**Tabelle 14-7. Filtermodifizierer für vom Agenten erzwingbare Einstellungen**

| Modifizierer                  | Beschreibung  |
|-------------------------------|---|
| <b>m</b> (Zusammenführen)     | Horizon Client wendet die View Agent-Filterrichtlinieneinstellung zusätzlich zur Horizon Client-Filterrichtlinieneinstellung an. Im Falle der booleschen Einstellungen „true/false“ werden die Agent-Einstellungen verwendet, wenn die Client-Richtlinie nicht festgelegt wurde. Wenn die Client-Richtlinie festgelegt wurde, werden die Agent-Einstellungen mit Ausnahme der Einstellung <b>Alle Geräte ausschließen</b> ignoriert. Wenn die Richtlinie <b>Alle Geräte ausschließen</b> auf der Agenten-Seite festgelegt wird, überschreibt die Richtlinie die Client-Einstellung. |
| <b>o</b> (Außer Kraft setzen) | Horizon Client verwendet die View Agent-Filterrichtlinieneinstellung anstelle der Horizon Client-Filterrichtlinieneinstellung.  |

Beispiel: Die folgende Richtlinie auf der Agenten-Seite überschreibt alle Einbeziehungsregeln auf dem Client, und nur das Gerät VID-0911\_PID-149a enthält eine angewendete Einbeziehungsregel:

```
IncludeVidPid: o:VID-0911_PID-149a
```

Sie können auch Sternchen als Platzhalterzeichen verwenden wie beispielsweise:

```
o:vid-0911_pid-****
```

**Wichtig** Wenn Sie die Agenten-Seite ohne den Modifizierer **o** bzw. **m** konfigurieren, dann wird die Konfigurationsregel als ungültig betrachtet und ignoriert.

## Interaktion der vom Client interpretierten USB-Einstellungen

Die folgende Tabelle zeigt die Modifizierer an, die festlegen, wie Horizon Client mit einer View Agent-Filterrichtlinieneinstellung für eine Client-interpretierte Einstellung umgeht.

**Tabelle 14-8. Filtermodifizierer für Client-interpretierte Einstellungen**

| Modifizierer   | Beschreibung   |
|--|--|
| Default (Standardeinstellung) ( <b>d</b> in der Registrierungseinstellung) | Wenn keine Horizon Client-Filterrichtlinieneinstellung vorhanden ist, verwendet Horizon Client die View Agent-Filterrichtlinieneinstellung.<br>Wenn eine Horizon Client-Filterrichtlinieneinstellung vorhanden ist, wendet Horizon Client diese Richtlinieneinstellung an und ignoriert die View Agent-Filterrichtlinieneinstellung. |
| Override (Außer Kraft setzen) ( <b>o</b> in der Registrierungseinstellung) | Horizon Client verwendet die View Agent-Filterrichtlinieneinstellung anstelle einer äquivalenten Horizon Client-Filterrichtlinieneinstellung.  |

View Agent wendet die Filterrichtlinieneinstellungen für Client-interpretierte Einstellungen auf seiner Seite der Verbindung nicht an.

Die folgende Tabelle zeigt Beispiele dafür an, wie Horizon Client die Einstellungen für Smartcards zu lassen verarbeitet, wenn Sie verschiedene Filtermodifizierer verwenden.

**Tabelle 14-9. Beispiele für das Anwenden von Filtermodifizierern auf Client-interpretierte Einstellungen**

| Einstellung „Allow Smart Cards (Smart Cards zulassen)“ auf View Agent  | Einstellung „Smartcards zulassen“ auf Horizon Client | Effektive, von Horizon Client verwendete Richtlinieneinstellung zum Zulassen von Smartcards |
|--|--|---|
| Disable – Default Client Setting<br>(Deaktivieren – Standardeinstellung für Client)<br>( <b>d:false</b> in der Registrierungseinstellung)      | <b>true</b> (Zulassen)                               | <b>true</b> (Zulassen)  |
| Disable – Override Client Setting<br>(Deaktivieren – Client-Einstellung außer Kraft setzen) ( <b>o:false</b> in der Registrierungseinstellung) | <b>true</b> (Zulassen)                               | <b>false</b> (Deaktivieren)   |

Wenn Sie die Richtlinie Remote-Konfigurations-Download deaktivieren auf **true** setzen, ignoriert Horizon Client sämtliche Filterrichtlinieneinstellungen, die von View Agent eingehen.

View Agent wendet die Filterrichtlinieneinstellungen in durch den Agenten erzwingbaren Einstellungen auf seiner Seite der Verbindung immer an, selbst dann, wenn Sie Horizon Client so konfigurieren, dass eine andere Filterrichtlinieneinstellung verwendet werden soll oder Sie für Horizon Client festlegen, keine Filterrichtlinieneinstellungen von View Agent herunterzuladen. Horizon Client informiert nicht darüber, dass View Agent die Umleitung eines Geräts verhindert.

## Rangfolge von Einstellungen

Horizon Client evaluiert die Filterrichtlinieneinstellungen entsprechend einer Rangfolge. Eine Filterrichtlinieneinstellung, die verhindert, dass ein passendes Gerät umgeleitet wird, hat Vorrang vor der äquivalenten Filterrichtlinieneinstellung, die das Gerät einschließt. Wenn Horizon Client auf keine Filterrichtlinieneinstellung trifft, die ein Gerät ausschließt, lässt Horizon Client zu, dass es umgeleitet wird, es sei denn, Sie haben die Richtlinie Alle Geräte ausschließen auf **true** gesetzt. Wenn Sie jedoch auf View Agent eine Filterrichtlinieneinstellung zum Ausschließen des Geräts konfiguriert haben, blockiert der Desktop jeden Versuch, das Gerät auf ihn umzuleiten.

Horizon Client evaluiert die Filterrichtlinieneinstellungen in der Rangfolge, wobei die Horizon Client-Einstellungen und die View Agent-Einstellungen zusammen mit den Modifiziererwerten beachtet werden, die für die View Agent-Einstellungen gelten. Die folgende Liste zeigt die Rangfolge an, wobei Element 1 den höchsten Rang hat.

- 1 Exclude Path
- 2 Include Path
- 3 Exclude Vid/Pid Device
- 4 Include Vid/Pid Device
- 5 Exclude Device Family
- 6 Include Device Family

- 7 Allow Audio Input Devices (Audioeingabegeräte zulassen), Allow Audio Output Devices (Audioausgabegeräte zulassen), Allow HIDBootable (HIDBootable zulassen), Allow HID (Non Bootable and Not Mouse Keyboard) (HID zulassen (Nicht-Bootable und Nicht-Maus-Tastatur), Allow Keyboard and Mouse Devices (Tastatur- und Mausgeräte zulassen), Allow Smart Cards (Smart Cards zulassen) und Allow Video Devices (Videogeräte zulassen)
- 8 Kombinierte effektive Richtlinie zum Ausschließen aller Geräte (Exclude All Devices) evaluiert zum Ausschließen oder Einschließen aller USB-Geräte

Sie können die Filterrichtlinieneinstellungen Pfad ausschließen und Pfad einschließen nur für Horizon Client festlegen. Die Filterrichtlinien Allow (Zulassen), die sich auf separate Gerätefamilien beziehen, haben denselben Rang.

Wenn Sie eine Richtlinieneinstellung zum Ausschließen von Geräten konfigurieren, die auf Anbieter- oder Produkt-ID-Werten basiert, schließt Horizon Client ein Gerät aus, dessen Anbieter- oder Produkt-ID-Werte dieser Richtlinieneinstellung entsprechen, obwohl Sie möglicherweise eine Richtlinieneinstellung Zulassen für die Familie konfiguriert haben, zu der das Gerät gehört.

Die Rangfolge für Richtlinieneinstellungen löst Konflikte zwischen den Richtlinieneinstellungen. Wenn Sie Allow Smart Cards (Smart Cards zulassen) konfigurieren, um die Umleitung von Smart Cards zuzulassen, hat jede Ausschlussrichtlinie höheren Ranges Vorrang vor dieser Richtlinie. Möglicherweise haben Sie eine Richtlinieneinstellung Exclude Vid/Pid Device (Vid/Pid-Gerät ausschließen) konfiguriert, um Smart Card-Geräte mit übereinstimmenden Pfad-, Anbieter- oder Produkt-ID-Werten auszuschließen, oder vielleicht haben Sie eine Richtlinieneinstellung Exclude Device Family (Gerätefamilie ausschließen) konfiguriert, die die smart-card-Gerätefamilie insgesamt ausschließt.

Wenn Sie beliebige View Agent-Filterrichtlinieneinstellungen konfiguriert haben, evaluiert View Agent diese und erzwingt die Filterrichtlinieneinstellungen in der folgenden Rangfolge auf dem Remote-Desktop, wobei Element 1 den höchsten Rang hat.

- 1 Exclude Vid/Pid Device
- 2 Include Vid/Pid Device
- 3 Exclude Device Family
- 4 Include Device Family
- 5 Ein vom Agenten erzwungener Richtliniensatz Exclude All Devices (Alle Geräte ausschließen) , der alle USB-Geräte ein- oder ausschließt

View Agent erzwingt diesen begrenzten Satz Filterrichtlinieneinstellungen auf seiner Seite der Verbindung.

Durch das Definieren von Richtlinieneinstellungen für View Agent können Sie eine Filterrichtlinie für nicht verwaltete Clientcomputer erstellen. Die Funktion ermöglicht es Ihnen auch, die Umleitung von Geräten von Clientcomputern zu blockieren, selbst dann, wenn die Filterrichtlinieneinstellungen für Horizon Client die Umleitung zulassen.



Wenn Sie z. B. eine Richtlinie konfigurieren, die zulässt, dass Horizon Client ein Gerät umleiten lässt, blockiert View Agent das Gerät, wenn Sie eine Richtlinie für View Agent konfigurieren, nach der das Gerät ausgeschlossen werden soll.

## Beispiele für das Festlegen von Richtlinien zum Filtern von USB-Geräten

Die hier verwendeten Hersteller- und Produkt-IDs sind nur Beispiele. Weitere Informationen zum Festlegen der Hersteller- und Produkt-ID für ein bestimmtes Gerät finden Sie unter [Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs](#).

- Schließen Sie auf dem Client ein bestimmtes Gerät von der Umleitung aus:

```
Exclude Vid/Pid Device:    Vid-0341_Pid-1a11
```

- Blockieren Sie alle Speichergeräte von der Umleitung zu diesem Desktop-Pool. Verwenden Sie eine Einstellung der Agenten-Seite:

```
Exclude Device Family:    o:storage
```

- Blockieren Sie Audio- und Videogeräte für alle Benutzer in einem Desktop-Pool, um sicherzustellen, dass diese Geräte immer für die Echtzeit-Audio/Video-Funktion verfügbar sind. Verwenden Sie eine Einstellung der Agenten-Seite:

```
Exclude Device Family:    o:video;audio
```

Eine andere Strategie würde im Ausschließen bestimmter Geräte nach Hersteller- und Produkt-ID bestehen.

- Blockieren Sie auf dem Client alle Geräte von der Umleitung mit Ausnahme eines bestimmten Geräts:

```
Exclude All Devices:      true
Include Vid/Pid Device:    Vid-0123_Pid-abcd
```

- Schließen Sie alle Geräte aus, die von einem bestimmten Unternehmen hergestellt wurden, da diese Geräte zu Problemen für Ihre Endbenutzer führen können. Verwenden Sie eine Einstellung der Agenten-Seite:

```
Exclude Vid/Pid Device:    o:Vid-0341_Pid-*
```

- Schließen Sie auf dem Client zwei bestimmte Geräte ein, alle anderen Geräte jedoch aus:

```
Exclude All Devices:      true
Include Vid/Pid Device:    Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
```

## USB-Gerätefamilien

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

**Hinweis** Einige Geräte zeigen keine Gerätefamilie an.

**Tabelle 14-10. USB-Gerätefamilien**

| Gerätefamilienname | Beschreibung  |
|--------------------|---|
| audio              | Ein Audioeingabe- oder Audioausgabegerät beliebigen Typs.   |
| audio-in           | Audioeingabegeräte, z. B. Mikrofone.  |
| audio-out          | Audioausgabegeräte, z. B. Lautsprecher und Kopfhörer.   |
| bluetooth          | Per Bluetooth verbundene Geräte.  |
| comm               | Kommunikationsgeräte wie Modems und kabelgebundene Netzwerkadapter.                                       |
| hid                | Eingabegeräte (Human Interface Devices) außer Tastaturen und Zeigegeräten.                                |
| hid-bootable       | Eingabegeräte (Human Interface Devices), die beim Start verfügbar sind, außer Tastaturen und Zeigegeräte. |
| imaging            | Bildverarbeitungsgeräte, z. B. Scanner.   |
| keyboard           | Tastaturgerät.  |
| mouse              | Zeigegerät, z. B. eine Maus.  |
| other              | Familie nicht angegeben.  |
| pda                | PDA (Personal Digital Assistant)  |
| physical           | Force-Feedback-Geräte, z. B. Force-Feedback-Joysticks.  |
| printer            | Druckergeräte.  |
| security           | Sicherheitsgeräte, z. B. Fingerabdruckleser.  |
| smart-card         | SmartCard-Geräte.   |
| storage            | Massenspeichergeräte wie z. B. Flash-Laufwerke und externe Festplattenlaufwerke.                          |
| unknown            | Familie nicht bekannt.  |
| vendor             | Geräte mit herstellerspezifischen Funktionen.   |
| video              | Videoeingabegeräte.   |
| wireless           | Drahtlose Netzwerkadapter.  |
| wusb               | Drahtlose USB-Geräte.   |

## USB-Einstellungen in der ADM-Vorlage für die View Agent-Konfiguration

Sie können USB-Richtlinieneinstellungen sowohl für View Agent als auch für Horizon Client definieren. Nach dem Herstellen der Verbindung lädt Horizon Client die USB-Richtlinieneinstellungen von View Agent herunter und verwendet diese zusammen mit den Horizon Client-USB-Richtlinieneinstellungen, um zu entscheiden, welche Geräte vom Clientcomputer umgeleitet werden dürfen.

Die ADM-Vorlagendatei (`vdm_agent.adm`) für die View Agent-Konfiguration enthält Richtlinieneinstellungen in Bezug auf die Authentifizierung und die Umgebungskomponenten von View Agent, einschließlich der USB-Umleitung. Die Einstellungen gelten auf Computerebene. View Agent liest die Einstellungen vorzugsweise aus dem GPO auf der Computerebene, andernfalls aus der Registrierung unter `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB`.

## Einstellung für die Konfiguration der USB-Geräteaufschlüsselung

Die folgende Tabelle beschreibt jede Richtlinieneinstellung zum Splitten von USB-Verbundgeräten in der ADM-Vorlagendatei für die View Agent-Konfiguration. View Agent erzwingt diese Einstellungen nicht. View Agent übergibt die Einstellungen an Horizon Client zwecks Interpretation und Erzwingung in Abhängigkeit davon, ob Sie den Modifizierer zum Zusammenführen (`m`) oder Außerkraftsetzen (`o`) angeben. Horizon Client verwendet die Einstellungen, um zu entscheiden, ob USB-Verbundgeräte in ihre Komponentengeräte gesplittet und die Komponentengeräte von der Verfügbarkeit für die Umleitung ausgeschlossen werden sollen. Eine Beschreibung dazu, wie View die Richtlinien für das Splitten von Composite USB-Geräten anwendet, finden Sie unter [Konfigurieren der Gerätesplittingsrichtlinieneinstellungen für Composite USB-Geräte](#).

**Tabelle 14-11. View Agent-Konfigurationsvorlage: Einstellungen zum Splitten von Geräten**

| Einstellung   | Eigenschaften  |
|---|--|
| Allow Auto Device Splitting<br>Eigenschaft: <code>AllowAutoDeviceSplitting</code> | Lässt das automatische Splitten von Composite USB-Geräten zu.<br>Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.   |
| Exclude Vid/Pid Device From Split<br>Eigenschaft: <code>SplitExcludeVidPid</code> | Schließt ein Composite USB-Gerät vom Splitten aus, das durch Anbieter- und Produkt-IDs angegeben ist. Das Format des Splittens ist <code>{m o}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</code><br>Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden.<br>Beispiel: <b><code>o:vid-0781_pid-55**</code></b><br>Der Standardwert ist nicht definiert.  |
| Split Vid/Pid Device<br>Eigenschaft: <code>SplitVidPid</code>                     | Behandelt die Komponenten eines Composite USB-Gerätes, die durch Anbieter- und Produkt-IDs angegeben sind, als separate Geräte. Das Format der Einstellung ist <code>{m o}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])</code> oder <code>{m o}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])</code><br>Sie können das Stichwort <code>exintf</code> verwenden, um Komponenten durch Angabe ihrer Schnittstellennummer von der Umleitung auszuschließen. Sie müssen hexadezimale ID-Nummern und dezimale Schnittstellennummern einschließlich der 0 am Anfang angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden.<br>Beispiel: <b><code>o:vid-0781_pid-554c(exintf:01;exintf:02)</code></b><br><br><b>Hinweis</b> View schließt nicht automatisch die Komponenten ein, die Sie nicht explizit ausgeschlossen haben. Sie müssen eine Filterrichtlinie wie z. B. <code>Include Vid/Pid Device</code> ( <code>Vid/Pid-Gerät</code> einschließen) angeben, um diese Komponenten einzuschließen.<br><br>Der Standardwert ist nicht definiert. |

## Von View Agent erzwungene USB-Einstellungen

Die folgende Tabelle beschreibt alle von Agent erzwungenen Richtlinieneinstellungen für USB in der ADM-Vorlagendatei für die View Agent-Konfiguration. View Agent verwendet die Einstellungen, um zu entscheiden, ob ein USB-Gerät zur Host-Maschine umgeleitet werden kann. View Agent übergibt die Einstellungen an Horizon Client zwecks Interpretation und Erzwingung in Abhängigkeit davon, ob Sie den Modifizierer zum Zusammenführen (m) oder Außerkraftsetzen (o) angeben. Horizon Client verwendet die Einstellungen, um zu entscheiden, ob ein USB-Gerät für die Umleitung verfügbar ist. Da View Agent immer eine von Agent erzwungene Richtlinieneinstellung erzwingt, die Sie angeben, könnte die Konsequenz sein, dass Sie der Richtlinie entgegensteuern, die Sie für Horizon Client festgelegt haben. Eine Beschreibung dazu, wie View die Richtlinien für das Filtern von Composite USB-Geräten anwendet, finden Sie unter [Konfigurieren der Filterrichtlinieneinstellungen für USB-Geräte](#).

**Tabelle 14-12. View Agent-Konfigurationsvorlage: Von Agent erzwungene Einstellungen**

| Einstellung   | Eigenschaften   |
|---|---|
| Exclude All Devices<br>Eigenschaft: ExcludeAllDevices | <p>Schließt alle USB-Geräte von der Umleitung aus. Wenn für diese Einstellung <b>true</b> festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zuzulassen, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden. Wenn für diese Einstellung <b>false</b> festgelegt ist, können Sie andere Richtlinieneinstellungen verwenden, um zu verhindern, dass bestimmte Geräte oder Gerätefamilien umgeleitet werden.</p> <p>Wenn diese Einstellung auf <b>true</b> festgelegt ist und an Horizon Client übergeben wird, setzt diese Einstellung immer die Einstellung auf Horizon Client außer Kraft. Sie können die Modifizierer für das Zusammenführen (m) oder Außerkraftsetzen (o) mit dieser Einstellung nicht verwenden.</p> <p>Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.</p> |
| Exclude Device Family<br>Eigenschaft: ExcludeFamily   | <p>Schließt Gerätefamilien von der Umleitung aus. Das Format der Einstellung ist {m o}:<i>Familienname_1</i>[;<i>Familienname_2</i>]...</p> <p>Beispiel: <b>o:bluetooth;smart-card</b></p> <p>Wenn Sie das automatische Gerätesplitten aktiviert haben, prüft View die Gerätefamilie jeder Schnittstelle eines Composite USB-Gerätes, um zu entscheiden, welche Schnittstelle ausgeschlossen werden sollte. Wenn Sie das automatische Gerätesplitten deaktiviert haben, prüft View die Gerätefamilie des gesamten Composite USB-Gerätes.</p> <p>Der Standardwert ist nicht definiert.</p>   |
| Exclude Vid/Pid Device<br>Eigenschaft: ExcludeVidPid  | <p>Schließt Geräte mit einer angegebenen Anbieter- oder Produkt-ID von der Umleitung aus. Das Format des Splittens ist {m o}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</p> <p>Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden.</p> <p>Beispiel: <b>m:vid-0781_pid-****;vid-0561_pid-554c</b></p> <p>Der Standardwert ist nicht definiert.</p>   |

| Einstellung  | Eigenschaften   |
|--|---|
| Include Device Family<br>Eigenschaft: IncludeFamily  | Bestimmt Gerätefamilien, die umgeleitet werden können. Das Format der Einstellung ist {m o}: <i>Familienname_1</i> [: <i>Familienname_2</i> ]...<br>Beispiel: <b>m:storage</b><br>Der Standardwert ist nicht definiert.   |
| Include Vid/Pid Device<br>Eigenschaft: IncludeVidPid | Bestimmt Geräte mit einer angegebenen Anbieter- und Produkt-ID, die umgeleitet werden können. Das Format des Splittens ist {m o}:vid-xxx1_pid-yyy2[:vid-xxx2_pid-yyy2]...<br>Sie müssen hexadezimale ID-Nummern angeben. Sie können das Platzhalterzeichen (*) anstelle einzelner Ziffern in einer ID verwenden.<br>Beispiel: <b>o:vid-0561_pid-554c</b><br>Der Standardwert ist nicht definiert. |

## Von Client interpretierte USB-Einstellungen

Die folgende Tabelle beschreibt alle in der ADM-Vorlagendatei für die View Agent-Konfiguration enthaltenen von Client interpretierten Richtlinieneinstellungen. View Agent erzwingt diese Einstellungen nicht. View Agent übergibt diese Einstellungen an Horizon Client zur Interpretation und Erzwingung. Horizon Client verwendet die Einstellungen, um zu entscheiden, ob ein USB-Gerät für die Umleitung verfügbar ist.

**Tabelle 14-13. View Agent-Konfigurationsvorlage: Von Client interpretierte Einstellungen**

| Einstellung   | Eigenschaften  |
|---|--|
| Allow Audio Input Devices<br>Eigenschaft: AllowAudioIn              | Lässt zu, dass Audioeingabegeräte umgeleitet werden.<br>Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>true</b> ist.   |
| Allow Audio Output Devices<br>Eigenschaft: AllowAudioOut            | Lässt zu, dass Audioausgabegeräte umgeleitet werden.<br>Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.  |
| Allow HIDBootable<br>Eigenschaft: AllowHIDBootable                  | Lässt zu, dass Eingabegeräte außer Tastaturen und Mäuse, die zur Startzeit verfügbar sind (auch als HID-startfähige Geräte bekannt) umgeleitet werden.<br>Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>true</b> ist. |
| Allow Other Input Devices   | Lässt zu, dass Eingabegeräte außer HID-startfähigen Geräten oder Tastaturen mit integrierten Zeigegeräten umgeleitet werden.<br>Der Standardwert ist nicht definiert.  |
| Allow Keyboard and Mouse Devices<br>Eigenschaft: AllowKeyboardMouse | Lässt zu, dass Tastaturen mit eingebauten Zeigegeräten (Maus, Trackball oder Touchpad) umgeleitet werden.<br>Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.   |
| Allow Smart Cards<br>Eigenschaft: AllowSmartcard                    | Lässt zu, dass SmartCard-Geräte umgeleitet werden.<br>Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>false</b> ist.  |
| Allow Video Devices<br>Eigenschaft: AllowVideo                      | Lässt zu, dass Videogeräte umgeleitet werden.<br>Der Standardwert ist nicht definiert, was gleichbedeutend mit <b>true</b> ist.  |

## Fehlerbehebung bei Problemen mit der USB-Umleitung

Bei der USB-Umleitung in Horizon Client können verschiedene Probleme auftreten.

## Problem

Bei der USB-Umleitung in Horizon Client werden lokale Geräte nicht auf dem Remote-Desktop verfügbar gemacht oder einige Geräte werden für die Umleitung in Horizon Client nicht als verfügbar angezeigt.

## Ursache

Im Folgenden sind mögliche Ursachen aufgeführt, aufgrund derer die USB-Umleitung nicht ordnungsgemäß oder wie erwartet ausgeführt werden kann.

- Das Gerät ist ein Verbund-USB-Gerät und eines der enthaltenen Geräte wird standardmäßig gesperrt. Beispielsweise wird ein Diktiergerät mit einer Maus standardmäßig gesperrt, da Mauszeigergeräte standardmäßig gesperrt werden. Informationen zum Umgehen dieses Problems finden Sie unter [Konfigurieren der Gerätesplittingsrichtlinieneinstellungen für Composite USB-Geräte](#).
- Die USB-Umleitung wird für Windows 2008-Systeme oder für sitzungsbasierte Remote-Desktops mit RDS-Host nicht unterstützt.
- Die Umleitung wird für Webcams nicht unterstützt.
- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz.
- Die USB-Umleitung wird für Startgeräte nicht unterstützt. Wenn Sie Horizon Client auf einem Windows-System ausführen, das von einem USB-Gerät startet, und Sie dieses Gerät auf den Remote-Desktop umleiten, reagiert das lokale Betriebssystem möglicherweise nicht oder kann nicht verwendet werden. Siehe <http://kb.vmware.com/kb/1021409>.
- Standardmäßig ermöglicht Ihnen Horizon Client für Windows nicht, Taste, Maus, Smartcard und Audio-Ausgangsgeräte zur Umleitung auszuwählen. Siehe <http://kb.vmware.com/kb/1011600>.
- RDP bietet keine Unterstützung für die Umleitung von USB-Eingabegeräten für die Konsolensitzung oder für Smartcard-Leser. Siehe <http://kb.vmware.com/kb/1011600>.
- Windows Mobile-Gerätecenter kann die Umleitung von USB-Geräten für RDP-Sitzungen verhindern. Siehe <http://kb.vmware.com/kb/1019205>.
- Für einige USB-Eingabegeräte müssen Sie die virtuelle Maschine so konfigurieren, dass die Position des Mauszeigers aktualisiert wird. Siehe <http://kb.vmware.com/kb/1022076>.
- Einige Audiogeräte erfordern möglicherweise Änderungen an Richtlinieneinstellungen oder Registrierungseinstellungen. Siehe <http://kb.vmware.com/kb/1023868>.
- Netzwerklatenz kann zu einer langsamen Geräteinteraktion führen. Zudem ist es möglich, dass Anwendungen nicht zu reagieren scheinen, da sie für die Interaktion mit lokalen Geräten konzipiert sind. Bei USB-Festplattenlaufwerken mit sehr hoher Kapazität kann es einige Minuten dauern, bis diese im Windows Explorer angezeigt werden.
- USB-Flashkarten, die mit dem FAT32-Dateisystem formatiert sind, werden langsam geladen. Siehe <http://kb.vmware.com/kb/1022836>.
- Ein Prozess oder Dienst auf dem lokalen System hat das Gerät geöffnet, bevor Sie sich mit dem Remote-Desktop verbunden haben.

- Ein umgeleitetes USB-Gerät arbeitet nicht mehr, wenn Sie eine Desktop-Sitzung wiederherstellen – selbst wenn der Desktop anzeigt, dass das Gerät verfügbar ist.
- Die USB-Umleitung ist in View Administrator deaktiviert.
- Fehlende oder deaktivierte Treiber für die USB-Umleitung auf dem Gast.

### Lösung

- ◆ Verwenden Sie, wenn möglich, PCoIP anstelle von RDP als Desktop-Protokoll.
- ◆ Wenn ein umgeleitetes Gerät weiterhin nicht verfügbar ist oder nach einer vorübergehenden Verbindungstrennung nicht mehr arbeitet, entfernen Sie das Gerät, schließen Sie es wieder an, und führen Sie erneut eine Umleitung durch.
- ◆ Wechseln Sie in View Administrator zu **Richtlinien > Globale Richtlinien** und prüfen Sie, ob USB-Zugriff unter „View-Richtlinien“ auf **Zulassen** gesetzt ist.
- ◆ Überprüfen Sie das Protokoll auf dem Gast auf Einträge der Klasse `ws_vhub` und das Protokoll auf dem Client auf Einträge der Klasse `vmware-view-usbd`.

Einträge dieser Klassen werden in die Protokolle geschrieben, wenn es sich bei einem Benutzer nicht um einen Administrator handelt oder wenn die Treiber für die USB-Umleitung nicht installiert sind oder nicht ordnungsgemäß funktionieren. Informationen zum Speicherort dieser Protokolldateien finden Sie unter [Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs](#).

- ◆ Öffnen Sie auf dem Gast den Geräte-Manager, erweitern Sie die USB-Controller und installieren Sie die Treiber VMware View Virtual USB Host Controller und VMware View Virtual USB Hub erneut, wenn diese Treiber nicht vorhanden sind, bzw. aktivieren Sie die Treiber, wenn diese deaktiviert sind.

# Reduzieren und Verwalten von Speichieranforderungen

# 15

Das Bereitstellen von Desktops auf virtuellen Maschinen, die von vCenter Server verwaltet werden, bietet sämtliche Speichervorteile, die zuvor nur für virtuelle Server möglich waren. Durch Verwenden von View Composer wird die Speichernutzung optimiert, da alle virtuelle Maschinen in einem Pool eine virtuelle Festplatte mit einem Basis-Image gemeinsam nutzen.

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten des Speichers mit vSphere](#)
- [Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung](#)
- [Reduzieren von Speichieranforderungen mit View Composer](#)
- [Speichergrößen für Linked-Clone-Desktop-Pools](#)
- [Speichermehrfachvergabe für virtuellen Linked-Clone-Computer](#)
- [Datenfestplatten von verknüpften Klonen](#)
- [Speichern von verknüpften Klonen auf lokalen Datenspeichern](#)
- [Speichern von View Composer-Replikaten und verknüpften Klonen in separaten Datenspeichern](#)
- [Konfigurieren der View-Speicherbeschleunigung für Desktop-Pools](#)
- [Rückgewinnung von Festplattenspeicherplatz auf virtuellen Linked-Clone-Maschinen](#)
- [Verwenden der View Composer Array Integration mit systemeigener NFS-Snapshot-Technologie \(VAAI\)](#)
- [Festlegen von Ausfallzeiten für ESXi-Vorgänge auf View-VMs](#)

## Verwalten des Speichers mit vSphere

vSphere ermöglicht eine Virtualisierung von Festplattenlaufwerken und Dateisystemen, sodass Sie den Speicher verwalten und konfigurieren können, ohne berücksichtigen zu müssen, wo die Daten physisch gespeichert sind.



Fibre Channel SAN-, iSCSI SAN- und NAS-Arrays sind weit verbreitete Speichertechnologien, die von vSphere zur Erfüllung verschiedener Speicheranforderungen von Rechenzentren unterstützt werden. Die Speicher-Arrays werden mithilfe von Speichernetzwerken (SANs) mit Gruppen von Servern verbunden, die diese dann gemeinsam nutzen. Diese Vorgehensweise erlaubt die Zusammenführung von Speicherressourcen und bietet mehr Flexibilität bei ihrer Bereitstellung für virtuelle Maschinen.

## Kompatible Funktionen von vSphere 4.1 oder höher

Mit vSphere 4.1 oder höher können Sie nun auch folgende Funktionen verwenden:

- vStorage-Thin Provisioning – ermöglicht Ihnen, mit so wenig Festplattenspeicher wie nötig zu beginnen und die Festplatte später nach Bedarf zu vergrößern
- Mehrstufiger Speicher – ermöglicht Ihnen die Verteilung virtueller Festplatten in der View-Umgebung über Hochleistungsspeicher und kostengünstigere Speicherschichten, um die Leistung zu optimieren und Kosten zu senken
- Lokaler Speicher auf dem ESXi-Server für die Auslagerungsdateien der virtuellen Maschine auf dem Gastbetriebssystem

## Kompatible Funktionen von vSphere 5.0 oder 5.1 oder höher

Mit vSphere 5.0 oder einer neueren Version können Sie nun folgende Funktionen verwenden:

- Mit der View-Speicherbeschleunigungsfunktion können Sie ESXi-Hosts so konfigurieren, dass dort Festplattendaten von virtuellen Maschinen in einem Cache-Speicher zwischengespeichert werden.  
  
Mithilfe dieses inhaltsbasierten Lese-Cache-Speichers (CBRC) kann der IOPS-Wert reduziert und die Systemleistung bei sogenannten Boot Storms verbessert werden, wenn viele Maschinen gestartet werden und gleichzeitig Antivirus-Scans durchführen. Statt das gesamte Betriebssystem wieder und wieder aus dem Speichersystem zu lesen, kann ein Host gemeinsame Datenblöcke aus dem Cache lesen.
- Wenn Remote-Desktops das mit vSphere 5.1 und höher verfügbare platzsparende Diskformat nutzen, wird der Speicherplatz veralteter oder gelöschter Daten innerhalb eines Gastbetriebssystems mit einem Bereinigungs- oder Verkleinerungsprozess automatisch zurückgewonnen.
- Sie können einen Desktop-Pool auf einem Cluster bereitstellen, der bis zu 32 ESXi-Hosts umfasst, müssen dabei jedoch einige Einschränkungen beachten.

Replikatfestplatten müssen in VMFS5-Datenspeichern (oder einer höheren VMFS-Version) bzw. in NFS-Datenspeichern gespeichert werden. Wenn Sie Replikate in einem Datenspeicher einer früheren VMFS-Version als VMFS5 speichern, kann ein Cluster über maximal acht Hosts verfügen. Betriebssystemfestplatten und persistente Festplatten können in NFS- oder VMFS-Datenspeichern gespeichert werden.

## Kompatible Funktionen von vSphere 5.5 Update 1 oder höher

Mit vSphere 5.5 Update 1 oder einer neueren Version können Sie Virtual SAN verwenden, um die lokalen physischen Solid-State-Disks und Festplattenlaufwerke, die auf ESXi-Hosts vorhanden sind, in einen von allen Hosts in einem Cluster gemeinsam genutzten Datenspeicher zu virtualisieren. Virtual SAN bietet Hochleistungsspeicher mit richtlinienbasierter Verwaltung, sodass Sie bei der Erstellung eines Desktop-Pools nur einen Datenspeicher angeben. Die unterschiedlichen Komponenten wie Dateien virtueller Maschinen, Replikate, Benutzerdaten und Betriebssystemdateien werden auf den geeigneten Solid-State-Drive-Festplatten (SSD) oder direkt angeschlossene Festplatten (HDD) platziert.

Mithilfe von Virtual SAN können Sie auch den Speicher und die Leistung von virtuellen Maschinen verwalten, indem Sie Profile mit Speicherrichtlinien verwenden. Wenn die Richtlinie wegen eines Host-, Festplatten- oder Netzwerkfehlers oder wegen Änderungen der Arbeitslast nicht mehr eingehalten wird, konfiguriert Virtual SAN die Daten der betroffenen virtuellen Maschinen neu und optimiert die Nutzung der Ressourcen im ganzen Cluster. Sie können einen Desktop-Pool auf einem Cluster bereitstellen, der bis zu 32 ESXi-Hosts enthält.

---

**Hinweis** Virtual SAN ist mit der View-Speicherbeschleunigungsfunktion, aber nicht mit der Funktion platzsparendes Diskformat kompatibel, das Speicherplatz durch Bereinigung und Verkleinerung von Festplatten zurückgewinnt.

---

## Verwenden von Virtual SAN für Hochleistungsspeicher und richtlinienbasierte Verwaltung

VMware Virtual SAN ist eine softwaredefinierte Speicherebene im Lieferumfang von vSphere 5.5 Update 1 oder einer neueren Version, die die in einem Cluster von vSphere-Hosts verfügbaren lokalen physischen Speicherfestplatten virtualisiert. Sie geben bei der Erstellung eines Desktop-Pools nur einen Datenspeicher an. Die unterschiedlichen Komponenten wie Dateien virtueller Maschinen, Replikate, Benutzerdaten und Betriebssystemdateien werden auf den geeigneten Solid-State-Drive-Festplatten (SSD) oder direkt angeschlossene Festplatten (HDD) platziert.

Virtual SAN implementiert einen richtlinienbasierten Ansatz zur Speicherverwaltung. Wenn Sie Virtual SAN verwenden, definiert View die Speicheranforderungen für virtuelle Maschinen (wie Kapazität, Leistung und Verfügbarkeit) in Form von Standardprofilen mit Speicherrichtlinien, die Sie ändern können. Der Speicher wird gemäß den zugewiesenen Richtlinien bereitgestellt und automatisch konfiguriert. Sie können Virtual SAN für Linked-Clone-Desktop-Tools oder Full-Clone-Desktop-Pools verwenden.

Jede virtuelle Maschine pflegt ihre Richtlinie unabhängig von ihrer physischen Position im Cluster. Wenn die Richtlinie aufgrund eines Host-, Festplatten- oder Netzwerkfehlers oder von Arbeitsauslastungsänderungen nicht mehr konform ist, konfiguriert Virtual SAN die Daten der betroffenen virtuellen Maschinen und Lastausgleiche neu, um die Richtlinien der einzelnen virtuellen Maschinen zu erfüllen.

Virtual SAN unterstützt VMware-Funktionen wie HA, vMotion und DRS, die gemeinsamen Speicher voraussetzen, macht jedoch eine externe gemeinsame Speicherinfrastruktur überflüssig und vereinfacht die Speicherkonfiguration und die Bereitstellung virtueller Maschinen.

## Virtual SAN-Workflow in View

- 1 Verwenden Sie vCenter Server 5.5 Update 1 oder eine neuere Version zur Aktivierung von Virtual SAN. Weitere Informationen finden Sie im Dokument *vSphere Storage*.
- 2 Wenn Sie einen Desktop-Pool in View Administrator erstellen, wählen Sie unter **Speicherrichtlinienverwaltung** die Option **vSphere Virtual SAN verwenden** und dann den zu verwendenden Virtual SAN-Datenspeicher aus.

Nachdem Sie **vSphere Virtual SAN verwenden** ausgewählt haben, werden nur Virtual SAN-Datenspeicher angezeigt.

Standardmäßige Speicherrichtlinienprofile werden gemäß den von Ihnen gewählten Optionen erstellt. Wenn Sie beispielsweise eine Linked-Clone- und dynamischen Desktop-Pool erstellen, werden automatisch ein Replikatfestplattenprofil und ein Betriebssystemfestplattenprofil erstellt. Wenn Sie einen Linked-Clone- und dauerhaften Desktop-Pool erstellen, werden ein Replikatfestplattenprofil und ein dauerhaftes Festplattenprofil erstellt. Für alle Desktop-Pools wird ein Profil für Dateien von virtuellen Maschinen erstellt.

- 3 Um vorhandene View Composer-Desktop-Pools von einem anderen Datentyp zu einem Virtual SAN-Datenspeicher zu verschieben, bearbeiten Sie in View Administrator den Pool, um die Auswahl des alten Datenspeichers aufzuheben und stattdessen den Virtual SAN-Datenspeicher auszuwählen, und verwenden Sie den Befehl zur Gleichgewichtswiederherstellung.
- 4 (Optional) Verwenden Sie vCenter Server, um die Parameter der Speicherrichtlinienprofile zu ändern, zu denen z. B. die Anzahl der zu tolerierenden Fehler und die Größe des zu reservierenden SSD-Lesecaches gehören.

Die Namen der Richtlinien lauten OS\_DISK (für Betriebssystemdateien), PERSISTENT\_DISK (für Benutzerdatendateien), REPLICA\_DISK (für Replikate) und VM\_HOME (für Dateien virtueller Maschinen wie .vmx- und .vmsn-Dateien). Änderungen an der Richtlinie werden an neu erstellte virtuelle Maschinen und alle vorhandenen virtuellen Maschinen im Desktop-Pool verteilt.

- 5 Verwenden Sie vCenter Server, um den Virtual SAN-Cluster und die am Datenspeicher beteiligten Festplatten zu überwachen. Weitere Informationen finden Sie im Dokument *vSphere Storage* und im Handbuch *Überwachung und Leistung von vSphere*.
- 6 (Optional) Für Linked-Clone-Desktop-Pools von View Composer verwenden Sie den Aktualisierungs- und den Neuzusammenstellungsbefehl wie gewohnt.

## Anforderungen und Einschränkungen

Die Virtual SAN-Funktion hat bei Verwendung in einer View-Bereitstellung folgende Einschränkungen:

- Diese Version unterstützt die Verwendung der platzsparenden Diskformatfunktion von View nicht, die Speicherplatz durch Bereinigung und Verkleinerung von Festplatten zurückgewinnt.

- Virtual SAN unterstützt die VAAI-Funktion (View Composer Array Integration) nicht, da Virtual SAN keine NAS-Geräte verwendet.

---

**Hinweis** Virtual SAN ist mit der Funktion „View-Speicherbeschleunigung“ kompatibel. Virtual SAN bietet eine Cachingschicht auf SSD-Festplatten, und die Funktion „View-Speicherbeschleunigung“ bietet einen inhaltsbasierten Cache, der E/A-Vorgänge pro Sekunde reduziert und die Leistung bei Startüberlastungen erhöht.

---

Die Virtual SAN-Funktion hat folgende Anforderungen:

- vSphere 5.5 Update 1 oder eine neuere Version.
- Geeignete Hardware. Beispiel: VMware empfiehlt eine 10-GB-Netzwerkkarte und mindestens eine SSD-Festplatte und eine direkt angeschlossene Festplatte für jeden kapazitätsbeitragenden Knoten. Siehe im [VMware-Kompatibilitätshandbuch](#).
- Ein aus mindestens drei ESXi-Hosts bestehender Cluster. Sie benötigen eine ausreichende Anzahl von ESXi-Hosts für Ihr Setup. Weitere Informationen finden Sie im Dokument *Maximalwerte für die Konfiguration von VMware vSphere* unter <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html>.
- SSD-Kapazität, die mindestens 10 % der Festplattenkapazität beträgt.
- Eine ausreichende Anzahl von Festplatten für Ihr Setup. Überschreiten Sie eine 75-prozentige Auslastung auf einer Magnetfestplatte nicht.

Weitere Informationen zu Virtual SAN-Anforderungen finden Sie unter „Arbeiten mit Virtual SAN“ im Dokument *vSphere Storage*. Informationen zur Größenanpassung und zur Gestaltung der Schlüsselkomponenten von virtuellen View-Desktop-Infrastrukturen für VMware Virtual SAN finden Sie im White Paper unter <http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>.

## Standardmäßige Speicherrichtlinienprofile für Virtual SAN-Datenspeicher

Wenn Sie Virtual SAN verwenden, definiert View die Speicheranforderungen für virtuelle Maschinen (wie Kapazität, Leistung und Verfügbarkeit) in Form von Standardprofilen mit Speicherrichtlinien, die Sie ändern können. Der Speicher wird gemäß den zugewiesenen Richtlinien bereitgestellt und automatisch konfiguriert.

Die Standardrichtlinien, die während der Erstellung des Desktop-Pools erstellt werden, hängen vom Typ des von Ihnen erstellten Pools ab. Die Namen der Richtlinien lauten OS\_DISK (für Betriebssystemdateien), PERSISTENT\_DISK (für Benutzerdatendateien), REPLICA\_DISK (für Replikate) und VM\_HOME (für Dateien virtueller Maschinen wie .vmx- und .vmsn-Dateien). Beispiel: Eine REPLICA\_DISK-Richtlinie wird nur für Linked-Clone-Pools erstellt. Änderungen an der Richtlinie werden an neu erstellte virtuelle Maschinen und alle vorhandenen virtuellen Maschinen im Desktop-Pool verteilt.

Virtual SAN bietet ein Speicherrichtlinien-Framework an, sodass Sie das Verhalten verschiedener virtueller Maschinen-Objekte steuern können, die sich auf dem Virtual SAN-Datenspeicher befinden. Ein Beispiel eines Objekts in Virtual SAN stellt eine virtuelle Festplattendatei (VMDK-Datei) dar. Es gibt vier Merkmale eines jeden Objekts, die über die Richtlinie gesteuert werden:

- **Stripes:** Anzahl von Daten-Stripes. Die Anzahl von Festplatten-Stripes wirkt sich darauf aus, über wie viele Magnetfestplatten (HDDs) Sie verfügen.
- **Resilienz:** Anzahl der zu tolerierenden Ausfälle. Die Anzahl der zu tolerierenden Hostausfälle hängt selbstverständlich von der Anzahl der Hosts ab, über die Sie verfügen.
- **Speicher-Bereitstellung:** Thick oder Thin.
- **Cache-Reservierung:** Lesecache-Reservierung.

Die Reservierungseinstellungen für Stripes und Cache werden für die Leistungssteuerung verwendet. Die Resilienz-Einstellung steuert die Verfügbarkeit. Die Speicher-Bereitstellungseinstellungen steuern die Kapazität. Wenn sie zusammen vorgenommen werden, wirken sich diese Einstellungen darauf aus, wie viele vSphere-Hosts und Magnetfestplatten erforderlich sind.

Beispiel: Wenn Sie die Anzahl der Festplatten-Stripes pro Objekt auf 2 festlegen, entfernt Virtual SAN das Objekt auf mindestens 2 HDDs. Wenn Sie die Anzahl der zu tolerierenden Hostausfälle auf 1 festlegen, erstellt Virtual SAN in Kombination mit dieser Einstellung eine zusätzliche Kopie für die Resilienz. Aus diesem Grund sind 4 HDDs erforderlich. Zudem sind für das Festlegen der Anzahl der zu tolerierenden Hostausfälle auf 1 mindestens 3 ESXi-Hosts erforderlich, wovon zwei für die Resilienz und eins für das Trennen der Verbindung im Falle einer Partitionierung verwendet werden.

---

**Hinweis** Falls Sie unabsichtlich versuchen, widersprüchliche Einstellungen anzuwenden, schlägt der Vorgang fehl und eine Fehlermeldung informiert Sie darüber, dass Sie nicht über ausreichende Hosts verfügen.

---

Es sind keine Anforderungen an Benutzeraktionen vorhanden, die mit diesen Standardrichtlinien verknüpft sind. Die Richtlinien werden sowohl für Linked-Clone-Desktop-Pools als auch für Full-Clone-Desktop-Pools erstellt.

Sie können entweder die vSphere-Befehlszeilenschnittstelle (`esxcli`) oder den vSphere Web Client verwenden, um die standardmäßigen Speicherrichtlinienprofile zu ändern. Jede virtuelle Maschine pflegt ihre Richtlinie unabhängig von ihrer physischen Position im Cluster. Wenn die Richtlinie aufgrund eines Host-, Festplatten- oder Netzwerkfehlers oder von Arbeitsauslastungsänderungen nicht mehr konform ist, konfiguriert Virtual SAN die Daten der betroffenen virtuellen Maschinen und Lastausgleiche neu, um die Richtlinien der einzelnen virtuellen Maschinen zu erfüllen.

## Reduzieren von Speicheranforderungen mit View Composer

Da View Composer Desktop-Images erstellt, die virtuelle Festplatten mit einem Basis-Image gemeinsam nutzen, kann die erforderliche Speicherkapazität um 50-90 % reduziert werden.

View Composer arbeitet mit einem Basis-Image (bzw. einer übergeordneten virtuellen Maschine) und erstellt einen Pool mit bis zu 2,000 virtuellen Maschinen auf Basis verknüpfter Klone. Jeder verknüpfte Klon fungiert als unabhängiger Desktop (mit eindeutigem/r Hostnamen/IP-Adresse), aber dennoch benötigt der verknüpfte Klon wesentlich weniger Speicherplatz.

## Replizierte und verknüpfte Klone auf dem gleichen Datenspeicher

Wenn Sie einen Linked-Clone-Desktop-Pool erstellen, wird von der übergeordneten virtuellen Maschine ein erster vollständiger Klon erstellt. Der vollständige Klon (bzw. das Replikat) und die Klone, die damit verknüpft sind, können im selben Datenspeicher bzw. derselben LUN (Logical Unit Number) abgelegt werden. Bei Bedarf können Sie mithilfe der Neuverteilungsfunktion das Replikat und die verknüpften Klone aus einer LUN in eine andere LUN oder verknüpfte Klone in einen Virtual SAN-Datenspeicher bzw. von einem Virtual SAN-Datenspeicher in eine LUN verschieben.

## Replizierte und verknüpfte Klone auf verschiedenen Datenspeichern

Alternativ dazu können Sie View Composer-Replikate und verknüpfte Klone in separaten Datenspeichern mit unterschiedlichen Leistungsmerkmalen ablegen. Beispielsweise können Sie die virtuellen Replikatmaschinen auf einer SSD (Solid-State Disk) speichern. Solid-State-Laufwerke besitzen eine niedrige Speicherkapazität und eine hohe Leseleistung, indem sie in der Regel Zehntausende E/As pro Sekunde (IOPS) unterstützen. Sie können verknüpfte Klone auf herkömmlichen, auf drehenden Medien basierenden Datenspeichern speichern. Diese Datenträger bieten eine niedrigere Leistung, sind jedoch kostengünstig und stellen eine hohe Speicherkapazität bereit, wodurch sie zur Speicherung der zahlreichen verknüpften Klone in einem großen Pool geeignet sind. Konfigurationen des mehrstufigen Speichers können zur kosteneffektiven Verarbeitung intensiver E/A-Szenarios verwendet werden. Hierzu gehören gleichzeitige Neustarts vieler virtueller Maschinen oder die Ausführung geplanter Antivirenschans.

Weitere Informationen finden Sie im Handbuch mit empfohlenen Vorgehensweisen namens *Storage Considerations for VMware View* (Speicheraspekte bei VMware View).

Bei Verwendung von Virtual SAN-Datenspeichern ist es nicht möglich, manuell andere Datenspeicher für Replikate und verknüpfte Klone auszuwählen. Da Virtual SAN Objekte automatisch auf dem passenden Festplattentyp ablegt und alle E/A-Vorgänge zwischenspeichert, ist die Verwendung der mehrstufigen Replikatspeicherung für Virtual SAN-Datenspeicher nicht erforderlich.

## Löschbare Festplatten für Auslagerungsdateien und temporäre Dateien

Bei der Erstellung eines Linked-Clone-Pools können Sie optional auch eine separate, temporäre virtuelle Festplatte konfigurieren, auf der die während der Benutzersitzungen generierten Auslagerungsdateien und temporären Dateien des Gastbetriebssystems gespeichert werden. Wenn die virtuelle Maschine ausgeschaltet wird, wird die temporäre Festplatte gelöscht. Durch die Verwendung temporärer Festplatten können Sie Speicherplatz sparen, da das Anwachsen verknüpfter Klone verlangsamt und der durch ausgeschaltete virtuelle Maschinen belegte Speicherplatz reduziert wird.

## Persistente Festplatten für dedizierte Desktops

Wenn Sie Desktop-Pools mit fester Zuweisung erstellen, kann View Composer optional auch eine separate persistente virtuelle Festplatte für jeden virtuellen Desktop erstellen. Auf dieser persistenten Festplatte werden das Windows-Profil und die Anwendungsdaten des Benutzers gespeichert. Wird ein verknüpfter Klon aktualisiert, neu zusammengestellt oder neu verteilt, bleibt der Inhalt der persistenten virtuellen Festplatte erhalten. VMware empfiehlt, die persistenten View Composer-Festplatten in einem anderen Datenspeicher abzulegen. Sie können dann die gesamte LUN sichern, die die persistenten Festplatten enthält.

## Virtual SAN-Datenspeicher, die lokale Speicherfestplatten eines vSphere-Clusters zusammenfassen

Virtual SAN virtualisiert die lokalen physischen Speicherfestplatten, die auf den ESXi-Hosts verfügbar sind, in einem einzelnen Datenspeicher, der von allen Hosts in einem vSphere-Cluster gemeinsam verwendet wird. Ein Virtual SAN-Datenspeicher besteht aus Solid-State-Laufwerken (SSDs) und Festplattenlaufwerken (HDDs), die auch als Datenfestplatten bezeichnet werden. SSDs werden zum Zwischenspeichern von Lesevorgängen und für die Pufferung von Schreibvorgängen verwendet. Datenfestplatten dienen als dauerhafter Speicher. Diese Strategie bietet einen Hochleistungsspeicher mit automatischer Zwischenspeicherung, sodass Sie beim Erstellen eines Desktop-Pools nur einen Datenspeicher angeben. Die verschiedenen Komponenten, wie Dateien virtueller Maschinen, Replikate, Benutzerdaten und Dateien des Betriebssystems, werden auf den passenden SSDs oder Datenfestplatten abgelegt.

---

**Hinweis** Virtual SAN erfordert vSphere 5.5 Update 1 oder eine neuere Version sowie die entsprechende Hardware. Siehe im [VMware-Kompatibilitätshandbuch](#).

---

Wenn Sie Virtual SAN verwenden, definiert View die Speichieranforderungen für virtuelle Maschinen (wie Kapazität, Leistung und Verfügbarkeit) in Form von Standardprofilen mit Speicherrichtlinien, die Sie ändern können. Virtual SAN organisiert die virtuelle Festplatte im logischen Datenspeicher, um die angegebenen Anforderungen zu erfüllen. Weiterhin überwacht Virtual SAN die Richtlinieneinhaltung während des Lebenszyklus der virtuellen Maschine und erstellt entsprechende Berichte. Wenn die Richtlinie wegen eines Host-, Festplatten- oder Netzwerkfehlers oder wegen Änderungen der Arbeitslast nicht mehr eingehalten wird, konfiguriert Virtual SAN die Daten der betroffenen virtuellen Maschinen neu und optimiert die Nutzung der Ressourcen im ganzen Cluster.

---

**Hinweis** Wenn Sie einen Linked-Clone-Desktop-Pool erstellen, wird von der übergeordneten virtuellen Maschine ein erster vollständiger Klon erstellt. Ausgehend von diesem vollständigen Klon oder diesem Replikat werden verknüpfte Klone erstellt. Bei Verwendung eines Virtual SAN-Datenspeichers werden standardmäßig gemäß der Verfügbarkeitsrichtlinie zusätzliche Kopien des Replikats und der verknüpften Klone erstellt.

---

## Speichergrößen für Linked-Clone-Desktop-Pools

View stellt grundlegende Richtlinien bereit, mit deren Hilfe Sie bestimmen können, wie viel Speicherplatz für einen Linked-Clone-Desktop-Pool benötigt wird. Eine Tabelle im Assistenten zum Hinzufügen von Desktop-Pools zeigt eine allgemeine Schätzung der Speichieranforderungen für die Linked-Clone-Festplatten, wenn der Pool erstellt wird und die verknüpften Klone mit der Zeit an Größe zunehmen.

Die Tabelle zu den Speichergrößen zeigt außerdem den freien Speicherplatz in den Datenspeichern an, die Sie zum Speichern von Betriebssystemfestplatten, persistenten View Composer-Festplatten und Replikaten ausgewählt haben. Sie können entscheiden, welche Datenspeicher Sie verwenden sollten, indem Sie den tatsächlichen freien Speicherplatz mit den geschätzten Anforderungen für die Linked-Clone-Festplatten vergleichen.

Die von View verwendeten Formeln stellen lediglich eine allgemeine Schätzung zur Speicherverwendung dar. Das tatsächliche Wachstum Ihrer verknüpften Klone hängt von zahlreichen Faktoren ab:

- Menge des Arbeitsspeichers, der der übergeordneten virtuellen Maschine zugeordnet ist
- Häufigkeit von Aktualisierungen
- Größe der Auslagerungsdatei des Gastbetriebssystems
- Keine Umleitung/Umleitung von Auslagerungsdateien und temporären Dateien auf eine separate Festplatte
- Keine Konfiguration/Konfiguration separater persistenter View Composer-Festplatten
- Arbeitslast der Linked-Clone-Maschinen, primär bestimmt durch die Anwendungstypen, die Benutzer im Gastbetriebssystem ausführen

---

**Hinweis** In einer Bereitstellung, die Hunderte oder Tausende von verknüpften Klonen umfasst, sollten Sie Ihre Linked-Clone-Pools so konfigurieren, dass bestimmte Datenspeichersätze dediziert für bestimmte ESXi-Cluster verwendet werden. Konfigurieren Sie Pools nicht wahllos über alle Datenspeicher, sodass die meisten oder alle ESXi-Host auf zahlreiche oder alle LUNs zugreifen müssen.

Wenn zu viele ESXi-Hosts versuchen, Schreibvorgänge auf Linked-Clone-Betriebssystemfestplatten auf einer bestimmten LUN auszuführen, können Konflikte auftreten, die eine Beeinträchtigung der Leistung und Skalierbarkeit zur Folge haben können. Weitere Informationen zur Datenspeicherplanung in großen Bereitstellungen finden Sie im Dokument *Planung der View-Architektur*.

---

## Größenrichtlinien für Linked-Clone-Pools

Wenn Sie einen Linked-Clone-Desktop-Pool erstellen oder bearbeiten, wird auf der Seite **Datenspeicher verknüpfter Klone auswählen** eine Tabelle mit Richtlinien für die Datenspeichergröße angezeigt. Anhand dieser Tabelle können Sie einfacher entscheiden, welche Datenspeicher Sie für die Linked-Clone-Festplatten auswählen sollten. Die Richtlinien berechnen den für neue verknüpfte Klone benötigten Speicherplatz.



## Größenrichtlinien für Linked-Clone-Festplatten

**Tabelle 15-1. Tabelle mit Größenrichtlinien für Linked-Clone-Festplatten** zeigt ein Beispiel mit Empfehlungen für die Speichergrößen, die für einen Pool mit 10 virtuellen Maschinen angezeigt werden können, wenn die übergeordnete virtuelle Maschine einen Arbeitsspeicher von 1 GB und ein Replikat mit 10 GB aufweist. In diesem Beispiel werden unterschiedliche Datenspeicher für Betriebssystemfestplatten und persistente View Composer-Festplatten ausgewählt.

**Tabelle 15-1. Tabelle mit Größenrichtlinien für Linked-Clone-Festplatten**

| Datentyp                 | Ausgewählter freier Speicherplatz (GB) | Empfohlenes Minimum (GB) | 50% Auslastung (GB) | Empfohlenes Maximum (GB) |
|--------------------------|--|--------------------------|---------------------|--------------------------|
| Betriebssystemfestplatte | 184.23                                 | 40.00                    | 80.00               | 130.00                   |
| Persistente Festplatten  | 28.56                                  | 4.00                     | 10.00               | 20.00                    |

Die Spalte **Ausgewählter freier Speicherplatz** zeigt den insgesamt verfügbaren Speicherplatz in allen Datenspeichern an, die Sie für einen Festplattentyp wie z.B. Betriebssystemfestplatten ausgewählt haben.

Die Spalte **Mind. empfohlen** zeigt die mindestens empfohlene Menge an Speicherplatz für einen Pool.

Die Spalte **50% Auslastung** zeigt die empfohlene Speicherplatzmenge, wenn die Linked-Clone-Festplatten auf eine Größe von 50% der übergeordneten virtuellen Maschine anwachsen.

Die Spalte **Max. empfohlen** zeigt die empfohlene Speicherplatzmenge, wenn die Linked-Clone-Festplatten die vollständige Größe der übergeordneten virtuellen Maschine erreichen.

Wenn Sie Betriebssystemfestplatten und persistente Festplatten im selben Datenspeicher ablegen, berechnet View die Speicheranforderungen beider Festplattentypen. Als **Datentyp** wird anstelle eines bestimmten Festplattentyps der Wert **Verknüpfte Klon** angezeigt.

Wenn Sie View Composer-Replikate in einem separaten Datenspeicher speichern, zeigt die Tabelle auch Speicherempfehlungen für die Replikate und passt die Empfehlungen für Betriebssystemfestplatten an.

## Größenrichtlinien

Die Tabelle liefert allgemeine Richtlinien. Für die Speicherberechnung müssen Sie zusätzliche Faktoren berücksichtigen, die sich auf das tatsächliche Speicherwachstum im Linked-Clone-Pool auswirken können.

Für Betriebssystemfestplatten richtet sich die Größeneinschätzung danach, wie häufig Sie den Pool aktualisieren und neu zusammenstellen.

Wenn Sie Ihren Linked-Clone-Pool zwischen einmal täglich und einmal wöchentlich aktualisieren, stellen Sie sicher, dass für **Ausgewählter freier Speicherplatz** eine Speicherbelegung möglich ist, die zwischen **Mind. empfohlen** und **50% Auslastung** liegt.

Wenn Sie den Pool nur selten aktualisieren oder neu erstellen, wachsen die Linked-Clone-Festplatten weiter an. Stellen Sie sicher, dass für **Ausgewählter freier Speicherplatz** eine Speicherbelegung möglich ist, die zwischen **50% Auslastung** und **Max. empfohlen** liegt.

Für persistente Festplatten richtet sich die Größeneinschätzung nach der Menge der Windows-Profildaten, die Benutzer auf ihren Desktops generieren. Aktualisierungen und Neuzusammenstellungen wirken sich nicht auf persistente Festplatten aus.

## Größenrichtlinien beim Bearbeiten eines vorhandenen Desktop-Pools

View schätzt den für neue verknüpfte Klone benötigten Speicherplatz. Wenn Sie einen Desktop-Pool erstellen, umfassen die Größenrichtlinien den gesamten Pool. Wenn Sie einen vorhandenen Desktop-Pool bearbeiten, umfassen die Richtlinien nur die neuen verknüpften Klone, die Sie zum Pool hinzufügen.

Beispiel: Wenn Sie 100 verknüpfte Klone zu einem Desktop-Pool hinzufügen und einen neuen Datenspeicher auswählen, schätzt View den Speicherbedarf für die 100 neuen Klone.

Wenn Sie einen neuen Datenspeicher auswählen, das Desktop-Pool jedoch dieselbe Größe beibehält, oder die Anzahl der verknüpften Klone reduzieren, werden die Größenrichtlinien als 0 angezeigt. Die Werte 0 stellen dar, dass keine neuen Klone nun auf dem ausgewählten Datenspeicher erstellt werden müssen. Die Speicherplatzanforderungen für die vorhandenen Klone wurden bereits berücksichtigt.

## Berechnung der Empfehlungen für die Mindestgröße durch View

Um eine Mindestempfehlung für Betriebssystemfestplatten ausgeben zu können, geht View bei der anfänglichen Erstellung und Inbetriebnahme davon aus, dass jeder Klon die zweifache Größe seines Arbeitsspeichers belegt. Wenn kein Arbeitsspeicher für einen Klon reserviert ist, wird eine ESXi-Auslagerungsdatei für den Klon erstellt, sobald dieser eingeschaltet wird. Die Größe der Auslagerungsdatei des Gastbetriebssystems wirkt sich ebenfalls auf das Wachstum einer Betriebssystemfestplatte für einen Klon aus.

Bei den Mindestempfehlungen für Betriebssystemfestplatten schließt View auch Speicherplatz für zwei Replikate in jedem Datenspeicher ein. View Composer erstellt ein Replikat, wenn ein Pool erstellt wird. Wenn der Pool zum ersten Mal neu zusammengestellt wird, erstellt View Composer ein zweites Replikat im Datenspeicher, verknüpft die verknüpften Klone mit dem neuen Replikat und löscht das erste Replikat, wenn keiner der Klone den ursprünglichen Snapshot verwendet. Der Datenspeicher muss während der Neuzusammenstellung über die Kapazität zum Speichern der zwei Replikate verfügen.

Standardmäßig verwenden Replikate vSphere Thin Provisioning, um jedoch die Richtlinien einfach zu halten, geht View von zwei Replikaten aus, die denselben Speicherplatz belegen wie die übergeordnete virtuelle Maschine.

Um eine Mindestempfehlung für persistente Festplatten ausgeben zu können, geht View von 20% der Festplattengröße aus, die Sie auf der Seite **View Composer-Festplatten** im Assistenten **Desktop-Pool hinzufügen** angegeben haben.

---

**Hinweis** Die Berechnungen für persistente Festplatten basieren auf statischen Schwellenwerten (in Gigabyte). Wenn Sie beispielsweise eine persistente Festplatte mit einer Größe zwischen 1024 MB und 2047 MB festlegen, berechnet View die Größe der persistenten Festplatte als 1 GB. Wenn Sie eine Festplattengröße von 2048 MB festlegen, berechnet View die Festplattengröße als 2 GB.

---

Um eine Mindestempfehlung für das Speichern von Replikaten in einem separaten Datenspeicher ausgeben zu können, setzt View Speicherplatz für zwei Replikate im Datenspeicher an. Für die Mindest- und Höchstauslastung wird derselbe Wert berechnet.

Weitere Informationen finden Sie unter [Größenformeln für Linked-Clone-Pools](#).

## Größenrichtlinien und Speichermehrfachvergabe

Nachdem Sie die Speicheranforderungen geschätzt, Datenspeicher ausgewählt und den Pool bereitgestellt haben, stellt View basierend auf dem freien Speicherplatz und den vorhandenen Klonen in jedem Datenspeicher Linked-Clone-VMs in verschiedenen Datenspeichern bereit.

Abhängig von der Option für die Speichermehrfachvergabe, die Sie auf der Seite **Datenspeicher verknüpfter Klon auswählen** im Assistenten „Desktop-Pools hinzufügen“ ausgewählt haben, stellt View die Bereitstellung neuer Klone ein und reserviert freien Speicherplatz für vorhandene Klone. Durch dieses Verhalten wird sichergestellt, dass ein Wachstumspuffer für jeden Computer im Datenspeicher vorhanden ist.

Wenn Sie einen sehr hohen Wert für die Speichermehrfachvergabe wählen, übersteigen die geschätzten Speicheranforderungen möglicherweise in der Spalte **Ausgewählter freier Speicherplatz** angezeigte Kapazität. Der Grad der Speichermehrfachvergabe wirkt sich darauf aus, wie viele virtuelle Maschinen View tatsächlich in einem Datenspeicher erstellt.

Weitere Informationen finden Sie unter [Festlegen des Werts für die Speichermehrfachvergabe für virtuelle Linked-Clone-Computer](#).

## Größenformeln für Linked-Clone-Pools

Formeln für die Berechnung von Speichergrößen unterstützen Sie dabei, die Größe von Linked-Clone-Festplatten in Relation zum freien Speicherplatz in den Datenspeichern zu ermitteln, die Sie für Betriebssystemfestplatten, persistente View Composer-Festplatten und Replikate ausgewählt haben.

### Formeln zur Berechnung der Speichergrößen

[Tabelle 15-2. Formeln zur Berechnung der Speichergrößen für Linked-Clone-Festplatten in ausgewählten Datenspeichern](#) zeigt die Formeln zur Berechnung der geschätzten Größen von Linked-Clone-Festplatten, wenn Sie einen Pool erstellen und die Linked-Clone-Computer im Laufe der Zeit an Größe zunehmen. Diese Formeln beziehen den Speicherplatz für Replikatfestplatten ein, die mit den Klonen im Datenspeicher abgelegt werden.

Wenn Sie einen vorhandenen Pool bearbeiten oder Replikate in einem separaten Datenspeicher ablegen, verwendet View eine andere Formel für die Größenberechnung. Siehe [Formeln zur Größenberechnung von verknüpften Klonen beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern](#).

**Tabelle 15-2. Formeln zur Berechnung der Speichergrößen für Linked-Clone-Festplatten in ausgewählten Datenspeichern**

| Datentyp                   | Ausgewählter freier Speicherplatz (GB)                  | Empfohlenes Minimum (GB)   | 50% Auslastung (GB)   | Empfohlenes Maximum (GB)   |
|----------------------------|---|--|---|--|
| Betriebssystemfestplatte n | Freier Speicherplatz in den ausgewählten Datenspeichern | Anzahl der VMs * (2 * Arbeitsspeicher der VM) + (2 * Replikatfestplatte) | Anzahl der VMs * (50% der Replikatfestplatte + Arbeitsspeicher der VM) + (2 * Replikatfestplatte) | Anzahl der VMs * (100% der Replikatfestplatte + Arbeitsspeicher der VM) + (2 * Replikatfestplatte) |
| Persistente Festplatten    | Freier Speicherplatz in den ausgewählten Datenspeichern | Anzahl der VMs * 20% der persistenten Festplatte                         | Anzahl der VMs * 50% der persistenten Festplatte  | Anzahl der VMs * 100% der persistenten Festplatte  |

### Beispiel für eine geschätzte Speichergröße

In diesem Beispiel wird die übergeordnete virtuelle Maschine mit einem Arbeitsspeicher von 1 GB konfiguriert. Die Festplatte der übergeordneten virtuellen Maschine ist 10 GB groß. Es wird ein Linked-Clone-Pool mit 10 Computern erstellt. Die Größe der persistenten Festplatten wird auf 2048 MB festgelegt.

Die Betriebssystemfestplatten werden in einem Datenspeicher konfiguriert, der derzeit über 184,23 GB freien Speicherplatz verfügt. Die persistenten Festplatten werden in einem anderen Datenspeicher mit 28,56 GB freiem Speicherplatz konfiguriert.

[Tabelle 15-3. Beispiel einer geschätzten Speichergröße für Linked-Clone-Desktops in ausgewählten Datenspeichern](#) zeigt, wie mithilfe der Formeln zur Größenberechnung die geschätzten Speicheranforderungen für den beispielhaften Linked-Clone-Desktop-Pool ermittelt werden.

**Tabelle 15-3. Beispiel einer geschätzten Speichergröße für Linked-Clone-Desktops in ausgewählten Datenspeichern**

| Datentyp                   | Ausgewählter freier Speicherplatz (GB) | Empfohlenes Minimum (GB)                                | 50% Auslastung (GB)   | Empfohlenes Maximum (GB)  |
|----------------------------|--|---|---|---|
| Betriebssystemfestplatte n | 184.23                                 | $10 * (2 * 1 \text{ GB}) + (2 * 10 \text{ GB}) = 40.00$ | $10 * (50\% \text{ von } 10 \text{ GB} + 1 \text{ GB}) + (2 * 10 \text{ GB}) = 80.00$ | $10 * (100\% \text{ von } 10 \text{ GB} + 1 \text{ GB}) + (2 * 10 \text{ GB}) = 130.00$ |
| Persistente Festplatten    | 28.56                                  | $10 * (20\% \text{ von } 2 \text{ GB}) = 4.00$          | $10 * (50\% \text{ von } 2 \text{ GB}) = 10.00$                                       | $10 * (100\% \text{ von } 2 \text{ GB}) = 20.00$  |

### Formeln zur Größenberechnung von verknüpften Klonen beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern

View verwendet bei der Bearbeitung eines vorhandenen Linked-Clone-Desktop-Pools oder der Speicherung von Replikaten in einem separaten Datenspeicher andere Formeln zur Größenberechnung als bei der anfänglichen Erstellung eines Pools.

Wenn Sie einen vorhandenen Pool bearbeiten und Datenspeicher für den Pool auswählen, erstellt View Composer neue Klone in den ausgewählten Datenspeichern. Die neuen Klone werden mit dem vorhandenen Snapshot verknüpft und verwenden die vorhandene Replikatfestplatte. Es werden keine neuen Replikate erstellt.

View schätzt die Größenanforderungen für neue Klone, die zu dem Desktop-Pool hinzugefügt werden. Vorhandene Klone werden von View nicht in die Berechnung einbezogen.

Wenn Sie Replikate in einem separaten Datenspeicher ablegen, werden die weiteren ausgewählten Datenspeicher dediziert für Linked-Clone-Festplatten verwendet.

In diesen Fällen bezieht View keinen Speicherplatz für Replikate ein, wenn die Speicherempfehlungen für Linked-Clone-Festplatten berechnet werden.

**Tabelle 15-4. Formeln zur Größenberechnung von Linked-Clone-Festplatten beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern** zeigt die Formeln zur Berechnung der geschätzten Größen von Linked-Clone-Festplatten, wenn Sie einen Pool bearbeiten oder Replikate in einem separaten Datenspeicher ablegen.

**Tabelle 15-4. Formeln zur Größenberechnung von Linked-Clone-Festplatten beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern**

| Datentyp                   | Ausgewählter freier Speicherplatz (GB)                  | Empfohlenes Minimum (GB)                                | 50% Auslastung (GB)   | Empfohlenes Maximum (GB)  |
|----------------------------|---|---|---|---|
| Betriebssystemfestplatte n | Freier Speicherplatz in den ausgewählten Datenspeichern | Anzahl der neuen VMs * (2 * Arbeitsspeicher der VM)     | Anzahl der neuen VMs * (50 % der Replikatfestplatte + Arbeitsspeicher der VM) | Anzahl der neuen VMs * (100% der Replikatfestplatte + Arbeitsspeicher der VM) |
| Persistente Festplatten    | Freier Speicherplatz in den ausgewählten Datenspeichern | Anzahl der neuen VMs * 20 % der persistenten Festplatte | Anzahl der neuen VMs * 50% der persistenten Festplatte                        | Anzahl der neuen VMs * 100% der persistenten Festplatte                       |

### Beispiel einer geschätzte Speichergröße beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern

In diesem Beispiel wird die übergeordnete virtuelle Maschine mit einem Arbeitsspeicher von 1 GB konfiguriert. Die Festplatte der übergeordneten virtuellen Maschine ist 10 GB groß. Es wird ein Linked-Clone-Pool mit 10 Computern erstellt. Die Größe der persistenten Festplatten wird auf 2048 MB festgelegt.

Die Betriebssystemfestplatten werden in einem Datenspeicher konfiguriert, der derzeit über 184,23 GB freien Speicherplatz verfügt. Die persistenten Festplatten werden in einem anderen Datenspeicher mit 28,56 GB freiem Speicherplatz konfiguriert.

**Tabelle 15-5. Beispiel einer geschätzte Speichergröße für Linked-Clone-Festplatten beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern** zeigt, wie mithilfe der Formeln zur Größenberechnung die geschätzten Speicheranforderungen für den beispielhaften Linked-Clone-Pool ermittelt werden.

**Tabelle 15-5. Beispiel einer geschätzte Speichergröße für Linked-Clone-Festplatten beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern**

| Datentyp                   | Ausgewählter freier Speicherplatz (GB) | Empfohlenes Minimum (GB)                       | 50% Auslastung (GB)   | Empfohlenes Maximum (GB)  |
|----------------------------|--|--|---|---|
| Betriebssystemfestplatte n | 184.23                                 | $10 * (2 * 1 \text{ GB}) = 20.00$              | $10 * (50\% \text{ von } 10 \text{ GB} + 1 \text{ GB}) = 60.00$ | $10 * (100\% \text{ von } 10 \text{ GB} + 1 \text{ GB}) = 110.00$ |
| Persistente Festplatten    | 28.56                                  | $10 * (20\% \text{ von } 2 \text{ GB}) = 4.00$ | $10 * (50\% \text{ von } 2 \text{ GB}) = 10.00$                 | $10 * (100\% \text{ von } 2 \text{ GB}) = 20.00$                  |

## Speichermehrfachvergabe für virtuellen Linked-Clone-Computer

Mithilfe der Funktion zur Speichermehrfachvergabe können Sie die Speicherkosten reduzieren, indem Sie mehr virtuelle Linked-Clone-Computer in einem Datenspeicher platzieren, als dies bei vollständigen virtuellen Maschinen möglich ist. Die verknüpften Klone können das Mehrfache der physischen Datenspeicherkapazität als logischen Speicherplatz verwenden.

Mit dieser Funktion können Sie eine Speicherebene wählen, bei der eine Speichermehrfachvergabe für die Kapazität des Datenspeichers möglich ist. Zudem wird die Anzahl an verknüpften Klonen eingeschränkt, die View erstellt. Sie können einerseits die Vergeudung von Speicherkapazität durch eine zu konservative Bereitstellung und andererseits das Risiko verhindern, dass der Speicherplatz für die verknüpften Klone knapp wird und die zugehörigen Desktop-Anwendungen fehlschlagen.

Beispielsweise können Sie maximal zehn vollständige virtuelle Maschinen in einem Datenspeicher mit 100 GB erstellen, wenn die Größe jeder virtuellen Maschine 10 GB beträgt. Wenn Sie aus einer übergeordneten virtuellen Maschine mit 10 GB verknüpfte Klone erstellen, weist jeder Klon einen Bruchteil dieser Größe auf.

Wenn Sie einen konservativen Wert für die Speichermehrfachvergabe festlegen, können die Klone das Vierfache der physischen Datenspeichergöße verwenden. Für die Größe der einzelnen Klone wird von der Größe der übergeordneten virtuellen Maschine ausgegangen. Bei einem Datenspeicher mit 100 GB und einer übergeordneten virtuellen Maschine mit 10 GB stellt View etwa 40 verknüpfte Klone bereit. View stellt auch dann keine größere Anzahl an Klonen bereit, wenn der Datenspeicher über freien Speicherplatz verfügt. Diese Beschränkung bietet einen Puffer für das Wachstum vorhandener Klone.

**Tabelle 15-6. Grad der Speichermehrfachvergabe** zeigt die möglichen Werte für die Speichermehrfachvergabe.

**Tabelle 15-6. Grad der Speichermehrfachvergabe**

| Option      | Grad der Speichermehrfachvergabe                             |
|-------------|--|
| Keine       | Es findet keine Speichermehrfachvergabe statt.               |
| Konservativ | 4-fache Größe des Datenspeichers. Dies ist der Standardwert. |

| Option    | Grad der Speichermehrfachvergabe   |
|-----------|------------------------------------|
| Mäßig     | 7-fache Größe des Datenspeichers.  |
| Aggressiv | 15-fache Größe des Datenspeichers. |

Die Werte für die Speichermehrfachvergabe bieten eine allgemeine Richtlinie zum Bestimmen der Speicherkapazität. Um den idealen Wert zu ermitteln, überwachen Sie das Wachstum der verknüpften Klone in Ihrer Umgebung.

Legen Sie einen sehr hohen Wert fest, wenn die Betriebssystemfestplatten die mögliche Maximalgröße nie erreichen werden. Bei einem hohen Wert für die Speichermehrfachvergabe muss die Umgebung sorgfältig überwacht werden. Um sicherzustellen, dass der Speicherplatz für die verknüpften Klone nicht knapp wird, können Sie den Desktop-Pool regelmäßig aktualisieren oder neu verteilen und die Betriebssystemdaten der verknüpften Klone auf die ursprüngliche Größe reduzieren.

Beispielsweise ist ein hoher Wert für die Speichermehrfachvergabe für einen Desktop-Pool mit dynamischer Zuweisung sinnvoll, für dessen virtuelle Maschinen nach der Abmeldung ein Lösch- oder Aktualisierungsvorgang festgelegt ist.

Sie können für verschiedene Datenspeichertypen unterschiedliche Werte für die Speichermehrfachvergabe festlegen, um den unterschiedlichen Durchsatzleistungen in den einzelnen Datenspeichern Rechnung zu tragen. Für einen NAS-Datenspeicher kann beispielsweise eine andere Einstellung gewählt werden als für einen SAN-Datenspeicher.

## Festlegen des Werts für die Speichermehrfachvergabe für virtuelle Linked-Clone-Computer

Mithilfe der Funktion für die Speichermehrfachvergabe kann gesteuert werden, wie viele virtuelle Linked-Clone-Computer View in einem Datenspeicher erstellt. Über diese Funktion können Sie verknüpfte Klone erstellen, deren logische Größe insgesamt den physischen Speichergrenzwert des Datenspeichers überschreitet.

Diese Funktion kann nur mit Linked-Clone-Pools verwendet werden.

Der Grad der Speichermehrfachvergabe gibt an, um wie viel größer die Speichermenge gegenüber der physischen Größe des Datenspeichers ist, den die Klone verwenden würden, wenn es sich um vollständige virtuelle Maschinen handeln würde. Weitere Informationen finden Sie unter [Speichermehrfachvergabe für virtuellen Linked-Clone-Computer](#).

### Verfahren

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

- 2 Wenn Sie einen neuen Desktop-Pool erstellen oder einen vorhandenen Pool bearbeiten, navigieren Sie zur Seite **vCenter-Einstellungen**.

| Option                          | Aktion   |
|---------------------------------|--|
| <b>Neuer Desktop-Pool</b>       | a Klicken Sie auf <b>Hinzufügen</b> .<br>b Fahren Sie im Assistenten <b>Desktop-Pool hinzufügen</b> fort, bis die Seite <b>vCenter-Einstellungen</b> angezeigt wird. |
| <b>Vorhandener Desktop-Pool</b> | a Wählen Sie den Linked-Clone-Pool aus und klicken Sie auf <b>Bearbeiten</b> .<br>b Klicken Sie auf die Registerkarte <b>vCenter-Einstellungen</b> .                 |

- 3 Klicken Sie auf der Seite **vCenter-Einstellungen** auf **Durchsuchen** neben **Datenspeicher**.
- 4 Wählen Sie den Datenspeicher auf der Seite **Datenspeicher verknüpfter Klone auswählen** aus.  
Ein Dropdown-Menü wird in der Spalte „Speichermehrfachvergabe“ für den ausgewählten Datenspeicher angezeigt.
- 5 Wählen Sie über das Dropdown-Menü den Wert für die Speichermehrfachvergabe aus.

| Option             | Beschreibung   |
|--------------------|--|
| <b>Keine</b>       | Es findet keine Speichermehrfachvergabe statt.   |
| <b>Konservativ</b> | 4-fache Größe des Datenspeichers. Dies ist der Standardwert.   |
| <b>Mäßig</b>       | 7-fache Größe des Datenspeichers.  |
| <b>Aggressiv</b>   | 15-fache Größe des Datenspeichers.   |
| <b>Unbegrenzt</b>  | View beschränkt nicht die Anzahl der Linked-Clone-Computer, die auf der Basis der physikalischen Kapazität des Datenspeichers erstellt werden. Wählen Sie diese Ebene nur aus, wenn Sie sicher sind, dass der Datenspeicher über ausreichend Kapazität verfügt, um sämtliche Computer und deren künftige Zunahme abdecken zu können. |

- 6 Klicken Sie auf **OK**.

## Datenfestplatten von verknüpften Klonen

View Composer erstellt mehrere Datenfestplatten zum Speichern der Komponenten einer virtuellen Maschine mit verknüpftem Klon.

### Betriebssystemfestplatte

View Composer erstellt eine Betriebssystemfestplatte für jeden verknüpften Klon. Auf dieser Festplatte werden die Systemdaten gespeichert, die der Klon benötigt, um mit dem Basis-Image verknüpft zu bleiben und als eindeutig identifizierbare virtuelle Maschine zu fungieren.



## QuickPrep-Konfigurationsdatenfestplatte

View Composer erstellt mit der Betriebssystemfestplatte eine zweite Festplatte. Auf der zweiten Festplatte werden QuickPrep-Konfigurationsdaten und andere betriebssystembezogene Daten gespeichert, die während Aktualisierungen und Neuzusammenstellungen beibehalten werden müssen. Diese Festplatte ist klein und umfasst in der Regel etwa 20 MB. Diese Festplatte wird erstellt, wenn Sie mithilfe von QuickPrep oder Sysprep die virtuelle Maschine anpassen.

Wenn Sie separate persistente View Composer-Festplatten zum Speichern von Benutzerprofilen konfigurieren, werden jedem verknüpften Klon drei Festplatten zugewiesen: die Betriebssystemfestplatte, die zweite Festplatte der virtuellen Maschine und die persistente View Composer-Festplatte.

Die zweite Festplatte für die virtuelle Maschine wird in demselben Datenspeicher wie die Betriebssystemfestplatte gespeichert. Diese Festplatte kann nicht konfiguriert werden.

## Persistente View Composer-Festplatte

In einem Pool mit dedizierter Zuweisung können Sie separate persistente View Composer-Festplatten zum Speichern von Windows-Benutzerprofildaten konfigurieren. Diese Festplatte ist optional.

Separate persistente Festplatten ermöglichen Ihnen das Beibehalten von Benutzerdaten und -einstellungen. View Composer-Aktualisierungen, -Neuzusammenstellungen und Neuverteilungen wirken sich nicht auf persistente Festplatten aus. Sie können eine persistente Festplatte von einem verknüpften Klon trennen und mit einem anderen verknüpften Klon verknüpfen.

Wenn Sie keine separaten persistenten Festplatten konfigurieren, wird das Windows-Profil auf der Betriebssystemfestplatte gespeichert. Benutzerdaten und -einstellungen werden während Aktualisierungen, Neuzusammenstellungen und Neuverteilungen entfernt.

Sie können persistente Festplatten in demselben Datenspeicher wie die Betriebssystemfestplatte oder in einem anderen Datenspeicher ablegen.

## Festplatte für löschbare Daten

Bei der Erstellung eines Linked-Clone-Pools können Sie eine separate, nicht persistente Festplatte zum Speichern der Auslagerungs- und temporären Dateien des Gastbetriebssystems konfigurieren, die bei Benutzersitzungen generiert werden. Die Festplattengröße muss in Megabyte angegeben werden.

Diese Festplatte ist optional.

Beim Ausschalten des verknüpften Klons ersetzt View die Festplatte mit löschbaren Daten durch eine Kopie der ursprünglichen Festplatte, die View Composer mit dem Pool von verknüpften Klonen erstellt hat. Verknüpfte Klone können an Größe zunehmen, wenn Benutzer mit ihren Desktops interagieren. Durch Verwendung von Festplatten mit löschbaren Daten kann Speicherplatz eingespart werden, indem das Wachstum verknüpfter Klone verlangsamt wird.

Die Festplatte für löschbare Daten wird in demselben Datenspeicher wie die Betriebssystemfestplatte gespeichert.

## Speichern von verknüpften Klonen auf lokalen Datenspeichern

Virtuelle Maschinen mit verknüpften Klonen können auf lokalen Datenspeichern gespeichert werden, die interne Ersatzfestplatten auf ESXi-Hosts sind. Dies kann verschiedene Vorteile bieten, so z. B. eine kostengünstige Hardware, eine schnelle Bereitstellung von virtuellen Maschinen, mehrere hochleistungsfähige Vorgänge zum Ändern des Betriebsstatus und eine vereinfachte Verwaltung. Bei Verwendung von lokalen Speichern werden jedoch die Ihnen zur Verfügung stehenden Optionen für die Konfiguration der vSphere-Infrastruktur beschränkt. Die Verwendung von lokalen Speichern bietet in bestimmten View-Umgebungen Vorteile, ist jedoch für andere Umgebungen nicht geeignet.

---

**Hinweis** Die in diesem Thema beschriebenen Einschränkungen gelten nicht für Virtual SAN-Datenspeicher, die auch lokale Speicherfestplatten verwenden, jedoch spezifische Hardware benötigen.

---

Die Verwendung von lokalen Speichern funktioniert wahrscheinlich am besten, wenn die View-Desktops in Ihrer Umgebung zustandsfrei sind. So könnten Sie etwa lokale Datenspeicher verwenden, wenn Sie zustandsfreie Kiosks oder Unterrichts- und Schulungsstationen bereitstellen.

Ziehen Sie die Verwendung von lokalen Datenspeichern in Betracht, wenn Ihre virtuellen Maschinen dynamische Zuweisungen haben, nicht nur für einzelne Endbenutzer vorgesehen sind, keine persistenten Festplatten für Benutzerdaten benötigen und in regelmäßigen Abständen, wie beispielsweise bei der Abmeldung von Benutzern, gelöscht oder aktualisiert werden. Mit diesem Ansatz können Sie die Festplattennutzung auf jedem lokalen Datenspeicher steuern, ohne die virtuellen Maschinen über Datenspeicher hinweg zu verschieben oder deren Last auszugleichen.

Sie müssen jedoch die Einschränkungen in Betracht ziehen, die die Verwendung von lokalen Datenspeichern in Ihrer View-Desktop-Bereitstellung mit sich bringen:

- Sie können vMotion nicht zur Verwaltung von Datenträgern verwenden.
- Sie können die Last von virtuellen Maschinen nicht über einen Ressourcen-Pool hinweg ausgleichen. Beispielsweise können Sie den Vorgang zur Neuverteilung in View Composer mit verknüpften Klonen, die auf lokalen Datenspeichern gespeichert sind, nicht verwenden.
- Sie können VMware High Availability nicht verwenden.
- Sie können den vSphere Distributed Resource Scheduler (DRS) nicht verwenden.
- Sie können ein View Composer-Replikat und verknüpfte Klone nicht auf separaten Datenspeichern speichern, wenn sich das Replikat auf einem lokalen Datenspeicher befindet.

Wenn Sie verknüpfte Klone auf lokalen Datenspeichern speichern, empfiehlt VMware dringend, das Replikat auf demselben Datenträger wie die verknüpften Klone zu speichern. Obwohl die Möglichkeit besteht, verknüpfte Klone auf lokalen Datenspeichern und das Replikat auf einem freigegebenen Datenspeicher zu speichern, sofern alle ESXi-Hosts in dem Cluster auf das Replikat zugreifen können, empfiehlt VMware diese Konfiguration nicht.

- Wenn Sie lokale herkömmliche Festplatten auswählen, kommt die Performance möglicherweise nicht an kommerziell erhältliche Speicher-Arrays heran. Lokale herkömmliche Laufwerke und ein Speicher-Array mögen vielleicht ähnliche Kapazitäten aufweisen, jedoch haben lokale herkömmliche Laufwerke nicht dieselben Durchsatzraten wie ein Speicher-Array. Der Durchsatz erhöht sich mit steigender Spindelzahl.

Wenn Sie direkt angeschlossene SSDs (Solid-State-Drives) auswählen, übersteigt die Performance wahrscheinlich diejenige vieler Speicher-Arrays.

Sie können verknüpfte Klone auf einem lokalen Datenspeicher ohne Einschränkungen speichern, wenn Sie den Desktop-Pool auf einem einzelnen ESXi-Host oder einem Cluster, der einen einzigen ESXi-Host enthält, konfigurieren. Die Verwendung eines einzelnen ESXi-Hosts beschränkt jedoch die Größe des Desktop-Pools, den Sie konfigurieren können.

Um einen großen Desktop-Pool zu konfigurieren, müssen Sie einen Cluster auswählen, der mehrere ESXi-Hosts mit der kollektiven Fähigkeit, eine große Anzahl von virtuellen Maschinen zu unterstützen, enthält.

Wenn Sie vorhaben, die Vorteile von lokalem Speicher zu nutzen, müssen Sie sorgfältig die Auswirkungen bedenken, wenn Ihnen vMotion, HA, DRS und andere Funktionen nicht zur Verfügung stehen. Falls Sie die Nutzung der lokalen Festplatten durch Steuerung der Zahl der virtuellen Maschinen und deren Festplattenwachstum verwalten, dynamische Zuweisungen verwenden und regelmäßig Aktualisierungs- und Löschvorgänge ausführen, können Sie verknüpfte Klone erfolgreich auf lokalen Datenspeichern bereitstellen.

## Speichern von View Composer-Replikaten und verknüpften Klonen in separaten Datenspeichern

Sie können View Composer-Replikate und verknüpfte Klone in separaten Datenspeichern mit unterschiedlichen Leistungsmerkmalen ablegen. Diese flexible Konfiguration kann intensive Vorgänge wie die gleichzeitige Bereitstellung zahlreicher verknüpfter Klone oder die Ausführung von Antivirenschans beschleunigen.

Beispielsweise können Sie die virtuellen Replikatmaschinen in einem auf einer Solid-State-Disk basierenden Datenspeicher speichern. Solid-State-Disks besitzen eine niedrige Speicherkapazität und eine hohe Leseleistung, in der Regel mit Unterstützung für 20.000 E/A-Vorgänge pro Sekunde (IOPS). View Composer erstellt nur ein Replikat für jeden View Composer-Basis-Image-Snapshot in jedem ESXi-Cluster, sodass Replikate nicht viel Speicherplatz in Anspruch nehmen. Eine Solid-State-Disk kann die Geschwindigkeit verbessern, in der ESXi die Betriebssystemfestplatte eines Replikats liest, wenn eine Aufgabe gleichzeitig auf vielen verknüpften Klonen ausgeführt wird.

Sie können verknüpfte Klone auf herkömmlichen, auf drehenden Medien basierenden Datenspeichern speichern. Diese Festplatten bieten eine geringere Leistung und unterstützen in der Regel 200 E/A-Vorgänge pro Sekunde. Sie sind kostengünstig und bieten eine hohe Speicherkapazität, wodurch sie zur Speicherung der zahlreichen verknüpften Klone in einem großen Pool geeignet sind. ESXi muss keine intensiven, gleichzeitigen Lesevorgänge für einen verknüpften Klon ausführen.

Indem Sie Replikate und verknüpfte Klone auf diese Weise konfigurieren, können Sie die Auswirkungen von E/A-Überlastungen bei gleichzeitiger Erstellung vieler verknüpfter Klone reduzieren. Wenn Sie beispielsweise einen Pool mit dynamischer Zuweisung mit einer Richtlinie zum Löschen von Computern bei Abmeldung bereitstellen und die Benutzer gleichzeitig mit der Arbeit beginnen, muss View für alle gleichzeitig neue Computer bereitstellen.

---

**Wichtig** Diese Funktion ist auf bestimmte Speicherkonfigurationen ausgelegt, die von Herstellern mit Hochleistungsfestplatten-Lösungen bereitgestellt werden. Speichern Sie Replikate nicht in einem separaten Datenspeicher, wenn Ihre Speicherhardware keine hohe Leseleistung unterstützt.

---

Sie müssen bestimmte Anforderungen einhalten, wenn Sie das Replikat und verknüpfte Klone in einem Pool auf separaten Datenspeichern speichern:

- Sie können nur einen separaten Replikatdatenspeicher für einen Pool angeben.
- Wenn ein Replikatdatenspeicher gemeinsam genutzt wird, muss er von allen ESXi-Hosts im Cluster aus zugänglich sein.
- Werden die Linked-Clone-Datenspeicher gemeinsam verwendet, muss der Replikatdatenspeicher freigegeben werden. Das Replikat kann nicht auf einem lokalen Datenspeicher gespeichert werden.

Wenn es sich bei den Linked-Clone-Datenspeichern um lokale Datenspeicher handelt, empfiehlt VMware dringend, das Replikat auf demselben Volume wie die verknüpften Klone zu speichern. Obwohl die Möglichkeit besteht, verknüpfte Klone auf lokalen Datenspeichern und das Replikat auf einem freigegebenen Datenspeicher zu speichern, sofern alle ESXi-Hosts in dem Cluster auf das Replikat zugreifen können, empfiehlt VMware diese Konfiguration nicht.

---

**Hinweis** Diese Einschränkung trifft nicht zu, wenn Sie Virtual SAN-Datenspeicher verwenden. Diese fassen die lokalen Speicherfestplatten aller ESXi-Hosts in dem Cluster zusammen. Bei Virtual SAN-Datenspeichern ist der Speicherplatz sowohl lokaler als auch freigegebener Speicherplatz.

---

## Überlegungen zur Verfügbarkeit beim Speichern von Replikaten in einem separaten oder in gemeinsam genutzten Datenspeichern

Sie können View Composer-Replikate in einem separaten Datenspeicher oder in denselben Datenspeichern wie virtuelle Linked-Clone-Maschinen speichern. Diese Konfigurationen wirken sich unterschiedlich auf die Verfügbarkeit des Pools aus.

Wenn Sie Replikate in denselben Datenspeichern wie verknüpfte Klone ablegen, erstellt View Composer zur besseren Verfügbarkeit in jedem Datenspeicher ein separates Replikat. Steht ein Datenspeicher nicht mehr zur Verfügung, sind nur die verknüpften Klone im jeweiligen Datenspeicher betroffen. Verknüpfte Klone in anderen Datenspeichern werden weiterhin ausgeführt.

Wenn Sie Replikate in einem separaten Datenspeicher ablegen, werden alle verknüpften Klone im Pool mit den Replikaten in dem jeweiligen Datenspeicher gekoppelt. Fällt der Datenspeicher aus, steht der gesamte Pool nicht länger zur Verfügung.

Um die Verfügbarkeit von virtuellen Linked-Clone-Computern zu verbessern, können Sie für den Datenspeicher, in dem Sie die Replikate speichern, eine Hochverfügbarkeitslösung konfigurieren.

## Konfigurieren der View-Speicherbeschleunigung für Desktop-Pools

Sie können Desktop-Pools so konfigurieren, dass ESXi-Hosts Festplattendaten von virtuellen Maschinen zwischenspeichern können. Diese Funktion, die View-Speicherbeschleunigung, verwendet die CBRC-Funktion (Content Based Read Cache) in ESXi-Hosts. Die View-Speicherbeschleunigung kann die E/A-Vorgänge pro Sekunde verringern und die Performance bei Startüberlastungen steigern, wenn viele Computer gleichzeitig starten oder Antivirenschans durchführen. Die Funktion ist außerdem nützlich, wenn Administratoren oder Benutzer häufig Anwendungen oder Daten laden. Stellen Sie zur Verwendung dieser Funktion sicher, dass die View-Speicherbeschleunigung für einzelne Desktop-Pools aktiviert ist.

Die View-Speicherbeschleunigung ist standardmäßig für einen Pool aktiviert. Sie können die View-Speicherbeschleunigung aktivieren oder deaktivieren, wenn Sie einen Pool erstellen oder bearbeiten.

Sie können die View-Speicherbeschleunigung für 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.

Wenn eine virtuelle Maschine erstellt wird, indiziert View die Inhalte jeder virtuellen Festplattendatei. Diese Indizes werden in einer Digest-Datei der virtuellen Maschine gespeichert. Zur Laufzeit liest der ESXi-Host die Digest-Dateien und speichert gemeinsame Datenblöcke im Speicher zwischen. Um den ESXi-Host-Cache aktuell zu halten, erzeugt View die Digest-Dateien in festgelegten Intervallen neu und auch, wenn die virtuelle Maschine neu zusammengestellt wird. Sie können das Intervall für die Neugenerierung ändern.

### 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-Berechtigungen für den vCenter Server-Benutzer behandelt werden.
- Stellen Sie sicher, dass die View-Speicherbeschleunigung in vCenter Server aktiviert ist. Weitere Informationen finden Sie im Dokument *ViewVerwaltung von*.

## Verfahren

- 1 Öffnen Sie in View Administrator die Seite **Erweiterte Speicheroptionen**.

| Option                          | Beschreibung   |
|---------------------------------|--|
| <b>Neuer Desktop-Pool</b>       | Starten Sie den Assistenten zum Hinzufügen von Desktop-Pools, um mit der Erstellung eines automatisierten Desktop-Pools zu beginnen. Befolgen Sie die Eingabeaufforderungen des Assistenten, bis Sie zur Seite <b>Erweiterter Speicher</b> gelangen.   |
| <b>Vorhandener Desktop-Pool</b> | Wählen Sie den vorhandenen Pool aus, klicken Sie auf <b>Bearbeiten</b> und anschließend auf die Registerkarte <b>Erweiterter Speicher</b> .<br>In einem vorhandenen Pool werden Digest-Dateien der View-Speicherbeschleunigung für virtuelle Maschinen erst konfiguriert, wenn diese ausgeschaltet werden. |

- 2 Zum Aktivieren der View-Speicherbeschleunigung für den Pool stellen Sie sicher, dass das Kontrollkästchen **View-Speicherbeschleunigung verwenden** aktiviert ist.  
  
Diese Einstellung ist standardmäßig ausgewählt. Zum Deaktivieren der Einstellung heben Sie die Markierung des Kontrollkästchens **View-Speicherbeschleunigung verwenden** auf.
- 3 (Optional) Geben Sie an, welche Festplattentypen im Cache gespeichert werden sollen. Wählen Sie dazu im Menü **Festplattentypen** die Option **Betriebssystemfestplatten** oder **Betriebssystem- und persistente Festplatten** aus.

Die Option **Betriebssystemfestplatten** ist standardmäßig ausgewählt.

Wenn Sie die View-Speicherbeschleunigung für vollständige virtuelle Maschinen konfigurieren, können Sie keinen Festplattentyp auswählen. Die View-Speicherbeschleunigung wird auf der gesamten virtuellen Maschine ausgeführt.

- 4 (Optional) Geben Sie im Textfeld **Speicherbeschleunigung neu generieren nach** das Intervall in Tagen an, nach dem die Neugenerierung der Digest-Dateien für die View-Speicherbeschleunigung erfolgen soll.

Das standardmäßige Intervall für die Neugenerierung lautet sieben Tage.

## Nächste Schritte

Sie können Ausfalltage und -zeiten festlegen, an denen keine Zurückgewinnung von Datenträgerplatz und keine Neugenerierung der View-Speicherbeschleunigung erfolgt. Siehe [Festlegen von Ausfallzeiten für ESXi-Vorgänge auf View-VMs](#).

## Rückgewinnung von Festplattenspeicherplatz auf virtuellen Linked-Clone-Maschinen

In vSphere 5.1 und höher können Sie die Funktion zur Rückgewinnung von Datenträgerplatz für Linked-Clone-Desktop-Pools konfigurieren. Ab der 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 ihren Desktops interagieren, nimmt die Größe der Betriebssystemfestplatte der Klone zu und kann schließlich fast so viel Festplattenspeicherplatz belegen wie virtuelle Full-Clone-Maschinen. 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 Desktops interagieren.

In View Administrator können Sie nicht direkt die Rückgewinnung von Datenträgerplatz für einen Pool initiieren. Sie legen fest, wann View die Rückgewinnung von Datenträgerplatz initiiert, indem Sie die Mindestmenge an ungenutztem Festplattenspeicherplatz angeben, der sich auf einer Linked-Clone-Betriebssystemfestplatte ansammeln muss, um den Vorgang auszulösen. Wenn der ungenutzte Festplattenspeicherplatz den angegebenen Grenzwert überschreitet, weist View den ESXi-Host an, Speicherplatz auf der Betriebssystemfestplatte zurückzugewinnen. View wendet den Grenzwert auf jede virtuelle Maschine im Pool an.

Sie können die Option `vdmadmin -M` verwenden, um die Rückgewinnung von Datenträgerplatz auf einer bestimmten virtuellen Maschine für Demonstrations- oder Fehlerbehebungszwecke zu initiieren. Weitere Informationen finden Sie im Dokument *View*.

Sie können die Rückgewinnung von Datenträgerplatz auf verknüpften Klonen konfigurieren, wenn Sie einen neuen Pool erstellen oder einen vorhandenen Pool bearbeiten. Weitere Informationen zur Vorgehensweise bei vorhandenen Pools finden Sie unter „Aufgaben für die Aktualisierung von Pools, um Speicherplatzrückgewinnung zu gewinnen“ im Dokument „Upgrades von View“.

Wenn View Composer verknüpfte Klone aktualisiert, neu zusammenstellt oder neu verteilt, findet auf diesen verknüpften Klonen keine Rückgewinnung von Datenträgerplatz statt.

Sie funktioniert nur auf Betriebssystemfestplatten in verknüpften Klonen. Diese Funktion wirkt sich nicht auf persistente View Composer-Festplatten aus und funktioniert nicht auf virtuellen Full-Clone-Maschinen.

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

### Voraussetzungen

- Stellen Sie sicher, dass Ihr vCenter Server und die ESXi-Hosts, einschließlich aller ESXi-Hosts in einem Cluster, in der Version 5.1 mit ESXi 5.1-Download-Patch ESXi510-201212001 oder höher vorliegen.
- Überprüfen Sie, dass VMware Tools, die mit vSphere Version 5.1 oder höher geliefert werden, auf allen virtuellen Linked-Clone-Maschinen im Pool installiert sind.
- Überprüfen Sie, ob alle virtuellen Linked-Clone-Maschinen im Pool die virtuelle Hardwareversion 9 oder höher aufweisen.
- Überprüfen Sie, dass die virtuellen Maschinen SCSI-Controller verwenden. Die Rückgewinnung von Datenträgerplatz wird auf virtuellen Maschinen mit IDE-Controllern nicht unterstützt.

- Überprüfen Sie bei virtuellen Maschinen unter Windows 8 oder 8.1, ob diese Maschinen in vSphere 5.5 oder höher ausgeführt werden. Die Rückgewinnung von Festplattenspeicherplatz wird von virtuellen Maschinen unter Windows 8 oder 8.1 mit vSphere 5.5 oder höher unterstützt.
- Überprüfen Sie bei virtuellen Maschinen unter Windows 7 oder Windows XP, ob diese Maschinen in vSphere 5.1 oder höher ausgeführt werden.
- Stellen Sie sicher, dass die Rückgewinnung von Datenträgerplatz in vCenter Server aktiviert ist. Diese Option sorgt dafür, dass die virtuellen Maschinen im Pool in dem effizienten Festplattenformat erstellt werden, das für die Rückgewinnung von Datenträgerplatz erforderlich ist. Weitere Informationen finden Sie im Dokument *View*.

## Verfahren

- 1 Öffnen Sie in View Administrator die Seite **Erweiterter Speicher**.

| Option                          | Beschreibung   |
|---------------------------------|--|
| <b>Neuer Desktop-Pool</b>       | Starten Sie den Assistenten zum Hinzufügen von Desktop-Pools, um mit der Erstellung eines automatisierten Desktop-Pools zu beginnen. Befolgen Sie die Eingabeaufforderungen des Assistenten, bis Sie zur Seite <b>Erweiterter Speicher</b> gelangen.   |
| <b>Vorhandener Desktop-Pool</b> | Wählen Sie den vorhandenen Pool aus, klicken Sie auf <b>Bearbeiten</b> und anschließend auf die Registerkarte <b>Erweiterter Speicher</b> . Weitere Informationen zum Aktualisieren eines Pools, damit dieser die Rückgewinnung von Speicherplatz unterstützt, finden Sie unter „Upgrade von Desktop-Pools für die Rückgewinnung von Speicherplatz“ im Dokument „Upgrades von View“. |

- 2 Aktivieren Sie das Kontrollkästchen **VM-Datenträgerplatz zurückgewinnen**.
- 3 Geben Sie im Textfeld **Zurückgewinnung initiieren, wenn der nicht belegte Speicherplatz auf der VM größer ist als** die Mindestmenge an ungenutztem Festplattenspeicherplatz in Gigabyte ein, der sich auf einer Linked-Clone-Betriebssystemfestplatte ansammeln muss, bevor ESXi beginnt, Speicherplatz auf der Festplatte zurückzugewinnen.

Beispiel: 2 GB.

Der Standardwert ist 1 GB.

## Nächste Schritte

Sie können Ausfalltage und -zeiten festlegen, an denen keine Rückgewinnung von Festplattenspeicherplatz und keine Neugenerierung für die View-Speicherbeschleunigung erfolgt. Siehe [Festlegen von Ausfallzeiten für ESXi-Vorgänge auf View-VMs](#).

Sie können in View Administrator die Option **Katalog > Desktop-Pools** und dann einen Computer auswählen, um anzuzeigen, wann die letzte Rückgewinnung von Speicherplatz erfolgte und welche Menge an Speicherplatz auf diesem Computer zurückgewonnen wurde.



## Verwenden der View Composer Array Integration mit systemeigener NFS-Snapshot-Technologie (VAAI)

Wenn Ihre Bereitstellung NAS-Geräte umfasst, die die vStorage APIs for Array Integration (VAAI) unterstützen, können Sie die View Composer Array Integration-Funktion (VCAI) auf Linked-Clone-Pools aktivieren. Diese Funktion nutzt die systemeigene NFS-Snapshot-Technologie zum Klonen virtueller Maschinen.

Mit dieser Technologie kloniert das NFS-Festplatten-Array die Dateien der virtuellen Maschine, ohne dass der ESXi-Host die Daten lesen oder schreiben muss. Dieser Vorgang kann die Zeit und die Netzwerkbelastung beim Klonen von virtuellen Maschinen verringern.

Befolgen Sie beim Verwenden der nativen NFS-Snapshot-Technologie folgende Anweisungen:

- Sie können diese Funktion nur dann verwenden, wenn Sie Desktop-Pools auf Datenspeichern konfigurieren, die sich auf NAS-Geräten befinden, die über VAAI systemeigene Klonvorgänge unterstützen.
- Sie können Funktionen von View Composer verwenden, um verknüpfte Klone zu verwalten, die durch native NFS-Snapshot-Technologie erstellt wurden. So können Sie beispielsweise persistente Festplatten aktualisieren, neu zusammenstellen, neu verteilen und erstellen und QuickPrep-Anpassungsskripts auf diesen Klone ausführen.
- Sie können diese Funktion nicht verwenden, wenn Sie Replikate und Betriebssystemfestplatten in separaten Datenspeichern speichern.
- Diese Funktion wird unter vSphere 5.0 und höher unterstützt.
- Wenn Sie einen Pool bearbeiten oder die native NFS-Klonfunktion auswählen oder deren Auswahl aufheben, hat dies keinen Einfluss auf vorhandene virtuelle Maschinen.

Um bei vorhandenen virtuellen Maschinen aus nativen NFS-Klonen herkömmliche Redo-Protokollklone zu machen, müssen Sie die Auswahl der nativen NFS-Klonfunktion aufheben und den Pool zu einem neuen Basisimage neu zusammenstellen. Um die Klonmethode für alle virtuellen Maschinen in einem Pool zu ändern und einen anderen Datenspeicher zu verwenden, müssen Sie einen neuen Datenspeicher auswählen, die Auswahl der nativen NFS-Klonfunktion aufheben, den Pool auf den neuen Datenspeicher neu verteilen und den Pool auf ein neues Basisimage neu zusammenstellen.

Auf ähnliche Weise müssen Sie, wenn Sie bei virtuellen Maschinen aus herkömmlichen Redo-Protokollklonen native NFS-Klone machen möchten, einen NAS-Datenspeicher auswählen, der VAAI unterstützt, die native NFS-Klonfunktion auswählen, den Pool auf den neuen Datenspeicher neu verteilen und den Pool neu zusammenstellen.

- In einem ESXi-Cluster müssen Sie zur Konfiguration systemeigener Klonvorgänge auf einem ausgewählten NFS-Datenspeicher in View Administrator ggf. anbieterspezifische NAS-Plug-ins installieren, die systemeigene Klonvorgänge auf VAAI auf allen ESXi-Hosts im Cluster unterstützen. Schlagen Sie in der Dokumentation des Speicheranbieters nach, um Informationen zu den Konfigurationsanforderungen zu erhalten.

- Die systemeigene NFS-Snapshot-Technologie (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.
- Im VMware Knowledgebase-Artikel 2061611 finden Sie Antworten auf häufig gestellte Fragen zur VCAI-Unterstützung in View.

---

**Wichtig** NAS-Speicheranbieter bieten eventuell zusätzliche Einstellungen an, die sich auf die Leistung und den Betrieb von VAAI auswirken können. Sie sollten die Empfehlungen des Anbieters beachten und die entsprechenden Einstellungen im NAS-Speicher-Array und auf ESXi vornehmen. Schlagen Sie in der Dokumentation des Speicheranbieters nach, um Informationen zu den vom Anbieter empfohlenen Konfigurationseinstellungen zu erhalten.

---

## Festlegen von Ausfallzeiten für ESXi-Vorgänge auf View-VMs

Das Neugenerieren von Digest-Dateien für die View-Speicherbeschleunigung und die Rückgewinnung von Datenträgerplatz virtueller Maschinen kann ESXi-Ressourcen kosten. Um sicherzustellen, dass ESXi-Ressourcen bei Bedarf für im Vordergrund ausgeführte Aufgaben verwendet werden, können Sie festlegen, dass ESXi-Hosts diese Aufgaben an bestimmten Tagen in bestimmten Zeiträumen nicht ausführen.

So können Sie z. B. eine Ausfallzeit während der frühen Morgenstunden an Werktagen festlegen, wenn Benutzer ihre Arbeit beginnen und Startüberlastungen und Überlastungen durch Antiviren-E/A stattfinden. Sie können verschiedene Sperrzeiten an verschiedenen Tagen festlegen.

Während der von Ihnen festgelegten Ausfallzeiten erfolgt keine Neugenerierung der Digest-Datei für die Rückgewinnung von Datenträgerplatz und View-Speicherbeschleunigung. Sie können für jeden Vorgang separate Ausfallzeiten festlegen.

View erlaubt während der Bereitstellungsphase das Erstellen von Digest-Dateien für die View-Speicherbeschleunigung für neue Computer, auch wenn eine Ausfallzeit gilt.

### Voraussetzungen

- Überprüfen Sie, dass **View-Speicherbeschleunigung aktivieren, Zurückgewinnung von Datenträgerplatz** oder beide Funktionen für vCenter Server ausgewählt sind.
- Überprüfen Sie, dass **View-Speicherbeschleunigung verwenden, VM-Datenträgerplatz zurückgewinnen** oder beide Funktionen für den Desktop-Pool ausgewählt sind.

## Verfahren

- 1 Wechseln Sie im Assistenten „Desktop-Pool hinzufügen“ auf der Seite **Erweiterter Speicher** zu **Ausfallzeiten** und klicken Sie auf **Hinzufügen**.

Wenn Sie einen vorhandenen Pool bearbeiten, klicken Sie auf die Registerkarte **Erweiterter Speicher**.

- 2 Überprüfen Sie die Sperrtage, und geben Sie Start- und Endzeiten an.

Bei der Zeitauswahl wird eine Uhr mit 24 Stunden verwendet. So steht 10:00 für 10 Uhr morgens und 22:00 für 10 Uhr abends.

- 3 Klicken Sie auf **OK**.
- 4 Um eine weitere Sperrzeit hinzuzufügen, klicken Sie auf **Hinzufügen** und geben einen anderen Zeitraum an.
- 5 Um eine Sperrzeit zu ändern oder zu entfernen, wählen Sie den Zeitraum in der Liste „Sperrzeiten“ aus, und klicken Sie auf **Bearbeiten** oder **Entfernen**.

# Konfigurieren von Richtlinien für Desktop- und Anwendungspools

# 16

Sie können Richtlinien konfigurieren, um das Verhalten von Desktop- und Anwendungspools, Computern und Benutzern zu steuern. Sie können mithilfe von View Administrator Richtlinien für Clientsitzungen festlegen. Sie können über Active Directory-Gruppenrichtlinieneinstellungen das Verhalten von View Agent, Horizon Client für Windows und Funktionen steuern, die sich auf einzelne Benutzer-Computer, auf RDS-Hosts oder auf das PCoIP-Anzeigeprotokoll auswirken.

Dieses Kapitel enthält die folgenden Themen:

- [Festlegen von Richtlinien in View Administrator](#)
- [Verwenden von Active Directory-Gruppenrichtlinien](#)
- [Verwenden von administrativen Vorlagendateien für Gruppenrichtlinien \(ADM\) für View](#)
- [ADM- und ADMX-Vorlagendateien für View](#)
- [ADM-Vorlageneinstellungen für die View Agent-Konfiguration](#)
- [ADM-Vorlageneinstellungen für View-PCoIP-Sitzungsvariablen](#)
- [Verwenden von Gruppenrichtlinien für Remote-Desktop-Dienste](#)
- [Einrichten des standortbasierten Druckens](#)
- [Beispiel einer Active Directory-Gruppenrichtlinie](#)

## 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 Clientsitzungsbutzer angewendet werden. Richtlinien, die für bestimmte Benutzer und Desktop-Pools gelten, werden als Richtlinien auf Benutzer- und Desktop-Pool-Ebene bezeichnet. Richtlinien, die sich auf alle Sitzungen und Benutzer auswirken, werden als globale Richtlinien bezeichnet.

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

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

## 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. Richtlinienereinstellungen auf Benutzerebene haben immer Vorrang vor äquivalenten globalen Richtlinienereinstellungen und Richtlinienereinstellungen 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 Richtlinienereinstellungen. Wenn eine Einstellung von der äquivalenten globalen Richtlinie vererbt wird, wird in der Spalte **Desktop-Poolrichtlinie** der Wert **Vererben** angezeigt.
- 3 Klicken Sie auf **Benutzeraußerkraftsetzung** 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 16-1. View-Richtlinien](#) beschreibt alle View-Richtlinieneinstellungen.

**Tabelle 16-1. View-Richtlinien**

| <b>Richtlinie</b>            | <b>Beschreibung</b>  |
|------------------------------|--|
| 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 <b>Verweigern</b>.</p> <p>Wenn Clientsysteme über unzureichende Ressourcen zum Verarbeiten der lokalen Multimedia-Decodierung verfügen, lassen Sie die Einstellung auf <b>Verweigern</b>.</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 <b>Zulassen</b>. Um aus Sicherheitsgründen die Verwendung externer Geräte zu unterbinden, ändern Sie die Einstellung in <b>Verweigern</b>.</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 <b>Zulassen</b>, mit dem Prioritätswert <b>Mittel</b>.</p>  |

## Verwenden von Active Directory-Gruppenrichtlinien

Sie können Microsoft Windows-Gruppenrichtlinien dazu verwenden, Ihre Remote-Desktops zu optimieren und zu schützen, das Verhalten der View-Komponenten zu steuern und den standortbasierten Druck zu konfigurieren.

Gruppenrichtlinien sind eine Funktion der Microsoft Windows-Betriebssysteme, die eine zentrale Verwaltung und Konfiguration von Computern und Remote-Benutzern in einer Active Directory-Umgebung ermöglichen.

Gruppenrichtlinieneinstellungen sind in Entitäten enthalten, die als GPOs (Group Policy Objects, Gruppenrichtlinienobjekte) bezeichnet werden. GPOs sind mit Active Directory-Objekten verknüpft. GPOs können auf Domänenebene auf View-Komponenten angewendet werden, um verschiedene Bereiche der View-Umgebung zu steuern. Nach der Aktivierung von GPOs werden GPO-Einstellungen in der lokalen Windows-Registrierung der betreffenden Komponente gespeichert.

Zur Verwaltung von Gruppenrichtlinieneinstellungen verwenden Sie den Gruppenrichtlinienobjekt-Editor von Microsoft Windows. Der Gruppenrichtlinienobjekt-Editor ist ein MMC-Snap-In (Microsoft Management Console). Die MMC ist Bestandteil der Gruppenrichtlinien-Verwaltungskonsolle von Microsoft. Informationen zu Installation und Verwendung der Gruppenrichtlinien-Verwaltungskonsolle finden Sie auf der Microsoft TechNet-Website.

## Erstellen einer OU für Remote-Desktops

Sie sollten in Active Directory eine Organisationseinheit (OU) speziell für Ihre Remote-Desktops erstellen.

Um zu verhindern, dass Gruppenrichtlinieneinstellungen auf andere Windows-Server oder -Arbeitsstationen in derselben Domäne wie Ihre Remote-Desktops angewendet werden, erstellen Sie ein Gruppenrichtlinienobjekt für Ihre View-Gruppenrichtlinien und verknüpfen es mit der OU, die Ihre Remote-Desktops enthält.

Informationen zum Erstellen von OUs und GPOs finden Sie in der Microsoft Active Directory-Dokumentation auf der Microsoft TechNet-Website.

## Aktivieren der Loopback-Verarbeitung für Remote-Desktops

Standardmäßig stammen die Richtlinieneinstellungen für einen Benutzer aus einem Satz an Gruppenrichtlinienobjekten (Group Policy Objects, GPOs), die in Active Directory auf das Benutzerobjekt angewendet werden. In der View-Umgebung jedoch sollten GPOs basierend auf dem Computer angewendet werden, bei dem sich der Benutzer anmeldet.

Wenn Sie die Loopback-Verarbeitung aktivieren, wird ein konsistenter Richtliniensatz auf alle Benutzer angewendet, die sich an einem bestimmten Computer anmelden – unabhängig von ihrer Position in Active Directory.

Informationen zum Aktivieren der Loopback-Verarbeitung finden Sie in der Dokumentation zu Microsoft Active Directory.

---

**Hinweis** Die Loopback-Verarbeitung ist nur ein Ansatz bei der Verarbeitung von GPOs in View. Sie müssen möglicherweise einen anderen Ansatz implementieren.

---

## 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 16-2. 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.<br><br>Siehe <a href="#">ADM-Vorlageneinstellungen für die View Agent-Konfiguration</a> .   |
| Horizon Client-Konfiguration  | vdm_client.adm | Enthält Richtlinieneinstellungen in Bezug auf Horizon Client für Windows.<br><br>Auf Clients, die von außerhalb der View-Verbindungsserver-Hostdomäne eine Verbindung herstellen, wirken sich die auf Horizon Client angewendeten Richtlinien nicht aus.<br><br>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.<br><br>Weitere Informationen finden Sie im Dokument <i>Verwaltung von View</i> .   |
| Allgemeine View-Konfiguration | vdm_common.adm | Enthält Richtlinieneinstellungen, die für alle View-Komponenten gelten.<br><br>Weitere Informationen finden Sie im Dokument <i>Verwaltung von View</i> .   |
| View-PCoIP-Sitzungsvariablen  | pcoip.adm      | Enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll.<br><br>Siehe <a href="#">ADM-Vorlageneinstellungen für View-PCoIP-Sitzungsvariablen</a> .  |

| 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.<br><br>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.<br><br>Siehe <a href="#">Gruppenrichtlinieneinstellungen für View Persona Management</a> .  |
| View-Remotedesktopdienste              | vmware_rdsh.admx<br>vmware_rdsh_server.admx | Enthält Richtlinieneinstellungen in Bezug auf Remotedesktopdienste.<br><br>Siehe <a href="#">Verwenden von Gruppenrichtlinien für Remote-Desktop-Dienste</a> .   |
| Konfiguration von Echtzeit-Audio/Video | vdm_agent_rtav.adm                          | Enthält Richtlinieneinstellungen in Bezug auf Webcams, die zusammen mit der Echtzeit-Audio/Video-Funktion verwendet werden.<br><br>Siehe <a href="#">Gruppenrichtlinieneinstellungen für Echtzeit-Audio/Video</a> .                          |
| Scannerumleitung                       | vdm_agent_scanner.adm                       | Enthält Richtlinieneinstellungen in Bezug auf Scangeräte, die zur Verwendung mit Remote-Desktops und Remote-Anwendungen umgeleitet werden.<br><br>Siehe <a href="#">Gruppenrichtlinieneinstellungen für Scannerumleitung</a> .               |

## ADM-Vorlageneinstellungen für die View Agent-Konfiguration

Die ADM-Vorlagendatei (vdm\_agent.adm) für die View Agent-Konfiguration enthält Richtlinieneinstellungen in Bezug auf die Authentifizierung und die Umgebungskomponenten von View Agent.

Diese ADM-Datei steht in einer mitgelieferten .zip-Datei namens VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyy.zip zur Verfügung, die Sie von der Download-Site VMware Horizon (mit View) unter <http://www.vmware.com/go/downloadview> herunterladen können.

Die folgende Tabelle beschreibt Richtlinieneinstellungen in der ADM-Vorlagendatei für die View Agent-Konfiguration, die von den mit USB-Geräten verwendeten Einstellungen abweichen. Die Vorlage enthält sowohl Einstellungen für die Computerkonfiguration als auch Einstellungen für die Benutzerkonfiguration. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

**Tabelle 16-3. Vorlageneinstellungen für die View Agent-Konfiguration**

| Einstellung               | Computer | Benutzer | Eigenschaften   |
|---------------------------|----------|----------|---|
| AllowDirectRDP            | X        |          | <p>Legt fest, ob sich andere Clients außer Horizon Client-Geräten über RDP direkt mit View-Desktops verbinden können. Ist diese Einstellung deaktiviert, lässt View Agent nur View-verwaltete Verbindungen über Horizon Client zu.</p> <p>Wenn Sie die Verbindung zu einem Remote-Desktop über Horizon Client für Mac OS X herstellen, deaktivieren Sie nicht die Einstellung AllowDirectRDP. Wenn diese Einstellung deaktiviert ist, schlägt die Verbindungsherstellung mit einem Fehler vom Typ Access is denied (Zugriff verweigert) fehl.</p> <p>Standardmäßig können Sie RDP verwenden, um eine Verbindung zur virtuellen Maschine von außerhalb von View herzustellen, während ein Benutzer bei einer View-Desktopsitzung angemeldet ist. Die RDP-Verbindung beendet die View-Desktopsitzung und die nicht gespeicherten Daten und Einstellungen des View-Benutzers gehen u. U. verloren. Der View-Benutzer kann sich erst dann am Desktop anmelden, wenn die externe RDP-Verbindung beendet wurde. Deaktivieren Sie die Einstellung AllowDirectRDP, um diese Situation zu vermeiden.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p> |
| AllowSingleSignon         | X        |          | <p>Legt fest, ob zur Verbindungsherstellung mit View-Desktops die einmalige Anmeldung (Single Sign-On, SSO) zulässig ist. Bei Aktivierung dieser Einstellung werden Benutzer nur dann zur Eingabe ihrer Anmeldeinformationen aufgefordert, wenn sie eine Verbindung mit Horizon Client herstellen. Ist diese Einstellung deaktiviert, müssen sich die Benutzer beim Herstellen einer Remote-Verbindung erneut authentifizieren.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>   |
| CommandsToRunOnConnect    | X        |          | <p>Gibt eine Liste mit Befehlen oder Befehlsskripts an, die bei der ersten Verbindungsherstellung ausgeführt werden.</p> <p>Weitere Informationen finden Sie unter <a href="#">Ausführen von Befehlen auf View-Desktops</a>.</p>  |
| CommandsToRunOnDisconnect | X        |          | <p>Gibt eine Liste mit Befehlen oder Befehlsskripts an, die ausgeführt werden, wenn eine Sitzung getrennt wird.</p> <p>Weitere Informationen finden Sie unter <a href="#">Ausführen von Befehlen auf View-Desktops</a>.</p>   |
| CommandsToRunOnReconnect  | X        |          | <p>Gibt eine Liste mit Befehlen oder Befehlsskripts an, die ausgeführt werden, wenn eine Sitzung nach einer Verbindungstrennung wiederhergestellt wird.</p> <p>Weitere Informationen finden Sie unter <a href="#">Ausführen von Befehlen auf View-Desktops</a>.</p>   |

| Einstellung                       | Computer | Benutzer | Eigenschaften   |
|-----------------------------------|----------|----------|---|
| Connect using DNS Name            | X        |          | <p>Legt fest, ob View-Verbindungsserver beim Herstellen der Verbindung anstelle der IP-Adresse des Hosts den DNS-Namen verwendet. Diese Einstellung ist häufig in einer NAT- oder Firewall-Umgebung aktiviert, wenn Horizon Client oder View-Verbindungsserver die IP-Adresse des Remote-Desktops nicht direkt verwenden kann.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>  |
| ConnectionTicketTimeout           | X        |          | <p>Gibt die Gültigkeitsdauer des View-Verbindungstickets in Sekunden an.</p> <p>Horizon Client-Geräte verwenden bei der Verbindungsherstellung mit View Agent zur Überprüfung und für die einmalige Anmeldung ein Verbindungsticket. Ein Verbindungsticket ist aus Sicherheitsgründen nur für einen begrenzten Zeitraum gültig. Wenn ein Benutzer eine Verbindung zu einem View-Desktop herstellt, muss die Authentifizierung innerhalb des Gültigkeitszeitraums des Verbindungstickets erfolgen, ansonsten wird die Sitzung aufgrund einer Zeitüberschreitung beendet.</p> <p>Wenn diese Einstellung nicht konfiguriert ist, beträgt die standardmäßige Dauer bis zur Zeitüberschreitung 900 Sekunden.</p> |
| CredentialFilterExceptions        | X        |          | <p>Gibt die ausführbaren Dateien an, die nicht zum Laden des CredentialFilter-Agenten berechtigt sind. Dateinamen dürfen weder einen Pfad noch ein Suffix enthalten. Verwenden Sie ein Semikolon zum Trennen mehrerer Dateinamen.</p>   |
| Disable Time Zone Synchronization | X        | X        | <p>Legt fest, ob die Zeitzone des View-Desktops mit der des verbundenen Clients synchronisiert wird. Diese Einstellung wird bei Aktivierung nur angewendet, wenn die Einstellung Zeitzonenweiterleitung deaktivieren der Richtlinie für die Horizon Client-Konfiguration nicht auf „Deaktiviert“ gesetzt wurde.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>   |
| Enable multi-media acceleration   | X        |          | <p>Legt fest, ob die Multimedia-Umleitung (Multimedia Redirection, MMR) auf dem View-Desktop aktiviert ist.</p> <p>MMR ist ein Microsoft DirectShow-Filter, der Multimediadaten von bestimmten Codecs auf dem Remote-System direkt über einen TCP-Socket an den Client weiterleitet. Die Daten werden direkt auf dem Client decodiert, auf dem sie wiedergegeben werden. Sie können MMR deaktivieren, wenn der Client nicht genügend Ressourcen hat, um eine lokale Multimedia-Decodierung durchzuführen.</p> <p>MMR funktioniert nicht ordnungsgemäß, wenn die Horizon Client-Hardware zur Videoanzeige keine Overlay-Unterstützung bietet.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>      |

| Einstellung                                    | Computer | Benutzer | Eigenschaften   |
|--|----------|----------|---|
| Enable system tray redirection for Hosted Apps | X        |          | <p>Legt fest, ob die Infobereich-Umleitung aktiviert ist, wenn ein Benutzer Remote-Anwendungen ausführt.</p> <p>Diese Einstellung befindet sich im Ordner <b>VMware View Agent Configuration &gt; Unity Touch and Hosted Apps</b> im Gruppenrichtlinienverwaltungs-Editor.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>  |
| Enable Unity Touch                             | X        |          | <p>Legt fest, ob die Unity Touch-Funktionalität auf dem View-Desktop aktiviert ist. Unity Touch unterstützt das Bereitstellen von Remote-Anwendungen in View und ermöglicht den Benutzern mobiler Geräte den Zugriff auf Anwendungen in der Unity Touch-Sidebar.</p> <p>Diese Einstellung befindet sich im Ordner <b>VMware View Agent Configuration &gt; Unity Touch and Hosted Apps</b> im Gruppenrichtlinienverwaltungs-Editor.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>  |
| Force MMR to use software overlay              | X        |          | <p>Legt fest, ob die MMR-Funktion (Multimedia Redirection) anstelle eines Hardware-Overlays ein Software-Overlay verwendet.</p> <p>Zur Optimierung der Leistung verwendet MMR Videoanzeige-Hardware mit Overlay-Unterstützung. Da Hardware-Overlays bei einem Multi-Monitor-System im Allgemeinen nur auf dem primären Monitor verwendet werden, funktioniert die Videoanzeige nicht, wenn sie vom primären Monitor auf einen sekundären Monitor gezogen wird.</p> <p>Durch Aktivierung dieser Einstellung wird MMR gezwungen, ein Software-Overlay auf allen Monitoren zu verwenden.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p> |
| ShowDiskActivityIcon                           | X        |          | Diese Einstellung wird in der vorliegenden Version nicht unterstützt.   |
| Toggle Display Settings Control                | X        |          | <p>Legt fest, ob die Registerkarte <b>Einstellungen</b> unter <b>Anzeige</b> in der Systemsteuerung deaktiviert werden soll, wenn eine Clientsitzung das PCoIP-Anzeigeprotokoll verwendet.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>  |

## USB-Einstellungen für View Agent

Siehe [USB-Einstellungen in der ADM-Vorlage für die View Agent-Konfiguration](#).

## An View-Desktops gesendete Clientsysteminformationen

Wenn Benutzer sich mit einem View-Desktop verbinden oder erneut verbinden, ruft Horizon Client Informationen zum Clientsystem ab und der View-Verbindungsserver sendet diese Informationen an den Remote-Desktop.

View Agent schreibt die Clientcomputerinformationen in den Systemregistrierungspfad HKCU\Volatile Environment auf Remote-Desktops, die auf Computern für Einzelbenutzer bereitgestellt sind.

Bei Remote-Desktops, die in RDS-Sitzungen bereitgestellt sind, schreibt View Agent die Clientcomputerinformationen in den Systemregistrierungspfad HKCU\Volatile Environment\x, wobei x die Sitzungs-ID auf dem RDS-Host ist.

Sie können den View Agent-Gruppenrichtlinieneinstellungen `CommandsToRunOnConnect`, `CommandsToRunOnReconnect` und `CommandsToRunOnDisconnect` Befehle hinzufügen, um Befehle oder Befehlsskripts auszuführen, die diese Informationen aus der Systemregistrierung lesen, wenn sich Benutzer mit Desktops verbinden oder erneut verbinden. Weitere Informationen finden Sie unter [Ausführen von Befehlen auf View-Desktops](#).

**Tabelle 16-4. Clientsysteminformationen** beschreibt die Registrierungsschlüssel, die Clientsysteminformationen enthalten, und listet die Arten von Clientsystemen auf, die diese unterstützen.

**Tabelle 16-4. Clientsysteminformationen**

| Registrierungsschlüssel        | Beschreibung   | Unterstützte Desktops                    | Unterstützte Client-Systeme  |
|--------------------------------|--|--|--|
| ViewClient_IP_Address          | Die IP-Adresse des Clientsystems.                                    | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro   |
| ViewClient_MAC_Address         | Die MAC-Adresse des Clientsystems.                                   | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac, Android   |
| ViewClient_Machine_Name        | Der Computername des Clientsystems.                                  | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro   |
| ViewClient_Machine_Domain      | Die Domäne des Clientsystems.  | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Metro   |
| ViewClient_LoggedOn_Username   | Der Benutzername, der zur Anmeldung am Clientsystem verwendet wurde. | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac  |
| ViewClient_LoggedOn_Domainname | Der Domänenname, der zur Anmeldung am Clientsystem verwendet wurde.  | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Metro<br>Informationen zu Linux- und Mac-Clients finden Sie unter <code>ViewClient_Machine_Domain</code> .<br><code>ViewClient_LoggedOn_Domainname</code> wird vom Linux- bzw. Mac-Client nicht bereitgestellt, da Linux- bzw. Mac-Konten nicht an Windows-Domänen gebunden sind. |
| ViewClient_Type                | Der Thin Client-Name oder Betriebssystemtyp des Clientsystems.       | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro   |

| Registrierungsschlüssel             | Beschreibung  | Unterstützte Desktops                    | Unterstützte Client-Systeme  |
|-------------------------------------|---|--|--|
| ViewClient_Broker_DNS_Name          | Der DNS-Name der View-Verbindungsserver-Instanz.  | VDI (Computer für Einzelbenutzer)<br>RDS | Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben. |
| ViewClient_Broker_URL               | Die URL der View-Verbindungsserver-Instanz.   | VDI (Computer für Einzelbenutzer)<br>RDS | Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben. |
| ViewClient_Broker_Tunnel            | Der Status der Tunnelverbindung für View-Verbindungsserver, der entweder true (aktiviert) oder false (deaktiviert) lauten kann.   | VDI (Computer für Einzelbenutzer)<br>RDS | Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben. |
| ViewClient_Broker_Tunnel_URL        | Die URL der View-Verbindungsserver-Tunnelverbindung, wenn die Tunnelverbindung aktiviert ist.   | VDI (Computer für Einzelbenutzer)<br>RDS | Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben. |
| ViewClient_Broker_Remote_IP_Address | Die IP-Adresse des Clientsystems, die der View-Verbindungsserver-Instanz angezeigt wird.  | VDI (Computer für Einzelbenutzer)<br>RDS | Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben. |
| ViewClient_TZID                     | Die Olson-Zeitzone-ID.<br>Zum Deaktivieren der Zeitzonensynchronisierung aktivieren Sie die View Agent-Gruppenrichtlinieneinstellung Disable Time Zone Synchronization. | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac, Android, iOS  |
| ViewClient_Windows_Timezone         | Die GMT-Normalzeit.<br>Zum Deaktivieren der Zeitzonensynchronisierung aktivieren Sie die View Agent-Gruppenrichtlinieneinstellung Disable Time Zone Synchronization.    | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Metro   |
| ViewClient_Broker_DomainName        | Zur Authentifizierung beim View-Verbindungsserver verwendeter Domänenname.  | VDI (Computer für Einzelbenutzer)<br>RDS | Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben. |
| ViewClient_Broker_UserName          | Zur Authentifizierung beim View-Verbindungsserver verwendeter Benutzername.   | VDI (Computer für Einzelbenutzer)<br>RDS | Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben. |
| ViewClient_Client_ID                | Gibt die eindeutige Client-Hardware-ID an, die als Link zum Lizenzschlüssel verwendet wird.   | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro   |
| ViewClient_Displays.Number          | Gibt die Anzahl an Monitoren an, die auf dem Client verwendet werden.   | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro   |

| Registrierungsschlüssel       | Beschreibung  | Unterstützte Desktops                    | Unterstützte Client-Systeme  |
|-------------------------------|---|--|--|
| ViewClient_Displays.Topology  | Gibt die Anordnung, Auflösung und Dimensionen von Anzeigen auf dem Client an.                           | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro   |
| ViewClient_Keyboard.Type      | Gibt den Tastaturtyp an, der auf dem Client verwendet wird. Beispiel: Japanisch, Koreanisch.            | VDI (Computer für Einzelbenutzer)<br>RDS | Windows  |
| ViewClient_Launch_SessionType | Gibt den Sitzungstyp an. Dabei kann es sich um eine Desktopsitzung oder eine Anwendungssitzung handeln. | VDI (Computer für Einzelbenutzer)<br>RDS | Der Wert wird direkt vom View-Verbindungsserver gesendet und nicht durch Horizon Client erhoben. |
| ViewClient_Mouse.Identifier   | Gibt den Typ der Maus an.   | VDI (Computer für Einzelbenutzer)<br>RDS | Windows  |
| ViewClient_Mouse.NumButtons   | Gibt die Anzahl der Tasten an, die von der Maus unterstützt werden.                                     | VDI (Computer für Einzelbenutzer)<br>RDS | Windows  |
| ViewClient_Mouse.SampleRate   | Gibt in Berichten pro Sekunden die Rate an, in der Eingaben von einer PS/2-Maus aufgenommen werden.     | VDI (Computer für Einzelbenutzer)<br>RDS | Windows  |
| ViewClient_Protocol           | Gibt das verwendete Protokoll an.   | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro   |
| ViewClient_Language           | Gibt die Sprache des Betriebssystems an.  | VDI (Computer für Einzelbenutzer)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro   |
| ViewClient_Launch_ID          | Gibt die eindeutige Desktop-Pool-ID an.   | VDI (Computer für Einzelbenutzer)        | Windows, Linux, Mac, Android, iOS, Metro   |

**Hinweis** Die Definitionen von ViewClient\_LoggedOn\_Username und ViewClient\_LoggedOn\_Domainname in [Tabelle 16-4. Clientsysteminformationen](#) gelten für Horizon Client 2.2 für Windows und spätere Versionen.

Bei Horizon Client 5.4 für Windows und früheren Versionen sendet ViewClient\_LoggedOn\_Username den in Horizon Client eingegebenen Benutzernamen, und ViewClient\_LoggedOn\_Domainname sendet den Domänennamen, der in Horizon Client eingegeben wurde.

Horizon Client 2.2 für Windows ist eine spätere Version als Horizon Client 5.4 für Windows. Ab Horizon Client 2.2 stimmen die Versionsnummern für Windows mit den Horizon Client-Versionen auf anderen Betriebssystemen und Geräten überein.

## Ausführen von Befehlen auf View-Desktops

Sie können die View Agent-Gruppenrichtlinieneinstellungen CommandsToRunOnConnect, CommandsToRunOnReconnect und CommandsToRunOnDisconnect dazu verwenden, um Befehle und



Befehlsskripts auf View-Desktops auszuführen, wenn sich Benutzer verbinden, erneut verbinden oder ihre Verbindung trennen.

Um einen Befehl oder ein Befehlsskript auszuführen, fügen Sie den Befehlsnamen oder den Dateipfad des Skripts zur Liste der Befehle für die Gruppenrichtlinieneinstellung hinzu. Beispiel:

date

C:\Scripts\myscript.cmd

Um Skripts auszuführen, die einen Konsolenzugriff erfordern, stellen Sie die Option `-C` oder `-c` voran, gefolgt von einem Leerzeichen. Beispiel:

`-c C:\Scripts\Cli_clip.cmd`

`-C e:\procexp.exe`

Zu den unterstützten Dateitypen gehören `.CMD`, `.BAT` und `.EXE`. `.VBS`-Dateien werden erst nach einer Analyse mit `cscript.exe` oder `wscript.exe` ausgeführt. Beispiel:

`-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs`

Die Gesamtlänge der Zeichenfolge, einschließlich der Option `-C` oder `-c`, darf 260 Zeichen nicht überschreiten.

## ADM-Vorlageneinstellungen für View-PCoIP-Sitzungsvariablen

Die ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen (`pcoip.adm`) enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll. Sie können die Einstellungen entweder mit den Standardwerten konfigurieren, die durch einen Administrator außer Kraft gesetzt werden können, oder die Einstellungen mit nicht überschreibbaren Werten konfigurieren.

Diese ADM-Datei steht in einer mitgelieferten `.zip`-Datei namens `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip` zur Verfügung, die Sie von der Download-Site VMware Horizon (mit View) unter <http://www.vmware.com/go/downloadview> herunterladen können.

Die ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen enthält zwei Unterkategorien:

**Standardwerte, die durch einen Administrator außer Kraft gesetzt werden können**

Gibt Standardwerte für PCoIP-Sitzungsvariablen an. Diese Einstellungen können durch einen Administrator außer Kraft gesetzt werden. Für diese Einstellungen werden Werte in den Registrierungsschlüssel `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults` geschrieben.

**Einstellungen, die nicht durch einen Administrator außer Kraft gesetzt werden können**

Enthält dieselben Einstellungen wie die erste Unterkategorie, diese Einstellungen können jedoch von einem Administrator nicht außer Kraft gesetzt werden. Für diese Einstellungen werden Werte in den Registrierungsschlüssel `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin` geschrieben.

Die Vorlage enthält ausschließlich Einstellungen für die Computerkonfiguration.

## Nicht richtliniengesteuerte Registrierungsschlüssel

Wenn eine Einstellung auf einen lokalen Computer angewendet werden muss, die nicht in HKLM\Software\Policies\Teradici platziert werden kann, können die Einstellungen in Registrierungsschlüsseln unter HKLM\Software\Teradici eingefügt werden. In HKLM\Software\Teradici können dieselben Registrierungsschlüssel platziert werden wie in HKLM\Software\Policies\Teradici. Wenn ein Registrierungsschlüssel in beiden Verzeichnissen angegeben wurde, hat die Einstellung in HKLM\Software\Policies\Teradici Vorrang vor der Einstellung für den lokalen Computer.

## Allgemeine View-PCoIP-Sitzungsvariablen

Die ADM-Vorlagendatei für die View-PCoIP-Sitzungsvariablen enthält Gruppenrichtlinieneinstellungen, mit denen allgemeine Sitzungskriterien wie PCoIP-Bildqualität, USB-Geräte und Netzwerkports konfiguriert werden.

**Tabelle 16-5. Allgemeine View-PCoIP-Sitzungsvariablen**

| Einstellung                                    | Beschreibung   |
|--|--|
| Configure clipboard redirection                | <p>Bestimmt die Richtung, in der die Zwischenablagenumleitung zulässig ist. Sie können einen der folgenden Werte wählen:</p> <ul style="list-style-type: none"> <li>■ <b>Nur Client zu Agent aktiviert</b> (Dadurch ist der Kopier- und Einfügevorgang nur vom Clientsystem zum Remote-Desktop zulässig.)</li> <li>■ <b>In beide Richtungen deaktiviert</b></li> <li>■ <b>In beide Richtungen aktiviert</b></li> <li>■ <b>Nur Agent zu Client aktiviert</b> (Dadurch ist der Kopier- und Einfügevorgang nur vom Remote-Desktop zum Clientsystem zulässig.)</li> </ul> <p>Die Zwischenablageumleitung wird als virtueller Kanal implementiert. Wenn virtuelle Kanäle deaktiviert sind, funktioniert die Zwischenablageumleitung nicht.</p> <p>Diese Einstellung gilt nur für View Agent.</p> <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, lautet der Standardwert <b>Nur Client zu Agent aktiviert</b>.</p> |
| Configure PCoIP client image cache size policy | <p>Reguliert die Größe des PCoIP-Client-Bildcaches. Der Client verwendet die Bild-Zwischenspeicherung, um Teile der vorab übertragenen Anzeige zu speichern. Durch die Bild-Zwischenspeicherung wird die Menge der erneut übermittelten Daten minimiert.</p> <p>Diese Einstellung gilt nur für Windows- und Linux-Clients, wenn Horizon Client, View Agent und View-Verbindungsserver auf View 5.0 oder einer neueren Version basieren.</p> <p>Ist diese Einstellung nicht konfiguriert oder deaktiviert, verwendet PCoIP eine Standard-Clientbildcachegröße von 250 MB.</p> <p>Bei Aktivierung dieser Einstellung können Sie die Client-Bildcachegröße von mindestens 50 MB auf 300 MB konfigurieren. Der Standardwert ist 250MB.</p>   |

| Einstellung                                       | Beschreibung   |
|---|--|
| Configure PCoIP event log cleanup by size in MB   | <p>Aktiviert die Konfiguration der PCoIP-Ereignisprotokollbereinigung nach Größe in MB.</p> <p>Wenn diese Richtlinie konfiguriert ist, wird mit dieser Einstellung gesteuert, wie groß eine Protokolldatei vor der Bereinigung werden kann. Protokolldateien größer als <math>m</math> MB werden für eine Einstellung von <math>m</math> ungleich null automatisch und unbeaufsichtigt gelöscht. Die Einstellung 0 gibt an, dass keine Datei-Bereinigung nach Größe durchgeführt wird.</p> <p>Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, beträgt die standardmäßige Ereignisprotokollbereinigung nach Größe 100 MB.</p> <p>Die Bereinigung der Protokolldatei wird einmal beim Sitzungsstart durchgeführt. Eine Änderung an der Einstellung wird erst bei der nächsten Sitzung angewendet.</p> |
| Configure PCoIP event log cleanup by time in days | <p>Aktiviert die Konfiguration der PCoIP-Ereignisprotokollbereinigung nach Zeit in Tagen.</p> <p>Wenn die Richtlinie konfiguriert ist, wird mit dieser Einstellung gesteuert, wie viele Tage vergehen können, bevor die Protokolldatei bereinigt wird. Protokolldateien älter als <math>n</math> Tage werden für eine Einstellung von <math>n</math> ungleich null automatisch und unbeaufsichtigt gelöscht. Die Einstellung 0 gibt an, dass keine Datei-Bereinigung nach Zeit durchgeführt wird.</p> <p>Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, beträgt die standardmäßige Ereignisprotokollbereinigung 7 Tage.</p> <p>Die Bereinigung der Protokolldatei wird einmal beim Sitzungsstart durchgeführt. Eine Änderung an der Einstellung wird erst bei der nächsten Sitzung angewendet.</p> |
| Configure PCoIP event log verbosity               | <p>Legt die Ausführlichkeit der PCoIP-Ereignisprotokolle fest. Sie können einen Wert zwischen 0 (geringste Ausführlichkeit) und 3 (höchste Ausführlichkeit) festlegen.</p> <p>Bei Aktivierung dieser Einstellung können Sie einen Ausführlichkeitsgrad zwischen 0 und 3 festlegen. Wenn die Einstellung nicht konfiguriert oder deaktiviert ist, wird der standardmäßige Ausführlichkeitsgrad 2 verwendet.</p> <p>Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, ist die neue Einstellung umgehend wirksam.</p>  |

| Einstellung                          | Beschreibung  |
|--------------------------------------|---|
| Configure PCoIP image quality levels | <p data-bbox="676 226 1417 344">Steuert die PCoIP-Bilddarstellung während einer Netzwerküberlastung. Das Zusammenspiel der Werte <b>Mindestqualität für Bilder</b>, <b>Maximale anfängliche Bildqualität</b> und <b>Maximale Frame-Rate</b> ermöglicht eine genaue Steuerung in Umgebungen mit begrenzter Netzwerkbandbreite.</p> <p data-bbox="676 361 1417 638">Verwenden Sie den Wert <b>Mindestqualität für Bilder</b> zur Abstimmung von Bildqualität und Frame-Rate, wenn die Bandbreite begrenzt ist. Sie können einen Wert zwischen 30 und 100 angeben. Der Standardwert beträgt 40. Ein niedrigerer Wert ermöglicht höhere Frame-Rates, kann jedoch zu einer Beeinträchtigung der Anzeigequalität führen. Ein höherer Wert bietet eine höhere Bildqualität, unter Umständen jedoch niedrigere Frame-Rates, wenn die Netzwerkbandbreite begrenzt ist. Wenn die Netzwerkbandbreite keiner Einschränkung unterliegt, stellt PCoIP unabhängig von diesem Wert eine maximale Qualität sicher.</p> <p data-bbox="676 655 1417 991">Verwenden Sie die Einstellung <b>Maximale anfängliche Bildqualität</b>, um Spitzen bei der Belegung von Netzwerkbandbreite durch PCoIP zu vermeiden. Beschränken Sie hierzu die anfängliche Qualität der geänderten Bereiche für die Bildanzeige. Sie können einen Wert zwischen 30 und 100 angeben. Der Standardwert beträgt 80. Ein niedrigerer Wert verringert die Bildqualität bei Inhaltsänderungen und verhindert Spitzen bei der Bandbreitenbelegung. Ein höherer Wert verbessert die Bildqualität bei Inhaltsänderungen und erhöht die Bandbreitenanforderungen. Die nicht geänderten Bildbereiche erreichen unabhängig von diesem Wert stufenweise eine verlustfreie (perfekte) Qualität. Zur optimalen Nutzung der verfügbaren Bandbreite empfiehlt sich ein Wert von 80 oder niedriger.</p> <p data-bbox="676 1008 1417 1058">Der Wert <b>Mindestqualität für Bilder</b> darf den Wert <b>Maximale anfängliche Bildqualität</b> nicht überschreiten.</p> <p data-bbox="676 1075 1417 1318">Verwenden Sie den Wert <b>Maximale Frame-Rate</b> zur Verwaltung der pro Benutzer durchschnittlich genutzten Bandbreite. Begrenzen Sie dazu die Anzahl der Bildschirmaktualisierungen pro Sekunde. Geben Sie einen Wert zwischen 1 und 120 Frames pro Sekunde an. Der Standardwert beträgt 30. Ein höherer Wert kann mehr Bandbreite belegen, jedoch weniger Jitter verursachen und so weichere Bildübergänge ermöglichen, z.B. bei einem Video. Bei einem geringeren Wert wird weniger Bandbreite belegt, allerdings mehr Jitter verursacht.</p> <p data-bbox="676 1335 1417 1386">Diese Werte für die Bildqualität gelten nur für den Softhost und haben auf einen Softclient keine Auswirkung.</p> <p data-bbox="676 1402 1417 1453">Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, werden die Standardwerte verwendet.</p> <p data-bbox="676 1470 1417 1520">Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, ist die neue Einstellung umgehend wirksam.</p> |

| Einstellung                                   | Beschreibung   |
|---|--|
| Configure PCoIP session encryption algorithms | <p>Steuert die Verschlüsselungsalgorithmen, die vom PCoIP-Endpunkt während der Sitzungsaushandlung angeboten werden.</p> <p>Durch Aktivierung eines Kontrollkästchens wird der entsprechende Verschlüsselungsalgorithmus deaktiviert. Sie müssen mindestens einen Algorithmus aktivieren.</p> <p>Diese Einstellung gilt sowohl für den Agenten als auch für den Client. Die Endpunkte handeln den tatsächlich verwendeten Algorithmus für die Sitzungsverschlüsselung aus. Wenn der FIPS140-2-validierte Modus aktiviert ist, wird der Wert <b>AES-128-GCM-Verschlüsselung deaktivieren</b> immer außer Kraft gesetzt, sodass die AES-128-GCM-Verschlüsselung aktiviert wird.</p> <p>Unterstützte Verschlüsselungsalgorithmen sind in der bevorzugten Reihenfolge SALSA20/12-256, AES-GCM-128 und AES-GCM-256. Standardmäßig sind alle unterstützten Verschlüsselungsalgorithmen zur Aushandlung durch diesen Endpunkt verfügbar.</p> <p>Wenn beide Endpunkte für die Unterstützung aller drei Algorithmen konfiguriert sind und die Verbindung kein Security Gateway (SG) verwendet, wird der Algorithmus SALSA20 ausgehandelt und verwendet. Wenn die Verbindung dennoch ein SG verwendet, wird SALSA20 automatisch deaktiviert und AES128 wird ausgehandelt und verwendet. Wenn der Endpunkt oder das SG entweder SALSA20 deaktiviert oder der Endpunkt AES128 deaktiviert, wird AES256 ausgehandelt und verwendet.</p> |

| Einstellung  | Beschreibung  |                                 |  |  |  |  |  |  |  |
|--|---|---------------------------------|--|--|--|--|--|--|--|
| Configure PCoIP USB allowed and unallowed device rules     | <p data-bbox="675 226 1394 407">Legt fest, welche USB-Geräte für PCoIP-Sitzungen autorisiert oder nicht autorisiert sind, die einen Zero-Client verwenden, der Teradici-Firmware ausführt. In PCoIP-Sitzungen verwendete USB-Geräte müssen in der USB-Autorisierungstabelle aufgeführt sein. USB-Geräte, die in der USB-Ausschlussliste erscheinen, können in PCoIP-Sitzungen nicht verwendet werden.</p> <p data-bbox="675 422 1386 510">Sie können maximal 10 USB-Autorisierungsregeln und höchstens 10 USB-Ausschlussregeln definieren. Trennen Sie mehrere Regeln durch einen senkrechten Strich ( ) voneinander.</p> <p data-bbox="675 525 1422 640">Jede Regel kann eine Kombination aus einer Anbieter-ID und einer Produkt-ID sein, oder die Regel beschreibt eine Klasse von USB-Geräten. Eine Klassenregel kann eine gesamte Geräteklasse, eine einzelne Unterklasse oder ein Protokoll innerhalb einer Unterklasse zulassen oder ausschließen.</p> <p data-bbox="675 655 1406 806">Das Format einer kombinierten Regel aus Anbieter- und Produkt-ID lautet <b>1xxxxyyyy</b>, wobei <b>xxxx</b> die Anbieter-ID im Hexadezimalformat und <b>yyyy</b> die Produkt-ID im Hexadezimalformat darstellt. Die Regel zum Zulassen oder Sperren eines Geräts mit der Anbieter-ID <b>0x1a2b</b> und Produkt-ID <b>0x3c4d</b> würde beispielsweise <b>11a2b3c4d</b> lauten.</p> <p data-bbox="675 821 1224 844">Für Klassenregeln stehen folgende Formate zur Auswahl:</p> <table data-bbox="675 871 1337 1314"> <tr> <td data-bbox="675 871 858 926"><b>Alle USB-Geräte zulassen</b></td><td data-bbox="898 871 1075 938">Format: <b>23XXXXXX</b><br/>Beispiel: <b>23XXXXXX</b></td></tr> <tr> <td data-bbox="675 968 858 1083"><b>USB-Geräte mit einer bestimmten Klassen-ID zulassen</b></td><td data-bbox="898 968 1123 1035">Format: <b>22KlasseXXXX</b><br/>Beispiel: <b>22aaXXXX</b></td></tr> <tr> <td data-bbox="675 1113 858 1201"><b>Eine bestimmte Unterklasse zulassen</b></td><td data-bbox="898 1113 1241 1180">Format: <b>21Klasse–UnterklasseXX</b><br/>Beispiel: <b>21aabbXX</b></td></tr> <tr> <td data-bbox="675 1228 858 1314"><b>Ein bestimmtes Protokoll zulassen</b></td><td data-bbox="898 1228 1337 1295">Format: <b>20Klasse–Unterklasse–Protokoll</b><br/>Beispiel: <b>20aabbcc</b></td></tr> </table> <p data-bbox="675 1346 1422 1465">Die Zeichenfolge zur Autorisierung von USB-Eingabegeräten (Maus und Tastatur, Klassen-ID 0x03) und Webcams (Klassen-ID 0x0e) lautet beispielsweise <b>2203XXXX 220eXXXX</b>. Die Zeichenfolge zum Ausschließen von USB-Massenspeichergeräten (Klassen-ID 0x08) lautet <b>2208XXXX</b>.</p> <p data-bbox="675 1480 1414 1568">Eine leere Zeichenfolge für die USB-Autorisierung bedeutet, dass keine USB-Geräte zugelassen sind. Eine leere Zeichenfolge für den USB-Ausschluss bedeutet, dass für USB-Geräte keine Einschränkungen gelten.</p> <p data-bbox="675 1583 1402 1698">Diese Einstellung gilt ausschließlich für View Agent und nur dann, wenn sich der Remote-Desktop in einer Sitzung mit einem Zero-Client befindet, der Teradici-Firmware ausführt. Die Geräteverwendung wird zwischen den Endpunkten ausgehandelt.</p> <p data-bbox="675 1713 1402 1768">Standardmäßig sind sämtliche Geräte zugelassen, und es sind keine Geräte ausgeschlossen.</p> | <b>Alle USB-Geräte zulassen</b> | Format: <b>23XXXXXX</b><br>Beispiel: <b>23XXXXXX</b> | <b>USB-Geräte mit einer bestimmten Klassen-ID zulassen</b> | Format: <b>22KlasseXXXX</b><br>Beispiel: <b>22aaXXXX</b> | <b>Eine bestimmte Unterklasse zulassen</b> | Format: <b>21Klasse–UnterklasseXX</b><br>Beispiel: <b>21aabbXX</b> | <b>Ein bestimmtes Protokoll zulassen</b> | Format: <b>20Klasse–Unterklasse–Protokoll</b><br>Beispiel: <b>20aabbcc</b> |
| <b>Alle USB-Geräte zulassen</b>                            | Format: <b>23XXXXXX</b><br>Beispiel: <b>23XXXXXX</b>  |                                 |  |  |  |  |  |  |  |
| <b>USB-Geräte mit einer bestimmten Klassen-ID zulassen</b> | Format: <b>22KlasseXXXX</b><br>Beispiel: <b>22aaXXXX</b>  |                                 |  |  |  |  |  |  |  |
| <b>Eine bestimmte Unterklasse zulassen</b>                 | Format: <b>21Klasse–UnterklasseXX</b><br>Beispiel: <b>21aabbXX</b>  |                                 |  |  |  |  |  |  |  |
| <b>Ein bestimmtes Protokoll zulassen</b>                   | Format: <b>20Klasse–Unterklasse–Protokoll</b><br>Beispiel: <b>20aabbcc</b>  |                                 |  |  |  |  |  |  |  |

| Einstellung                      | Beschreibung  |
|----------------------------------|---|
| Configure PCoIP virtual channels | <p>Gibt die virtuellen Kanäle an, die bei PCoIP-Sitzungen verwendet bzw. nicht verwendet werden können. Diese Einstellung legt auch fest, ob die Zwischenablageverarbeitung auf dem PCoIP-Host deaktiviert wird.</p> <p>Virtuelle Kanäle, die in PCoIP-Sitzungen verwendet werden, müssen in der Tabelle der autorisierten virtuellen Kanäle aufgeführt sein. Virtuelle Kanäle, die in der Ausschlussliste für virtuelle Kanäle erscheinen, können in PCoIP-Sitzungen nicht verwendet werden.</p> <p>Sie können maximal 15 virtuelle Kanäle zur Verwendung in PCoIP-Sitzungen angeben.</p> <p>Trennen Sie mehrere Kanäle durch einen senkrechten Strich ( ) voneinander. Die Zeichenfolge zum Zulassen der virtuellen Kanäle „mksvchan“ und „vdp_rdpvcbridge“ lautet z.B. <b>mksvchan vdp_rdpvcbridge</b>.</p> <p>Wenn ein Kanalname einen senkrechten Strich oder einen umgekehrten Schrägstrich (\) enthält, fügen Sie vor dem Kanalnamen einen umgekehrten Schrägstrich ein. Der Kanalname „awk ward\channel“ wird beispielsweise folgendermaßen eingegeben: <b>awk\ ward\channel</b>.</p> <p>Ist die Tabelle der autorisierten virtuellen Kanäle leer, ist die Verwendung von virtuellen Kanälen nicht zulässig. Ist die Ausschlusstabelle für virtuelle Kanäle leer, sind alle virtuellen Kanäle zugelassen.</p> <p>Die Einstellung der virtuellen Kanäle gilt sowohl für den Agenten als auch für den Client. Zum Verwenden virtueller Kanäle müssen diese sowohl auf dem Agenten als auch auf dem Client aktiviert werden.</p> <p>Bei Festlegung der virtuellen Kanäle wird ein separates Kontrollkästchen angezeigt, mit dem Sie die Remote-Zwischenablageverarbeitung auf dem PCoIP-Host deaktivieren können. Dieser Wert gilt nur für den Agenten.</p> <p>Standardmäßig sind alle virtuellen Kanäle aktiviert, einschließlich der Zwischenablageverarbeitung.</p> |

| Einstellung                          | Beschreibung   |
|--------------------------------------|--|
| Configure the PCoIP transport header | <p data-bbox="676 226 1334 281">Konfiguriert den PCoIP-Übertragungsheader und legt die Priorität der Transportsitzung fest.</p> <p data-bbox="676 296 1406 478">Der PCoIP-Übertragungsheader ist ein 32-Bit-Header, der zu allen PCoIP-UDP-Paketen hinzugefügt wird (sofern der Übertragungsheader auf beiden Seiten aktiviert ist und unterstützt wird). Anhand des PCoIP-Übertragungsheaders können Netzwerkgeräte bei Netzwerkkonflikten eine bessere Priorisierung vornehmen bzw. bessere QoS-Entscheidungen treffen. Der Übertragungsheader ist standardmäßig aktiviert.</p> <p data-bbox="676 493 1406 611">Die Priorität einer Transportsitzung bestimmt die PCoIP-Sitzungspriorität, die im PCoIP-Übertragungsheader angegeben wird. Netzwerkgeräte können basierend auf der angegebenen Priorität einer Transportsitzung eine bessere Priorisierung vornehmen und bessere QoS-Entscheidungen treffen.</p> <p data-bbox="676 625 1358 711">Bei Aktivierung der Einstellung PCoIP-Übertragungsheader konfigurieren sind die folgenden Prioritäten für eine Transportsitzung verfügbar:</p> <ul style="list-style-type: none"> <li data-bbox="676 726 767 747">■ <b>Hoch</b></li> <li data-bbox="676 762 919 783">■ <b>Mittel</b> (Standardwert)</li> <li data-bbox="676 798 788 819">■ <b>Niedrig</b></li> <li data-bbox="676 833 858 854">■ <b>Nicht definiert</b></li> </ul> <p data-bbox="676 869 1422 1121">Der Prioritätswert für die Transportsitzung wird vom PCoIP-Agent und -Client ausgehandelt. Wenn der PCoIP-Agent einen Prioritätswert für die Transportsitzung angibt, wird die vom Agent angegebene Sitzungspriorität für die Sitzung verwendet. Wenn nur auf dem Client eine Priorität für die Transportsitzung angegeben ist, wird die vom Client angegebene Priorität für die Sitzung verwendet. Wenn weder der Agent noch der Client eine Priorität für die Transportsitzung angibt oder der Wert <b>Nicht definiert</b> festgelegt wurde, wird der Standardwert (<b>Mittel</b>) für die Sitzung verwendet.</p> |



| Einstellung  | Beschreibung   |
|--|--|
| Configure the TCP port to which the PCoIP host binds and listens | <p>Gibt den TCP-Agenten-Port für Software-PCoIP-Hosts an.</p> <p>Der Wert des TCP-Ports gibt den TCP-Basisport für die Agentbindungen an. Der TCP-Portbereich legt fest, wie viele zusätzliche Ports ausprobiert werden, falls der Basisport nicht verfügbar ist. Der Portbereich muss zwischen 1 und 10 liegen.</p> <p>Der Bereich erstreckt sich vom Basisport bis zur Summe aus Basisport und Portbereich. Wenn der Basisport beispielsweise 4172 lautet und der Portbereich auf 10 festgelegt ist, umfasst der Bereich die Ports 4172 bis 4182.</p> <p>Legen Sie die Größe des Wiederholungs-Portbereichs nicht auf 0 fest. Die Festlegung dieses Wertes auf 0 führt zu einem Verbindungsfehler, wenn sich Benutzer beim Desktop mit dem PCoIP-Anzeigeprotokoll anmelden. Horizon Client generiert die Fehlermeldung Das Anzeigeprotokoll für diesen Desktop steht zurzeit nicht zur Verfügung. Wenden Sie sich an Ihren Systemadministrator.</p> <p>Diese Einstellung gilt nur für View Agent.</p> <p>Der standardmäßige TCP-Basisport auf einzelnen Benutzer-Computern ist 4172 in View 4.5 und höher. Der standardmäßige Basisport ist 50002 in View 4.0.x und früheren Versionen. Der Portbereich lautet standardmäßig 1.</p> <p>Der standardmäßige TCP-Basisport ist auf RDS-Hosts 4173. Wenn PCoIP mit RDS-Hosts verwendet wird, wird für jede Benutzerverbindung ein separater PCoIP-Port verwendet. Der standardmäßige Portbereich, der vom Remote-Desktop-Dienst festgelegt wird, ist groß genug, um die maximal erwartete Anzahl von parallelen Benutzerverbindungen unterzubringen.</p> <hr/> <p><b>Wichtig</b> Es hat sich bewährt, diese Richtlinieneinstellung nicht zu verwenden, um den standardmäßigen Portbereich auf RDS-Hosts zu ändern, oder den TCP-Portwert vom Standardwert 4173 zu ändern. Vor allem ist der TCP-Portwert nicht auf 4172 festzulegen. Das Zurücksetzen dieses Wertes auf 4172 wirkt sich negativ auf die PCoIP-Leistung in RDS-Sitzungen aus.</p> |

| Einstellung  | Beschreibung   |
|--|--|
| Configure the UDP port to which the PCoIP host binds and listens | <p>Gibt den UDP-Agenten-Port für Software-PCoIP-Hosts an.</p> <p>Der Wert des UDP-Ports gibt den UDP-Basisport für die Agentbindung an. Der Wert für den UDP-Portbereich legt fest, wie viele zusätzliche Ports ausprobiert werden, falls der Basisport nicht verfügbar ist. Der Portbereich muss zwischen 1 und 10 liegen.</p> <p>Legen Sie die Größe des Wiederholungs-Portbereichs nicht auf 0 fest. Die Festlegung dieses Wertes auf 0 führt zu einem Verbindungsfehler, wenn sich Benutzer beim Desktop mit dem PCoIP-Anzeigeprotokoll anmelden. Horizon Client generiert die Fehlermeldung Das Anzeigeprotokoll für diesen Desktop steht zurzeit nicht zur Verfügung. Wenden Sie sich an Ihren Systemadministrator.</p> <p>Der Bereich erstreckt sich vom Basisport bis zur Summe aus Basisport und Portbereich. Wenn der Basisport beispielsweise 4172 lautet und der Portbereich auf 10 festgelegt ist, umfasst der Bereich die Ports 4172 bis 4182. Diese Einstellung gilt nur für View Agent.</p> <p>Der standardmäßige UDP-Basisport auf einzelnen Benutzer-Computern ist 4172 für View 4.5 und höher bzw. 50002 für View 4.0.x und früher. Der Portbereich lautet standardmäßig 10.</p> <p>Der standardmäßige UDP-Basisport ist auf RDS-Hosts 4173. Wenn PCoIP mit RDS-Hosts verwendet wird, wird für jede Benutzerverbindung ein separater PCoIP-Port verwendet. Der standardmäßige Portbereich, der vom Remote-Desktop-Dienst festgelegt wird, ist groß genug, um die maximal erwartete Anzahl von parallelen Benutzerverbindungen unterzubringen.</p> <p><b>Wichtig</b> Es hat sich bewährt, diese Richtlinieneinstellung nicht zu verwenden, um den standardmäßigen Portbereich auf RDS-Hosts zu ändern, oder den UDP-Portwert vom Standardwert 4173 zu ändern. Vor allem ist der UDP-Portwert nicht auf 4172 festzulegen. Das Zurücksetzen dieses Wertes auf 4172 wirkt sich negativ auf die PCoIP-Leistung in RDS-Sitzungen aus.</p> |
| Enable access to a PCoIP session from a vSphere console          | <p>Legt fest, ob in einer vSphere Client-Konsole die Anzeige einer aktiven PCoIP-Sitzung und das Senden von Eingaben an den Desktop gestattet werden soll. Standardmäßig zeigt der Bildschirm der vSphere Client-Konsole nichts an, wenn ein Client über PCoIP verbunden ist, und die Konsole kann keine Eingaben senden. Diese Standardeinstellung verhindert, dass ein anderer Benutzer den Desktop des Benutzers anzeigen kann oder mit böswilligen Absichten lokal am Host Eingaben vornimmt, während eine PCoIP-Remote-Sitzung aktiv ist.</p> <p>Diese Einstellung gilt nur für View Agent.</p> <p>Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, ist ein Konsolenzugriff nicht zulässig. Wenn diese Einstellung aktiviert ist, zeigt die Konsole die PCoIP-Sitzung an und eine Konsoleneingabe ist zulässig.</p> <p>Wenn diese Einstellung aktiviert ist, kann die Konsole nur dann eine PCoIP-Sitzung anzeigen, die mit einem Windows 7-System ausgeführt wird, wenn die virtuelle Maschine für Windows 7 mit Hardware v8 arbeitet. Hardware v8 ist nur für ESXi 5.0 und neuere Versionen verfügbar. Im Gegensatz hierzu sind Konsoleneingaben in ein Windows 7-System für alle Hardwareversionen der virtuellen Maschinen zulässig.</p> <p>Auf Windows XP- oder Windows Vista-Systemen kann die Konsole eine PCoIP-Sitzung anzeigen, wenn die virtuelle Maschine über egal welche Hardwareversion verfügt.</p>  |

| Einstellung   | Beschreibung   |
|---|--|
| Enable the FIPS 140-2 approved mode of operation                      | <p>Legt fest, ob zum Herstellen einer Remote-PCoIP-Verbindung ausschließlich FIPS 140-2-validierte kryptografische Algorithmen und Protokolle verwendet werden dürfen. Die Aktivierung dieser Einstellung setzt die Deaktivierung der AES128-GCM-Verschlüsselung außer Kraft.</p> <p>Diese Einstellung gilt sowohl für den Agenten als auch für den Client. Sie können entweder einen oder beide Endpunkte zum Betrieb im FIPS-Modus konfigurieren. Das Konfigurieren eines einzigen Endpunkts im FIPS-Modus begrenzt die bei der Sitzungsaushandlung verfügbaren Verschlüsselungsalgorithmen.</p> <p>Der FIPS-Modus ist für View 4.5 und höhere Versionen verfügbar. Für View 4.0.x und frühere Versionen steht der FIPS-Modus nicht zur Verfügung, daher hat eine Konfiguration dieser Einstellung keine Auswirkung.</p> <p>Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird der FIPS-Modus nicht verwendet.</p> |
| Enable/disable audio in the PCoIP session                             | <p>Legt fest, ob die Audiofunktion während PCoIP-Sitzungen aktiviert ist. Die Audiofunktion muss für beide Endpunkte aktiviert sein. Ist diese Einstellung aktiviert, ist die Verwendung von PCoIP-Audio zulässig. Wurde diese Einstellung deaktiviert, kann die PCoIP-Audiofunktion nicht verwendet werden. Wurde diese Einstellung nicht konfiguriert, ist die Audiofunktion standardmäßig aktiviert.</p>  |
| Enable/disable microphone noise and DC offset filter in PCoIP session | <p>Legt fest, ob Mikrofongeräusche und der Gleichstrom-Offset-Filter für die Mikrofoneingabe während der PCoIP-Sitzung aktiviert werden sollen.</p> <p>Diese Einstellung gilt nur für View Agent und den Teradici-Audiotreiber.</p> <p>Wenn diese Einstellung nicht konfiguriert ist, verwendet der Teradici-Audiotreiber standardmäßig die Mikrofongeräusche und den Gleichstrom-Offset-Filter.</p>   |
| Turn on PCoIP user default input language synchronization             | <p>Legt fest, ob die Standardeingabesprache des Benutzers in der PCoIP-Sitzung mit der standardmäßigen Eingabesprache des PCoIP-Clientendpunktes synchronisiert wird. Wenn diese Einstellung aktiviert ist, ist eine Synchronisierung zugelassen. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, ist eine Synchronisierung nicht erlaubt.</p> <p>Diese Einstellung gilt nur für View Agent.</p>   |

## View-PCoIP-Sitzungsbandbreitenvariablen

Die ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen enthält Gruppenrichtlinieneinstellungen zur Konfiguration von PCoIP-Sitzungsbandbreitenmerkmalen.

**Tabelle 16-6. View-PCoIP-Sitzungsbandbreitenvariablen**

| Einstellung                                   | Beschreibung   |
|---|--|
| Configure the maximum PCoIP session bandwidth | <p>Legt die maximale Bandbreite für eine PCoIP-Sitzung in Kilobits pro Sekunde fest. Die Bandbreite umfasst den gesamten Sitzungsdatenverkehr, Bilddarstellung, Audio, virtuelle Kanäle, USB und PCoIP-Steuerung eingeschlossen.</p> <p>Legen Sie diesen Wert auf die Gesamtkapazität der Verbindung fest, über die Ihr Endpunkt verbunden ist, und berücksichtigen Sie dabei die Anzahl der erwarteten gleichzeitigen PCoIP-Sitzungen. Beispielsweise legen Sie diesen Wert für eine Einzelbenutzer-VDI-Konfiguration (eine einzelne PCoIP-Sitzung), die eine 4 MBit/s-Internetverbindung verwendet, auf 4 MBit oder einen 10 % niedrigeren Wert fest, um etwas Spielraum für anderen Netzwerkdatenverkehr zu lassen. Wenn Sie erwarten, dass sich mehrere gleichzeitige PCoIP-Sitzungen, die entweder mehrere VDI-Benutzer oder eine RDS-Konfiguration umfassen, einen Link teilen, können Sie die Einstellung entsprechend anpassen. Durch eine Senkung dieses Werts wird jedoch die maximale Bandbreite für jede aktive Sitzung beschränkt.</p> <p>Durch eine Festlegung dieses Werts verhindern Sie, dass der Agent eine die Verbindungskapazität übersteigende Übertragungsrate wählt – was zu einem übermäßigen Paketverlust und einem schlechteren Benutzererlebnis führen würde. Dieser Wert ist symmetrisch. Client und Agent werden gezwungen, den niedrigeren der beiden Werte zu verwenden, die auf Client- und Agenteseite festgelegt sind. Beispielsweise wird der Agent bei Festlegung einer maximalen Bandbreite von 4 MBit/s gezwungen, eine niedrigere Übertragungsrate zu verwenden – auch wenn die Einstellung auf dem Client konfiguriert ist.</p> <p>Wenn diese Einstellung deaktiviert wurde oder auf einem Endpunkt nicht konfiguriert ist, legt der Endpunkt keine Bandbreiteneinschränkungen fest. Wenn diese Einstellung konfiguriert ist, wird sie als maximale Bandbreiteneinschränkung des Endpunkts in KBit/s verwendet.</p> <p>Der Standardwert für die nicht konfigurierte Einstellung liegt bei 900000 KBit/s. Diese Einstellung gilt sowohl für View Agent als auch für den Client. Haben die beiden Endpunkte unterschiedliche Einstellungen, wird der niedrigere Wert verwendet.</p> |
| Configure the PCoIP session bandwidth floor   | <p>Legt die Mindestbandbreite in Kilobits pro Sekunde fest, die von der PCoIP-Sitzung reserviert wird.</p> <p>Mit dieser Einstellung wird die minimale erwartete Bandbreitenübertragungsrate für den Endpunkt konfiguriert. Wenn Sie diese Einstellung zum Reservieren der Bandbreite für einen Endpunkt verwenden, muss der Benutzer nicht warten, bis Bandbreite verfügbar ist, was die Reaktionszeit während der Sitzung verbessert.</p> <p>Achten Sie jedoch darauf, dass Sie allen Endpunkten gemeinsam nicht mehr Bandbreite zuweisen, als insgesamt zur Verfügung steht. Die Summe der Mindestbandbreitenwerte für alle Verbindungen in Ihrer Konfiguration darf die Netzwerkcapazität nicht überschreiten.</p> <p>Der Standardwert lautet 0, d.h. es wird keine Mindestbandbreite reserviert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird keine Mindestbandbreite reserviert.</p> <p>Diese Einstellung gilt sowohl für View Agent als auch für den Client, wirkt sich allerdings nur auf den Endpunkt aus, für den sie konfiguriert wurde.</p> <p>Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, wird die Änderung umgehend wirksam.</p>  |

| Einstellung                     | Beschreibung   |
|---------------------------------|--|
| Configure the PCoIP session MTU | <p data-bbox="676 226 1406 283">Legt die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) für UDP-Pakete bei einer PCoIP-Sitzung fest.</p> <p data-bbox="676 296 1390 415">Die MTU-Größe umfasst den IP- und UDP-Paketvorspann. TCP verwendet den standardmäßigen MTU-Ermittlungsmechanismus zum Festlegen der maximalen Übertragungseinheit und wird von dieser Einstellung nicht beeinflusst.</p> <p data-bbox="676 428 1366 485">Die maximale MTU-Größe beträgt 1.500 Byte. Die minimale MTU-Größe beträgt 500 Byte. Der Standardwert lautet 1.300 Byte.</p> <p data-bbox="676 497 1406 583">Normalerweise muss die MTU-Größe nicht geändert werden. Ändern Sie diesen Wert, wenn Sie in einer nicht standardmäßig eingerichteten Netzwerkumgebung arbeiten, die zu einer PCoIP-Paketfragmentierung führt.</p> <p data-bbox="676 596 1321 623">Diese Einstellung gilt sowohl für View Agent als auch für den Client.</p> <p data-bbox="676 630 1422 686">Unterscheiden sich die MTU-Größeneinstellungen der beiden Endpunkte, wird der niedrigere Wert verwendet.</p> <p data-bbox="676 699 1422 756">Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, verwendet der Client bei der Aushandlung mit View Agent den Standardwert.</p> |

| Einstellung                                       | Beschreibung  |
|---|---|
| Configure the PCoIP session audio bandwidth limit | <p>Legt die maximale Bandbreite fest, die in einer PCoIP-Sitzung für Audiodaten (Soundwiedergabe) verwendet werden kann.</p> <p>Der Audioprozessor überwacht die für Audiodaten verwendete Bandbreite. Er wählt auch den Algorithmus zur Audiokomprimierung, der bei der aktuellen Bandbreitennutzung die bestmögliche Audioqualität liefert. Wenn ein Bandbreitenlimit festgelegt wurde, reduziert der Audioprozessor durch einen Wechsel des Komprimierungsalgorithmus so lange die Qualität, bis das Bandbreitenlimit erreicht ist. Wenn die minimale Audioqualität mit dem festgelegten Bandbreitenlimit nicht erreicht werden kann, wird die Audiofunktion deaktiviert.</p> <p>Stellen Sie diesen Wert höher als 1.600 KBit/s ein, um Audiodaten nicht zu komprimieren und eine hohe Stereo-Qualität zu erzielen. Ein Wert ab 450 KBit/s bietet Stereo-Qualität mit komprimierten Audiodaten. Ein Wert zwischen 50 KBit/s und 450 KBit/s liefert eine Audioqualität, die zwischen einem UKW-Radio und einem Telefongespräch liegt. Bei einem Wert unter 50 KBit/s ist unter Umständen keine Audiowiedergabe mehr möglich.</p> <p>Diese Einstellung gilt nur für View Agent. Diese Einstellung wird erst wirksam, wenn Sie die Audiofunktion an beiden Endpunkten aktivieren.</p> <p>Zudem hat diese Einstellung keinerlei Auswirkungen auf USB-Audio.</p> <p>Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird standardmäßig ein Bandbreitenlimit von 500 KBit/s konfiguriert, um den ausgewählten Algorithmus für die Audiokomprimierung zu begrenzen. Bei Konfiguration dieser Einstellung wird der Wert in KBit/s gemessen, mit einem standardmäßigen Audiobandbreitenlimit von 500 KBit/s.</p> <p>Diese Einstellung gilt für View 4.6 und höhere Versionen. Bei früheren View-Versionen hat diese Einstellung keine Auswirkung.</p> <p>Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, wird die Änderung umgehend wirksam.</p> |
| Turn off Build-to-Lossless feature                | <p>Legt fest, ob die Build-to-Lossless-Funktion des PCoIP-Protokolls aktiviert oder deaktiviert werden soll. Diese Funktion ist standardmäßig deaktiviert.</p> <p>Wenn diese Einstellung aktiviert wurde oder nicht konfiguriert ist, ist die Build-to-Lossless-Funktion deaktiviert und Bilder sowie andere Desktop- und Anwendungsinhalte werden nie zu einem verlustfreien Anzeigestadium aufgebaut. In Netzwerkumgebungen mit begrenzter Bandbreite kann die Deaktivierung der Build-to-Lossless-Funktion Einsparungen bei der Bandbreite ermöglichen.</p> <p>Wenn diese Einstellung deaktiviert wurde, ist die Build-to-Lossless-Funktion aktiviert. Das Aktivieren dieser Funktion wird für Umgebungen, in denen ein Aufbau von Bildern und Desktop-Inhalten zu einem verlustfreien Anzeigestadium erforderlich ist, nicht empfohlen.</p> <p>Wird diese Einstellung während einer aktiven PCoIP-Sitzung geändert, wird die Änderung umgehend wirksam.</p> <p>Weitere Informationen über die PCoIP-Build-to-Lossless-Funktion finden Sie unter <a href="#">View PCoIP Build-to-Lossless-Funktion</a>.</p>  |

## View-PCoIP-Sitzungsvariablen für die Tastatur

Die ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen enthält Gruppenrichtlinieneinstellungen zur Konfiguration von PCoIP-Sitzungsmerkmalen, die sich auf die Verwendung der Tastatur auswirken.

**Tabelle 16-7. View-PCoIP-Sitzungsvariablen für die Tastatur**

| Einstellung   | Beschreibung   |
|---|--|
| Disable sending CAD when users press Ctrl+Alt+Del       | <p>Wenn diese Richtlinie aktiviert ist, müssen Benutzer anstelle der Tastenkombination Strg+Alt+Entf die Tastenkombination Strg+Alt+Eingf drücken, um während einer PCoIP-Sitzung einen Sicherheitsaufruf (SAS) an den Remote-Desktop zu senden.</p> <p>Sie können diese Einstellung aktivieren, um eine Verwirrung der Benutzer zu vermeiden, wenn diese zum Sperren des Clientendpunktes Strg+Alt+Entf drücken, und sowohl an den Host als auch an den Gast ein Sicherheitsaufruf gesendet wird.</p> <p>Diese Einstellung gilt nur für View Agent und hat keine Auswirkung auf einen Client.</p> <p>Wenn diese Richtlinie nicht konfiguriert ist oder deaktiviert wurde, können Benutzer die Tastenkombination Strg+Alt+Entf oder Strg+Alt+Eingf drücken, um einen Sicherheitsaufruf an den Remote-Desktop zu senden.</p>  |
| Use alternate key for sending Secure Attention Sequence | <p>Gibt eine alternative Taste (anstelle der Eingf-Taste) zum Senden eines Sicherheitsaufrufs (Secure Attention Sequence, SAS) an.</p> <p>Sie können mit dieser Einstellung die Tastenkombination Strg+Alt+Eingf in virtuellen Maschinen beibehalten, die während einer PCoIP-Sitzung aus einem Remote-Desktop gestartet werden.</p> <p>Beispielsweise kann ein Benutzer eine vSphere Client-Instanz aus einem PCoIP-Desktop starten und auf einer virtuellen Maschine in vCenter Server eine Konsole öffnen. Wenn die Tastenkombination Strg+Alt+Eingf im Gastbetriebssystem auf der virtuellen vCenter Server-Maschine verwendet wird, wird ein Strg+Alt+Entf-Sicherheitsaufruf an die virtuelle Maschine gesendet. Diese Einstellung ermöglicht, dass mit der Tastenkombination Strg +Alt+<i>Alternative Taste</i> ein Strg+Alt+Entf-Sicherheitsaufruf an den PCoIP-Desktop gesendet wird.</p> <p>Wenn diese Einstellung aktiviert ist, müssen Sie eine alternative Taste aus einem Dropdown-Menü auswählen. Es ist nicht möglich, die Einstellung zu aktivieren und keinen Wert anzugeben.</p> <p>Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird die Tastenkombination Strg+Alt+Eingf zum Senden eines Sicherheitsaufrufs verwendet.</p> <p>Diese Einstellung gilt nur für View Agent und hat keine Auswirkung auf einen Client.</p> |

## View PCoIP Build-to-Lossless-Funktion

Sie können das PCoIP-Anzeigeprotokoll so konfigurieren, dass es eine Kodierungsmethode namens „Progressive Build“ (Progressiver Aufbau oder Build-to-Lossless) verwendet, die auf die Gewährleistung einer optimalen allgemeinen Benutzerumgebung selbst unter eingeschränkten Netzwerkbedingungen abzielt. Diese Funktion ist standardmäßig deaktiviert.

Die Build-to-Lossless-Funktion bietet ein hochgradig komprimiertes Erstbild, auch „verlustbehaftetes Bild“ genannt, welches dann stufenweise zu einem vollständig verlustfreien Anzeigestadium erweitert wird. Unter einem „verlustfreien Stadium“ versteht man, dass das Bild mit der beabsichtigten Originaltreue angezeigt wird.

In einem LAN zeigt PCoIP Text immer unter Verwendung der verlustfreien Komprimierung an. Ist die Build-to-Lossless-Funktion aktiviert und sinkt die verfügbare Bandbreite pro Sitzung auf unter 1 MBit/s, zeigt PCoIP zuerst ein verlustbehaftetes Textbild an und baut das Bild dann innerhalb kürzester Zeit zu einem verlustfreien Anzeigestadium auf. Durch diese Vorgehensweise kann der Desktop weiterhin reagieren und auch bei wechselnden Netzwerkbedingungen das bestmögliche Bild anzeigen, was zu einer optimalen Benutzererfahrung führt.

Die Build-to-Lossless-Funktion verfügt über folgende Leistungsmerkmale:

- Dynamische Anpassung der Bildqualität
- Verringerung der Bildqualität in überlasteten Netzwerken
- Aufrechterhaltung der Reaktionsfähigkeit durch Minimierung der Wartezeiten bei der Bildschirmaktualisierung
- Wiederaufnahme der maximalen Bildqualität nach Beheben der Netzwerküberlastung

Sie können die Funktion „Build-to-Lossless“ aktivieren, indem Sie die Gruppenrichtlinieneinstellung Build-to-Lossless-Funktion abschalten/deaktivieren. Siehe [View-PCoIP-Sitzungsbandbreitenvariablen](#).

## Verwenden von Gruppenrichtlinien für Remote-Desktop-Dienste

Sie können Gruppenrichtlinien für Remote-Desktop-Dienste (RDS) verwenden, um die Konfiguration und Leistung von RDS-Hosts sowie RDS-Desktop- und Anwendungssitzungen zu steuern. View stellt ADMX-Dateien bereit, die Microsoft-RDS-Gruppenrichtlinien enthalten, die in View unterstützt werden.

Es hat sich bewährt, die Gruppenrichtlinien, die in den ADMX-Dateien von View bereitgestellt werden, anstatt entsprechender Microsoft-Gruppenrichtlinien zu konfigurieren. Die View-Gruppenrichtlinien sind für die Unterstützung Ihrer View-Bereitstellung zertifiziert.

## Hinzufügen der ADMX-Dateien der Remote-Desktop-Dienste zu Active Directory

Sie können die Richtlinieneinstellungen in den View-RDS-ADMX-Dateien zu Gruppenrichtlinienobjekten (GPOs) in Active Directory hinzufügen. Sie können die RDS-ADMX-Dateien auch auf einzelnen RDS-Hosts installieren.

### Voraussetzungen

- Erstellen Sie GPOs für die RDS-Gruppenrichtlinieneinstellungen und verknüpfen Sie sie mit der Organisationseinheit (Organizational Unit, OU), die Ihre RDS-Hosts enthält.
- Stellen Sie sicher, dass die Funktion „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server verfügbar ist.



Die Schritte zum Öffnen der Verwaltungskonsolle für Gruppenrichtlinien unterscheiden sich in den Versionen Windows 2012, Windows 2008 und Windows 2003 Active Directory. Siehe [Erstellen von GPOs für View-Gruppenrichtlinien](#).

## Verfahren

- 1 Laden Sie die View GPO-Bundle-ZIP-Datei von der Download-Site von VMware Horizon (mit View) unter <http://www.vmware.com/go/downloadview> herunter.

Der Dateiname ist VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip (x.x.x ist die Version, yyyyyyy die Build-Nummer). Alle ADM- und ADMX-Dateien, die Gruppenrichtlinieneinstellungen für View bereitstellen, sind in dieser Datei verfügbar.

- 2 Extrahieren Sie die Datei VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip und kopieren Sie die RDS ADMX-Dateien auf Ihren Active Directory- oder RDS-Host.
  - a Kopieren Sie die Dateien vmware\_rdsh.admx und vmware\_rdsh\_server.admx in den Ordner C:\Windows\PolicyDefinitions in Ihrem Active Directory oder auf Ihrem RDS-Host.
  - b (Optional) Wenn Sie die Richtlinieneinstellungen lokalisieren möchten, kopieren Sie die ADML-Dateien vmware\_rdsh.adml und vmware\_rdsh\_server.adml in den entsprechenden Unterordner in C:\Windows\PolicyDefinitions\ in Ihrem Active Directory oder auf Ihrem RDS-Host.

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

Auf einem einzelnen RDS-Host können Sie den lokalen Gruppenrichtlinieneditor mit dem Dienstprogramm gpedit.msc öffnen.

Die View-RDS-Gruppenrichtlinieneinstellungen werden im Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > View-RDSH-Dienste > Remote-Desktop-Sitzungshost** installiert.

- 4 (Optional) Konfigurieren Sie die Gruppenrichtlinieneinstellungen im Ordner **View-RDSH-Dienste > Remote-Desktop-Sitzungshost**.

## Einstellungen zur Kompatibilität der RDS-Anwendung

Die Gruppenrichtlinieneinstellungen zur Kompatibilität der RDS-Anwendung steuern die Kompatibilität des Windows-Installationsprogramms, die IP-Virtualisierung des Remote-Desktops, die Auswahl des Netzwerkadapters und die Verwendung der IP-Adresse des RDS-Hosts.

**Tabelle 16-8. Gruppenrichtlinieneinstellungen zur Kompatibilität der RDS-Anwendung**

| Einstellung                                  | Beschreibung  |
|--|---|
| Turn off Windows Installer RDS Compatibility | <p>Die Richtlinieneinstellung legt fest, ob die RDS-Kompatibilität des Windows-Installationsprogramms für vollständig installierte Anwendungen auf Benutzerbasis ausgeführt wird. Das Windows-Installationsprogramm lässt das Ausführen von jeweils nur einer Instanz des <code>msiexec</code>-Prozesses zu. Standardmäßig ist die RDS-Kompatibilität des Windows-Installationsprogramms eingeschaltet.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, ist die RDS-Kompatibilität des Windows-Installationsprogramms ausgeschaltet. Zudem kann jeweils nur eine Instanz des <code>msiexec</code>-Prozesses ausgeführt werden.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die RDS-Kompatibilität des Windows-Installationsprogramms eingeschaltet, und mehrere Anforderungen zur Anwendungsinstallation pro Benutzer werden in die Warteschlange eingereiht sowie vom <code>msiexec</code>-Prozess in der Reihenfolge des Erhalts behandelt.</p> |
| Turn on Remote Desktop IP Virtualization     | <p>Diese Richtlinieneinstellung legt fest, ob die IP-Virtualisierung des Remote-Desktops eingeschaltet wird.</p> <p>Standardmäßig wird die IP-Virtualisierung des Remote-Desktops ausgeschaltet.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird die IP-Virtualisierung des Remote-Desktops eingeschaltet. Sie können den Modus auswählen, in dem die Einstellung angewendet wird. Wenn Sie den Modus „Pro Programm“ verwenden, müssen Sie für die Verwendung virtueller IP-Adressen eine Liste von Programmen eingeben. Listen Sie jedes Programm in einer separaten Zeile auf (geben Sie keine leeren Zeilen zwischen Programmen ein).<br/>Beispiel:</p> <div data-bbox="794 1224 941 1276" style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <pre>explorer.exe mstsc.exe</pre> </div> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die IP-Virtualisierung des Remote-Desktops ausgeschaltet.</p>                               |

| Einstellung   | Beschreibung   |
|---|--|
| Select the network adapter to be used for Remote Desktop IP Virtualization                        | <p>Diese Richtlinieneinstellung legt die IP-Adress- und Netzwerkmaske fest, die dem Netzwerkadapter entspricht, der für die virtuellen IP-Adressen verwendet wird. Die IP-Adress- und Netzwerkmaske muss in der Notierung „Klassenloses domänenübergreifendes Routing“ eingegeben werden. Beispiel: 192.0.2.96/24.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird die angegebene IP-Adress- und Netzwerkmaske verwendet, um den Netzwerkadapter für die virtuellen IP-Adressen auszuwählen.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die IP-Virtualisierung des Remote-Desktops ausgeschaltet. Ein Netzwerkadapter muss konfiguriert werden, damit die IP-Virtualisierung des Remote-Desktops funktioniert.</p> |
| Do not use Remote Desktop Session Host server IP address when virtual IP address is not available | <p>Die Richtlinieneinstellung legt fest, ob eine Sitzung die IP-Adresse des Servers des Remote-Desktop-Sitzungshosts verwendet, wenn eine virtuelle IP-Adresse nicht verfügbar ist.</p> <p>Wenn Sie die Richtlinieneinstellung aktivieren, wird die IP-Adresse des Servers des Remote-Desktop-Sitzungshosts nicht verwendet, wenn eine virtuelle IP-Adresse nicht verfügbar ist. Die Sitzung verfügt über keine Netzwerkverbindung.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die IP-Adresse des Servers des Remote-Desktop-Sitzungshosts verwendet, wenn eine virtuelle IP-Adresse nicht verfügbar ist.</p>  |

## Einstellungen zu RDS-Verbindungen

Mithilfe der Gruppenrichtlinieneinstellung für RDS-Verbindungen können Sie die gleichmäßige CPU-Planung deaktivieren.

**Tabelle 16-9. Gruppenrichtlinieneinstellungen für RDS-Verbindungen**

| Einstellung                        | Beschreibung   |
|------------------------------------|--|
| Turn off Fair Share CPU Scheduling | <p>Die gleichmäßige CPU-Planung verteilt die Prozessorzeit dynamisch auf alle RDS-Sitzungen auf einem RD-Sitzungs-Hostserver, basierend auf der Anzahl der Sitzungen und ihrem jeweiligen Bedarf an Prozessorzeit.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, wird die gleichmäßige CPU-Planung deaktiviert.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, ist die gleichmäßige CPU-Planung aktiviert.</p> |

## Einstellungen zur Umleitung von RDS-Geräten und Ressourcen

Die Gruppenrichtlinieneinstellungen zur Umleitung von Remote-Desktop-Dienste-Geräten und Ressourcen steuern die Geräte und Ressourcen auf einem Clientcomputer in RDS-Sitzungen.

**Tabelle 16-10. Gruppenrichtlinieneinstellungen zur Umleitung von RDS-Geräten und Ressourcen**

| Einstellung                 | Beschreibung   |
|-----------------------------|--|
| Allow time zone redirection | <p>Mit dieser Richtlinieneinstellung können Sie festlegen, ob der Clientcomputer seine Zeitzoneneinstellungen an die Remote-Desktop-Dienste-Sitzung umleitet.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, senden Clients, die eine Zeitzonenumleitung durchführen können, ihre Zeitoneninformationen an den Server. Über die Basiszeit des Servers wird die aktuelle Sitzungszeit berechnet (aktuelle Sitzungszeit = Serverbasiszeit + Clientzeitzone).</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, leitet der Clientcomputer seine Zeitoneninformationen nicht um, und die Sitzungszeitzone entspricht der Serverzeitzone.</p> |

## Einstellungen zur RDS-Lizenzierung

Die Gruppenrichtlinieneinstellungen für RDS-Lizenzierung steuern die Reihenfolge, in der RDS-Lizenzserver positioniert werden, ob Problem benachrichtigungen angezeigt werden und ob für RDS-CALs (Client Access Licenses) eine Lizenzierung auf Benutzer- oder Gerätebasis verwendet wird.

**Tabelle 16-11. Gruppenrichtlinieneinstellungen für RDS-Lizenzierung**

| Einstellung   | Beschreibung   |
|---|--|
| Use the specified Remote Desktop license servers                                      | <p data-bbox="778 279 1394 363">Diese Richtlinieneinstellung ermöglicht Ihnen, die Reihenfolge anzugeben, in der ein RD-Sitzungshostserver versucht, Remote-Desktop-Lizenzserver zu finden.</p> <p data-bbox="778 380 1414 531">Wenn Sie diese Richtlinieneinstellung aktivieren, versucht ein RD-Sitzungshostserver zunächst, die von Ihnen angegebenen Lizenzserver zu finden. Wenn die angegebenen Lizenzserver nicht gefunden werden können, versucht der RD-Sitzungshostserver eine automatische Lizenzservererkennung.</p> <p data-bbox="778 548 1414 632">Bei der automatischen Lizenzservererkennung versucht ein RD-Sitzungshostserver in einer Domäne auf Windows Server-Basis, in der folgenden Reihenfolge einen Lizenzserver zu finden:</p> <ol data-bbox="778 648 1426 837" style="list-style-type: none"> <li>1 Lizenzserver, die im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts angegeben sind</li> <li>2 Lizenzserver, die in den Active Directory-Domänendiensten veröffentlicht sind</li> <li>3 Lizenzserver, die auf Domänencontrollern in derselben Domäne wie der RD-Sitzungshostserver installiert sind</li> </ol> <p data-bbox="778 854 1394 972">Falls Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, verwendet der RD-Sitzungshostserver den Lizenzservererkennungsmodus, der im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts angegeben ist.</p> |
| Hide notifications about RD Licensing problems that affect the RD Session Host server | <p data-bbox="778 997 1414 1115">Diese Richtlinieneinstellung legt fest, ob Benachrichtigungen auf einem RD-Sitzungshostserver angezeigt werden, wenn Probleme bei der RD-Lizenzierung auftreten, die den RD-Sitzungshostserver betreffen.</p> <p data-bbox="778 1131 1426 1341">Standardmäßig werden Benachrichtigungen auf einem RD-Sitzungshostserver angezeigt, nachdem Sie sich als lokaler Administrator angemeldet haben, falls Probleme bei der RD-Lizenzierung auftreten, die den RD-Sitzungshostserver betreffen. Falls zutreffend, wird auch eine Benachrichtigung angezeigt, die die Anzahl von Tagen bis zum Ablauf der Lizenzfrist für den RD-Sitzungshostserver angibt.</p> <p data-bbox="778 1358 1374 1442">Wenn Sie diese Richtlinieneinstellung aktivieren, werden diese Benachrichtigungen auf dem RD-Sitzungshostserver nicht angezeigt.</p> <p data-bbox="778 1459 1402 1577">Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden diese Benachrichtigungen auf dem RD-Sitzungshostserver nach der Anmeldung als lokaler Administrator angezeigt.</p>   |
| Set the Remote Desktop licensing mode   | <p data-bbox="778 1602 1414 1719">Diese Richtlinieneinstellung ermöglicht Ihnen, den Typ der Client-Zugriffslizenz für Remote-Desktop-Dienste (RDS CAL) anzugeben, der für die Verbindung mit diesem RD-Sitzungshostserver erforderlich ist.</p> <p data-bbox="778 1736 1406 1820">Sie können diese Richtlinieneinstellung verwenden, um einen von zwei Lizenzierungsmodi auszuwählen: benutzer- oder gerätebasiert.</p> <p data-bbox="778 1837 1362 1955">Beim benutzerbasierten Lizenzierungsmodus muss jedes Benutzerkonto, das eine Verbindung mit diesem RD-Sitzungshostserver herstellt, eine benutzerbasierte RDS-CAL haben.</p> <p data-bbox="778 1971 1426 2055">Beim gerätebasierten Lizenzierungsmodus muss jedes Gerät, das eine Verbindung mit diesem RD-Sitzungshostserver herstellt, eine gerätebasierte RDS-CAL haben.</p> <p data-bbox="778 2072 1315 2093">Wenn Sie diese Richtlinieneinstellung aktivieren, hat der</p>   |

## Einstellungen zu RDS-Profilen

Die Gruppenrichtlinieneinstellungen für RDS-Profile steuern die Einstellungen für servergespeicherte Profile und das Basisverzeichnis bei Sitzungen der Remote-Desktop-Dienste.

Tabelle 16-12. Gruppenrichtlinieneinstellungen für RDS-Profile

| Einstellung   | Beschreibung  |
|---|---|
| Limit the size of the entire roaming user profile cache | <p>Mithilfe dieser Richtlinieneinstellung können Sie die Größe des gesamten servergespeicherten Benutzerprofil-Caches auf dem lokalen Laufwerk begrenzen. Diese Richtlinieneinstellung gilt nur für Computer, auf denen der Remote-Desktop-Sitzungshost-Rollendienst installiert ist.</p> <p><b>Hinweis</b> Wenn Sie die Größe eines einzelnen Benutzerprofils begrenzen möchten, verwenden Sie die Richtlinieneinstellung <b>Profilgröße</b> begrenzen unter <b>Benutzerkonfiguration \Richtlinien\Administrative Vorlagen\System\Benutzerprofile</b>.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, müssen Sie ein Überwachungsintervall (in Minuten) und eine maximale Größe (in Gigabyte) für den gesamten servergespeicherten Benutzerprofil-Cache angeben. Das Überwachungsintervall bestimmt, wie oft die Größe des gesamten servergespeicherten Benutzerprofil-Caches überprüft wird. Wenn die Größe des gesamten servergespeicherten Benutzerprofil-Caches die von Ihnen angegebene Maximalgröße übersteigt, werden die ältesten servergespeicherten Benutzerprofile (deren Verwendung am längsten zurückliegt) gelöscht, bis die Größe des gesamten servergespeicherten Benutzerprofil-Caches geringer ist als die angegebene Maximalgröße.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die Größe des gesamten servergespeicherten Benutzerprofil-Caches auf dem lokalen Laufwerk nicht begrenzt.</p> <p>Hinweis: Diese Richtlinieneinstellung wird ignoriert, wenn die Richtlinieneinstellung Weitergabe von Änderungen bei servergespeicherten Profilen an den Server verhindern unter <b>Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Benutzerprofile</b> aktiviert ist.</p> |
| Set Remote Desktop Services User Home Directory         | <p>Gibt an, ob die Remote-Desktop-Dienste die angegebene Netzwerkfreigabe oder den lokalen Verzeichnispfad als Stamm für das Basisverzeichnis des Benutzers für eine RDS-Sitzung verwenden.</p> <p>Um diese Einstellung zu verwenden, wählen Sie den Speicherort für das Basisverzeichnis (Netzwerk oder lokal) aus der Dropdown-Liste für den Speicherort. Wenn Sie das Verzeichnis auf einer Netzwerkfreigabe anlegen, geben Sie den Stammpfad für das Basisverzeichnis in der Form <code>\\Computername\Freigabename</code> an und wählen Sie dann den Laufwerkbuchstaben aus, dem Sie die Netzwerkfreigabe zuordnen möchten.</p> <p>Wenn Sie das Basisverzeichnis auf dem lokalen Computer anlegen möchten, geben Sie den Stammpfad für das Basisverzeichnis in der Form <code>Laufwerk:\Pfad</code> an, ohne Umgebungsvariablen oder Auslassungszeichen (drei Punkte). Geben Sie keinen Platzhalter für einen Benutzer-Alias an, da RDS diesen bei der Anmeldung automatisch anhängt.</p> <p><b>Hinweis</b> Das Feld für den Laufwerkbuchstaben wird ignoriert, wenn Sie einen lokalen Pfad angeben. Wenn Sie einen lokalen Pfad angeben, aber im Stammpfad für das Basisverzeichnis den Namen einer Netzwerkfreigabe eingeben, legt RDS die Basisverzeichnisse für die Benutzer im Netzwerk-Speicherort an.</p> <p>Wenn der Status auf „Aktiviert“ gesetzt ist, erstellt RDS das Basisverzeichnis für den betreffenden Benutzer in dem angegebenen Speicherort auf dem lokalen Computer oder im Netzwerk. Der Basisverzeichnispfad für jeden Benutzer entspricht</p>  |

| Einstellung   | Beschreibung   |
|---|--|
| Use mandatory profiles on the RD Session Host server      | <p>Mithilfe dieser Richtlinieneinstellung können Sie angeben, ob RDS ein obligatorisches Profil für alle Benutzer verwenden soll, die eine Remote-Verbindung zum RD-Sitzungshostserver herstellen.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, verwendet RDS den in der Richtlinieneinstellung Pfad für servergespeichertes Remote-Desktop-Dienste-Benutzerprofil festlegen angegebenen Pfad als Stammordner für das obligatorische Benutzerprofil. Alle Benutzer, die eine Remote-Verbindung zum RD-Sitzungshostserver herstellen, verwenden das gleiche Benutzerprofil.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden obligatorische Benutzerprofile nicht von Benutzern verwendet, die eine Remote-Verbindung zum RD-Sitzungshostserver herstellen.</p> <hr/> <p><b>Hinweis</b> Damit diese Einstellung übernommen wird, müssen Sie auch die Richtlinieneinstellung Pfad für servergespeichertes Remote-Desktop-Dienste-Benutzerprofil festlegen aktivieren und konfigurieren.</p>  |
| Set path for Remote Desktop Services Roaming User Profile | <p>Mithilfe dieser Richtlinieneinstellung können Sie den Netzwerkpfad angeben, den RDS für servergespeicherte Benutzerprofile verwendet.</p> <p>RDS speichert standardmäßig sämtliche Benutzerprofile lokal auf dem RD-Sitzungshostserver. Sie können diese Richtlinieneinstellung verwenden, um eine Netzwerkfreigabe anzugeben, in der Benutzerprofile zentral gespeichert werden können, sodass ein Benutzer für Sitzungen auf allen RD-Sitzungshostservern, die für die Verwendung dieser Netzwerkfreigabe für Benutzerprofile konfiguriert sind, auf das gleiche Benutzerprofil zugreifen kann.</p> <p>Wenn Sie diese Richtlinieneinstellung aktivieren, verwendet RDS den angegebenen Pfad als Stammverzeichnis für alle Benutzerprofile. Die Profile befinden sich in Unterordnern, die nach dem Kontonamen des jeweiligen Benutzers benannt sind.</p> <p>Um diese Richtlinieneinstellung zu konfigurieren, geben Sie den Pfad zu der Netzwerkfreigabe in der Form \\Computername\Freigabename an. Geben Sie keinen Platzhalter für den Benutzerkontonamen an, da RDS diesen automatisch hinzufügt, wenn der Benutzer sich anmeldet und das Profil erstellt wird. Wenn die angegebene Netzwerkfreigabe nicht vorhanden ist, zeigt RDS eine Fehlermeldung auf dem RD-Sitzungshostserver an und speichert die Benutzerprofile lokal auf dem RD-Sitzungshostserver.</p> <p>Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden die Benutzerprofile lokal auf dem RD-Sitzungshostserver gespeichert. Sie können den Profilpfad eines Benutzers auf der Registerkarte „Remote-Desktop-Dienste-Profil“ im Dialogfeld „Eigenschaften“ des Benutzerkontos konfigurieren.</p> <p>Anmerkungen:</p> <ol style="list-style-type: none"> <li>Die durch diese Richtlinieneinstellung aktivierten, servergespeicherten Benutzerprofile gelten nur für RDS-Verbindungen. Es kann vorkommen, dass ein Benutzer außerdem ein servergespeichertes Windows-Benutzerprofil konfiguriert hat. Ein servergespeichertes Remote-Desktop-Dienste-Benutzerprofil hat immer Vorrang in einer RDS-Sitzung.</li> <li>Verwenden Sie diese Richtlinieneinstellung zusammen mit der Richtlinieneinstellung Obligatorische Profile auf dem</li> </ol> |



## Umgebungseinstellungen zur RDS-Remote-Sitzung

Die Gruppenrichtlinieneinstellungen der RDS-Remotesitzungsumgebung steuern die Konfiguration der Benutzerschnittstelle in Remote-Desktop-Dienst-Sitzungen.

**Tabelle 16-13. Gruppenrichtlinieneinstellung der RDS-Remotesitzungsumgebung**

| Einstellung                                  | Beschreibung  |
|--|---|
| Remove Windows Security item from Start menu | <p>Gibt an, ob der Eintrag „Windows-Sicherheit“ aus dem Einstellungsmenü auf Remote-Desktop-Clients entfernt werden soll. Sie können diese Einstellung verwenden, um unerfahrene Benutzer davon abzuhalten, sich unbeabsichtigt von Remote-Desktop-Diensten abzumelden.</p> <p>Wenn der Status auf Aktiviert gesetzt ist, wird Windows-Sicherheit nicht in den Einstellungen im Start-Menü angezeigt. In der Folge müssen Benutzer eine Sicherheitssequenz wie beispielsweise STRG+ALT+Ende eingeben, um das Dialogfeld „Windows-Sicherheit“ auf dem Clientcomputer zu öffnen.</p> <p>Wenn der Status auf Deaktiviert oder Nicht konfiguriert gesetzt ist, bleibt Windows-Sicherheit im Einstellungsmenü.</p> |

## RDS-Sicherheitseinstellungen

Die Gruppenrichtlinieneinstellung zur RDS-Sicherheit steuert, ob lokale Administratoren Berechtigungen anpassen dürfen.

**Tabelle 16-14. Gruppenrichtlinieneinstellungen für RDS-Sicherheitsgruppe**

| Einstellung  | Beschreibung  |
|--|---|
| Do not allow local administrators to customize permissions | <p>Gibt an, ob die Administratorrechte zum Anpassen der Sicherheitsberechtigungen im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts deaktiviert werden.</p> <p>Sie können diese Einstellung verwenden, um Administratoren daran zu hindern, im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts auf der Registerkarte „Berechtigungen“ Änderungen an den Benutzergruppen vorzunehmen. Administratoren sind standardmäßig in der Lage, derartige Änderungen vorzunehmen.</p> <p>Wenn der Status auf „Aktiviert“ gesetzt ist, kann die Registerkarte „Berechtigungen“ im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts nicht verwendet werden, um die Sicherheitsbeschreibungen für jede Verbindung anzupassen oder um die Standard-Sicherheitsbeschreibungen für eine bestehende Gruppe zu verändern. Sämtliche Sicherheitsbeschreibungen sind schreibgeschützt.</p> <p>Wenn der Status auf „Deaktiviert“ oder „Nicht konfiguriert“ gesetzt ist, haben Server-Administratoren auf der Registerkarte „Berechtigungen“ im Tool für die Konfiguration des Remote-Desktop-Sitzungshosts vollen Lese-/Schreibzugriff auf die Sicherheitsbeschreibungen für Benutzer.</p> <hr/> <p><b>Hinweis</b> Die bevorzugte Methode zur Verwaltung des Benutzerzugriffs besteht darin, einen Benutzer zu der Gruppe der Remote-Desktop-Benutzer hinzuzufügen.</p> |

## Einstellungen zu temporären RDS-Ordern

Die Gruppenrichtlinieneinstellungen von RDS-Verbindungen steuern das Erstellen und Löschen temporärer Ordner für RDS-Sitzungen.

**Tabelle 16-15. Gruppenrichtlinieneinstellungen zu temporären RDS-Ordern**

| Einstellung                              | Beschreibung  |
|--|---|
| Do not delete temp folder upon exit      | <p data-bbox="778 279 1358 336">Legt fest, ob Remote-Desktop-Dienste temporäre Ordner pro Sitzung eines Benutzers beim Abmelden beibehalten.</p> <p data-bbox="778 348 1410 531">Sie können diese Einstellung verwenden, um die sitzungsspezifischen, temporären Ordner eines Benutzers auf einem Remote-Computer beizubehalten, auch wenn der Benutzer sich von einer Sitzung abmeldet. Standardmäßig löschen die Remote-Desktop-Dienste die temporären Ordner eines Benutzers, wenn sich der Benutzer abmeldet.</p> <p data-bbox="778 543 1418 632">Wenn der Status auf „Aktiviert“ festgelegt ist, werden die temporären Ordner pro Sitzung eines Benutzers beibehalten, wenn sich der Benutzer von einer Sitzung abmeldet.</p> <p data-bbox="778 644 1401 764">Wenn der Status auf „Deaktiviert“ festgelegt ist, werden die temporären Ordner gelöscht, wenn sich ein Benutzer abmeldet, auch wenn der Administrator Anderweitiges im Konfigurationstool des Remote-Desktop-Sitzungshosts angibt.</p> <p data-bbox="778 777 1426 896">Wenn der Status auf „Nicht konfiguriert“ festgelegt ist, löschen die Remote-Desktop-Dienste die temporären Ordner beim Abmelden aus dem Remote-Computer – es sei denn, der Server-Administrator hat Anderweitiges festgelegt.</p> <hr/> <p data-bbox="778 921 1418 1071"><b>Hinweis</b> Diese Einstellung wird nur wirksam, wenn die temporären Ordner pro Sitzung auf dem Server verwendet werden. Dies bedeutet, dass die Einstellung keine Auswirkung hat, wenn Sie die Einstellung „Temporäre Ordner pro Sitzung nicht verwenden“ aktivieren.</p> |
| Do not use temporary folders per session | <p data-bbox="778 1106 1390 1192">Durch diese Richtlinieneinstellung können Sie verhindern, dass Remote-Desktop-Dienste sitzungsspezifische temporäre Ordner erstellen.</p> <p data-bbox="778 1205 1422 1453">Sie können diese Richtlinieneinstellung verwenden, um das Erstellen separater temporärer Ordner auf einem Remote-Computer für jede Sitzung zu deaktivieren. Standardmäßig erstellen die Remote-Desktop-Dienste einen separaten temporären Ordner für jede aktive Sitzung, die ein Benutzer auf einem Remote-Computer beibehält. Diese temporären Ordner werden auf dem Remote-Computer in einem temporären Ordner unter dem Profilordner des Benutzers erstellt und sessionid benannt.</p> <p data-bbox="778 1465 1422 1648">Wenn Sie diese Richtlinieneinstellung aktivieren, werden die temporären Ordner pro Sitzung nicht erstellt. Stattdessen werden die temporären Dateien eines Benutzers für alle Sitzungen auf dem Remote-Computer in einem gemeinsamen temporären Ordner unter dem Profilordner des Benutzers auf dem Remote-Computer gespeichert.</p> <p data-bbox="778 1661 1410 1780">Wenn Sie diese Richtlinieneinstellung deaktivieren, werden immer temporäre Ordner pro Sitzung erstellt; selbst wenn Sie Anderweitiges im Konfigurationstool des Remote-Desktop-Sitzungshosts angeben.</p> <p data-bbox="778 1793 1401 1913">Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, werden temporäre Ordner pro Sitzung erstellt; es sei denn, Sie geben Anderweitiges im Konfigurationstool des Remote-Desktop-Sitzungshosts an.</p>                      |

## Einrichten des standortbasierten Druckens

Die standortbasierte Druckfunktion ordnet Drucker, die sich physisch in der Nähe von Clientsystemen befinden, View-Desktops zu. Auf diese Weise können Benutzer von ihren View-Desktops über ihre lokalen Drucker oder Netzwerkdrucker drucken.

Das standortbasierte Drucken ermöglicht es IT-Organisationen, View-Desktops demjenigen Drucker mit dem geringsten Abstand zum Endpunkt-Clientgerät zuzuordnen. Wenn ein Arzt im Krankenhaus sich beispielsweise von Raum zu Raum bewegt, wird der Druckauftrag bei jedem Ausdrucken eines Dokuments an den nächstgelegenen Drucker gesendet.

Die standortbasierte Druckfunktion ist für Windows, Mac OS X, Linux und Mobil-Clientgeräte verfügbar.

In Horizon 6.0.1 und höher wird das standortbasierte Drucken von den folgenden Remote-Desktops und Remote-Anwendungen unterstützt:

- Desktops, die auf Computern für Einzelbenutzer bereitgestellt werden, z. B. Windows Desktop- und Windows Server 2008 R2-Maschinen
- Desktops, die auf RDS-Hosts bereitgestellt werden, wobei die RDS-Hosts virtuelle Maschinen sind
- Gehostete Apps
- Gehostete Apps, die von Horizon Client in Remote-Desktops gestartet werden

In Horizon 6.0 und früher wird das standortbasierte Drucken auf Desktops unterstützt, die auf Windows Desktop-Maschinen für Einzelbenutzer bereitgestellt werden.

Um die standortbasierte Druckfunktion zu verwenden, müssen Sie die Setup-Optionen für den virtuellen Druck mit View Agent sowie die korrekten Druckertreiber auf dem Desktop installieren.

Sie richten das standortbasierte Drucken ein, indem Sie die Active Directory-Gruppenrichtlinieneinstellung `AutoConnect Map Additional Printers for VMware View` konfigurieren, die sich im Gruppenrichtlinienobjekt-Editor von Microsoft im Ordner **Softwareeinstellungen** unter **Computerkonfiguration** befindet.

---

**Hinweis** `AutoConnect Map Additional Printers for VMware View` ist eine computerspezifische Richtlinie. Computerspezifische Richtlinien gelten für alle View-Desktops, unabhängig davon, wer sich mit dem Desktop verbindet.

---

`AutoConnect Map Additional Printers for VMware View` ist als eine Tabelle für die Namensübersetzung implementiert. Sie verwenden jede Zeile in der Tabelle, um einen bestimmten Drucker zu identifizieren und einen Satz an Übersetzungsregeln für diesen Drucker zu definieren. Die Übersetzungsregeln legen fest, ob der Drucker zum View-Desktop für ein bestimmtes Clientsystem zugeordnet wird.

Wenn sich ein Benutzer mit einem View-Desktop verbindet, vergleicht View das Clientsystem mit den Übersetzungsregeln, die mit jedem Drucker in der Tabelle verknüpft sind. Wenn das Clientsystem allen Übersetzungsregeln für einen Drucker entspricht, oder wenn mit einem Drucker keine Übersetzungsregeln verknüpft sind, ordnet View den Drucker während der Benutzersitzung dem View-Desktop zu.

Sie können Übersetzungsregeln basierend auf der IP-Adresse, dem Namen und der MAC-Adresse des Clientsystems sowie basierend auf dem Benutzernamen und der Benutzergruppe definieren. Sie können für einen bestimmten Drucker eine Übersetzungsregel oder eine Kombination aus mehreren Übersetzungsregeln festlegen.

Die Informationen für die Zuordnung des Druckers zum View-Desktop werden in einem Eintrag im Registrierungsschlüssel HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect auf dem View-Desktop gespeichert.

## Druckereinstellungen für standortbasiertes Drucken

In Horizon 6.0.2 und höher werden Druckereinstellungen für standortbasierten Druck beibehalten, wenn sich ein Benutzer vom Desktop abmeldet oder die Verbindung zum Desktop trennt. Beispiel: Ein Benutzer konfiguriert einen standortbasierten Drucker für die Verwendung des Schwarzweißmodus. Nachdem der Benutzer sich vom Desktop abgemeldet und erneut bei ihm angemeldet hat, verwendet der standortbasierte Drucker weiterhin den Scharzweißmodus.

Um Druckereinstellungen sitzungsübergreifend in einer gehosteten Anwendung zu speichern, muss der Benutzer im Dialogfeld „Drucken“ der Anwendung einen standortbasierten Drucker auswählen, mit der rechten Maustaste auf den ausgewählten Drucker klicken und anschließend **Druckereinstellungen** auswählen. Druckereinstellungen werden nicht gespeichert, wenn der Benutzer im Dialogfeld „Drucken“ der Anwendung einen Drucker auswählt und auf die Schaltfläche **Einstellungen** klickt.

Dauerhafte Einstellungen für standortbasierte Drucker werden nicht unterstützt, wenn die Einstellungen im „private space“ (geräteabhängigen Teil) des Druckertreibers statt, wie von Microsoft empfohlen, im erweiterten (geräteunabhängigen) DEVMODE-Teil des Druckertreibers gespeichert werden. Um dauerhafte Einstellungen zu unterstützen, sollen Sie Drucker bereitstellen, die ihre Einstellungen im DEVMODE-Teil des Druckertreibers speichern lassen.

## Registrieren der Gruppenrichtlinien-DLL für den standortbasierten Druck

Um die Gruppenrichtlinieneinstellung für den standortbasierten Druck konfigurieren zu können, muss die DLL-Datei TPVMGPoACmap.dll registriert werden.

In Horizon 6.0.1 oder höher stehen 32- und 64-Bit-Versionen von TPVMGPoACmap.dll 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.

Frühere View-Versionen stellen 32- und 64-Bit-Versionen von TPVMGPoACmap.dll im Verzeichnis *install\_directory\VMware\VMware View\Server\extras\GroupPolicyFiles\ThinPrint* auf Ihrem View-Verbindungsserver-Host zur Verfügung.

### Verfahren

- 1 Kopieren Sie die geeignete Version der DLL-Datei TPVMGPoACmap.dll auf Ihren Active Directory-Server oder den Domänencomputer, den Sie zum Konfigurieren von Gruppenrichtlinien verwenden.

- 2 Verwenden Sie das Dienstprogramm `regsvr32`, um die Datei `TPVMGPoACmap.dll` zu registrieren.

Beispiel: `regsvr32 "C:\TPVMGPoACmap.dll"`

### Nächste Schritte

Konfigurieren Sie die Gruppenrichtlinieneinstellung für den standortbasierten Druck.

## Konfigurieren der Gruppenrichtlinie für den standortbasierten Druck

Um den standortbasierten Druck einzurichten, konfigurieren Sie die Gruppenrichtlinieneinstellung *Automatische Zuordnung zusätzlicher Drucker für VMware View*. Die Gruppenrichtlinieneinstellung ist eine Tabelle mit Namensübersetzungen, die Drucker zu View-Desktops zuordnet.

### Voraussetzungen

- Stellen Sie sicher, dass die Microsoft Management Console (MMC) und der Gruppenrichtlinienobjekt-Editor auf Ihrem Active Directory-Server oder dem Domänencomputer zur Verfügung stehen, den Sie zum Konfigurieren von Gruppenrichtlinien verwenden.
- Registrieren Sie die DLL-Datei `TPVMGPoACmap.dll` auf Ihrem Active Directory-Server oder dem Domänencomputer, den Sie zum Konfigurieren von Gruppenrichtlinien verwenden. Siehe [Registrieren der Gruppenrichtlinien-DLL für den standortbasierten Druck](#).
- Machen Sie sich mit der Syntax der Gruppenrichtlinieneinstellung *Automatische Zuordnung zusätzlicher Drucker für VMware View* vertraut. Siehe [Syntax einer Gruppenrichtlinieneinstellung für den standortbasierten Druck](#).
- Erstellen Sie ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) für die Gruppenrichtlinieneinstellung für den standortbasierten Druck und verknüpfen Sie es mit der Organisationseinheit (Organizational Unit, OU), die Ihre View-Desktops enthält. Unter [Erstellen von GPOs für View-Gruppenrichtlinien](#) finden Sie ein Beispiel für die Erstellung von GPOs für View-Gruppenrichtlinien.
- Überprüfen Sie, ob die Setuptools „Virtueller Druck“ mit View Agent auf Ihren Desktops installiert wurde. Überprüfen Sie dazu, ob die Dienste „TP AutoConnect Service“ und „TP VC Gateway Service“ auf dem Desktop-Betriebssystem installiert sind.
- Da Druckaufträge direkt vom View-Desktop zum Drucker gesendet werden, müssen Sie sicherstellen, dass die erforderlichen Druckertreiber auf Ihren Desktops installiert sind.

## Verfahren

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

| AD-Version   | Navigationspfad   |
|--------------|---|
| Windows 2003 | <ol style="list-style-type: none"> <li>a Wählen Sie <b>Start &gt; Alle Programme &gt; Verwaltung &gt; Active Directory-Benutzer und -Computer</b>.</li> <li>b Klicken Sie mit der rechten Maustaste auf die OU, die Ihre View-Desktops enthält, und wählen Sie <b>Eigenschaften</b>.</li> <li>c Klicken Sie auf der Registerkarte <b>Gruppenrichtlinie</b> auf <b>Öffnen</b>, um das Plug-In Gruppenrichtlinienverwaltung zu öffnen.</li> <li>d Klicken Sie im rechten Fensterbereich auf das GPO, das Sie für die Gruppenrichtlinieneinstellung für den standortbasierten Druck erstellt haben, und wählen Sie <b>Bearbeiten</b>.</li> </ol> |
| Windows 2008 | <ol style="list-style-type: none"> <li>a Wählen Sie <b>Start &gt; Verwaltung &gt; Gruppenrichtlinienverwaltung</b>.</li> <li>b Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf das GPO, das Sie für die standortbasierte Druckgruppenrichtlinieneinstellung erstellt haben, und wählen Sie <b>Bearbeiten</b> aus.</li> </ol>   |

Das Fenster **Gruppenrichtlinienobjekt-Editor** wird angezeigt.

- 2 Erweitern Sie die Ansicht **Computerkonfiguration**, öffnen Sie den Ordner **Softwareeinstellungen** und wählen Sie **Automatische Zuordnung zusätzlicher Drucker für VMware View** aus.
- 3 Doppelklicken Sie im Fensterbereich „Richtlinie“ auf **Automatische Zuordnung zusätzlicher Drucker konfigurieren**.

Das Fenster **Automatische Zuordnung zusätzlicher Drucker für VMware View** wird angezeigt.

- 4 Wählen Sie die Option **Aktiviert**, um die Gruppenrichtlinieneinstellung zu aktivieren.

Im Gruppenrichtlinienfenster werden die Überschriften und Schaltflächen der Übersetzungstabelle angezeigt.

**Wichtig** Durch Klicken auf **Deaktiviert** werden alle Tabelleneinträge gelöscht. Als Vorsichtsmaßnahme sollten Sie Ihre Konfiguration speichern, um sie später importieren zu können.

- 5 Fügen Sie alle Drucker hinzu, die Sie View-Desktops zuordnen möchten, und definieren Sie die zugehörigen Übersetzungsregeln.
- 6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

## Syntax einer Gruppenrichtlinieneinstellung für den standortbasierten Druck

Sie verwenden die Gruppenrichtlinieneinstellung AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View), um Drucker zu Remote-Desktops zuzuordnen.

AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View) ist eine Tabelle für die Namensübersetzung, die Drucker identifiziert und verknüpfte Übersetzungsregeln definiert. [Tabelle 16-16. Spalten und Werte in der Übersetzungstabelle](#) beschreibt die Syntax der Übersetzungstabelle.

Speicherortbasiertes Drucken weist Druckern Remote-Desktops zu, unterstützt jedoch nicht die Zuweisung von Netzwerkdruckern, die durch Verwendung von UNC-Pfaden konfiguriert wurden.

**Tabelle 16-16. Spalten und Werte in der Übersetzungstabelle**

| Spalte       | Beschreibung  |
|--------------|---|
| IP Range     | <p>Eine Übersetzungsregel, die einen Bereich mit IP-Adressen für Clientsysteme angibt.</p> <p>Verwenden Sie die folgende Notierung, um IP-Adressen in einem bestimmten Bereich anzugeben:</p> <p><b><i>ip_address-IP-Adresse</i></b></p> <p>Beispiel: <b>10.112.116.0-10.112.119.255</b></p> <p>Verwenden Sie die folgende Notierung, um alle IP-Adressen in einem bestimmten Subnetz anzugeben:</p> <p><b><i>ip_adresse/subnetz_masken_bits</i></b></p> <p>Beispiel: <b>10.112.4.0/22</b></p> <p>Diese Notierung gibt die verwendbaren IPv4-Adressen von 10.112.4.1 bis 10.112.7.254 an.</p> <p>Geben Sie für eine beliebige IP-Adresse ein Sternchen (*) ein.</p> |
| Client Name  | <p>Eine Übersetzungsregeln, die einen Computernamen angibt.</p> <p>Beispiel: <b>Marias Computer</b></p> <p>Geben Sie für einen beliebigen Computernamen ein Sternchen (*) ein.</p>  |
| Mac Address  | <p>Eine Übersetzungsregeln, die eine MAC-Adresse angibt. Im GPO-Editor muss dasselbe Format wie im Clientsystem verwendet werden. Beispiel:</p> <ul style="list-style-type: none"> <li>■ Windows-Clients verwenden Bindestriche: <b>01-23-45-67-89-ab</b></li> <li>■ Linux-Clients verwenden Doppelpunkte: <b>01:23:45:67:89:ab</b></li> </ul> <p>Geben Sie für eine beliebige MAC-Adresse ein Sternchen (*) ein.</p>   |
| User/Group   | <p>Eine Übersetzungsregeln, die einen Benutzer oder eine Benutzergruppe angibt.</p> <p>Um einen bestimmten Benutzer oder eine bestimmte Gruppe anzugeben, verwenden Sie die folgende Notierung:</p> <p><b><i>\\domäne\benutzer_oder_gruppe</i></b></p> <p>Beispiel: <b>\\meinedomäne\Marie</b></p> <p>Geben Sie für einen beliebigen Benutzernamen bzw. eine beliebige Benutzergruppe ein Sternchen (*) ein.</p>  |
| Printer Name | <p>Der Name des Druckers bei der Zuweisung zum Remote-Desktop.</p> <p>Beispiel: <b>DRUCKER-2-CLR</b></p> <p>Der zugewiesene Name muss nicht dem Druckernamen auf dem Clientsystem entsprechen.</p> <p>Der Drucker muss lokal am Clientgerät angeschlossen sein. Die Zuweisung eines Netzwerkdruckers in einem UNC-Pfad wird nicht unterstützt.</p>  |



| Spalte                 | Beschreibung   |
|------------------------|--|
| Printer Driver         | <p>Der Name des Treibers, den der Drucker verwendet.</p> <p>Beispiel: <b>HP Color LaserJet 4700 PS</b></p> <hr/> <p><b>Wichtig</b> Da Druckaufträge direkt vom Desktop zum Drucker gesendet werden, muss der Druckertreiber auf dem Desktop installiert sein.</p>  |
| IP Port/ThinPrint Port | <p>Für Netzwerkdrucker wird der IP-Adresse des Druckers das Präfix <b>IP_</b> vorangestellt.</p> <p>Beispiel: <b>IP_10.114.24.1</b></p> <p>Der Standardport ist 9001. Sie können einen nicht standardmäßigen Port durch Anhängen der Portnummer an die IP-Adresse angeben.</p> <p>Beispiel: <b>IP_10.114.24.1:9004</b></p> |
| Default                | Gibt an, ob es sich bei dem Drucker um den Standarddrucker handelt.  |

Sie verwenden die Schaltflächen, die oberhalb der Spaltenüberschriften angezeigt werden, um Tabelleneinträge hinzuzufügen, zu löschen, Zeilen zu verschieben und zu importieren. Jede Schaltfläche verfügt über eine äquivalente Tastaturkombination. Bewegen Sie die Maus über jede Schaltfläche, um eine Beschreibung der Schaltfläche und die zugehörige Tastaturkombination anzuzeigen. Um beispielsweise eine Zeile am Ende der Tabelle einzufügen, klicken Sie auf die erste Tabellenschaltfläche und drücken Alt+A. Klicken Sie auf die letzten zwei Schaltflächen, um Tabelleneinträge zu importieren und zu speichern.

[Tabelle 16-17. Gruppenrichtlinieneinstellung für den standortbasierten Druck – Beispiel](#) zeigt ein Beispiel für zwei Zeilen einer Übersetzungstabelle.

**Tabelle 16-17. Gruppenrichtlinieneinstellung für den standortbasierten Druck – Beispiel**

| IP-Bereich                    | Clientname | Mac-Adresse | Benutzer / Gruppe | Druckername   | Druckertreiber            | IP Port/ThinPrint Port (IP-Port/ThinPrint-Port) | Standard |
|-------------------------------|------------|-------------|-------------------|---------------|---------------------------|---|----------|
| *                             | *          | *           | *                 | DRUCKER-1-CLR | HP Color LaserJet 4700 PS | IP_10.114.24.1                                  |          |
| 10.112.116.140-10.112.116.145 | *          | *           | *                 | DRUCKER-2-CLR | HP Color LaserJet 4700 PS | IP_10.114.24.2                                  | X        |

Der in der ersten Zeile angegebene Netzwerkdrucker wird einem Remote-Desktop für ein beliebiges Clientsystem zugeordnet, da in allen Spalten für die Übersetzungsregeln Sternchen angezeigt werden. Der in der zweiten Zeile angegebene Netzwerkdrucker wird nur dann einem Remote-Desktop zugeordnet, wenn sich die IP-Adresse des Clientsystems im Bereich 10.112.116.140 bis 10.112.116.145 befindet.

## Beispiel einer Active Directory-Gruppenrichtlinie

Eine Möglichkeit zur Implementierung von Active Directory-Gruppenrichtlinien in View besteht darin, eine Organisationseinheit (OU) für Ihre View-Computer zu erstellen, die Remote-Desktop-Sitzungen

übermitteln, und mindestens ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) mit dieser OU zu verknüpfen. Sie können diese GPOs verwenden, um Gruppenrichtlinieneinstellungen auf Ihre View-Computer anzuwenden.

GPOs können direkt mit einer Domäne verbunden werden, wenn die Gruppenrichtlinieneinstellungen für alle Computer in dieser Domäne gelten. Es hat sich jedoch bewährt, die GPOs in den meisten Bereitstellungen mit einzelnen OUs zu verbinden, um zu vermeiden, dass Richtlinien auf allen Computern in der Domäne verarbeitet werden.

Sie können Richtlinien auf Ihrem Active Directory-Server oder einem beliebigen anderen Computer in Ihrer Domäne konfigurieren. Dieses Beispiel zeigt, wie Sie Richtlinien direkt auf Ihrem Active Directory-Server konfigurieren.

---

**Hinweis** Da jede View-Umgebung anders ist, müssen Sie möglicherweise unterschiedliche Schritte ausführen, um die Anforderungen der jeweiligen Organisation zu erfüllen.

---

## Erstellen einer OU für View-Computer

Um Gruppenrichtlinien auf View-Computer anzuwenden, die Remote-Desktop-Sitzungen bereitstellen, ohne dass sich dies auf andere Windows-Computer in derselben Active Directory-Domäne auswirkt, erstellen Sie eine Organisationseinheit (OU) speziell für Ihre View-Computer. Möglicherweise erstellen Sie eine Organisationseinheit für Ihre gesamte View-Bereitstellung oder separate Organisationseinheiten für einzelne Computer und RDS-Hosts.

### Verfahren

- 1 Wählen Sie auf Ihrem Active Directory-Server **Start > Alle Programme > Verwaltung > Active Directory-Benutzer und -Computer** aus.
- 2 Klicken Sie mit der rechten Maustaste auf die Domäne, die Ihre View-Computer enthält, und wählen Sie **Neu > Organisationseinheit** aus.
- 3 Geben Sie einen Namen für die OU ein und klicken Sie auf **OK**.  
Die neue OU wird im linken Fensterbereich angezeigt.
- 4 So fügen Sie der neuen OU View-Computer hinzu:
  - a Klicken Sie im linken Fensterbereich auf **Computer**.  
Alle Computerobjekte in der Domäne werden im rechten Fensterbereich angezeigt.
  - b Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf das Computerobjekt, das den View-Computer repräsentiert, und wählen Sie **Verschieben** aus.
  - c Wählen Sie die OU und klicken Sie auf **OK**.  
Der View-Computer wird im rechten Fensterbereich angezeigt, wenn Sie die OU auswählen.

### Nächste Schritte

Erstellen Sie GPOs für View-Gruppenrichtlinien.

## Erstellen von GPOs für View-Gruppenrichtlinien

Erstellen Sie Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) für Gruppenrichtlinien, die Sie für View-Komponenten und den standortbasierten Druck konfigurieren, und verknüpfen Sie diese GPOs anschließend mit der Organisationseinheit (Organizational Unit, OU) für Ihre View-Computer.

### Voraussetzungen

- Erstellen Sie eine OU für Ihre View-Computer.
- Stellen Sie sicher, dass die Funktion „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server verfügbar ist.

### Verfahren

- 1 Öffnen Sie auf dem Active Directory-Server die Verwaltungskonsolle für Gruppenrichtlinien.

| AD-Version   | Navigationspfad   |
|--------------|---|
| Windows 2012 | Wählen Sie <b>Server Manager &gt; Tools &gt; Group Policy Management</b> .  |
| Windows 2008 | Wählen Sie <b>Start &gt; Administrative Tools &gt; Group Policy Management</b> .  |
| Windows 2003 | <ol style="list-style-type: none"> <li>a Wählen Sie <b>Start &gt; Alle Programme &gt; Verwaltung &gt; Active Directory-Benutzer und -Computer</b>.</li> <li>b Klicken Sie mit der rechten Maustaste auf die OU, die Ihre View-Computer enthält, und wählen Sie <b>Eigenschaften</b>.</li> <li>c Klicken Sie auf der Registerkarte <b>Gruppenrichtlinie</b> auf <b>Öffnen</b>, um das Plug-In „Gruppenrichtlinienverwaltung“ zu öffnen.</li> </ol> |

- 2 Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf die OU, die Ihre View-Computer enthält, und wählen Sie **GPO in dieser Domäne erstellen und hier verknüpfen**.

Unter Windows 2003 Active Directory heißt diese Option **Gruppenrichtlinienobjekt hier erstellen und verknüpfen**.

- 3 Geben Sie einen Namen für das GPO ein und klicken Sie auf **OK**.

Das neue GPO wird im linken Fensterbereich unterhalb der OU angezeigt.

- 4 (Optional) So wenden Sie das GPO nur auf bestimmte View-Computer in der OU an:

- a Wählen Sie das GPO im linken Fensterbereich aus.
- b Wählen Sie **Sicherheitsfilterung > Hinzufügen**.
- c Geben Sie die Computernamen der View-Computer ein und klicken Sie auf **OK**.

Die View-Computer werden im Fensterbereich „Sicherheitsfilterung“ angezeigt. Die Einstellungen im GPO werden nur auf diese Computer angewendet.

### Nächste Schritte

Fügen Sie die View-ADM-Vorlagen zum GPO für Gruppenrichtlinien hinzu.

## Hinzufügen von View-ADM-Vorlagen zu einem GPO

Um Gruppenrichtlinieneinstellungen für View-Komponenten auf Ihre Remote-Desktops und Anwendungen anzuwenden, fügen Sie die zugehörigen ADM-Vorlagendateien zu GPOs hinzu.

### Voraussetzungen

- Erstellen Sie GPOs für die Gruppenrichtlinieneinstellungen für View-Komponenten und verknüpfen Sie sie mit der Organisationseinheit, die Ihre View-Computer enthält.
- Stellen Sie sicher, dass die Funktion „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server verfügbar ist.

Die Schritte zum Öffnen der Verwaltungskonsolle für Gruppenrichtlinien unterscheiden sich in den Versionen Windows 2012, Windows 2008 und Windows 2003 Active Directory. Siehe [Erstellen von GPOs für View-Gruppenrichtlinien](#).

### Verfahren

- 1 Laden Sie die View GPO-Bundle-ZIP-Datei von der Download-Site von VMware Horizon (mit View) unter <http://www.vmware.com/go/downloadview> herunter.

Der Dateiname ist VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyy.zip (x.x.x ist die Version, yyyyyy die Build-Nummer). Alle ADM- und ADMX-Dateien, die Gruppenrichtlinieneinstellungen für View bereitstellen, sind in dieser Datei verfügbar.

- 2 Kopieren Sie die Datei auf Ihren Active Directory-Server und extrahieren Sie die Datei.
- 3 Öffnen Sie auf dem Active Directory-Server die Verwaltungskonsolle für Gruppenrichtlinien.
- 4 Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **Bearbeiten** aus.
- 5 Klicken Sie im Gruppenrichtlinienverwaltungs-Editor mit der rechten Maustaste auf den Ordner **Computerkonfiguration > Richtlinien > Administrative Vorlagen: Richtliniendefinitionen** und wählen Sie **Vorlagen hinzufügen/entfernen**.
- 6 Klicken Sie auf **Hinzufügen**, suchen Sie nach der ADM-Vorlagendatei, und klicken Sie auf **Öffnen**.
- 7 Klicken Sie auf **Schließen**, um die Richtlinieneinstellungen in der ADM-Vorlagendatei auf das GPO anzuwenden.

In Windows Server 2012 oder 2008 Active Directory wird der Vorlagenname im linken Bereich unter **Administrative Vorlagen > Klassische administrative Vorlagen (ADM)** angezeigt. In Windows Server 2003 Active Directory wird die Vorlage unter **Administrative Vorlagen** angezeigt.

- 8 Konfigurieren Sie die Gruppenrichtlinieneinstellungen.

### Nächste Schritte

Aktivieren Sie die Loopback-Verarbeitung für Ihre View-Computer.

## Aktivieren der Loopback-Verarbeitung für Remote-Desktops

Um Benutzerkonfigurationseinstellungen, die normalerweise für einen Computer gelten, auf alle Benutzer anzuwenden, die sich an diesem Computer anmelden, aktivieren Sie die Loopback-Verarbeitung.

### Voraussetzungen

- Erstellen Sie GPOs für die Gruppenrichtlinieneinstellungen für View-Komponenten und verknüpfen Sie sie mit der Organisationseinheit, die Ihre View-Computer enthält.
- Stellen Sie sicher, dass die Funktion „Gruppenrichtlinienverwaltung“ auf Ihrem Active Directory-Server verfügbar ist.

Die Schritte zum Öffnen der Verwaltungskonsole für Gruppenrichtlinien unterscheiden sich in den Versionen Windows 2012, Windows 2008 und Windows 2003 Active Directory. Siehe [Erstellen von GPOs für View-Gruppenrichtlinien](#).

### Verfahren

- 1 Öffnen Sie auf dem Active Directory-Server die Verwaltungskonsole für Gruppenrichtlinien.
- 2 Erweitern Sie Ihre Domäne, klicken Sie mit der rechten Maustaste auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **Bearbeiten** aus.
- 3 Erweitern Sie im **Gruppenrichtlinienverwaltungs-Editor** die Ordner **Computerkonfiguration**, **Richtlinien**, **Administrative Vorlagen: Richtliniendefinitionen** und **System**.
- 4 Doppelklicken Sie auf den Ordner **Gruppenrichtlinie**.
- 5 Doppelklicken Sie im rechten Bereich auf **Loopback-Verarbeitungsmodus für Benutzergruppenrichtlinie konfigurieren**.
- 6 Wählen Sie **Aktiviert** und danach einen Loopback-Verarbeitungsmodus im Dropdown-Menü **Modus** aus.

| Option                        | Aktion  |
|-------------------------------|---|
| <b>Merge (Zusammenführen)</b> | Die angewendeten Benutzerrichtlinieneinstellungen sind eine Kombination der Richtlinien in den Computer- und Benutzer-GPOs. Bei Konflikten haben die Computer-GPOs Vorrang. |
| <b>Replace (Ersetzen)</b>     | Die Benutzerrichtlinie wird ausschließlich anhand der mit dem Computer verknüpften GPOs definiert. Mit dem Benutzer verknüpfte GPOs werden ignoriert.                       |

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

# Konfigurieren von Benutzerprofilen mit View Persona Management

17

Mit View Persona Management können Sie Benutzerprofile konfigurieren, die dynamisch mit einem Remote-Profil-Repository synchronisiert werden. Diese Funktion gibt Benutzern Zugriff auf eine persönliche Desktop-Erfahrung bei jeder Desktop-Anmeldung. View Persona Management erweitert die Funktionalität und verbessert die Leistung von servergespeicherten Windows-Profilen; dabei müssen jedoch keine servergespeicherten Windows-Profile betrieben werden.

Sie konfigurieren Gruppenrichtlinieneinstellungen, um View Persona Management zu aktivieren und verschiedene Aspekte Ihrer View Persona Management Bereitstellung zu steuern.

Um View Persona Management zu aktivieren und zu verwenden, müssen Sie die entsprechende VMware Horizon-Lizenz haben. Siehe VMware-Endbenutzerlizenzvereinbarung (EULA) unter <http://www.vmware.com/download/eula>.

Dieses Kapitel enthält die folgenden Themen:

- [Bereitstellen von Benutzerpersonas in View](#)
- [Verwenden von View Persona Management mit eigenständigen Systemen](#)
- [Migration von Benutzerprofilen mit View Persona Management](#)
- [Persona-Verwaltung und servergespeicherte Windows-Profile](#)
- [Konfigurieren einer View Persona Management Bereitstellung](#)
- [Empfohlene Vorgehensweisen beim Konfigurieren einer View Persona Management Bereitstellung](#)
- [Gruppenrichtlinieneinstellungen für View Persona Management](#)

## Bereitstellen von Benutzerpersonas in View

Mit der View Persona Management Funktion wird das Remote-Profil eines Benutzers automatisch heruntergeladen, wenn sich der Benutzer bei einem View-Desktop anmeldet. Sie können View für das Speichern von Benutzerprofilen in einem sicheren, zentralisierten Repository konfigurieren. View lädt Persona-Informationen herunter, wenn der Benutzer sie benötigt.

View Persona Management ist eine Alternative zu servergespeicherten Windows-Profilen. View Persona Management erweitert die Funktionalität und verbessert die Leistung im Vergleich zu servergespeicherten Windows-Profilen.

Sie können mit View alle Aspekte von Personas konfigurieren und verwalten. Es ist nicht erforderlich, servergespeicherte Windows-Profile zu konfigurieren. Wenn Sie eine Konfiguration mit servergespeicherten Windows-Profilen verwenden, können Sie die vorhandene Repository-Konfiguration mit View verwenden.

Ein Benutzerprofil ist unabhängig vom View-Desktop. Wenn sich ein Benutzer an einem beliebigen Desktop anmeldet, wird dasselbe Profil angezeigt.

Beispielsweise kann sich der Benutzer an einem Linked-Clone-Desktop-Pool mit dynamischer Zuweisung anmelden und den Desktop-Hintergrund und die Microsoft Word-Einstellungen ändern. Wenn der Benutzer die nächste Sitzung startet, wird eine andere virtuelle Maschine verwendet, der Benutzer sieht jedoch dieselben Einstellungen.

Ein Benutzerprofil umfasst verschiedene, vom Benutzer generierte Informationen:

- Benutzerspezifische Daten und Desktop-Einstellungen
- Anwendungsdaten und -einstellungen
- Von Benutzeranwendungen konfigurierte Windows-Registrierungseinträge

Wenn Sie Desktops mit ThinApp-Anwendungen bereitstellen, können die ThinApp Sandbox-Daten ebenfalls im Benutzerprofil gespeichert und dem Benutzer bei Bedarf zur Verfügung gestellt werden.

View Persona Management minimiert die Zeit, die zum An- und Abmelden von Desktops aufgebracht werden muss. Die An- und Abmeldedauer kann bei servergespeicherten Windows-Profilen zu einem Problem werden.

- Während der Anmeldung lädt View nur die für Windows erforderlichen Dateien herunter, beispielsweise die Benutzerregistrierungsdateien. Andere Dateien werden auf den lokalen Desktop kopiert, wenn der Benutzer oder eine Anwendung sie vom lokalen Profilordner aus öffnet.
- View kopiert kürzlich vorgenommene Änderungen am lokalen Profil in das Remote-Repository, im Normalfall alle paar Minuten. Der Standardwert lautet alle 10 Minuten. Sie können festlegen, wie oft das lokale Profil hochgeladen werden soll.
- Beim Abmelden werden nur solche Dateien, die seit der letzten Änderung aktualisiert wurden, in das Remote-Repository kopiert.

## Verwenden von View Persona Management mit eigenständigen Systemen

Sie können eine eigenständige Version von View Persona Management auf physischen Computern und virtuellen Maschinen installieren, die nicht von View verwaltet werden. Mit dieser Software können Sie Benutzerprofile auf View-Desktops und eigenständigen Systemen verwalten.

Die eigenständige View Persona Management-Software läuft auf den Betriebssystemen Windows XP SP3, Windows Vista, Windows 7 und Windows 8.

Sie können die eigenständige View Persona Management-Software zum Erreichen folgender Ziele verwenden:

- Freigabe von Benutzerprofilen für mehrere eigenständige Systeme und View-Desktops.

Ihre Benutzer können ihre eigenständigen Systeme weiter verwenden sowie View-Desktops mit View Persona Management nutzen. Wenn Sie dieselben View Persona Management-Gruppenrichtlinieneinstellungen für die Steuerung von View-Desktops und physischen Systemen verwenden, erhalten Benutzer ihre aktuellen Profile bei jeder Anmeldung, unabhängig davon, ob sie ihre älteren Computer oder View-Desktops verwenden.

---

**Hinweis** View Persona Management unterstützt keine parallelen aktiven Sitzungen. Benutzer müssen sich bei einer Sitzung abmelden, bevor sie sich bei einer anderen anmelden können.

---

- Migrieren von Benutzerprofilen von physischen Systemen auf View-Desktops

Wenn Sie beabsichtigen, ältere physische Computer künftig in einer View-Bereitstellung zu nutzen, können Sie auf den älteren Systemen ein eigenständiges View Persona Management installieren, bevor Sie Ihren Benutzern View-Desktops bereitstellen. Wenn sich Benutzer bei ihren alten Systemen anmelden, werden ihre Profile im View-Remote-Profil-Repository gespeichert. Wenn sich Benutzer zum ersten Mal bei ihren View-Desktops anmelden, werden ihre bestehenden Profile auf ihre View-Desktops heruntergeladen.

- Durchführen einer stufenweisen Migration von physischen Systemen zu View-Desktops

Wenn Sie Ihre Bereitstellung stufenweise bereitstellen, können Benutzer, die noch keinen Zugriff auf View-Desktops haben, das eigenständige View Persona Management verwenden. Während jede Gruppe von View-Desktops bereitgestellt wird, können Benutzer auf ihre Profile auf ihren View-Desktops zugreifen, und die alten Systeme können nach und nach ausgemustert werden. Dieses Szenario setzt sich aus den beiden vorherigen Szenarien zusammen.

- Unterstützung aktueller Profile, wenn Benutzer offline gehen.

Benutzer von eigenständigen Laptops können die Verbindung zum Netzwerk trennen. Wenn sich ein Benutzer wieder verbindet, lädt View Persona Management die letzten Änderungen am lokalen Profil des Benutzers an das Remote-Profil-Repository hoch.

---

**Hinweis** Bevor ein Benutzer offline gehen kann, muss das Benutzerprofil vollständig auf das lokale System heruntergeladen werden.

---

## Migration von Benutzerprofilen mit View Persona Management

Mit View Persona Management können Sie vorhandene Benutzerprofile mit einer Vielzahl von Einstellungen auf View-Desktops migrieren. Wenn sich Benutzer nach einer abgeschlossenen Profilmigration auf ihren View-Desktops anmelden, finden sie ihre persönlichen Einstellungen und Daten vor, die sie auf den älteren Systemen verwendet haben.



Durch die Migration von Benutzerprofilen können Sie folgende Desktop-Migrationsziele erreichen:

- Sie können die Systeme der Benutzer von Windows XP auf Windows 7 oder Windows 8 aktualisieren und Ihre Benutzer von physischen Computern zum ersten mal auf View migrieren.
- In einer vorhandenen View-Bereitstellung können Sie ein Upgrade von Windows XP-View-Desktops auf Windows 7- oder Windows 8-View-Desktops durchführen.
- Sie können eine Migration von physischen Computern auf View-Desktops durchführen, ohne die Betriebssysteme zu aktualisieren.

Damit diese Szenarien unterstützt werden, bietet View Persona Management ein Dienstprogramm zur Profilmigration und ein eigenständiges View Persona Management-Installationsprogramm für physische oder virtuelle Maschinen, auf denen nicht View Agent 5.x installiert ist.

[Tabelle 17-1. Szenarien für die Benutzerprofilmigration](#) zeigt verschiedene Migrationsszenarien und beschreibt die Aufgaben, die Sie in jedem Szenario jeweils durchführen sollten.

Tabelle 17-1. Szenarien für die Benutzerprofilmigration

| Wenn dies Ihre ursprüngliche Bereitstellung ist ...   | und dies Ihre Zielbereitstellung ...                 | führen Sie diese Aufgaben durch:  |
|---|--|---|
| Physische Windows XP-Computer   | Windows 7-View-Desktops oder Windows 8-View-Desktops | <ol style="list-style-type: none"> <li>1 Konfigurieren Sie Windows 7- oder Windows 8-View-Desktops für Ihre Benutzer mit View Persona Management. Siehe <a href="#">Konfigurieren einer View Persona Management Bereitstellung</a>.</li> </ol> <p><b>Hinweis</b> Stellen Sie Ihren Benutzern Windows 7- oder Windows 8-View-Desktops erst bereit, nachdem Sie Schritt 2 abgeschlossen haben.</p> <ol style="list-style-type: none"> <li>2 Führen Sie das Profilmigrationsdienstprogramm View V1 auf V2 aus. <ul style="list-style-type: none"> <li>■ Geben Sie für die Quellprofile die lokalen Profile auf den physischen Windows XP-Computern an.</li> <li>■ Geben Sie für Zielprofile das Remote-Profil-Repository an, das Sie für die View-Bereitstellung konfiguriert haben.</li> </ul> <p>Weitere Informationen finden Sie im Dokument <i>Benutzerprofilmigration von View</i>.</p> </li> <li>3 Erlauben Sie Ihren Benutzern, sich bei ihren Windows 7- oder Windows 8-View-Desktops anzumelden.</li> </ol> |
| Physische Windows XP-Computer oder virtuelle Maschinen, die eine Roaming-Benutzerprofillosung verwenden. Ihre Bereitstellung kann beispielsweise eine dieser Lösungen nutzen: <ul style="list-style-type: none"> <li>■ View Persona Management</li> <li>■ RTO Virtual Profiles</li> <li>■ Servergespeicherte Windows-Profile</li> </ul> Bei diesem Szenario müssen die ursprünglichen Benutzerprofile in einem Remote-Profil-Repository beibehalten werden. | Windows 7-View-Desktops oder Windows 8-View-Desktops | <ol style="list-style-type: none"> <li>1 Konfigurieren Sie Windows 7- oder Windows 8-View-Desktops für Ihre Benutzer mit View Persona Management. Siehe <a href="#">Konfigurieren einer View Persona Management Bereitstellung</a>.</li> </ol> <p><b>Hinweis</b> Stellen Sie Ihren Benutzern Windows 7- oder Windows 8-View-Desktops erst bereit, nachdem Sie Schritt 2 abgeschlossen haben.</p> <ol style="list-style-type: none"> <li>2 Führen Sie das Profilmigrationsdienstprogramm View V1 auf V2 aus. <ul style="list-style-type: none"> <li>■ Geben Sie für die Quellprofile das Remote-Profil-Repository für die Windows XP-Systeme an.</li> <li>■ Geben Sie für Zielprofile das Remote-Profil-Repository an, das Sie für die View-Bereitstellung konfiguriert haben.</li> </ul> <p>Weitere Informationen finden Sie im Dokument <i>Benutzerprofilmigration von View</i>.</p> </li> <li>3 Erlauben Sie Ihren Benutzern, sich bei ihren Windows 7-View-Desktops anzumelden.</li> </ol>                     |

| Wenn dies Ihre ursprüngliche Bereitstellung ist ...  | und dies Ihre Zielbereitstellung ...                 | führen Sie diese Aufgaben durch:   |
|--|--|--|
| Physische Windows XP-Computer oder virtuelle Maschinen.<br>Auf den älteren Systemen darf nicht View Agent 5.x installiert sein.                | Windows XP-View-Desktops                             | <ol style="list-style-type: none"> <li>1 Konfigurieren Sie Windows XP-View-Desktops für Ihre Benutzer mit View Persona Management. Siehe <a href="#">Konfigurieren einer View Persona Management Bereitstellung</a>.</li> <li>2 Installieren Sie die eigenständige View Persona Management-Software auf den Windows XP-Systemen. Siehe <a href="#">Installieren eines eigenständigen View Persona Management</a>.</li> <li>3 Konfigurieren Sie die älteren Windows XP-Systeme so, dass sie dasselbe Remote-Profil-Repository wie die View-Desktops verwenden. Siehe <a href="#">Konfigurieren eines Benutzerprofil-Repositorys</a>.<br/><br/>Der einfachste Ansatz besteht darin, in Active Directory dieselben Einstellungen für die View Persona Management-Gruppenrichtlinien zu verwenden, um sowohl die älteren Systeme als auch die View-Desktops zu steuern. Siehe <a href="#">Hinzufügen der View Persona Management ADM-Vorlagendatei</a>.</li> <li>4 Stellen Sie die Windows XP-View-Desktops Ihren Benutzern bereit.</li> </ol>   |
| Physische Windows 7- oder Windows 8-Computer oder virtuelle Maschinen.<br>Auf den älteren Systemen darf nicht View Agent 5.x installiert sein. | Windows 7-View-Desktops oder Windows 8-View-Desktops | <ol style="list-style-type: none"> <li>1 Konfigurieren Sie Windows 7- oder Windows 8-View-Desktops für Ihre Benutzer mit View Persona Management. Siehe <a href="#">Konfigurieren einer View Persona Management Bereitstellung</a>.</li> <li>2 Installieren Sie die eigenständige View Persona Management-Software auf den Windows 7- oder Windows 8-Systemen. Siehe <a href="#">Installieren eines eigenständigen View Persona Management</a>.</li> <li>3 Konfigurieren Sie die älteren Windows 7- oder Windows 8-Systeme so, dass sie dasselbe Remote-Profil-Repository wie die View-Desktops verwenden. Siehe <a href="#">Konfigurieren eines Benutzerprofil-Repositorys</a>.<br/><br/>Der einfachste Ansatz besteht darin, in Active Directory dieselben Einstellungen für die View Persona Management-Gruppenrichtlinien zu verwenden, um sowohl die älteren Systeme als auch die View-Desktops zu steuern. Siehe <a href="#">Hinzufügen der View Persona Management ADM-Vorlagendatei</a>.</li> <li>4 Stellen Sie Ihren Benutzern die Windows 7- oder Windows 8-View-Desktops bereit.</li> </ol> |

## Persona-Verwaltung und servergespeicherte Windows-Profile

Wenn Persona-Verwaltung aktiviert ist, können Sie die Personas der View-Benutzer nicht mit den servergespeicherten Windows-Profilen verwalten.

Wenn Sie sich z. B. beim Gastbetriebssystem eines Desktops anmelden, zur Registerkarte **Erweitert** im Dialogfeld „Systemeigenschaften“ navigieren und die Benutzerprofileinstellungen von **Servergespeichertes Profil** in **Lokales Profil** ändern, synchronisiert View Persona Management die Benutzerpersonas weiterhin zwischen dem lokalen Desktop und dem Remote-Persona-Repository.

Sie können jedoch Dateien und Ordner innerhalb von Benutzer-Personas angeben, die von servergespeicherte Windows-Profilen statt von View Persona Management verwaltet werden. Sie verwenden zum Angeben dieser Dateien und Ordner die Richtlinie **Synchronisierung von servergespeicherten Windows-Profilen**.

## Konfigurieren einer View Persona Management Bereitstellung

Um View Persona Management zu konfigurieren, richten Sie ein Remote-Repository ein, in dem Benutzerprofile gespeichert werden, installieren View Agent mit der **View Persona Management**-Setupoption auf virtuellen Maschinen, die Remote-Desktop-Sitzungen bereitstellen, fügen View Persona Management-Gruppenrichtlinieneinstellungen hinzu und konfigurieren diese, und stellen schließlich Desktop-Pools bereit.

Sie können View Persona Management auch für eine Bereitstellung ohne View konfigurieren. Sie installieren die eigenständige Version von View Persona Management auf Laptops, Desktops oder virtuellen Maschinen Ihrer Benutzer ohne View. Sie müssen auch ein Remote-Repository einrichten und Gruppenrichtlinieneinstellungen für View Persona Management konfigurieren.

## Übersicht über das Einrichten einer View Persona Management Bereitstellung

Um eine View-Desktop-Bereitstellung oder eigenständige Computer mit View Persona Management einzurichten, müssen Sie verschiedene Aufgaben auf hoher Ebene durchführen.

Diese Reihenfolge ist zu empfehlen, obwohl Sie diese Aufgaben auch in anderer Reihenfolge durchführen können. Beispielsweise können Sie Gruppenrichtlinieneinstellungen in Active Directory konfigurieren oder neu konfigurieren, nachdem Sie Desktop-Pools bereitgestellt haben.

- 1 Konfigurieren Sie ein Remote-Repository zum Speichern der Benutzerprofile.

Sie können eine Netzwerkfreigabe konfigurieren oder einen vorhandenen Active Directory-Benutzerprofilpfad verwenden, den Sie für servergespeicherte Windows-Profile konfiguriert haben.

- 2 Installieren Sie View Agent mit der Einrichtungsoption **View Persona Management** auf virtuellen Maschinen, die Sie zum Erstellen von Desktop-Pools verwenden.

Um View Persona Management für Laptops, Desktops oder virtuelle Maschinen ohne View zu konfigurieren, installieren Sie die eigenständige View Persona Management-Software auf jedem Computer in der beabsichtigten Bereitstellung.

- 3 Fügen Sie die View Persona Management ADM-Vorlagendatei der „Active Directory-Server“- oder der „Richtlinie für 'Lokaler Computer'“-Konfiguration auf der übergeordneten virtuellen Maschine hinzu.

Um View Persona Management für Ihre gesamte Bereitstellung mit oder ohne View zu konfigurieren, fügen Sie die ADM-Vorlagendatei zu Active Directory hinzu.

Um View Persona Management einem Desktop-Pool hinzuzufügen, können Sie folgendermaßen vorgehen:

- Fügen Sie die ADM-Vorlagendatei der virtuelle Maschine hinzu, die Sie zum Erstellen des Pools verwenden.
  - Fügen Sie die ADM-Vorlagendatei zu Active Directory hinzu und wenden Sie die Gruppenrichtlinieneinstellungen auf die OU an, die die Maschinen im Pool enthält.
- 4 Aktivieren Sie View Persona Management, indem Sie die Gruppenrichtlinieneinstellung **Benutzerpersona verwalten** aktivieren.
  - 5 Wenn Sie eine Netzwerkfreigabe für das Remoteprofil-Repository konfiguriert haben, aktivieren Sie die Gruppenrichtlinieneinstellung **Speicherort für das Persona-Repository**, und geben Sie den Netzwerkfreigabepfad an.
  - 6 (Optional) Konfigurieren Sie die Gruppenrichtlinieneinstellungen in Active Directory oder der Konfiguration für die „Richtlinie für 'Lokaler Computer'“.
  - 7 Erstellen Sie Desktop-Pools aus virtuellen Maschinen, auf denen Sie View Agent mit der Einrichtungsoption **View Persona Management** installiert haben.

## Konfigurieren eines Benutzerprofil-Repositorys

Sie können ein Remote-Repository konfigurieren, um die Benutzerdaten und -einstellungen, anwendungsspezifischen Daten und andere vom Benutzer generierte Informationen in Benutzerprofilen zu speichern. Wenn servergespeicherte Windows-Profiles in Ihrer Bereitstellung konfiguriert sind, können Sie stattdessen einen vorhandenen Active Directory-Benutzerprofilpfad verwenden.

---

**Hinweis** Sie können View Persona Management konfigurieren, ohne servergespeicherte Windows-Profiles konfigurieren zu müssen.

---

### Voraussetzungen

- Machen Sie sich mit den mindestens erforderlichen Zugriffsberechtigungen vertraut, die für die Konfiguration eines freigegebenen Ordners benötigt werden. Siehe [Festlegen von Zugriffsberechtigungen für freigegebene Ordner für View Persona Management](#).
- Machen Sie sich mit den Richtlinien zum Erstellen eines Benutzerprofil-Repositorys vertraut. Siehe [Erstellen einer Netzwerkfreigabe für View Persona Management](#)

## Verfahren

- 1 Bestimmen Sie, ob Sie einen vorhandenen Active Directory-Benutzerprofilpfad verwenden oder ein Benutzerprofil-Repository auf einer Netzwerkfreigabe konfigurieren möchten.

| Option   | Aktion  |
|--|---|
| <b>Verwenden Sie einen vorhandenen Active Directory-Benutzerprofilpfad</b>           | Wenn Sie über eine vorhandene Konfiguration servergespeicherter Windows-Profile verfügen, können Sie den in Active Directory angegebenen Benutzerprofilpfad verwenden, der servergespeicherte Profile unterstützt. Sie können die übrigen Schritte in dieser Schrittfolge überspringen. |
| <b>Konfigurieren einer Netzwerkfreigabe zur Speicherung des Persona-Repositories</b> | Wenn Sie keine servergespeicherten Windows-Profile konfiguriert haben, müssen Sie eine Netzwerkfreigabe für das Benutzerprofil-Repository konfigurieren. Befolgen Sie die verbleibenden Schritte in dieser Schrittfolge.  |

- 2 Erstellen Sie einen freigegebenen Ordner auf einem Computer, auf den Ihre Benutzer von den Gastbetriebssystemen auf ihren Desktops aus zugreifen können.

Wenn %Benutzername% nicht im von Ihnen konfigurierten Ordnerpfad enthalten ist, hängt View Persona Management %Benutzername%.%Benutzerdomäne% an den Pfad an.

Beispiel: \\server.domain.com\VPRepository\%username%.%userdomain%

- 3 Legen Sie Zugriffsberechtigungen für die Ordnerfreigaben fest, die Benutzerprofile enthalten.

**Vorsicht** Stellen Sie sicher, dass die Zugriffsberechtigungen korrekt konfiguriert werden. Die falsche Konfiguration der Zugriffsberechtigungen auf dem freigegebenen Ordner ist die häufige Ursache für Probleme mit View Persona Management.

## Festlegen von Zugriffsberechtigungen für freigegebene Ordner für View Persona Management

View Persona Management und servergespeicherte Windows-Profile erfordern ein bestimmtes Minimum an Berechtigungen für das Benutzerprofil-Repository. View Persona Management erfordert außerdem, dass die Sicherheitsgruppe der Benutzer, die Daten im freigegebenen Ordner ablegen, über Leseattribute für diesen Ordner verfügen muss.

Legen Sie die erforderlichen Zugriffsberechtigungen für Ihr Benutzerprofil-Repository und Ihre umgeleitete Ordnerfreigabe fest.

**Tabelle 17-2. Minimum an NTFS-Berechtigungen, die für das Benutzerprofil-Repository und die umgeleitete Ordnerfreigabe erforderlich sind.**

| Benutzerkonto       | Mindestens erforderliche Berechtigungen  |
|---------------------|--|
| Erstellungsbesitzer | Vollzugriff, Unterordner und Nur Dateien   |
| Administrator       | Keine. Aktivieren Sie stattdessen die Windows-Gruppenrichtlinieneinstellung <b>Administratorensicherheitsgruppe zu servergespeicherten Benutzerprofilen hinzufügen</b> . Diese Richtlinieneinstellung befindet sich im Gruppenrichtlinienobjekt-Editor im Verzeichnis <b>Computerkonfiguration\Administrative Vorlagen\System\Benutzerprofile\</b> . |

| Benutzerkonto  | Mindestens erforderliche Berechtigungen  |
|--|--|
| Sicherheitsgruppe von Benutzern, die Daten zur Freigabe ablegen müssen | Ordner auflisten/Daten lesen, Ordner erstellen/Daten anhängen, Leseattribute – Nur dieser Ordner |
| Alle   | Keine Berechtigungen   |
| Lokales System   | Vollzugriff, Dieser Ordner, Unterordner und Dateien  |

**Tabelle 17-3. Erforderliche Berechtigungen für die Freigabeebene (SMB-Berechtigungen) für ein Benutzerprofil-Repository und eine umgeleitete Ordnerfreigabe**

| Benutzerkonto  | Standardberechtigungen | Mindestens erforderliche Berechtigungen |
|--|------------------------|---|
| Alle   | Nur Lesezugriff        | Keine Berechtigungen                    |
| Sicherheitsgruppe von Benutzern, die Daten zur Freigabe ablegen müssen | –                      | Vollzugriff                             |

Weitere Informationen zur Sicherheit bei servergespeicherten Benutzerprofilen finden Sie im Microsoft TechNet-Thema *Security Recommendations for Roaming User Profiles Shared Folders*. [http://technet.microsoft.com/en-us/library/cc757013\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc757013(Ws.10).aspx)

## Erstellen einer Netzwerkfreigabe für View Persona Management

Sie müssen bestimmte Richtlinien befolgen, wenn Sie einen freigegebenen Ordner erstellen, der als Profil-Repository verwendet werden soll.

- Wenn Sie Windows 8-Desktops verwenden und Ihre Netzwerkfreigabe ein OneFS-Dateisystem auf einem EMC Isilon NAS-Gerät verwendet, muss das OneFS-Dateisystem Version 6.5.5.11 oder höher aufweisen.
- Sie erstellen den freigegebenen Ordner auf einem Server, einem NAS-Gerät (Network-Attached Storage) oder einem Netzwerkspeicher.
- Der freigegebene Ordner muss sich nicht in derselben Domäne befinden wie View-Verbindungsserver.
- Der freigegebene Ordner muss sich in derselben Active Directory-Ordnerstruktur befinden wie die Benutzer, die Profile im freigegebenen Ordner speichern.
- Sie müssen ein freigegebenes Laufwerk verwenden, das groß genug ist, um die Benutzerprofilinformationen für Ihre Benutzer zu speichern. Zum Unterstützen einer großen View-Bereitstellung können Sie separate Repositories für verschiedene Desktop-Pools konfigurieren.

Wenn Benutzer zu mehr als einem Pool berechtigt sind, müssen die Pools mit gemeinsamen Benutzern im selben Profil-Repository konfiguriert sein. Wenn Sie einen Benutzer zu zwei Pools mit verschiedenen Profil-Repositories berechnen, kann der Benutzer von Desktops in jedem Pool nicht auf dieselbe Version des Profils zugreifen.

- Sie müssen den vollständigen Profilpfad erstellen, unter dem die Benutzerprofilordner erstellt werden. Wenn der Pfad unvollständig ist, erstellt Windows die fehlenden Ordner, wenn sich der erste Benutzer anmeldet und die Sicherheitsbeschränkungen des Benutzers auf diese Ordner zuweist. Windows weist allen unter dem Pfad erstellten Ordnern dieselben Sicherheitsbeschränkungen zu.

Für Benutzer1 könnten Sie beispielsweise den View Persona Management-Pfad `\\server\VPRepository\profiles\Benutzer1` konfigurieren. Wenn Sie die Netzwerkfreigabe `\\\\server\VPRepository` erstellen und der Ordner `profiles` nicht vorhanden ist, erstellt Windows den Pfad `\profiles\Benutzer1`, wenn sich Benutzer1 anmeldet. Windows beschränkt den Zugriff auf die Ordner `\\profiles\Benutzer1` auf das Konto Benutzer1. Wenn sich ein anderer Benutzer mit einem Profilpfad in `\\server\VPRepository\profiles` anmeldet, kann der zweite Benutzer nicht auf das Repository zugreifen, und das Benutzerprofil wird nicht repliziert.

## Installieren von View Agent mit der View Persona Management Option

Zum Verwenden von View Persona Management mit View-Desktops müssen Sie View Agent mit der Einrichtungsoption **View Persona Management** auf den virtuellen Maschinen installieren, die Sie zum Erstellen von Desktop-Pools verwenden.

Für einen automatisierten Pool installieren Sie View Agent mit der Einrichtungsoption **View Persona Management** auf der virtuellen Maschine, die Sie als übergeordnetes Element oder als Vorlage verwenden. Wenn Sie einen Desktop-Pool von der virtuellen Maschine aus erstellen, wird die View Persona Management Software auf Ihren View-Desktops bereitgestellt.

Für einen manuellen Pool müssen Sie View Agent mit der Einrichtungsoption **View Persona Management** auf jeder virtuellen Maschine installieren, die als Desktop im Pool verwendet wird. Verwenden Sie Active Directory, um View Persona Management Gruppenrichtlinien für einen manuellen Pool zu konfigurieren. Alternativ können Sie auch auf jedem einzelnen Computer die ADM-Vorlagendatei hinzufügen und Gruppenrichtlinien konfigurieren.

---

**Hinweis** Ein Benutzer kann nicht auf dasselbe Profil zugreifen, wenn der Benutzer zwischen Desktops wechselt, die die Benutzerprofile „v1“ und „v2“ haben. Windows XP verwendet v1-Profile. Windows 8 und Windows 7 verwenden v2-Profile.

Wenn sich ein Benutzer beispielsweise bei einem Windows XP-Desktop und später bei einem Windows 7-Desktop anmeldet, kann die virtuelle Windows 7-Maschine das v1-Profil nicht lesen, das während der Windows XP-Desktopsitzung erstellt wurde.

Sie können das Befehlszeilendienstprogramm View-Profilmigration verwenden, um Windows XP-Profile in Windows 7- oder Windows 8-Profile zu migrieren. Weitere Informationen finden Sie im Dokument *Benutzerprofilmigration von View*.

---

### Voraussetzungen

- Stellen Sie sicher, dass Sie die Installation auf einer virtuellen Maschine mit Windows 8, Windows 7, Windows Vista oder Windows XP durchführen. View Persona Management funktioniert nicht auf Microsoft-RDS-Hosts.



Das Installieren von View Agent mit der Einrichtungsoption **View Persona Management** funktioniert auf physischen Computern nicht. Sie können die eigenständige View Persona Management-Software auf physischen Computern installieren. Siehe [Installieren eines eigenständigen View Persona Management](#) .

- Stellen Sie sicher, dass Sie sich als Administrator auf der virtuellen Maschine anmelden können.
- Stellen Sie sicher, dass kein natives RTO Virtual Profile 2.0 auf der virtuellen Maschine installiert ist. Wenn ein natives RTO Virtual Profile 2.0 vorhanden ist, deinstallieren Sie es, bevor Sie View Agent mit der Einrichtungsoption **View Persona Management** installieren.
- Laden Sie auf virtuellen Maschinen mit Windows XP das Dienstprogramm Microsoft User Profile Hive Cleanup Service (UPHClean) herunter und installieren Sie dieses im Gastbetriebssystem. Siehe [Installieren von UPHClean auf Windows XP-Computern, die View Persona Management verwenden](#).
- Machen Sie sich mit dem Installieren von View Agent vertraut. Siehe [Installieren von View Agent auf einer virtuellen Maschine](#) oder [Installieren von View Agent auf einer nicht verwalteten Maschine](#).

#### Verfahren

- ◆ Wenn Sie View Agent auf einer virtuellen Maschine installieren, wählen Sie die Einrichtungsoption **View Persona Management** aus.

#### Nächste Schritte

Fügen Sie die View Persona Management-ADM-Vorlagendatei der „Active Directory-Server“- oder der „Richtlinie für 'Lokaler Computer'“-Konfiguration auf der virtuellen Maschine selbst hinzu. Siehe [Hinzufügen der View Persona Management ADM-Vorlagendatei](#).

### Installieren von UPHClean auf Windows XP-Computern, die View Persona Management verwenden

Der Microsoft User Profile Hive Cleanup Service (UPHClean) stellt sicher, dass Benutzersitzungen vollständig getrennt werden, wenn sich ein Benutzer abmeldet. UPHClean bereinigt Registrierungsschlüssel-Handles, die sonst von anderen Vorgängen oder Anwendungen freigelegt werden könnten. Dieser Service hilft dabei sicherzustellen, dass die Registry-Struktur des Benutzers entladen wird, damit diese erfolgreich hochgeladen und die lokale Persona gelöscht werden kann.

Wenn Sie View Persona Management auf virtuellen Windows XP-Maschinen konfigurieren, laden Sie UPHClean in das Gastbetriebssystem herunter und installieren Sie den Dienst.

Sie können den UPHClean-Dienst von folgendem Speicherort herunterladen: <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6676>.

Der UPHClean-Dienst ist in die Betriebssysteme Windows 7 und Windows Vista integriert. Unter diesen Betriebssystemen müssen Sie den Dienst nicht installieren.

### Installieren eines eigenständigen View Persona Management

Installieren Sie die eigenständige Version von View Persona Management, um View Persona Management mit anderen physischen Computern oder virtuellen Maschinen ohne View verwenden zu

können. Sie können eine interaktive Installation oder eine vollautomatische Installation auf der Befehlszeile ausführen.

Installieren Sie die eigenständige View Persona Management-Software auf jedem einzelnen Computer oder jeder einzelnen virtuellen Maschine in der beabsichtigten Bereitstellung.

### Voraussetzungen

- Stellen Sie sicher, dass Sie die Installation auf einem physischen Computer oder einer virtuellen Maschine mit Windows 8, Windows 7, Windows Vista oder Windows XP SP3 durchführen. View Persona Management funktioniert nicht auf Windows-Servern oder Microsoft-RDS-Hosts. Stellen Sie sicher, dass das System die in „Unterstützte Betriebssysteme für die eigenständige View Persona Management-Software“ im Dokument *Installation von View* beschriebenen Anforderungen erfüllt.
- Stellen Sie sicher, dass Sie sich als Administrator beim System anmelden können.
- Überprüfen Sie, dass nicht View Agent 5.x oder höher auf dem Computer installiert ist.
- Stellen Sie sicher, dass kein natives RTO Virtual Profile 2.0 auf der virtuellen Maschine installiert ist.
- Falls Sie vorhaben, eine automatische Installation durchzuführen, machen Sie sich mit den Befehlszeilenoptionen des MSI-Installers vertraut. Siehe [Befehlszeilenoptionen für Microsoft Windows Installer](#).

### Verfahren

- 1 Laden Sie das Installationsprogramm für das eigenständige View Persona Management von der VMware-Produktseite unter <http://www.vmware.com/products/> herunter.

Der Dateiname des Installers lautet VMware-personamanagement-y.y.y-xxxxxx.exe oder VMware-personamanagement-x86\_64-y.y.y-xxxxxx.exe, wobei y.y.y die Versionsnummer und xxxxxx die Buildnummer ist.

- 2 Führen Sie das Installationsprogramm interaktiv aus oder führen Sie eine automatische Installation durch.

| Option                           | Beschreibung   |
|----------------------------------|--|
| <b>Interaktive Installation</b>  | <ol style="list-style-type: none"> <li>a Zum Starten des Installationsprogramms doppelklicken Sie auf die Installationsdatei.</li> <li>b Stimmen Sie den Lizenzbedingungen von VMware zu.</li> <li>c Klicken Sie auf <b>Installieren</b>.</li> </ol> <p>View Persona Management wird standardmäßig im Verzeichnis C:\Programme\VMware\VMware View Persona Management installiert.</p> <ol style="list-style-type: none"> <li>d Klicken Sie auf <b>Fertig stellen</b>.</li> </ol> |
| <b>Automatische Installation</b> | <p>Öffnen Sie eine Windows-Eingabeaufforderung auf der Maschine und geben Sie den Installationbefehl in einer Zeile ein.</p> <p>Beispiel: VMware-personamanagement-y.y.y-xxxxxx.exe /s /v"/qn /l*v ""c:\persona.log"" ALLUSERS=1"</p> <p><b>Wichtig</b> Sie müssen die Eigenschaft ALLUSERS=1 in der Befehlszeile einschließen.</p>  |

- 3 Starten Sie das System neu, damit die durch die Installation vorgenommenen Änderungen wirksam werden.

### Nächste Schritte

Fügen Sie die View Persona Management-ADM-Vorlagendatei zur Active Directory- oder lokalen Gruppenrichtlinienkonfiguration hinzu.

## Hinzufügen der View Persona Management ADM-Vorlagendatei

Die View Persona Management ADM-Vorlagendatei enthält Gruppenrichtlinieneinstellungen, mit denen Sie View Persona Management konfigurieren können. Bevor Sie die Richtlinien konfigurieren können, müssen Sie die ADM-Vorlagendatei den lokalen Systemen oder dem Active Directory-Server hinzufügen.

Um View Persona Management auf einem einzelnen System zu konfigurieren, können Sie die Gruppenrichtlinieneinstellungen der Konfiguration „Richtlinie für ‚Lokaler Computer‘“ auf dem lokalen System hinzufügen.

Zum Konfigurieren von View Persona Management für einen Desktop-Pool können Sie die Gruppenrichtlinieneinstellungen der Richtlinie „Local Computer Policy (Richtlinie für 'Lokaler Computer')“ auf der virtuellen Maschine hinzufügen, die Sie als übergeordnetes Element oder Vorlage zum Bereitstellen des Desktop-Pools verwenden.

Zum Konfigurieren von View Persona Management auf domänenweiter Ebene und zum Anwenden der Konfiguration auf viele View-Computer oder Ihre gesamte Bereitstellung können Sie die Gruppenrichtlinieneinstellungen den Gruppenrichtlinienobjekten (GPOs) auf Ihrem Active Directory-Server hinzufügen. In Active Directory können Sie eine Organisationseinheit (OU) für die View-Computer erstellen, die View Persona Management verwenden, ein oder mehrere GPOs erstellen und die GPOs mit der OU verknüpfen. Um separate View Persona Management-Richtlinien für unterschiedliche Benutzertypen zu konfigurieren, können Sie OUs für bestimmte Computersets von View erstellen und verschiedene GPOs auf die OUs anwenden.

Beispiel: Sie erstellen eine OU für View-Computer mit View Persona Management und eine andere OU für physische Computer, auf denen die eigenständige View Persona Management-Software installiert ist.

Ein Beispiel für das Implementieren von Active Directory-Gruppenrichtlinien in View finden Sie unter [Beispiel einer Active Directory-Gruppenrichtlinie](#).

## Hinzufügen der Persona-Verwaltung-ADM-Vorlage zu einem Einzelsystem

Um View Persona Management für einen einzelnen Desktop-Pool zu konfigurieren, fügen Sie die Persona Management-ADM-Vorlagendatei zur Richtlinie für den lokalen Computer auf der virtuellen Maschine hinzu, die Sie zum Erstellen des Pools verwenden. Um View Persona Management für ein einzelnes System zu konfigurieren, müssen Sie diesem System die Persona Management-ADM-Vorlagendatei hinzufügen.

### Voraussetzungen

- Stellen Sie sicher, dass View Agent mit der View Persona Management-Einrichtungsoption auf dem System installiert ist. Siehe [Installieren von View Agent mit der View Persona Management Option](#).

- Stellen Sie sicher, dass Sie sich als Administrator beim System anmelden können.

## Verfahren

- 1 Laden Sie die View GPO-Bundle-ZIP-Datei von der Download-Site von VMware Horizon (mit View) unter <http://www.vmware.com/go/downloadview> herunter.

Der Dateiname ist VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip (x.x.x ist die Version, yyyyyyy die Build-Nummer). Alle ADM- und ADMX-Dateien, die Gruppenrichtlinieneinstellungen für View bereitstellen, sind in dieser Datei verfügbar.

- 2 Extrahieren Sie die Datei und kopieren Sie die ADM-Datei „ViewPM.adm“ auf Ihr lokales System.
- 3 Klicken Sie auf dem lokalen System auf **Start > Ausführen**.
- 4 Geben Sie **gpedit.msc** ein und klicken Sie auf **OK**.
- 5 Navigieren Sie im Fenster **Richtlinie für 'Lokaler Computer'** zu **Computerkonfiguration** und klicken Sie mit der rechten Maustaste auf **Administrative Vorlagen**.

---

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

---

- 6 Klicken Sie auf **Vorlagen hinzufügen/entfernen** und dann auf **Hinzufügen**.
- 7 Navigieren Sie zu dem Verzeichnis, in dem sich die Datei „ViewPM.adm“ befindet.
- 8 Wählen Sie die Datei ViewPM.adm und klicken Sie dann auf **Hinzufügen**.
- 9 Schließen Sie das Fenster **AVorlagen hinzufügen/entfernen**.

Die Gruppenrichtlinieneinstellungen für View Persona Management werden der Konfiguration „Richtlinie für ‚Lokaler Computer‘“ auf dem lokalen System hinzugefügt. Sie müssen gpedit.msc verwenden, um diese Konfiguration anzuzeigen.

## Nächste Schritte

Konfigurieren Sie die Gruppenrichtlinieneinstellungen für View Persona Management auf dem lokalen System. Siehe [Konfigurieren von View Persona Management-Richtlinien](#).

## Hinzufügen der Persona-Verwaltung-ADM-Vorlage zu Active Directory

Um View Persona Management für Ihre Bereitstellung zu konfigurieren, können Sie die View Persona Management ADM-Vorlagendatei zu einem Gruppenrichtlinienobjekt (GPO) auf Ihrem Active Directory-Server hinzufügen.

## Voraussetzungen

- Erstellen Sie Gruppenrichtlinienobjekte für Ihre View Persona Management-Bereitstellung und verknüpfen Sie sie mit der OU, die die View-Maschinen enthält, welche View Persona Management verwenden. Siehe [Beispiel einer Active Directory-Gruppenrichtlinie](#).
- Vergewissern Sie sich, dass Microsoft Management Console (MMC) und das Snap-In „Gruppenrichtlinienobjekt-Editor“ auf Ihrem Active Directory-Server installiert sind.

- Stellen Sie sicher, dass View Agent mit der View Persona Management Einrichtungsoption auf einem System installiert ist, auf das von Ihrem Active Directory-Server aus zugegriffen werden kann. Siehe [Installieren von View Agent mit der View Persona Management Option](#).

## Verfahren

- 1 Laden Sie die View GPO-Bundle-ZIP-Datei von der Download-Site von VMware Horizon (mit View) unter <http://www.vmware.com/go/downloadview> herunter.  
  
Der Dateiname ist VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip (x.x.x ist die Version, yyyyyyy die Build-Nummer). Alle ADM- und ADMX-Dateien, die Gruppenrichtlinieneinstellungen für View bereitstellen, sind in dieser Datei verfügbar.
- 2 Extrahieren Sie die Datei und kopieren Sie die View Persona Management ADM-Vorlagendatei „ViewPM.adm“ auf Ihren Active Directory-Server.
- 3 Öffnen Sie auf Ihrem Active Directory-Server die Verwaltungskonsole für Gruppenrichtlinien.  
  
Rufen Sie z. B. das Dialogfeld „Ausführen“ auf, geben Sie **gpmmc.msc** ein und klicken Sie auf **OK**.
- 4 Wählen Sie im linken Fensterbereich die Domäne oder die OU aus, die Ihre View-Maschinen enthält.
- 5 Klicken Sie im rechten Fensterbereich auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **Bearbeiten**.  
  
Das Fenster **Gruppenrichtlinienobjekt-Editor** wird angezeigt.
- 6 Klicken Sie im Gruppenrichtlinienobjekt-Editor mit der rechten Maustaste unter **Computerkonfiguration** auf **Administrative Vorlagen** und wählen Sie **Vorlagen hinzufügen/entfernen**.
- 7 Klicken Sie auf **Hinzufügen**, suchen Sie nach der Datei ViewPM.adm und klicken Sie auf **Öffnen**.
- 8 Klicken Sie auf **Schließen**, um die Richtlinieneinstellungen in der ADM-Vorlagendatei auf das GPO anzuwenden.  
  
Der Name der Vorlage erscheint im linken Fensterbereich unterhalb von **Administrative Vorlagen**.

## Nächste Schritte

Konfigurieren Sie die Gruppenrichtlinieneinstellungen für View Persona Management auf Ihrem Active Directory-Server.

## Konfigurieren von View Persona Management-Richtlinien

Um View Persona Management zu verwenden, müssen Sie die Gruppenrichtlinieneinstellung **Benutzerpersona verwalten** aktivieren, wodurch die View Persona Management-Software aktiviert wird. Um ein Benutzerprofil-Repository ohne Verwendung eines Active Directory-Benutzerprofilpfades einzurichten, müssen Sie die Gruppenrichtlinieneinstellung **Speicherort für das Persona-Repository** konfigurieren.

Sie können die optionalen Gruppenrichtlinieneinstellungen konfigurieren, um andere Aspekte Ihrer View Persona Management-Bereitstellung zu konfigurieren.

Wenn servergespeicherte Windows-Profile bereits in Ihrer Bereitstellung konfiguriert sind, können Sie einen vorhandenen Active Directory-Benutzerprofilpfad verwenden. Sie können die Einstellung **Speicherort für das Persona-Repository** deaktiviert oder nicht konfiguriert lassen.

### Voraussetzungen

- Machen Sie sich mit den Gruppenrichtlinieneinstellungen **Benutzerpersona verwalten** und **Speicherort für das Persona-Repository** vertraut. Siehe [Gruppenrichtlinieneinstellungen für Serverspeicherung und Synchronisierung](#).
- Wenn Sie Gruppenrichtlinien auf einem lokalen System einrichten, machen Sie sich mit dem Öffnen des Fensters „Gruppenrichtlinie“ vertraut. Siehe Schritte [Schritt 3](#) und [Schritt 4](#) in [Hinzufügen der Persona-Verwaltung-ADM-Vorlage zu einem Einzelsystem](#).
- Wenn Sie auf Ihrem Active Directory-Server Gruppenrichtlinien festlegen, machen Sie sich mit dem Editor für Gruppenrichtlinienobjekte vertraut. Siehe Schritte [Schritt 3](#) bis [Schritt 5](#) in [Hinzufügen der Persona-Verwaltung-ADM-Vorlage zu Active Directory](#).

### Verfahren

- 1 Öffnen Sie das Fenster „Gruppenrichtlinie“.

| Option                         | Beschreibung  |
|--------------------------------|---|
| <b>Lokales System</b>          | Öffnet das Fenster „Richtlinie für 'Lokaler Computer'“. |
| <b>Active Directory-Server</b> | Öffnet das Fenster „GPO-Editor“.                        |

- 2 Erweitern Sie den Ordner **Computerkonfiguration**, und navigieren Sie zum Ordner **Persona-Verwaltung**.

| Option  | Beschreibung  |
|---|---|
| <b>Windows XP oder Windows Server 2003</b>                        | Erweitern Sie die folgenden Ordner: <b>Administrative Vorlagen</b> , <b>VMware View Agent-Konfiguration</b> , <b>Persona-Verwaltung</b>   |
| <b>Windows Vista und höher oder Windows Server 2008 und höher</b> | Erweitern Sie die folgenden Ordner: <b>Administrative Vorlagen</b> , <b>Klassische administrative Vorlagen (ADM)</b> , <b>VMware View Agent-Konfiguration</b> , <b>Persona-Verwaltung</b> |

- 3 Öffnen Sie den Ordner **Serverspeicherung und Synchronisierung**.
- 4 Doppelklicken Sie auf **Benutzerpersona verwalten**, und klicken Sie auf **Aktiviert**.  
Diese Einstellung aktiviert View Persona Management. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, funktioniert View Persona Management nicht.
- 5 Geben Sie das Profiluploadintervall in Minuten ein, und klicken Sie auf **OK**.  
Das Profiluploadintervall bestimmt, wie oft View Persona Management Änderungen an den Benutzerprofilen in das Remote-Repository kopiert. Die Standardeinstellung ist 10 Minuten.

- 6 Doppelklicken Sie auf **Speicherort für das Persona-Repository**, und klicken Sie dann auf **Aktiviert**.

Wenn Sie über eine vorhandene Bereitstellung servergespeicherter Windows-Profile verfügen, können Sie einen Active Directory-Benutzerprofilpfad für das Remote-Profil-Repository verwenden. Sie müssen keinen **Speicherort für das Persona-Repository** konfigurieren.

- 7 Geben Sie den UNC-Pfad zu einer Netzwerkdateiserverfreigabe ein, in der die Benutzerprofile gespeichert werden.

Beispiel: \\server.domain.com\UserProfilesRepository\%Benutzername%

Die virtuellen Maschinen in Ihrer Bereitstellung müssen auf diese Netzwerkfreigabe zugreifen können.

Wenn Sie vorhaben, einen Active Directory-Benutzerprofilpfad zu verwenden, brauchen Sie keinen UNC-Pfad anzugeben.

- 8 Wenn ein Active Directory-Benutzerprofilpfad in Ihrer Bereitstellung konfiguriert ist, bestimmen Sie, ob dieser Pfad benutzt oder außer Kraft gesetzt werden soll.

| Option   | Aufgabe   |
|--|---|
| Verwenden Sie die Netzwerkfreigabe.  | Markieren Sie das Kontrollkästchen <b>Active Directory-Benutzerprofilpfad außer Kraft setzen, wenn er konfiguriert ist</b> .      |
| Verwenden Sie, falls vorhanden, einen Active Directory-Benutzerprofilpfad. | Markieren Sie das Kontrollkästchen <b>Active Directory-Benutzerprofilpfad außer Kraft setzen, wenn er konfiguriert ist</b> nicht. |

- 9 Klicken Sie auf **OK**.

- 10 (Optional) Konfigurieren Sie andere Gruppenrichtlinieneinstellungen für View Persona Management.

## Erstellen von Desktop-Pools, die Persona Management verwenden

Um View Persona Management mit View-Desktops zu verwenden, müssen Sie Desktop-Pools mit einem auf jedem Computer installierten View Persona Management-Agent erstellen.

Sie können View Persona Management nicht auf RDS-Desktop-Pools verwenden, da diese auf RDS-Hosts (Remote-Desktop-Dienste) ausgeführt werden.

### Voraussetzungen

- Stellen Sie sicher, dass der View Agent mit der Einrichtungsoption **View Persona Management** auf der virtuellen Maschine installiert ist, die Sie zum Erstellen des Desktop-Pools verwenden. Siehe [Installieren von View Agent mit der View Persona Management Option](#).
- Wenn Sie beabsichtigen, View Persona Management-Richtlinien nur für diesen Desktop-Pool zu konfigurieren, stellen Sie sicher, dass Sie die View Persona Management-ADM-Vorlagendatei zur virtuellen Maschine hinzugefügt und Gruppenrichtlinieneinstellungen in der Richtlinie für den lokalen Computer konfiguriert haben. Siehe [Hinzufügen der Persona-Verwaltung-ADM-Vorlage zu einem Einzelsystem](#) und [Konfigurieren von View Persona Management-Richtlinien](#).



## Verfahren

- ◆ Generieren Sie eine Vorlage oder einen Snapshot der virtuellen Maschine und erstellen Sie einen automatisierten Desktop-Pool.

Sie können die View Persona Management mit Pools konfigurieren, die vollständige virtuelle Maschinen oder Linked-Clone-Desktops enthalten. Die Pools können hierbei eine dedizierte oder eine dynamische Zuweisung verwenden.

- ◆ (Optional) Um View Persona Management mit manuellen Desktop-Pools zu verwenden, wählen Sie die Computer aus, auf denen View Agent mit der Option **View Persona Management** installiert ist.

---

**Hinweis** Wenn Sie nach der Bereitstellung von View Persona Management auf Ihren View-Desktop-Pools die Einrichtungsoption **View Persona Management** auf den View-Computern entfernen oder View Agent komplett deinstallieren, werden die lokalen Benutzerprofile von den Computern der Benutzer entfernt, die aktuell nicht angemeldet sind. Für Benutzer, die aktuell angemeldet sind, werden die Benutzerprofile während des Deinstallationsprozesses vom Remote-Profil-Repository heruntergeladen.

---

## Empfohlene Vorgehensweisen beim Konfigurieren einer View Persona Management Bereitstellung

Sie sollten den empfohlenen Vorgehensweisen für das Konfigurieren von View Persona Management folgen, um die Erfahrung Ihrer Desktop-Benutzer zu verbessern und um sicherzustellen, dass View Persona Management effizient mit anderen View-Funktionen zusammenarbeitet.

### Bestimmen, ob lokale Benutzerprofile beim Abmelden entfernt werden sollen

Standardmäßig löscht View Persona Management die Benutzerprofile nicht von den lokalen Computern, wenn sich die Benutzer abmelden. Die Richtlinie **Lokale Persona beim Abmelden entfernen** ist deaktiviert. In vielen Fällen sollte die Standardeinstellung beibehalten werden, da sie die E/A-Vorgänge verringert und redundantes Verhalten vermeidet.

Lassen Sie diese Richtlinie deaktiviert, wenn Sie Pools mit dynamischer Zuweisung bereitstellen und die Computer beim Abmelden entweder aktualisieren oder löschen. Das lokale Profil wird gelöscht, sobald die virtuelle Maschine aktualisiert oder gelöscht wurde. Bei automatisierten Pools mit dynamischer Zuweisung können vollständige virtuelle Maschinen nach dem Abmelden gelöscht werden. Bei Pools mit dynamischer Zuweisung und verknüpften Klonen können die Klone beim Abmelden aktualisiert oder gelöscht werden.

Wenn Sie Pools mit dedizierter Zuweisung bereitstellen, können Sie die Richtlinie deaktiviert lassen, da die Benutzer bei jeder Sitzung zu denselben Computern zurückkehren. Wenn die Richtlinie deaktiviert ist und sich ein Benutzer anmeldet, muss View Persona Management keine Dateien herunterladen, die im lokalen Profil vorhanden sind. Wenn Sie Pools mit dedizierter Zuweisung und verknüpften Klonen mit persistenten Festplatten konfigurieren, lassen Sie die Richtlinie deaktiviert, um das Löschen von Benutzerdaten von den persistenten Festplatten zu vermeiden.

Unter Umständen möchten Sie die Richtlinie **Lokale Persona beim Abmelden entfernen** aktivieren.



## Umgang mit Bereitstellungen, die View Persona Management und servergespeicherte Windows-Profile enthalten

Bei Bereitstellungen, in denen servergespeicherte Windows-Profile konfiguriert werden und Benutzer mit View Persona Management und Standard-Desktops mit servergespeicherten Windows-Profilen auf View-Desktops zugreifen, besteht die empfohlene Vorgehensweise darin, verschiedene Profile für die zwei Desktop-Umgebungen zu verwenden. Wenn sich ein View-Desktop und der Clientcomputer, von dem aus der Desktop gestartet wird, innerhalb derselben Domäne befinden und Sie ein Active Directory-GPO zum Konfigurieren sowohl der servergespeicherten Windows-Profile als auch von View Persona Management verwenden, aktivieren Sie die Richtlinie **Speicherort für das Persona-Repository** und wählen Sie **Active Directory-Benutzerprofilpfad außer Kraft setzen, wenn er konfiguriert ist** aus.

Diese Vorgehensweise verhindert, dass servergespeicherte Windows-Profile ein View Persona Management Profil überschreiben, wenn sich der Benutzer vom Clientcomputer abmeldet.

Wenn Benutzer beabsichtigen, Daten zwischen vorhandenen servergespeicherten Windows-Profilen und View Persona Management Profilen auszutauschen, können Sie die Windows-Ordnerumleitung konfigurieren.

## Konfiguration von Pfaden für umgeleitete Ordner

Konfigurieren Sie bei Verwendung der Gruppenrichtlinieneinstellung **Ordnerumleitung** den Ordnerpfad so, dass er den %Benutzernamen% enthält, stellen Sie aber gleichzeitig sicher, dass der letzte Unterordner des Pfades den Namen des umgeleiteten Ordners verwendet, so z. B. Eigene Videos. Der letzte Ordner im Pfad wird als Ordnername auf dem Desktop des Benutzers angezeigt.

Wenn Sie z. B. einen Pfad wie \\Eigener Server\Videos\%Benutzername%\Eigene Videos konfigurieren, wird als Ordnername auf dem Desktop des Benutzers Eigene Videos angezeigt.

Ist der %Benutzername% der letzte Unterordner im Pfad, wird der Name des Benutzers als Ordnername angezeigt. Der Benutzer JDoe sieht dann beispielsweise nicht den Ordner Eigene Videos auf dem Desktop, sondern einen Ordner namens JDoe, den er nicht problemlos identifizieren kann.

## Verwenden des Windows-Ereignisprotokolls für das Überwachen der View Persona Management-Bereitstellung

Zur Unterstützung bei der Verwaltung Ihrer Bereitstellung bietet View Persona Management verbesserte Protokollmeldungen und Profilgrößen sowie die Erfassung der Anzahl von Dateien und Ordnern. View Persona Management verwendet die Datei- und Ordnerzählung zur Empfehlung von Ordnern für die Umleitung in das Windows-Ereignisprotokoll und bietet Statistiken für diese Ordner. Beispiel: Wenn sich ein Benutzer anmeldet, zeigt das Windows-Ereignisprotokoll möglicherweise die folgenden Anweisungen für die Umleitung von Ordnern an:

```
Profile path: \\server.domain.com\persona\user1V2
...
Folders to redirect:
\\server.domain.com\persona\user1V2 Reason: Folder size larger than 1GB
\\server.domain.com\persona\user1V2\Documents Reason: More than 10000 files and folders
```

## Zusätzliche empfohlene Vorgehensweisen

Sie können auch diese Empfehlungen befolgen:

- Viele Antivirenprodukte scannen standardmäßig Offlinedateien nicht. Wenn ein Benutzer sich z. B. bei einem Desktop anmeldet, scannen solche Antivirenprodukte die Benutzerprofildateien nicht, die nicht in einer der Gruppenrichtlinieneinstellungen **Dateien und Ordner für das Vorabladen** oder **Synchronisierung von servergespeicherten Windows-Profilen** angegeben sind. Für viele Bereitstellungen ist das Standardverhalten die empfohlene Vorgehensweise, da sie die E/A verringert, die zum Herunterladen von Dateien bei Scans nach Bedarf anfallen würde.

Wenn Sie keine Dateien aus dem Remote-Repository abfragen und das Scannen von Offlinedateien aktivieren möchten, lesen Sie die Dokumentation Ihres Antivirenprodukts aufmerksam durch.

- Für die Sicherung von Netzwerkfreigaben, auf denen View Persona Management das Profil-Repository speichert, wird die Verwendung von Standard-Vorgehensweisen empfohlen.

---

**Hinweis** Verwenden Sie mit View Persona Management keine Sicherungssoftware wie MozyPro oder den Windows Volume-Sicherungsdienst, um Benutzerprofile auf View-Desktops zu sichern.

View Persona Management garantiert, dass Benutzerprofile in das Remote-Profil-Repository gesichert werden, weswegen zur Sicherung von Benutzerdaten auf den Desktops keine zusätzlichen Tools erforderlich sind. In bestimmten Fällen können Tools wie MozyPro oder der Windows Volume-Sicherungsdienst View Persona Management beeinträchtigen und einen Datenverlust oder eine Datenbeschädigung hervorrufen.

- 
- Sie können View Persona Management Richtlinien festlegen, um die Leistung zu verbessern, wenn Benutzer ThinApp-Anwendungen starten. Siehe [Konfigurieren von Benutzerprofilen unter Einschluss von ThinApp Sandbox-Ordern](#).
  - Wenn Ihre Benutzer umfangreiche Persona-Daten generieren und Sie beabsichtigen, zum Verwalten von Desktops mit dedizierter Zuweisung und verknüpften Klonen zu aktualisieren und neu zusammenzustellen, konfigurieren Sie Ihren Desktop-Pool so, dass separate, persistente View Composer-Festplatten verwendet werden. Persistente Festplatten können die Leistung von View Persona Management verbessern. Siehe [Konfigurieren von persistenten View Composer-Festplatten mit View Persona Management](#).
  - Wenn Sie View Persona Management für eigenständige Laptops konfigurieren, stellen Sie sicher, dass die Profile synchronisiert bleiben, wenn sich Benutzer abmelden. Siehe [Verwalten von Benutzerprofilen auf eigenständigen Laptops](#).
  - Verwenden Sie die Windows-Client-Zwischenspeicherung nicht mit View Persona Management. Das Windows-Client-Zwischenspeicherungssystem ist ein Mechanismus, der die Funktion „Windows-Offlinedateien“ unterstützt. Wenn dieses System auf dem lokalen System aktiv ist, funktionieren die Funktionen von View Persona Management wie Ordnerumleitung, Offline-Dateiauffüllung während der Anmeldung, Hintergrund-Download und Replikation lokaler Profildateien im Remote-Profil-Repository nicht ordnungsgemäß.

Es hat sich bewährt, die Funktion „Windows-Offlinedateien“ vor der Verwendung von View Persona Management zu deaktivieren. Wenn Probleme bei View Persona Management auftreten, da die Windows-Client-Zwischenspeicherung in Ihren Desktops aktiv ist, können Sie diese Probleme lösen, indem Sie die Profildaten synchronisieren, die derzeit in der lokalen Datenbank der Client-Zwischenspeicherung vorhanden sind, und indem Sie die Funktion „Windows-Offlinedateien“ deaktivieren. Anweisungen finden Sie unter [KB 2016416: Funktionen von View Persona Management funktionieren nicht, wenn die Windows-Client-Zwischenspeicherung läuft](#)

## Konfigurieren von Benutzerprofilen unter Einschluss von ThinApp Sandbox-Ordern

View Persona Management behält die Benutzereinstellungen bei, die ThinApp-Anwendungen zugewiesen sind, indem ThinApp Sandbox-Ordner in Benutzerprofile eingeschlossen werden. Sie können View Persona Management-Richtlinien festlegen, um die Leistung zu verbessern, wenn Benutzer ThinApp-Anwendungen starten.

View Persona Management lädt vorab die ThinApp Sandbox-Ordner und -Dateien in das lokale Benutzerprofil, wenn sich ein Benutzer anmeldet. Die ThinApp Sandbox-Ordner werden erstellt, bevor ein Benutzer die Anmeldung abschließen kann. Zwecks Leistungsverbesserung lädt View Persona Management die ThinApp Sandbox-Daten beim Anmelden nicht, obwohl sie auf dem lokalen Desktop mit denselben grundlegenden Attributen und Größen wie die ThinApp Sandbox-Dateien im Remote-Profil des Benutzers erstellt werden.

Die empfohlene Vorgehensweise besteht darin, die tatsächlichen ThinApp Sandbox-Daten im Hintergrund herunterzuladen. Aktivieren Sie die Gruppenrichtlinieneinstellung **Ordner im Hintergrund herunterladen**, und fügen Sie die ThinApp Sandbox-Ordner hinzu. Siehe [Gruppenrichtlinieneinstellungen für Serverspeicherung und Synchronisierung](#).

Die tatsächlichen ThinApp Sandbox-Dateien können groß sein. Bei aktivierter Einstellung **Ordner im Hintergrund herunterladen** müssen die Benutzer nicht auf das Herunterladen großer Dateien warten, wenn Sie eine Anwendung starten. Außerdem müssen die Benutzer beim Anmelden nicht auf das Vorabladen der Dateien warten. Bei aktivierter Einstellung **Dateien und Ordner für das Vorabladen** wäre das bei großen Dateien der Fall.

## Konfigurieren von persistenten View Composer-Festplatten mit View Persona Management

Mit persistenten View Composer-Festplatten können Sie Benutzerdaten und Einstellungen speichern, während Sie Betriebssystemfestplatten mit verknüpften Klonen mit den Vorgängen Aktualisieren, Neuzusammenstellung und Neuverteilung verwalten. Das Konfigurieren von persistenten Festplatten kann die Leistung von View Persona Management verbessern, wenn die Benutzer große Persona-Datenmengen generieren. Sie können persistente Festplatten nur mit dediziert zugeordneten Desktops mit verknüpften Klonen konfigurieren.

View Persona Management speichert jedes Benutzerprofil auf einem Remote-Repository, das auf einer Netzwerkfreigabe konfiguriert ist. Nach der Anmeldung eines Benutzers bei einem Desktop werden die Persona-Dateien dynamisch heruntergeladen, sobald der Benutzer sie benötigt.

Wenn Sie persistente Festplatten mit View Persona Management konfigurieren, können Sie die Betriebssystemfestplatten mit verknüpften Klonen aktualisieren und neu zusammenstellen und eine lokale Kopie jedes Benutzerprofils auf den persistenten Festplatten speichern.

Die persistenten Festplatten können als Cache für Benutzerprofile dienen. Wenn ein Benutzer Persona-Dateien benötigt, braucht View Persona Management keine Daten herunterzuladen, die identisch auf der lokalen persistenten Festplatte und auf dem Remote-Repository vorliegen. Nur nicht synchronisierte Persona-Daten müssen heruntergeladen werden.

Wenn Sie persistente Festplatten konfigurieren, aktivieren Sie die Richtlinie **Lokale Persona beim Abmelden entfernen** nicht. Durch das Aktivieren dieser Richtlinie werden die Benutzerdaten beim Abmelden von den persistenten Festplatten gelöscht.

## Verwalten von Benutzerprofilen auf eigenständigen Laptops

Falls Sie View Persona Management auf eigenständigen (View-freien) Laptops installieren, stellen Sie sicher, dass die Benutzerprofile synchronisiert bleiben, wenn Benutzer ihre eigenständigen Laptops offline nehmen.

Um sicherzustellen, dass ein Benutzer eines eigenständigen Laptops über ein aktuelles lokales Profil verfügt, können Sie die View Persona Management-Gruppenrichtlinieneinstellung `Enable background download for laptops` konfigurieren. Diese Einstellung lädt das gesamte Benutzerprofil im Hintergrund auf den eigenständigen Laptop herunter.

Als Vorgehensweise wird empfohlen, Ihre Benutzer zu benachrichtigen, um sicherzustellen, dass ihre Benutzerprofile vollständig heruntergeladen wurden, bevor sie die Verbindung mit dem Netzwerk trennen. Informieren Sie die Benutzer, dass sie warten sollen, bis die Nachricht Hintergrunddownload abgeschlossen auf dem Laptop-Bildschirm angezeigt wird, bevor sie die Verbindung trennen.

Damit die Nachricht Hintergrunddownload abgeschlossen auf den Benutzer-Laptops angezeigt werden kann, konfigurieren Sie die View Persona Management-Gruppenrichtlinieneinstellung `Show critical errors to users via tray icon alerts`.

Falls ein Benutzer die Verbindung zum Netzwerk trennt, bevor das Herunterladen des Profils abgeschlossen ist, kann dies dazu führen, dass das lokale Profil und das Remote-Profil nicht synchronisiert sind. Während sich der Benutzer im Offlinemodus befindet, aktualisiert er möglicherweise eine lokale Datei, die nicht vollständig heruntergeladen wurde. Wenn der Benutzer die Verbindung zum Netzwerk wiederherstellt, wird das lokale Profil hochgeladen und überschreibt das Remote-Profil. Daten aus dem ursprünglichen Remote-Profil gehen möglicherweise verloren.

Die folgenden Schritte können als Beispiel für Ihr Vorgehen dienen.

### Voraussetzungen

Stellen Sie sicher, dass View Persona Management für die eigenständigen Laptops Ihrer Benutzer konfiguriert ist. Siehe [Konfigurieren einer View Persona Management Bereitstellung](#).

## Verfahren

- 1 Aktivieren Sie in der Active Directory OU, die Ihre eigenständigen Laptops steuert, die Einstellung `Enable background download for laptops`.

Erweitern Sie im Gruppenrichtlinienobjekt-Editor die folgenden Ordner: **Computerkonfiguration**, **Administrative Vorlagen**, **Klassische administrative Vorlagen (ADM)**, **VMware View Agent-Konfiguration**, **Persona-Verwaltung**, **Serverspeicherung und Synchronisierung**.

Der Ordner **Klassische administrative Vorlagen (ADM)** wird nur in Windows Vista oder höher und in Windows Server 2008 oder höheren Versionen angezeigt.

- 2 Für eigenständige Laptops müssen Sie eine View-freie Methode verwenden, um Benutzer bei der Anmeldung zu benachrichtigen.

Sie können z. B. diese Nachricht verteilen:

**Ihre persönlichen Daten werden dynamisch auf Ihren Laptop heruntergeladen, nachdem Sie sich angemeldet haben. Stellen Sie sicher, dass Ihre persönlichen Daten vollständig heruntergeladen wurden, bevor Sie den Laptop vom Netzwerk trennen. Die Nachricht „Hintergrunddownload abgeschlossen“ öffnet sich, wenn das Herunterladen Ihrer persönlichen Daten abgeschlossen ist.**

## Gruppenrichtlinieneinstellungen für View Persona Management

Die View Persona Management ADM-Vorlagendatei enthält Gruppenrichtlinieneinstellungen, die Sie zur Gruppenrichtlinienkonfiguration auf einzelnen Systemen oder einem Active Directory-Server hinzufügen. Sie müssen die Gruppenrichtlinieneinstellungen konfigurieren, um verschiedene Aspekte von View Persona Management zu steuern.

Die ADM-Vorlagendatei heißt `ViewPM.adm`.

Diese ADM-Datei steht in einer mitgelieferten `.zip`-Datei namens `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyy.zip` zur Verfügung, die Sie von der Download-Site VMware Horizon (mit View) unter <http://www.vmware.com/go/downloadview> herunterladen können.

Nachdem Sie die Datei `ViewPM.adm` zu Ihrer Gruppenrichtlinienkonfiguration hinzugefügt haben, befinden sich die Richtlinieneinstellungen im Ordner **Persona-Verwaltung** im Gruppenrichtlinienfenster.

**Tabelle 17-4. Speicherort der View Persona Management Einstellungen im Gruppenrichtlinienfenster**

| Betriebssystem   | Speicherort  |
|--|--|
| Windows Vista und höher oder Windows Server 2008 und höher | <b>Computerkonfiguration &gt; Administrative Vorlagen &gt; Klassische administrative Vorlagen (ADM) &gt; VMware View Agent-Konfiguration &gt; Persona Management</b> |
| Windows XP oder Windows Server 2003                        | <b>Computer-Konfiguration &gt; Administrative Vorlagen &gt; VMware View Agent-Konfiguration &gt; Persona Management</b>  |

Die Gruppenrichtlinieneinstellungen befinden sich in diesen Ordnern:

- Roaming (Serverspeicherung) & Synchronization (Synchronisierung)
- Ordnerumleitung
- Desktop-Benutzeroberfläche
- Protokollierung

## **Gruppenrichtlinieneinstellungen für Serverspeicherung und Synchronisierung**

Die Gruppenrichtlinieneinstellungen für Serverspeicherung und Synchronisierung schalten View Persona Management ein und aus, legen den Speicherort des Remote-Profil-Repositorys fest, bestimmen, welche Ordner und Dateien zum Benutzerprofil gehören, und steuern, wie Dateien und Ordner synchronisiert werden.

| Gruppenrichtlinieneinstellung          | Beschreibung  |
|--|---|
| Benutzerpersona verwalten              | <p>Bestimmt, ob Benutzerprofile dynamisch mit View Persona Management oder mit servergespeicherten Windows-Profilen verwaltet werden sollen. Diese Einstellung schaltet View Persona Management ein und aus.</p> <p>Wenn diese Einstellung aktiviert ist, verwaltet View Persona Management die Benutzerprofile.</p> <p>Wenn diese Einstellung aktiviert ist, können Sie ein Profiluploadintervall in Minuten angeben. Dieser Wert bestimmt, wie oft Änderungen am Benutzerprofil in das Remote-Repository kopiert werden. Der Standardwert lautet 10 Minuten.</p> <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert wurde, werden die Benutzerprofile von Windows verwaltet.</p>   |
| Speicherort für das Persona-Repository | <p>Gibt den Speicherort des Benutzerprofil-Repositorys an. Diese Einstellung bestimmt auch, ob eine in View Persona Management angegebene Netzwerkfreigabe oder ein in Active Directory konfigurierter Pfad verwendet wird, um servergespeicherte Windows-Profile zu unterstützen.</p> <p>Wenn diese Einstellung aktiviert ist, können Sie <b>Freigabepfad</b> verwenden, um den Speicherort des Benutzerprofil-Repositorys zu bestimmen.</p> <p>Im Textfeld <b>Freigabepfad</b> geben Sie einen UNC-Pfad zu einer Netzwerkfreigabe an, auf die View Persona Managements-Desktops zugreifen können. Mit dieser Einstellung kann View Persona Management den Speicherort des Benutzerprofil-Repositorys steuern.</p> <p>Beispiel: <code>\\server.domain.com\VPRepository</code></p> <p>Wenn %Benutzername% nicht im von Ihnen konfigurierten Ordnerpfad enthalten ist, hängt View Persona Management %Benutzername%.%Benutzerdomäne% an den Pfad an.</p> <p>Beispiel: <code>\\server.domain.com\VPRepository\%username%.%userdomain%</code></p> <p>Wenn Sie unter <b>Freigabepfad</b> einen Speicherort angeben, müssen Sie weder in Windows servergespeicherte Profile einrichten noch einen Benutzerprofilpfad in Active Directory konfigurieren, um servergespeicherte Windows-Profile zu unterstützen.</p> <p>Detaillierte Informationen zum Konfigurieren einer UNC-Netzwerkfreigabe für View Persona Management finden Sie unter <a href="#">Konfigurieren eines Benutzerprofil-Repositorys</a>.</p> <p>Standardmäßig wird der Active Directory-Benutzerprofilpfad verwendet.</p> <p>Wenn <b>Freigabepfad</b> leer gelassen wurde, wird der Active Directory-Benutzerprofilpfad verwendet. Der <b>Freigabepfad</b> ist leer und inaktiv, wenn diese Einstellung deaktiviert oder nicht konfiguriert wurde. Sie können den Pfad auch leer lassen, wenn diese Einstellung aktiviert wurde.</p> <p>Wenn diese Einstellung aktiviert wurde, können Sie das Kontrollkästchen <b>Active Directory-Benutzerprofilpfad außer Kraft setzen, wenn er konfiguriert ist</b> markieren, um sicherzustellen, dass View Persona Management den in <b>Freigabepfad</b> angegebenen Pfad verwendet. Standardmäßig ist dieses Kontrollkästchen nicht markiert, und View Persona Management verwendet den Active Directory-Benutzerprofilpfad, wenn beide Speicherorte konfiguriert sind.</p> |

| Gruppenrichtlinieneinstellung                                 | Beschreibung   |
|---|--|
| Lokale Persona beim Abmelden entfernen                        | <p>Löscht das lokal gespeicherte Profil jedes Benutzers aus dem View-Computer, wenn sich der Benutzer abmeldet.</p> <p>Sie können auch ein Kästchen markieren, um die Ordner mit den lokalen Einstellungen jedes Ordners zu löschen, wenn das Benutzerprofil entfernt wird. Unter Windows 8, Windows 7 oder Windows Vista führt das Markieren dieses Kästchens zum Löschen des Ordners AppData\Local. In Windows XP führt das Markieren dieses Kästchens zum Löschen des Ordners Local Settings.</p> <p>Anweisungen zum Verwenden dieser Einstellungen finden Sie unter <a href="#">Empfohlene Vorgehensweisen beim Konfigurieren einer View Persona Management Bereitstellung</a>.</p> <p>Wenn diese Einstellung deaktiviert oder nicht konfiguriert wurde, werden die lokal gespeicherten Benutzerprofile, einschließlich der Ordner mit den lokalen Einstellungen, beim Abmelden des Benutzers nicht gelöscht.</p>  |
| Ordner mit den lokalen Einstellungen auf dem Server speichern | <p>Speichert die Ordner mit den lokalen Einstellungen mit dem Rest jedes Benutzerprofils auf dem Server.</p> <p>Bei Windows 8, Windows 7 oder Windows Vista betrifft diese Richtlinie den Ordner AppData\Local. Bei Windows XP betrifft diese Richtlinie den Ordner Local Settings.</p> <p>Standardmäßig werden die lokalen Einstellungen nicht auf dem Server gespeichert.</p>  |
| Dateien und Ordner für das Vorabladen                         | <p>Gibt eine Liste mit Dateien und Ordnern an, die in das lokale Benutzerprofil heruntergeladen werden, wenn sich der Benutzer anmeldet. Änderungen an den Dateien werden in das Remote-Repository kopiert, sobald sie auftreten.</p> <p>In einigen Situationen möchten Sie möglicherweise bestimmte Dateien und Ordner vorab in das lokal gespeicherte Benutzerprofil laden. Verwenden Sie diese Einstellung, um diese Dateien und Ordner anzugeben.</p> <p>Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.</p> <p>Beispiel: Application Data\Microsoft\Certificates</p> <p>Nachdem die angegebenen Dateien und Ordner vorab geladen wurden, verwaltet View Persona Management die Dateien und Ordner auf dieselbe Weise wie andere Profildaten. Wenn ein Benutzer vorab geladene Dateien oder Ordner ändert, kopiert View Persona Management die aktualisierten Daten während der Sitzung im darauffolgenden Profiluploadintervall in das Remote-Profil-Repository.</p> |
| Dateien und Ordner für das Vorabladen (Ausnahmen)             | <p>Verhindert, dass die angegebenen Dateien und Ordner vorab geladen werden.</p> <p>Die ausgewählten Ordnerpfade müssen sich in den Ordnern befinden, die Sie in der Einstellung <b>Dateien und Ordner für das Vorabladen</b> angegeben haben.</p> <p>Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.</p>   |
| Synchronisierung von servergespeicherten Windows-Profilen     | <p>Gibt eine Liste mit Dateien und Ordnern an, die von standardmäßigen servergespeicherten Windows-Profilen verwaltet werden. Die Dateien und Ordner werden vom Remote-Repository abgerufen, wenn sich der Benutzer anmeldet. Die Dateien werden erst in das Remote-Repository kopiert, wenn sich der Benutzer abmeldet.</p> <p>Für die angegebenen Dateien und Ordner ignoriert View Persona Management das Profilreplikationsintervall, das durch <b>Profilhochladeintervall</b> in der Einstellung <b>Benutzerpersona verwalten</b> konfiguriert ist.</p> <p>Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.</p>   |



| Gruppenrichtlinieneinstellung   | Beschreibung  |
|---|---|
| Synchronisierung von servergespeicherten Windows-Profilen (Ausnahmen) | <p>Die ausgewählten Dateien und Ordner sind Ausnahmen der Pfade, die in der Einstellung <b>Synchronisierung von servergespeicherten Windows-Profilen</b> angegeben sind.</p> <p>Die ausgewählten Ordnerpfade müssen sich in den Ordnern befinden, die Sie in der Einstellung <b>Synchronisierung von servergespeicherten Windows-Profilen</b> angegeben haben.</p> <p>Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.</p>  |
| Von der Serverspeicherung ausgenommene Dateien und Ordner             | <p>Gibt eine Liste der Ordner und Dateien an, die nicht mit dem Rest des Benutzerprofils auf dem Server gespeichert werden. Die angegebenen Dateien und Ordner sind nur auf dem lokalen System vorhanden.</p> <p>In manchen Situationen ist es erforderlich, dass bestimmte Dateien und Ordner nur im lokal gespeicherten Benutzerverzeichnis vorhanden sind. Sie können beispielsweise temporäre Dateien und zwischengespeicherte Dateien vom Roaming ausschließen. Diese Dateien müssen nicht in das Remote-Repository repliziert werden.</p> <p>Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.</p> <p>Standardmäßig sind die folgenden Ordner ausgenommen: der temporäre Ordner des Benutzerprofils, der Ordner des ThinApp-Caches und die Cache-Ordner für Internet Explorer, Firefox, Chrome und Opera.</p>  |
| Von der Serverspeicherung ausgenommene Dateien und Ordner (Ausnahmen) | <p>Die ausgewählten Dateien und Ordner sind Ausnahmen von den Pfaden, die in der Einstellung <b>Von der Serverspeicherung ausgenommene Dateien und Ordner</b> angegeben sind.</p> <p>Die ausgewählten Ordnerpfade müssen sich in den Ordnern befinden, die Sie in der Einstellung <b>Von der Serverspeicherung ausgenommene Dateien und Ordner</b> angegeben haben.</p> <p>Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.</p>   |
| Ladevorgänge im Hintergrund für Laptops aktivieren                    | <p>Lädt alle Dateien im Benutzerprofil, wenn sich ein Benutzer auf einem Laptop anmeldet, auf dem die View Persona Management-Software installiert ist. Die Dateien werden im Hintergrund heruntergeladen.</p> <p>Wenn der Vorgang abgeschlossen ist, erscheint auf dem Bildschirm des Benutzers eine Popup-Benachrichtigung: Hintergrunddownload abgeschlossen. Damit diese Benachrichtigung auf dem Laptop des Benutzers angezeigt werden kann, müssen Sie die Einstellung Benutzern kritische Fehler über Leistensymbolwarnungen anzeigen aktivieren.</p> <p><b>Hinweis</b> Wenn Sie diese Einstellung aktivieren, sollten Sie Ihre Benutzer am besten darüber informieren, um sicherzustellen, dass das Profil komplett heruntergeladen ist, bevor die Benutzer die Netzwerkverbindung trennen.</p> <p>Wenn ein Benutzer einen eigenständigen Laptop offline schaltet, bevor das Herunterladen des Profils abgeschlossen ist, hat der Benutzer womöglich keinen Zugriff auf lokale Profildateien. Während der Benutzer offline ist, kann er eine lokale Datei, die nicht vollständig heruntergeladen wurde, nicht öffnen.</p> <p>Siehe <a href="#">Verwalten von Benutzerprofilen auf eigenständigen Laptops</a>.</p> |

| Gruppenrichtlinieneinstellung                        | Beschreibung   |
|--|--|
| Im Hintergrund herunterzuladende Ordner              | <p>Die ausgewählten Ordner werden nach der Anmeldung des Benutzers beim Desktop im Hintergrund heruntergeladen.</p> <p>In bestimmten Fällen können Sie View Persona Management optimieren, indem Sie den Inhalt bestimmter Ordner im Hintergrund herunterladen. Bei aktivierter Einstellung müssen die Benutzer nicht auf das Herunterladen großer Dateien warten, wenn sie eine Anwendung starten. Außerdem müssen die Benutzer beim Anmelden nicht auf das Vorabladen der Dateien warten. Bei aktivierter Einstellung <b>Dateien und Ordner für das Vorabladen</b> wäre das bei sehr großen Dateien der Fall.</p> <p>Sie können z. B. VMware ThinApp Sandbox-Ordner in der Einstellung <b>Im Hintergrund herunterzuladende Ordner</b> einbeziehen. Das Herunterladen im Hintergrund beeinträchtigt die Leistung nicht, wenn sich ein Benutzer anmeldet oder andere Anwendungen auf dem Desktop verwendet. Wenn der Benutzer die ThinApp-Anwendung startet, werden die erforderlichen ThinApp Sandbox-Dateien wahrscheinlich vom Remote-Repository heruntergeladen und verkürzt so die Startzeit der Anwendung.</p> <p>Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.</p> |
| Im Hintergrund herunterzuladende Ordner) (Ausnahmen) | <p>Die ausgewählten Ordner sind Ausnahmen von den Pfaden, die in der Einstellung <b>Im Hintergrund herunterzuladende Ordner</b> festgelegt sind.</p> <p>Die ausgewählten Ordnerpfade müssen sich in den Ordnern befinden, die Sie in der Einstellung <b>Im Hintergrund herunterzuladende Ordner</b> angegeben haben.</p> <p>Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.</p>   |
| Ausgeschlossene Prozesse                             | <p>Die E/A der angegebenen Prozesse wird von View Persona Management ignoriert.</p> <p>Eventuell müssen Sie bestimmte Antivirus-Anwendungen zur Liste <b>Ausgeschlossene Prozesse</b> hinzufügen, um Leistungsprobleme zu vermeiden. Wenn eine Antivirus-Anwendung nicht über eine Funktion verfügt, den Offline-Dateiabruf während der Scans nach Bedarf zu deaktivieren, hindert die Einstellung <b>Ausgeschlossene Prozesse</b> die Anwendung daran, Dateien unnötig abzurufen. View Persona Management repliziert jedoch Änderungen an Dateien und Einstellungen in den Profilen der Benutzer, die von ausgeschlossenen Prozessen vorgenommen wurden.</p> <p>Wenn Sie Prozesse zur Liste <b>Ausgeschlossene Prozesse</b> hinzufügen möchten, aktivieren Sie diese Einstellung, klicken Sie auf <b>Anzeigen</b>, geben Sie den Prozessnamen ein und klicken Sie auf <b>OK</b>. Beispiel: <b>process.exe</b>.</p>  |
| Bereinigung von CLFS-Dateien                         | <p>Löscht die Dateien, die vom Gemeinsamen Protokolldateisystem (CLFS) für <code>ntuser.dat</code> und <code>usrclass.dat</code> über das Roaming-Profil bei der Anmeldung generiert werden.</p> <p>Aktivieren Sie diese Einstellung nur, wenn Sie Benutzerprofile reparieren müssen, die in diesen Dateien ein Problem aufweisen. Lassen Sie die Einstellungen andernfalls deaktiviert oder nicht konfiguriert.</p>   |

## Gruppenrichtlinieneinstellungen für Ordnerumleitung

Mit Gruppenrichtlinieneinstellungen für Ordnerumleitung können Sie Benutzerprofilordner auf eine Netzwerkfreigabe umleiten. Wenn ein Ordner umgeleitet wird, werden alle Daten während der Benutzersitzung direkt auf der Netzwerkfreigabe gespeichert.

Sie können diese Einstellungen verwenden, um Ordner umzuleiten, die hochgradig verfügbar sein müssen. View Persona Management kopiert die Aktualisierungen vom lokalen Benutzerprofil häufig in das Remote-Profil, bis zu einmal pro Minute, abhängig vom Wert, den Sie für das Profiluploadintervall festgelegt haben. Wenn es auf dem lokalen System jedoch zu einem Netzwerkausfall oder -fehler kommt,

werden die Aktualisierungen eines Benutzers seit der letzten Replikation möglicherweise nicht in das Remote-Profil gespeichert. In Situationen, bei denen es für die Benutzer ausgeschlossen ist, einen temporären Datenverlust der Arbeit der letzten paar Minuten hinzunehmen, können Sie jene Ordner umleiten, in denen diese kritischen Daten gespeichert werden.

Die folgenden Regeln und Richtlinien gelten für die Ordnerumleitung:

- Wenn Sie diese Einstellung für einen Ordner aktivieren, müssen Sie den UNC-Pfad der Netzwerkfreigabe eingeben, auf die der Ordner umgeleitet wird.
- Wenn %Benutzername% nicht im von Ihnen konfigurierten Ordnerpfad enthalten ist, hängt View Persona Management %Benutzername% an den UNC-Pfad an.
- Konfigurieren Sie als empfohlene Vorgehensweise den Ordnerpfad so, dass er den %Benutzernamen % enthält, stellen Sie aber gleichzeitig sicher, dass der letzte Unterordner des Pfades den Namen des umgeleiteten Ordners verwendet, so z. B. Eigene Videos. Der letzte Ordner im Pfad wird als Ordnername auf dem Desktop des Benutzers angezeigt. Weitere Informationen finden Sie unter [Konfiguration von Pfaden für umgeleitete Ordner](#).
- Sie können für jeden Ordner separate Einstellungen konfigurieren. Sie können bestimmte Ordner für die Umleitung auswählen und andere auf dem lokalen View-Desktop belassen. Sie können auch verschiedene Ordner auf verschiedene UNC-Pfade umleiten.
- Wenn eine Ordnerumleitungseinstellung deaktiviert oder nicht konfiguriert wurde, wird der Ordner auf dem lokalen View-Desktop gespeichert und gemäß den View Persona Management Gruppenrichtlinieneinstellungen verwaltet.
- Wenn View Persona Management und servergespeicherte Windows-Profile zur Umleitung desselben Ordners konfiguriert wurden, hat die View Persona Management Ordnerumleitung Vorrang vor servergespeicherten Windows-Profilen.
- Die Ordnerumleitung gilt für alle Anwendungen, die die Windows Shell-APIs verwenden, um gemeinsame Ordnerpfade umzuleiten. Wenn beispielsweise eine Anwendung eine Datei in %Benutzerprofil%\AppData\Roaming schreibt, wird die Datei in das lokale Profil geschrieben und nicht an einen Netzwerkspeicherort umgeleitet.
- Die Umleitung von Windows-Ordern gewährt Benutzern standardmäßig exklusive Rechte für umgeleitete Ordner. Um Domänenadministratoren Zugriff auf kürzlich umgeleitete Ordner zu gewähren, können Sie eine View Persona Management-Gruppenrichtlinieneinstellung verwenden.

Die Umleitung von Windows-Ordern verfügt über das Kontrollkästchen **Dem Benutzer exklusive Zugriffsrechte erteilen für Ordnername**, mit dem Sie dem angegebenen Benutzer exklusive Rechte für den umgeleiteten Ordner gewähren können. Aus Sicherheitsgründen ist dieses Kontrollkästchen standardmäßig aktiviert. Wenn dieses Kontrollkästchen aktiviert ist, haben Administratoren keinen Zugriff auf den umgeleiteten Ordner. Wenn ein Administrator dann versucht, die Zugriffsrechte für den umgeleiteten Ordner eines Benutzers zu ändern, ist View Persona Management für diesen Benutzer nicht mehr funktionsfähig.

Sie können Domänenadministratoren Zugriff auf kürzlich umgeleitete Ordner gewähren, indem Sie die Gruppenrichtlinieneinstellung **Administratorgruppe zu umgeleiteten Ordnern hinzufügen** verwenden. Mithilfe dieser Einstellung können Sie der Domänenadministratorgruppe volle Kontrolle über jeden umgeleiteten Ordner erteilen. Siehe [Tabelle 17-5. Gruppenrichtlinieneinstellungen zur Steuerung der Ordnerumleitung](#).

Informationen zur Vorgehensweise bei vorhandenen umgeleiteten Ordnern finden Sie unter [Domänenadministratoren Zugriff auf vorhandene umgeleitete Ordner gewähren](#).

Sie können Ordnerpfade angeben, die aus der Ordnerumleitung ausgeschlossen werden sollen. Siehe [Tabelle 17-5. Gruppenrichtlinieneinstellungen zur Steuerung der Ordnerumleitung](#).

---

**Vorsicht** View unterstützt das Aktivieren der Ordnerumleitung auf einen Ordner nicht, der bereits in einem von View Persona Management verwalteten Profil vorhanden ist. Diese Konfiguration kann Fehler in View Persona Management verursachen und zum Verlust von Benutzerdaten führen.

Wenn der Stammordner im Remote-Profil-Repository beispielsweise `\\Server\%Benutzername%` lautet und Sie Ordner auf `\\Server\%Benutzername%\Desktop` umleiten, würden diese Einstellungen einen Fehler bei der Ordnerumleitung in View Persona Management verursachen und zum Verlust aller Inhalte führen, die zuvor im Ordner `\\Server\%Benutzername%\Desktop` gespeichert waren.

---

Sie können die folgenden Ordner auf eine Netzwerkfreigabe umleiten:

- Anwendungsdaten (servergespeichert)
- Kontakte
- Cookies
- Desktop
- Downloads
- Favoriten
- Verlauf
- Links
- Eigene Dokumente
- Eigene Musik
- Eigene Bilder
- Eigene Videos
- Netzwerkumgebung
- Druckerumgebung
- Zuletzt verwendet
- Gespeicherte Spiele
- Suchvorgänge

- Startmenü
- Startobjekte
- Vorlagen
- Temporäre Internetdateien

Bestimmte Ordner sind nur unter Windows Vista und neueren Betriebssystemen verfügbar.

**Tabelle 17-5. Gruppenrichtlinieneinstellungen zur Steuerung der Ordnerumleitung**

| Gruppenrichtlinieneinstellung  | Beschreibung   |
|--|--|
| Administratorgruppe zu umgeleiteten Ordnern hinzufügen                 | Legt fest, ob die Administratorgruppe zu jedem umgeleiteten Ordner hinzugefügt werden soll. Benutzer verfügen standardmäßig über exklusive Rechte für umgeleitete Ordner. Wenn Sie diese Einstellung aktivieren, können Administratoren auch auf umgeleitete Ordner zugreifen. Diese Einstellung ist standardmäßig nicht konfiguriert.   |
| Von der Ordnerumleitung ausgeschlossene Dateien und Ordner             | Die ausgewählten Datei- und Ordnerpfade werden nicht auf eine Netzwerkfreigabe umgeleitet. In manchen Szenarien müssen bestimmte Dateien und Ordner im lokalen Benutzerprofil verbleiben. Wenn Sie einen Ordnerpfad zur Liste <b>Von der Ordnerumleitung ausgeschlossene Dateien und Ordner</b> hinzufügen möchten, aktivieren Sie diese Einstellung, klicken Sie auf <b>Anzeigen</b> , geben Sie den Pfadnamen ein und klicken Sie auf <b>OK</b> .<br>Geben Sie Ordnerpfade relativ zum Stamm des lokalen Profils des Benutzers an. Beispiel: <b>Desktop\Neuer Ordner</b> .   |
| Von der Ordnerumleitung ausgeschlossene Dateien und Ordner (Ausnahmen) | Die ausgewählten Datei- und Ordnerpfade sind Ausnahmen von den Pfaden, die in der Einstellung <b>Von der Ordnerumleitung ausgeschlossene Dateien und Ordner</b> angegeben sind. Wenn Sie einen Ordnerpfad zur Liste <b>Von der Ordnerumleitung ausgeschlossene Dateien und Ordner (Ausnahmen)</b> hinzufügen möchten, aktivieren Sie diese Einstellung, klicken Sie auf <b>Anzeigen</b> , geben Sie den Pfadnamen ein und klicken Sie auf <b>OK</b> .<br>Geben Sie Ordnerpfade an, die sich innerhalb eines Ordners befinden, die in der Einstellung <b>Von der Ordnerumleitung ausgeschlossene Dateien und Ordner</b> angegeben sind und relativ zum Stamm des lokalen Profils des Benutzers sind. Beispiel: <b>Desktop\Neuer Ordner\Eindeutiger Ordner</b> . |

## Domänenadministratoren Zugriff auf vorhandene umgeleitete Ordner gewähren

Die Umleitung von Windows-Ordnern gewährt Benutzern standardmäßig exklusive Rechte für umgeleitete Ordner. Um Domänenadministratoren Zugriff auf bestehende umgeleitete Ordner zu gewähren, müssen Sie das Dienstprogramm `icacls` verwenden.

Wenn Sie neue umgeleitete Ordner zur Verwendung mit View Persona Management einrichten, können Sie die neu umgeleiteten Ordner Domänenadministratoren zugänglich machen, indem Sie die Gruppenrichtlinieneinstellung **Hinzufügen der Administratorgruppe zu umgeleiteten Ordnern** verwenden. Siehe [Tabelle 17-5. Gruppenrichtlinieneinstellungen zur Steuerung der Ordnerumleitung](#).

### Verfahren

- 1 Setzen Sie das Besitzrecht für den Administrator auf die Dateien und Ordner.

```
icacls "\\file-server\persona-share\" /setowner "domain\admin" /T /C /L /Q
```

Beispiel: `icacls "\\myserver-123abc\folders\*" /setowner "mycompanydomain \vadmin" /T /C /L /Q`

## 2 Ändern Sie die ACLs für die Dateien und Ordner.

`icacls "\\file-server\persona-share\*" /grant "admin-group":F /T /C /L /Q`

Beispiel: `icacls "\\myserver-123abc\folders\*" /grant "Domain-Admins":F /T /C /L /Q`

## 3 Für jede Benutzerordner setzen Sie das Besitzrecht vom Administrator auf den entsprechenden Benutzer zurück.

`icacls "\\file-server\persona-share\*" /setowner "domain\folder-owner" /T /C /L /Q`

Beispiel: `icacls "\\myserver-123abc\folders\*" /setowner "mycompanydomain \user1" /T /C /L /Q`

# Gruppenrichtlinieneinstellungen für Desktop-Benutzeroberfläche

Die Gruppenrichtlinieneinstellungen für Desktop-Benutzeroberfläche steuern die View Persona Management-Einstellungen, die die Benutzer auf ihren Desktops sehen.

| Gruppenrichtlinieneinstellung  | Beschreibung   |
|--|--|
| Hide local offline file icon (Lokales Offline-Dateisymbol ausblenden)  | Bestimmt, ob das Offline-Symbol ausgeblendet wird, wenn ein Benutzer lokal gespeicherte Dateien anzeigt, die zum Benutzerprofil gehören. Durch Aktivieren dieser Einstellung wird das Offline-Symbol in Windows Explorer und in den meisten Windows-Dialogfeldern ausgeblendet.<br>Das Offline-Symbol ist standardmäßig ausgeblendet.  |
| Show progress when downloading large files (Beim Herunterladen von großen Dateien Fortschritt anzeigen)                | Legt fest, ob beim Herunterladen von Dateien ein Fortschrittsfenster auf dem Benutzer-Desktop angezeigt wird, wenn der Client große Dateien aus dem Remote-Repository abruft.<br>Bei Aktivierung dieser Einstellung können Sie die Mindestdateigröße (in Megabyte) angeben, ab der beim Herunterladen von Dateien ein Fortschrittsfenster angezeigt wird. Das Fenster wird angezeigt, wenn View Persona Management bestimmt, dass die angegebene Datenmenge vom Remote-Repository abgerufen wird. Dieser Wert ist die Summe für alle Dateien, die in einem Arbeitsschritt abgerufen werden.<br>Wenn z. B. der Einstellungswert 50 MB lautet und eine 40 MB große Datei abgerufen wird, wird dieses Fenster nicht angezeigt. Wenn eine 30 MB große Datei abgerufen wird, während die erste Datei noch heruntergeladen wird, überschreitet die Summe beider Dateien den Wert und das Fortschrittsfenster wird angezeigt. Das Fenster wird beim Start des Downloadvorgangs einer Datei angezeigt.<br>Dieser Wert ist standardmäßig auf 50 MB festgelegt.<br>Das Fortschrittsfenster wird standardmäßig nicht angezeigt. |
| Show critical errors to users via tray icon alerts (Benutzern kritische Fehler über Leistungssymbolwarnungen anzeigen) | Zeigt Benutzern kritische Fehler über Symbole in der Desktop-Leiste an, wenn es bei der Replikation oder bei der Netzwerkkonnektivität zu Fehlern kommt.<br>Diese Symbolwarnungen sind standardmäßig ausgeblendet.   |

# Protokollieren von Gruppenrichtlinieneinstellungen

Die Gruppenrichtlinieneinstellungen zum Protokollieren bestimmen den Namen, den Speicherort und das Verhalten von View Persona Management-Protokolldateien.

| Gruppenrichtlinieneinstellung               | Beschreibung   |
|---|--|
| Logging filename (Name der Protokolldatei)  | <p>Gibt den vollständigen Pfadnamen der lokalen Protokolldatei von View Persona Management an.</p> <p>Auf Windows 8- und Windows 7-Computern lautet der Standardpfad <code>Programme\VMware\VDM\logs\Dateiname</code>.</p> <p>Auf Windows XP-Computern lautet der Standardpfad <code>ALL Users\Anwendungsdaten\VMware\VDM\logs\Dateiname</code>.</p> <p>Der standardmäßige Protokolldateiname ist <code>VMWVp.txt</code>.</p>  |
| Logging destination (Protokollierungsziel)  | <p>Legt fest, ob alle Protokollmeldungen in die Protokolldatei, den Debug-Bericht oder in beide Ziele geschrieben werden.</p> <p>Standardmäßig werden Protokollmeldungen in der Protokolldatei ausgegeben.</p>   |
| Logging flags (Protokollierungskennzeichen) | <p>Legt die Art der zu protokollierenden Meldungen fest. Wenn diese Einstellung konfiguriert ist, können Sie einige oder alle der folgenden Protokollmeldungstypen generieren:</p> <ul style="list-style-type: none"> <li>■ Fehlermeldungen protokollieren</li> <li>■ Informationsmeldungen protokollieren</li> <li>■ Debug-Meldungen protokollieren</li> </ul> <p>Standardmäßig werden Fehler- und Informations-Protokollmeldungstypen generiert.</p>                                     |
| Debug flags (Debug-Kennzeichen)             | <p>Legt die Art der zu protokollierenden Debug-Meldungen fest. View Persona Management verarbeitet Debugmeldungen auf dieselbe Weise wie Protokollmeldungen. Wenn diese Einstellung aktiviert ist, können Sie einige oder alle der folgenden Debugmeldungstypen auswählen:</p> <ul style="list-style-type: none"> <li>■ Debugfehlermeldungen</li> <li>■ Debuginformationsmeldungen</li> <li>■ Debug-Port-Meldungen</li> </ul> <p>Standardmäßig werden keine Debug-Meldungen generiert.</p> |
| Protokollverlauftiefe                       | <p>Legt die Anzahl der historischen Protokolldateien fest, die View Persona Management pflegt.</p> <p>Sie können festlegen, dass minimal eine und maximal 10 historische Protokolldateien gepflegt werden.</p> <p>Standardmäßig wird eine historische Protokolldatei gepflegt.</p>   |
| Protokoll auf Netzwerk hochladen            | <p>Lädt die View Persona Management-Protokolldatei auf die angegebene Netzwerkfreigabe hoch, wenn sich der Benutzer abmeldet.</p> <p>Wenn diese Einstellung aktiviert ist, geben Sie den Pfad zur Netzwerkfreigabe an. Der Netzwerkfreigabepfad muss ein UNC-Pfad sein. View Persona Management erstellt die Netzwerkfreigabe nicht.</p> <p>Standardmäßig wird die Protokolldatei nicht auf die Netzwerkfreigabe hochgeladen.</p>  |

# Fehlerbehebung bei Computern und Desktop-Pools

# 18

Für die Diagnose und Behandlung von Problemen, die bei der Erstellung und Verwendung von Computern und Desktop-Pools auftreten, können Sie zwischen verschiedenen Vorgehensweisen wählen.

Für die Benutzer kann es bei Verwendung von Horizon Client für den Zugriff auf ihre Desktops und Anwendungen zu Problemen kommen. 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.

Dieses Kapitel enthält die folgenden Themen:

- [Anzeigen problematischer Computer](#)
- [Senden von Nachrichten an Desktop-Benutzer](#)
- [Fehlerbehebung bei Problemen während der Desktop-Pool-Erstellung](#)
- [Fehlerbehebung bei Problemen mit der Netzwerkverbindung](#)
- [Fehlerbehebung bei Problemen mit der USB-Umleitung](#)
- [Fehlerbehebung von GINA-Problemen auf Windows XP-Computern](#)
- [Verwalten von Maschinen und Richtlinien für nicht berechnete Benutzer](#)
- [Weitere Informationen zur Fehlerbehebung](#)

## Anzeigen problematischer Computer

Sie können eine Liste der von View Manager ermittelten Computer anzeigen, auf denen Probleme vermutet werden.

View Administrator zeigt Computer mit den folgenden Problemen an:

- Eingeschaltete Desktops, die nicht reagieren.
- Desktops, die während eines langen Zeitraums den Bereitstellungsstatus aufweisen.
- Desktops, die bereit sind, jedoch keine Verbindungen akzeptieren.
- Desktops, die auf einer vCenter Server-Instanz fehlen.
- Desktops, die über aktive Konsolenanmeldungen, Anmeldungen durch nicht berechnete Benutzer oder Anmeldungen über eine View-Verbindungsserver-Instanz verfügen.



## Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Maschinen** aus.
- 2 Klicken Sie auf der Registerkarte **vCenter-VMs** auf **Problematische Computer**.

## Nächste Schritte

Die erforderliche Maßnahme hängt davon ab, welches Problem View Administrator für einen Computer meldet.

- Wenn sich ein Computer mit verknüpftem Klon in einem Fehlerstatus befindet, versucht der automatische Wiederherstellungsmechanismus von View, den verknüpften Klon einzuschalten oder auszuschalten und neu zu starten. Wenn wiederholte Wiederherstellungsversuche fehlschlagen, wird der verknüpfte Klon gelöscht. In bestimmten Situationen kann ein verknüpfter Klon womöglich wiederholt gelöscht und wiederhergestellt werden. Siehe [Fehlerbehebung bei Computern, die wiederholt gelöscht und neu erstellt werden](#).
- Wenn ein Computer eingeschaltet ist, jedoch nicht reagiert, starten Sie die zugehörige virtuelle Maschine neu. Reagiert der Computer weiterhin nicht, stellen Sie sicher, dass das Betriebssystem die View Agent-Version unterstützt. Sie können den Befehl `vmadmin` mit der Option `-A` verwenden, um die Version von View Agent anzuzeigen. Weitere Informationen finden Sie im Dokument *Administration von View*.
- Wenn ein Computer während eines langen Zeitraums den Bereitstellungsstatus aufweist, löschen Sie die virtuelle Maschine und führen den Klonvorgang für diese Maschine erneut aus. Stellen Sie sicher, dass ausreichend Festplattenspeicherplatz für die Bereitstellung der Maschine verfügbar ist. Siehe [Virtuelle Maschinen können den Bereitstellungsstatus nicht verlassen](#).
- Wenn eine Maschine bereit ist, jedoch keine Verbindungen akzeptiert, überprüfen Sie die Firewall-Konfiguration, um sicherzustellen, dass das Anzeigeprotokoll (RDP oder PCoIP) nicht blockiert wird. Siehe [Connection Problems Between Machines and View-Verbindungsserver Instances](#).
- Wenn eine Maschine auf einer vCenter Server-Instanz nicht angezeigt wird, überprüfen Sie, ob die virtuelle Maschine auf der erwarteten vCenter Server-Instanz konfiguriert ist oder auf eine andere vCenter Server-Instanz verschoben wurde.
- Wenn eine Maschine über eine aktive Anmeldung verfügt, dies jedoch keine Konsolenanmeldung ist, muss es sich um eine Remote-Sitzung handeln. Wenn die angemeldeten Benutzer nicht kontaktiert werden können, muss die virtuelle Maschine möglicherweise neu gestartet werden, um die Abmeldung der Benutzer zu erzwingen.

## Senden von Nachrichten an Desktop-Benutzer

In einigen Fällen kann es erforderlich sein, Nachrichten an Benutzer zu senden, die gegenwärtig an Desktops angemeldet sind. Wenn Sie beispielsweise Wartungsaufgaben auf einem Computer ausführen müssen, können Sie die Benutzer bitten, sich vorübergehend abzumelden. Oder Sie senden eine Warnung zu zukünftigen Dienstunterbrechungen an die Benutzer. Sie können eine Nachricht an mehrere Benutzer senden.

## Verfahren

- 1 Klicken Sie in View Administrator auf **Katalog > Desktop-Pools**.
- 2 Doppelklicken Sie auf einen Pool und anschließend auf die Registerkarte **Sitzungen**.
- 3 Wählen Sie einen oder mehrere Computer aus und klicken Sie auf **Nachricht senden**.
- 4 Geben Sie den Nachrichtentext ein, wählen Sie den Nachrichtentyp aus und klicken Sie auf **OK**.

Als Nachrichtentyp stehen **Info**, **Warnung** oder **Fehler** zur Verfügung.

Die Nachricht wird an alle ausgewählten Computer in aktiven Sitzungen gesendet.

## Fehlerbehebung bei Problemen während der Desktop-Pool-Erstellung

Für die Diagnose und Behandlung von Problemen bei der Erstellung von Desktop-Pools gibt es mehrere Vorgehensweisen.

### Fehler bei der Pool-Erstellung, wenn keine Anpassungsspezifikationen gefunden werden

Beim Versuch, einen Desktop-Pool zu erstellen, schlägt der Vorgang fehl, wenn die Anpassungsspezifikationen nicht gefunden werden können.

#### Problem

Sie können keinen Desktop-Pool erstellen und Ihnen wird die folgende Nachricht in der Ereignisdatenbank angezeigt.

Bereitstellungsfehler für Computer *Machine\_Name*: Anpassung für Computer fehlgeschlagen

#### Ursache

Die Ursache dieses Problems ist wahrscheinlich, dass Sie nicht über ausreichende Berechtigungen verfügen, um auf die Anpassungsspezifikationen zuzugreifen oder einen Pool zu erstellen. Eine weitere mögliche Ursache ist, dass die Anpassungsspezifikation umbenannt oder gelöscht wurde.

#### Lösung

- ◆ Stellen Sie sicher, dass Sie über ausreichend Berechtigungen für den Zugriff auf die Anpassungsspezifikationen und die Erstellung eines Pools verfügen.
- ◆ Wenn die Anpassungsspezifikation nicht mehr vorhanden ist, da sie umbenannt oder gelöscht wurde, wählen Sie eine andere Spezifikation.

### Fehler bei der Pool-Erstellung aufgrund eines Berechtigungsproblems

Sie können keinen Desktop-Pool erstellen, wenn ein Berechtigungsproblem mit einem ESX/ESXi-Host, ESX/ESXi-Cluster oder Rechenzentrum vorliegt.

### Problem

In View Administrator kann kein Desktop-Pool erstellt werden, da kein Zugriff auf die Vorlagen, den ESX/ESXi-Host, den ESX/ESXi-Cluster oder das Rechenzentrum möglich ist.

### Ursache

Dieses Problem kann verschiedene Ursachen haben.

- Sie verfügen nicht über die erforderlichen Berechtigungen zum Erstellen eines Pools.
- Sie verfügen nicht über die erforderlichen Berechtigungen für den Zugriff auf die Vorlagen.
- Sie verfügen nicht über die erforderlichen Berechtigungen für den Zugriff auf den ESX/ESXi-Host, den ESX/ESXi-Cluster oder das Rechenzentrum.

### Lösung

- ◆ Wenn im Fenster zur Vorlagenauswahl keine verfügbaren Vorlagen angezeigt werden, stellen Sie sicher, dass Sie über ausreichende Berechtigungen für den Zugriff auf die Vorlagen verfügen.
- ◆ Stellen Sie sicher, dass Sie über ausreichende Berechtigungen für den Zugriff auf den ESX/ESXi-Host, den ESX/ESXi-Cluster oder das Rechenzentrum verfügen.
- ◆ Stellen Sie sicher, dass Sie über ausreichende Berechtigungen für das Erstellen eines Pools verfügen.

## Fehler bei der Pool-Bereitstellung aufgrund eines Konfigurationsproblems

Wenn eine Vorlage nicht verfügbar ist oder das Image einer virtuellen Maschine verschoben oder gelöscht wurde, kann die Bereitstellung eines Desktop-Pools fehlschlagen.

### Problem

Es wird kein Desktop-Pool bereitgestellt und Ihnen wird die folgende Meldung in der Ereignisdatenbank angezeigt.

Bereitstellungsfehler bei Pool *Desktop\_ID* aufgrund eines Konfigurationsproblems

### Ursache

Dieses Problem kann verschiedene Ursachen haben.

- Der Zugriff auf eine Vorlage ist nicht möglich.
- Der Name einer Vorlage wurde in vCenter geändert.
- Eine Vorlage wurde in vCenter in einen anderen Ordner verschoben.
- Das Image einer virtuellen Maschine wurde zwischen ESX/ESXi-Hosts verschoben oder gelöscht.

### Lösung

- ◆ Stellen Sie sicher, dass der Zugriff auf die Vorlage möglich ist.

- ◆ Stellen Sie sicher, dass der richtige Name und Ordner für die Vorlage angegeben wird.
- ◆ Wenn das Image einer virtuellen Maschine zwischen ESX/ESXi-Hosts verschoben wurde, verschieben Sie die virtuelle Maschine in den richtigen vCenter-Ordner.
- ◆ Wenn das Image einer virtuellen Maschine gelöscht wurde, löschen Sie den Eintrag für die virtuelle Maschine in View Administrator und erstellen Sie das Image neu bzw. stellen Sie das Image wieder her.

## **Fehler bei der Pool-Bereitstellung, da eine View-Verbindungsserver-Instanz keine Verbindung mit einer vCenter-Instanz herstellen kann**

Wenn eine View-Verbindungsserver-Instanz keine Verbindung mit einer vCenter-Instanz herstellen kann, schlägt die Bereitstellung eines Desktop-Pools möglicherweise fehl.

### **Problem**

Die Bereitstellung eines Desktop-Pools schlägt fehl und Ihnen wird eine der folgenden Fehlermeldungen in der Ereignisdatenbank angezeigt.

- Cannot log in to vCenter at address *VC-Adresse* (Anmeldung an vCenter bei Adresse *VC-Adresse* nicht möglich)
- The status of vCenter at address *VC-Adresse* is unknown (Der Status von vCenter bei Adresse *VC-Adresse* ist unbekannt)

### **Ursache**

Die View-Verbindungsserver-Instanz kann aus einem der folgenden Gründe keine Verbindung zur vCenter-Instanz herstellen.

- Der Webdienst auf der vCenter Server-Instanz wurde angehalten.
- Zwischen dem View-Verbindungsserver-Host und der vCenter Server-Instanz sind Netzwerkprobleme aufgetreten.
- Die Portnummern und Anmeldeinformationen für vCenter oder View Composer haben sich geändert.

### **Lösung**

- ◆ Stellen Sie sicher, dass der Webdienst auf der vCenter-Instanz ausgeführt wird.
- ◆ Stellen Sie sicher, dass zwischen dem View-Verbindungsserver-Host und der vCenter-Instanz keine Netzwerkprobleme aufgetreten sind.
- ◆ Überprüfen Sie in View Administrator die Portnummern und Anmeldeinformationen, die für vCenter und View Composer konfiguriert sind.

## Fehler bei der Pool-Bereitstellung aufgrund von Datenspeicherproblemen

Wenn der Festplattenspeicherplatz eines Datenspeichers belegt ist oder Sie nicht für den Zugriff auf den Datenspeicher berechtigt sind, kann die Bereitstellung eines Desktop-Pools fehlschlagen.

### Problem

Die Bereitstellung eines Desktop-Pools schlägt fehl und Ihnen wird eine der folgenden Fehlermeldungen in der Ereignisdatenbank angezeigt.

- Provisioning error occurred for Machine *Name\_der\_Maschine*: Cloning failed for Machine (Bereitstellungsfehler für Maschine *Name\_der\_Maschine*: Klonen der Maschine fehlgeschlagen)
- Provisioning error occurred on Pool *Desktop-ID* because available free disk space is reserved for linked clones (Bereitstellungsfehler für Pool *Desktop-ID*, da verfügbarer Speicherplatz für verknüpfte Klone reserviert ist)
- Provisioning error occurred on Pool *Desktop-ID* because of a resource problem (Bereitstellungsfehler aufgrund eines Ressourcenproblems für Pool *Desktop-ID*)

### Ursache

Sie sind nicht für den Zugriff auf den ausgewählten Datenspeicher berechtigt oder der für den Pool verwendete Datenspeicher ist belegt.

### Lösung

- ◆ Stellen Sie sicher, dass Sie über ausreichende Berechtigungen für den Zugriff auf den ausgewählten Datenspeicher verfügen.
- ◆ Überprüfen Sie, ob die Festplatte, auf welcher der Datenspeicher konfiguriert ist, voll ist.
- ◆ Wenn die Festplatte voll oder der Speicherplatz reserviert ist, geben Sie Speicherplatz frei, verteilen Sie die verfügbaren Datenspeicher neu oder migrieren Sie den Datenspeicher auf eine Festplatte mit höherer Kapazität.

## Fehler bei der Pool-Bereitstellung, da vCenter Server überlastet ist

Wenn vCenter Server durch das Volumen an Anforderungen überlastet ist, kann die Bereitstellung eines Desktop-Pools fehlschlagen.

### Problem

Die Bereitstellung eines Desktop-Pools schlägt fehl und Ihnen wird die folgende Fehlermeldung in der Ereignisdatenbank angezeigt.

Bereitstellungsfehler bei Pool *Desktop\_ID* aufgrund einer Zeitüberschreitung bei der Anpassung

### Ursache

vCenter ist durch das Volumen an Anforderungen überlastet.

### Lösung

- ◆ Verringern Sie in View Administrator die maximale Anzahl gleichzeitig ausgeführter Bereitstellungs- und Betriebsvorgänge für vCenter Server.
- ◆ Konfigurieren Sie zusätzliche vCenter Server-Instanzen.

Weitere Informationen zur Konfiguration von vCenter Server finden Sie im Dokument *Installation von View*.

## Virtuelle Maschinen können den Bereitstellungsstatus nicht verlassen

Nach dem Klonen verlassen virtuelle Maschinen den Bereitstellungsstatus nicht.

### Problem

Virtuelle Maschinen können den Bereitstellungsstatus nicht verlassen.

### Ursache

Die Ursache dieses Problems ist wahrscheinlich, dass Sie die View-Verbindungsserver-Instanz während eines Klonvorgangs neu gestartet haben.

### Lösung

- ◆ Löschen Sie die virtuellen Maschinen und führen Sie den Klonvorgang erneut aus.

## Virtuelle Maschinen können den Anpassungsstatus nicht verlassen

Nach dem Klonen verlassen virtuelle Maschinen den Anpassungsstatus nicht.

### Problem

Virtuelle Maschinen können den Anpassungsstatus nicht verlassen.

### Ursache

Die Ursache für dieses Problem ist wahrscheinlich, dass nicht genügend Festplattenspeicherplatz zum Starten der virtuellen Maschine verfügbar ist. Bevor eine Anpassung durchgeführt werden kann, muss eine virtuelle Maschine gestartet werden.

### Lösung

- ◆ Löschen Sie die virtuelle Maschine, um eine Wiederherstellung durchzuführen, wenn eine Maschine den Anpassungsstatus nicht verlassen kann.
- ◆ Wenn die Festplatte voll ist, geben Sie Speicherplatz frei oder migrieren Sie den Datenspeicher auf eine Festplatte mit höherer Kapazität.

## Entfernen verwaister oder gelöschter verknüpfter Klone

Unter bestimmten Umständen sind Daten verknüpfter Klone in View, View Composer und vCenter Server nicht mehr synchronisiert, und Sie können Maschinen mit verknüpftem Klon nicht bereitstellen oder löschen.

### Problem

- Sie können keinen Linked-Clone-Desktop-Pool bereitstellen.
- Die Bereitstellung von Linked-Clone-Maschinen (Maschinen mit verknüpftem Klon) schlägt fehl und der folgende Fehler wird gemeldet: `Virtual machine with Input Specification already exists` (Virtuelle Maschine mit eingegebener Spezifikation ist bereits vorhanden)
- In View Administrator können Maschinen mit verknüpftem Klon den Status `Deleting` nicht verlassen. Sie können den Befehl „Löschen“ in View Administrator nicht erneut ausführen, da sich die Maschinen bereits im Status `Deleting` befinden.

### Ursache

Dieses Problem tritt auf, wenn die View Composer-Datenbank Informationen zu verknüpften Klonen enthält, die nicht mit den Informationen in View LDAP, Active Directory oder vCenter Server konsistent sind. Mehrere Situationen können diese Inkonsistenz verursachen:

- Der Name der virtuellen Linked-Clone-Maschine wird manuell in vCenter Server geändert, nachdem der Pool erstellt wurde, was dazu führt, dass View Composer und vCenter Server mit verschiedenen Namen auf die gleiche virtuelle Maschine verweisen.
- Ein Speicherfehler oder manueller Vorgang führt dazu, dass die virtuelle Maschine aus vCenter Server gelöscht wird. Die Daten der virtuellen Maschine mit verknüpftem Klon bestehen noch in der View Composer-Datenbank, in View LDAP und in Active Directory.
- Während ein Pool aus View Administrator gelöscht wird, belässt ein Netzwerkausfall oder anderer Ausfall die virtuelle Maschine in vCenter Server.

Wenn der Name der virtuellen Maschine in vSphere Client umbenannt wurde, nachdem der Desktop-Pool bereitgestellt wurde, versuchen Sie, die virtuelle Maschine auf den Namen umzubenennen, der verwendet wurde, als er in View bereitgestellt wurde.

Wenn andere Datenbankinformationen inkonsistent sind, verwenden Sie den Befehl `SviConfig RemoveSviClone`, um diese Objekte zu entfernen:

- Die Linked-Clone-Datenbankeinträge aus der View Composer-Datenbank
- Das Linked-Clone-Maschinenkonto aus Active Directory
- Die virtuelle Linked-Clone-Maschine aus vCenter Server

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

**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.

Unternehmen Sie die folgenden Schritte:

- 1 Stellen Sie sicher, dass der View Composer-Dienst ausgeführt wird.
- 2 Führen Sie an einer Windows-Befehlseingabeaufforderung auf dem View Composer-Computer den Befehl SviConfig RemoveSviClone in folgender Form aus:

```
sviconfig -operation=removesviclone
          -VmName=Name der virtuellen Maschine
          [-AdminUser=Benutzername des lokalen Administrators]
          -AdminPassword=Kennwort des lokalen Administrators
          [-ServerUrl=View Composer Server-URL]
```

Beispiel:

```
sviconfig -operation=removesviclone -vmname=MyLinkedClone
          -adminuser=Admin -adminpassword=Pass -serverurl=ViewComposerURL
```

Die Parameter VmName und AdminPassword sind erforderlich. Der Standardwert des Parameters AdminUser lautet Administrator. Der Standardwert des Parameters ServerURL lautet https://localhost:18443/SviService/v2\_0

Weitere Informationen zum Entfernen von VM-Informationen aus View LDAP finden Sie im VMware-Knowledgebase-Artikel 2015112: *Manually deleting linked clones or stale virtual desktop entries from VMware View Manager 4.5 and later*.

## Fehlerbehebung bei Computern, die wiederholt gelöscht und neu erstellt werden

View kann wiederholt Linked-Clone- und Full-Clone-Computer löschen und neu erstellen, die sich in einem Fehlerstatus befinden.

### Problem

Ein Linked-Clone- oder Full-Clone-Computer wird in einem Fehlerstatus erstellt, gelöscht und in einem Fehlerstatus neu erstellt. Dieser Zyklus wiederholt sich.

### Ursache

Wenn ein großer Desktop-Pool bereitgestellt wird, können eine oder mehrere virtuelle Maschinen einen Fehlerstatus aufweisen. Der automatische Wiederherstellungsmechanismus von View versucht, die ausgefallene virtuelle Maschine einzuschalten. Wenn sich die virtuelle Maschine nach einer bestimmten Anzahl von Versuchen nicht einschaltet, löscht View die virtuelle Maschine.



View Manager erstellt entsprechend der Anforderungen für die Poolgröße eine neue virtuelle Maschine, oft mit demselben Computernamen wie dem des ursprünglichen Computers. Wenn die neue Maschine mit dem gleichen Fehler bereitgestellt wird, wird diese virtuelle Maschine gelöscht und der Zyklus wiederholt sich.

Auf Linked-Clone- und Full-Cloned-Computern wird eine automatische Wiederherstellung durchgeführt.

Wenn die automatischen Wiederherstellungsversuche bei einer virtuellen Maschine fehlschlagen, löscht View die virtuelle Maschine nur, wenn es sich um einen dynamischen Computer oder einen dedizierten Computer handelt, der keinem Benutzer zugewiesen ist. Außerdem löscht View keine virtuellen Maschinen, wenn die Poolbereitstellung deaktiviert ist.

Untersuchen Sie die übergeordnete virtuelle Maschine oder Vorlage, die zur Erstellung des Desktop-Pools verwendet wurde. Suchen Sie nach Fehlern auf der virtuellen Maschine oder dem Gastbetriebssystem, die den Fehler auf der virtuellen Maschine verursachen könnten.

Lösen Sie bei verlinkten Klonen Fehler auf der übergeordneten virtuellen Maschine und erstellen Sie einen neuen Snapshot.

- Wenn sich viele Computer im Fehlerstatus befinden, verwenden Sie den neuen Snapshot oder die Vorlage, um den Pool neu zu erstellen.
- Wenn die meisten Computer gesund sind, wählen Sie den Desktop-Pool in View Administrator aus, klicken Sie auf **Bearbeiten**, wählen Sie die Registerkarte „vCenter-Einstellungen“ aus, wählen Sie den neuen Snapshot als Standard-Basis-Image aus und speichern Sie die vorgenommenen Änderungen.

Neue Linked-Clone-Computer werden anhand des neuen Snapshots erstellt.

Lösen Sie bei vollständigen Klonen Fehler auf der virtuellen Maschine, erstellen Sie eine neue Vorlage und erstellen Sie den Pool neu.

## Beheben von Fehlern bei der QuickPrep-Anpassung

Ein View Composer QuickPrep-Anpassungsskript kann aus verschiedenen Gründen fehlschlagen.

### Problem

Ein nach der Synchronisierung ausgeführtes QuickPrep-Skript oder Abschaltskript wird nicht ausgeführt. In einigen Fällen wird ein Skript für einige verknüpfte Klone möglicherweise vollständig ausgeführt, auf anderen Klonen schlägt es jedoch fehl.

### Ursache

Häufige Ursachen für QuickPrep-Skriptfehler sind:

- Zeitüberschreitung bei der Skriptausführung
- Der Skriptpfad bezieht sich auf ein Skript, das einen Interpreter erfordert
- Das für die Ausführung des Skripts verwendete Konto verfügt nicht über ausreichende Berechtigungen, um eine Skriptaufgabe auszuführen

## Lösung

- ◆ Überprüfen Sie das Protokoll des Anpassungsskripts.

Die Informationen zur QuickPrep-Anpassung werden in eine Protokolldatei im Windows-Verzeichnis temp geschrieben:

C:\Windows\Temp\vmware-viewcomposer-ga-new.log

- ◆ Überprüfen Sie, ob bei der Skriptausführung eine Zeitüberschreitung aufgetreten ist.

View Composer beendet ein Anpassungsskript, wenn dessen Ausführung länger als 20 Sekunden dauert. In der Protokolldatei wird in einer Meldung angezeigt, dass das Skript gestartet wurde, in einer weiteren Meldung wird die Zeitüberschreitung angezeigt:

```
2010-02-21 21:05:47,687 [1500] INFO Ready -
[Ready.cpp, 102] Running the PostSync script: cmd /c
C:\temp\build\composer.bat
2010-02-21 21:06:07,348 [1500] FATAL Guest -
[Guest.cpp, 428] script cmd /c
C:\temp\build\composer.bat timed out
```

Um ein Zeitüberschreitungsproblem zu beheben, erhöhen Sie das Zeitüberschreitungslimit für das Skript und führen Sie es erneut aus.

- ◆ Überprüfen Sie, ob der Skriptpfad gültig ist.

Wenn Sie eine Skriptsprache verwenden, die zur Skriptausführung einen Interpreter erfordert, muss der Skriptpfad mit der Interpreter-Binärdatei beginnen.

Wenn Sie beispielsweise den Pfad C:\script\myvb.vbs als QuickPrep-Anpassungsskript angeben, kann View Composer Agent das Skript nicht ausführen. Sie müssen einen Pfad angeben, der mit der Interpreter-Binärdatei beginnt:

C:\windows\system32\cscript.exe c:\script\myvb.vbs

- ◆ Überprüfen Sie, ob das für die Ausführung des Skripts verwendete Konto über die erforderlichen Berechtigungen zur Ausführung von Skriptaufgaben verfügt.

QuickPrep führt die Skripts mit dem Konto aus, das zur Ausführung des VMware View Composer Gastagentserver-Dienstes konfiguriert ist. Standardmäßig handelt es sich hier um das Konto Lokales System.

Ändern Sie dieses Anmeldekonto nicht. Wenn Sie das Konto ändern, können die verknüpften Klone nicht starten.

## Suchen und Aufheben des Schutzes von nicht verwendeten View Composer-Replikaten

Unter bestimmten Bedingungen verbleiben möglicherweise View Composer-Replikate in vCenter Server, wenn keine Klone mehr mit ihnen verknüpft sind.

## Problem

In einem vCenter Server-Ordner verbleibt ein nicht verwendetes Replikat. Sie können das Replikat nicht mithilfe von vSphere Client entfernen.

## Ursache

Netzwerkausfälle während View Composer-Vorgängen oder das direkte Entfernen der verknüpften Klone aus vSphere, ohne dass die richtigen View-Befehle angewandt wurden, können zu einem nicht verwendeten Replikat in vCenter Server führen.

Replikate sind in vCenter Server geschützte Entitäten. Sie können nicht mithilfe gewöhnlicher vCenter Server- oder vSphere Client Management-Befehle entfernt werden.

Verwenden Sie den Befehl `SviConfig FindUnusedReplica`, um im angegebenen Ordner ein Replikat zu suchen. Mit dem Parameter `-Move` können Sie das Replikat in einen anderen Ordner verschieben. Der Parameter `-Move` hebt den Schutz eines nicht verwendeten Replikats vor dem Verschieben auf.

---

**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.

---

Das Dienstprogramm `SviConfig` befindet sich im Ordner der View Composer-Anwendung. Der Standardpfad lautet `C:\Programme (x86)\VMware\VMware View Composer\sviconfig.exe`.

Bevor Sie beginnen, stellen Sie bitte sicher, dass keine Klone mit dem Replikat verknüpft sind.

Machen Sie sich mit den `SviConfig FindUnusedReplica`-Parametern vertraut:

- `DsnName`. Der DSN muss für die Datenbankverbindung verwendet werden.
- `UserName`. Der für die Verbindung mit der Datenbank verwendete Benutzername. Wenn dieser Parameter nicht angegeben wird, wird die Windows-Authentifizierung verwendet.
- `Password` (Kennwort). Das Kennwort für den Benutzer, der sich mit der Datenbank verbindet. Wenn dieser Parameter nicht angegeben und die Windows-Authentifizierung nicht verwendet wird, werden Sie zu einem späteren Zeitpunkt zur Eingabe des Kennworts aufgefordert.
- `ReplicaFolder`. Der Name des Replikat-Ordners. Verwenden Sie für den Stammordner eine leere Zeichenfolge. Der Standardwert lautet `VMwareViewComposerReplicaFolder`.
- `UnusedReplicaFolder`. Der Name des Ordners, in dem alle nicht verwendeten Replikate enthalten sein sollen. Der Standardwert lautet `UnusedViewComposerReplicaFolder`. Verwenden Sie diesen Parameter, um den Zielordner anzugeben, wenn Sie den Parameter `Move` verwenden.
- `OutputDir`. Der Name des Ausgabeverzeichnis, in dem die Liste der nicht verwendeten Replikate generiert wird, die in der Datei `unused-replica-*.txt` gespeichert ist. Der Standardwert ist das aktuelle Arbeitsverzeichnis.
- `Move`. Legt fest, ob der Schutz nicht verwendeter virtueller Maschinen aufgehoben wird und diese in einen angegebenen Ordner verschoben werden. Der Parameter `UnusedReplicaFolder` gibt den Zielordner an. Der Standardwert des Parameters `Move` lautet `false`.

Die Parameter DsnName, Username und Password müssen angegeben werden. Der DsnName kann keine leere Zeichenfolge sein.

Unternehmen Sie die folgenden Schritte:

- 1 Halten Sie den View Composer-Dienst an.
- 2 Führen Sie an einer Windows-Befehlseingabeaufforderung auf dem View Composer-Computer den Befehl `SviConfig FindUnusedReplica` in folgender Form aus:

```
sviconfig -operation=findunusedreplica
          -DsnName=DSN-Name
          -Username=Benutzername des Datenbankadministrators
          -Password=Kennwort des Datenbankadministrators
          [-ReplicaFolder=Name des Replikat-Ordners]
          [-UnusedReplicaFolder=Name des nicht verwendeten Replikat-Ordners.]
          [-OutputDir=Ausgabedateiverzeichnis]
          [-Move=wahr or falsch]
```

Beispiel:

```
sviconfig -operation=FindUnusedReplica -DsnName=SVI
          -Username=SVIUser -Password=1234 -Move=True
```

- 3 Starten Sie den View Composer-Dienst neu.
- 4 (Optional) Entfernen Sie nach dem Verschieben des Replikats in den neuen Ordner das Replikat der virtuellen Maschine aus vCenter Server.

## Fehler beim Hinzufügen von verknüpften Windows XP-Klonen zur Domäne

Virtuelle Windows XP-Maschinen mit verknüpftem Klon können möglicherweise nicht zur Domäne hinzugefügt werden, wenn Active Directory unter Windows Server 2008 ausgeführt wird.

### Problem

Bei der Bereitstellung von Maschinen mit verknüpftem Klon können die verknüpften Klone nicht zur Domäne hinzugefügt werden. View Administrator zeigt die View Composer-Bereitstellungsfehlermeldungen an. Beispiel:

```
5/17/10 3:11:50 PM PDT: View Composer agent initialization state error (18): Failed
to join the domain (waited 565 seconds) (Statusfehler bei View Composer Agent-
Initialisierung (18): Beitreten zur Domäne fehlgeschlagen [565 Sekunden gewartet])
```

### Ursache

Dieses Problem kann auftreten, wenn Active Directory unter Windows Server 2008 ausgeführt wird. Der schreibgeschützte Domänencontroller (Read-Only Domain Controller, RODC) in Windows Server 2008 ist nicht mit virtuellen Windows XP-Maschinen abwärtskompatibel.

## Lösung

- 1 Überprüfen Sie das View Composer-Protokoll auf die folgende Fehlermeldung:

0x4f1: The system detected a possible attempt to compromise security. Please ensure that you can contact the server that authenticated you. (Das System hat eine mögliche Sicherheitsgefahr festgestellt. Stellen Sie sicher, dass Sie mit dem Server, der Sie authentifiziert hat, Verbindung aufnehmen können.)

Die View Composer-Protokolldatei wird standardmäßig im Windows-Verzeichnis Temp generiert:  
C:\Windows\Temp\vmware-viewcomposer-ga-new.log

- 2 Spielen Sie auf der übergeordneten virtuellen Maschine das Windows Server 2008-RODC-Kompatibilitäts-Update für Windows XP auf.

Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 944043 unter: <http://support.microsoft.com/kb/944043/en-us>.

- 3 Erstellen Sie einen Snapshot der aktualisierten übergeordneten virtuellen Maschine.
- 4 Stellen Sie die Maschinen mit verknüpftem Klon aus der aktualisierten übergeordneten virtuellen Maschine und dem Snapshot neu zusammen.

## View Composer-Bereitstellungsfehler

Wenn bei der Bereitstellung oder Neuzusammenstellung von Linked-Clone-Maschinen durch View Composer ein Fehler auftritt, wird die Fehlerursache durch einen Fehlercode angezeigt. Der Fehlercode wird in View Administrator in der Spalte mit dem Maschinen-Status angezeigt.

**Tabelle 18-1. View Composer-Bereitstellungsfehler** beschreibt die View Composer-Bereitstellungsfehlercodes.

In dieser Tabelle werden Fehler im Zusammenhang mit View Composer- und QuickPrep-Anpassungen aufgeführt. Im View-Verbindungsserver und in anderen View-Komponenten können weitere Fehler auftreten, die möglicherweise zu Problemen bei der Maschinen-Bereitstellung führen.

**Tabelle 18-1. View Composer-Bereitstellungsfehler**

| Fehler | Beschreibung  |
|--------|---|
| 0      | Die Richtlinie wurde erfolgreich angewendet.<br><br><b>Hinweis</b> Der Ergebniscode 0 wird in View Administrator nicht angezeigt. Die Linked-Clone-Maschine wechselt in den Status „Bereit“, sofern nicht ein View-Fehler außerhalb der View Composer-Domäne auftritt. Dieser Ergebniscode ist der Vollständigkeit halber enthalten.            |
| 1      | Der Computernamen konnte nicht festgelegt werden.   |
| 2      | Die Benutzerprofile konnten nicht an die persistente View Composer-Festplatte umgeleitet werden.  |
| 3      | Das Domänenkontokennwort des Computers konnte nicht festgelegt werden.  |
| 4      | Die Profilschlüssel eines Benutzers konnten nicht gesichert werden. Bei der nächsten Anmeldung des Benutzers bei dieser Linked-Clone-Maschine nach der Neuzusammenstellung erstellt das Betriebssystem ein neues Profilverzeichnis für den Benutzer. Da ein neues Profil erstellt wird, kann der Benutzer die alten Profildaten nicht anzeigen. |

| Fehler | Beschreibung   |
|--------|--|
| 5      | Ein Benutzerprofil konnte nicht wiederhergestellt werden. Der Benutzer sollte sich bei diesem Status nicht bei der Maschine anmelden, da der Profilstatus nicht definiert ist.   |
| 6      | <p>Fehler, die nicht durch andere Fehlercodes abgedeckt werden. Die View Composer Agent-Protokolldateien im Gastbetriebssystem umfassen möglicherweise weitere Informationen zu den Ursachen dieser Fehler.</p> <p>Beispielsweise kann dieser Fehlercode durch eine Windows PnP-Zeitüberschreitung (Plug and Play) generiert werden. In dieser Situation kommt es für View Composer zu einer Zeitüberschreitung, während auf die Installation neuer Volumes für die virtuelle Linked-Clone-Maschine durch den PnP-Dienst gewartet wird.</p> <p>PnP mountet abhängig von der Pool-Konfiguration bis zu drei Festplatten:</p> <ul style="list-style-type: none"> <li>■ Persistente View Composer-Festplatte</li> <li>■ Nicht persistente Festplatte zum Umleiten von temporären und Auslagerungsdateien des Gastbetriebssystems</li> <li>■ Interne Festplatte zum Speichern der QuickPrep-Konfiguration und anderer betriebssystembezogener Daten. Diese Festplatte wird immer mit einem verknüpften Klon konfiguriert.</li> </ul> <p>Der für die Zeitüberschreitung definierte Wert lautet 10 Minuten. Wenn das Mounten der Festplatten durch PnP nicht innerhalb von 10 Minuten abgeschlossen wird, schlägt View Composer mit dem Fehlercode 6 fehl.</p> |
| 7      | Eine zu große Anzahl an persistenten View Composer-Festplatten ist mit dem verknüpften Klon verbunden. Ein Klon kann über maximal drei persistente View Composer-Festplatten verfügen.   |
| 8      | Eine persistente Festplatte konnte nicht in dem bei der Pool-Erstellung ausgewählten Datenspeicher gemountet werden.   |
| 9      | View Composer konnte Dateien mit löschbaren Daten nicht auf die nicht persistente Festplatte umleiten. Die Auslagerungsdatei oder die Ordner mit temporären Dateien wurden nicht umgeleitet.   |
| 10     | View Composer kann die QuickPrep-Konfigurationsrichtliniendatei auf der angegebenen internen Festplatte nicht finden.  |
| 12     | View Composer kann die interne Festplatte mit der QuickPrep-Konfigurationsrichtliniendatei und andere betriebssystembezogene Daten nicht finden.   |
| 13     | Mehrere persistente Festplatten sind für die Umleitung des Windows-Benutzerprofils konfiguriert.   |
| 14     | View Composer konnte die interne Festplatte nicht unmounten.   |
| 15     | Der Computernamen, den View Composer aus der Konfigurationsrichtliniendatei gelesen hat, stimmt nach dem anfänglichen Einschalten des verknüpften Klon nicht mit dem aktuellen Systemnamen überein.  |
| 16     | View Composer Agent wurde nicht gestartet, da die Volumelizenz für das Gastbetriebssystem nicht aktiviert wurde.   |
| 17     | View Composer Agent wurde nicht gestartet. Für den Agenten ist es beim Warten auf den Sysprep-Start zu einer Zeitüberschreitung gekommen.  |
| 18     | View Composer Agent konnte die virtuelle Linked-Clone-Maschine während der Anpassung nicht mit einer Domäne verknüpfen.  |
| 19     | Der View Composer-Agent konnte das nach der Synchronisierung auszuführende Skript nicht anwenden.  |
| 20     | <p>Der View Composer-Agent konnte ein Synchronisierungsereignis für ein Computerkennwort nicht bearbeiten. Es handelt sich hier möglicherweise um einen vorübergehenden Fehler. Kann der verknüpfte Klon zur Domäne hinzugefügt werden, ist das Passwort in Ordnung.</p> <p>Kann der Klon nicht zur Domäne hinzugefügt werden, muss der Vorgang neu gestartet werden, den Sie vor Auftreten des Fehlers durchgeführt haben. Falls Sie den Klon neu gestartet haben, sollten Sie dies erneut tun. Falls Sie den Klon aktualisiert haben, sollten Sie dies erneut tun. Kann der Klon immer noch nicht zur Domäne hinzugefügt werden, muss er neu zusammengestellt werden.</p>  |

## Fehlerbehebung bei Problemen mit der Netzwerkverbindung

Für die Diagnose und Behandlung von Problemen mit der Netzwerkverbindung zu Maschinen, Horizon Client-Geräten und View-Verbindungsserver-Instanzen können Sie zwischen verschiedenen Vorgehensweisen wählen.

### Connection Problems Between Machines and View-Verbindungsserver Instances

Bei der Verbindung zwischen Computern und View-Verbindungsserver-Instanzen können Probleme auftreten.

#### Problem

Wenn für die Konnektivität zwischen einem Computer und einer View-Verbindungsserver-Instanz ein Fehler auftritt, wird in der Ereignisdatenbank eine der folgenden Meldungen angezeigt.

- Provisioning error occurred for Machine *Name\_der\_Maschine*: Customization error due to no network communication between the View agent and Connection Server (Bereitstellungsfehler für Maschine *Name\_der\_Maschine*: Anpassungsfehler, da keine Netzwerkkommunikation zwischen der View Agent- und Connection Server-Instanz möglich ist)
- Provisioning error occurred on Pool *Desktop-ID* because of a networking problem with a View Agent (Bereitstellungsfehler für Pool *Desktop-ID* aufgrund eines Netzwerkproblems mit einer View Agent-Instanz)
- Unable to launch from Pool *Desktop-ID* for user *Anzeigename\_des\_Benutzers*: Failed to connect to Machine *Name\_der\_Maschine* using *Protokoll* (Starten aus Pool *Desktop-ID* für Benutzer *Anzeigename\_des\_Benutzers* nicht möglich: Verbindung zu Maschine *Name\_der\_Maschine* konnte unter Verwendung von *Protokoll* nicht hergestellt werden)

#### Ursache

Bei der Konnektivität zwischen einem Computer und einer View-Verbindungsserver-Instanz können aus verschiedenen Gründen Probleme auftreten.

- Lookup-Fehler auf dem Computer für den DNS-Namen des View-Verbindungsserver-Hosts.
- Die Ports für die JMS-, RDP- oder AJP13-Kommunikation werden durch Firewall-Regeln blockiert.
- Ein Ausfall des JMS-Routers auf dem View-Verbindungsserver-Host.

#### Lösung

- ◆ Geben Sie an einer Eingabeaufforderung auf dem Computer den Befehl `nslookup` ein.

```
nslookup CS_FQDN
```

*CS-FQDN* ist der vollqualifizierte Domänenname (FQDN) des View-Verbindungsserver-Hosts. Wenn der Befehl die IP-Adresse des View-Verbindungsserver-Hosts nicht zurückgibt, korrigieren Sie die DNS-Konfiguration mithilfe der allgemeinen Verfahren zur Behandlung von Netzwerkproblemen.

- ◆ Stellen Sie an einer Eingabeaufforderung auf dem Computer sicher, dass TCP-Port 4001 ordnungsgemäß funktioniert. Dieser Port wird von der View Agent-Instanz für die JMS-Kommunikation mit dem View-Verbindungsserver-Host verwendet. Geben Sie zu diesem Zweck den `telnet`-Befehl ein.

```
telnet CS_FQDN 4001
```

Wenn die `telnet`-Verbindung hergestellt wird, funktioniert die Netzwerkkonnektivität für JMS ordnungsgemäß.

- ◆ Wenn ein Sicherheitsserver in der DMZ bereitgestellt wird, stellen Sie sicher, dass in der inneren Firewall Ausnahmeregeln konfiguriert sind, um RDP-Konnektivität zwischen dem Sicherheitsserver und virtuellen Maschinen an TCP-Port 3389 zuzulassen.
- ◆ Wenn sichere Verbindungen umgangen werden, stellen Sie sicher, dass die Firewall-Regeln Folgendes zulassen: Clients können eine direkte RDP-Verbindung mit der virtuellen Maschine an TCP-Port 3389 oder eine direkte PCoIP-Verbindung mit der virtuellen Maschine an TCP-Port 4172 und UDP-Port 4172 herstellen.
- ◆ Stellen Sie sicher, dass in der inneren Firewall Ausnahmeregeln konfiguriert sind, um Verbindungen zwischen jeder Sicherheitsserver-Instanz und dem zugehörigen View-Verbindungsserver-Host an TCP-Port 4001 (JMS) und TCP-Port 8009 (AJP13) zuzulassen.

## Verbindungsprobleme zwischen Horizon Client und dem PCoIP Secure Gateway

Es kann zu Verbindungsproblemen zwischen Horizon Client und einem Sicherheitsserver- oder View-Verbindungsserver-Host kommen, wenn das PCoIP Secure Gateway so konfiguriert ist, dass externe Benutzer, die über PCoIP kommunizieren, authentifiziert werden müssen.

### Problem

Clients, die PCoIP verwenden, können weder eine Verbindung mit View-Desktops herstellen noch diese anzeigen. Die anfängliche Anmeldung an einer Sicherheitsserver- oder View-Verbindungsserver-Instanz ist erfolgreich, die Verbindung schlägt jedoch fehl, wenn der Benutzer einen View-Desktop auswählt. Dieses Problem tritt auf, wenn das PCoIP Secure Gateway auf einem Sicherheitsserver- oder View-Verbindungsserver-Host konfiguriert ist.

---

**Hinweis** Normalerweise wird das PCoIP Secure Gateway auf einem Sicherheitsserver genutzt. In einer Netzwerkkonfiguration, bei der externe Clients eine direkte Verbindung mit dem View-Verbindungsserver-Host herstellen, kann das PCoIP Secure Gateway auch auf der View-Verbindungsserver-Instanz konfiguriert werden.

---



## Ursache

Es kann verschiedene Gründe dafür geben, dass Probleme bei der Verbindungsherstellung mit dem PCoIP Secure Gateway auftreten.

- In der Windows-Firewall wurde ein Port geschlossen, der für das PCoIP Secure Gateway erforderlich ist.
- Das PCoIP Secure Gateway ist auf der Sicherheitsserver- oder View-Verbindungsserver-Instanz nicht aktiviert.
- Die externe PCoIP-URL ist falsch konfiguriert. Sie müssen diese Einstellung auf die externe IP-Adresse festlegen, auf die Clients über das Internet zugreifen können.
- Die externen URLs für den sicheren Tunnel, für PCoIP und für Blast oder eine andere Adresse sind so konfiguriert, dass auf einen anderen Sicherheitsserver- oder View-Verbindungsserver-Host verwiesen wird. Wenn Sie diese Adressen auf einem Sicherheitsserver- oder View-Verbindungsserver-Host konfigurieren, müssen Clientsysteme mit allen Adressen eine Verbindung mit dem aktuellen Host herstellen können.
- Der Client stellt die Verbindung über einen externen Webproxy her, für den ein Port geschlossen wurde, der für das PCoIP Secure Gateway erforderlich ist. Beispielsweise kann ein Webproxy im Netzwerk eines Hotels oder eine öffentliche drahtlose Verbindung die erforderlichen Ports blockieren.
- Die View-Verbindungsserver-Instanz, die mit dem Sicherheitsserver kombiniert ist, auf dem das PCoIP Secure Gateway konfiguriert ist, verwendet View 4.5 oder eine frühere Version. Der Sicherheitsserver und die kombinierte View-Verbindungsserver-Instanz müssen View 4.6 oder eine höhere Version verwenden.

## Lösung

- ◆ Stellen Sie sicher, dass die folgenden Netzwerkports in der Firewall für den Sicherheitsserver- oder View-Verbindungsserver-Host geöffnet sind.

| Port     | Beschreibung  |
|----------|---|
| TCP 4172 | Von Horizon Client zum Sicherheitsserver- oder View-Verbindungsserver-Host.                                 |
| UDP 4172 | Zwischen Horizon Client und dem Sicherheitsserver- oder View-Verbindungsserver-Host, in beide Richtungen.   |
| TCP 4172 | Vom Sicherheitsserver- oder View-Verbindungsserver-Host zum View-Desktop.                                   |
| UDP 4172 | Zwischen dem Sicherheitsserver- oder View-Verbindungsserver-Host und dem View-Desktop, in beide Richtungen. |

- ◆ Stellen Sie in View Administrator sicher, dass das PCoIP Secure Gateway aktiviert ist.
  - a Klicken Sie auf **View-Konfiguration > Server**.
  - b Wählen Sie die View-Verbindungsserver-Instanz auf der Registerkarte **Verbindungsserver** aus und klicken Sie auf **Bearbeiten**.

- c Aktivieren Sie **PCoIP Secure Gateway für PCoIP-Verbindungen zum Computer verwenden**.  
Das PCoIP Secure Gateway ist standardmäßig deaktiviert.
- d Klicken Sie auf **OK**.
- ◆ Stellen Sie in View Administrator sicher, dass die externe PCoIP-URL ordnungsgemäß konfiguriert ist.
  - a Klicken Sie auf **View-Konfiguration > Server**.
  - b Wählen Sie den zu konfigurierenden Host aus.
    - Wenn Ihre Benutzer über einen Sicherheitsserver eine Verbindung mit dem PCoIP Secure Gateway herstellen, wählen Sie auf der Registerkarte **Sicherheitsserver** den Sicherheitsserver aus.
    - Wenn Ihre Benutzer über eine View-Verbindungsserver-Instanz eine Verbindung mit dem PCoIP Secure Gateway herstellen, wählen Sie auf der Registerkarte **Verbindungsserver** diese Instanz aus.
  - c Klicken Sie auf **Bearbeiten**.
  - d Stellen Sie sicher, dass im Textfeld **PCoIP – Externe URL** die externe IP-Adresse für den Sicherheitsserver- oder View-Verbindungsserver-Host angegeben ist, auf die Clients über das Internet zugreifen können.  
  
Geben Sie Port 4172 an. Schließen Sie keinen Protokollnamen ein.  
  
Beispiel: **10.20.30.40:4172**
  - e Stellen Sie sicher, dass Clientsysteme mit allen Adressen in diesem Dialogfeld eine Verbindung mit diesem Host herstellen können.  
  
Clientsysteme müssen mit allen Adressen im Dialogfeld „Sicherheitsserver-Einstellungen bearbeiten“ eine Verbindung mit diesem Sicherheitsserverhost herstellen können. Clientsysteme müssen mit allen Adressen im Dialogfeld „View-Verbindungsserver-Einstellungen bearbeiten“ eine Verbindung mit dieser View-Verbindungsserver-Instanz herstellen können.
  - f Klicken Sie auf **OK**.  
  
Wiederholen Sie diese Schritte für jede Sicherheitsserver- und View-Verbindungsserver-Instanz, über die Benutzer eine Verbindung mit dem PCoIP Secure Gateway herstellen.
- ◆ Wenn der Benutzer eine Verbindung über einen Webproxy herstellt, der sich außerhalb Ihres Netzwerks befindet und den erforderlichen Port blockiert, weisen Sie den Benutzer an, sich über einen anderen Netzwerkstandort zu verbinden.

## Connection Problems Between Machines and View-Verbindungsserver Instances

Bei der Verbindung zwischen Computern und View-Verbindungsserver-Instanzen können Probleme auftreten.

## Problem

Wenn für die Konnektivität zwischen einem Computer und einer View-Verbindungsserver-Instanz ein Fehler auftritt, wird in der Ereignisdatenbank eine der folgenden Meldungen angezeigt.

- Provisioning error occurred for Machine *Name\_der\_Maschine*: Customization error due to no network communication between the View agent and Connection Server (Bereitstellungsfehler für Maschine *Name\_der\_Maschine*: Anpassungsfehler, da keine Netzwerkkommunikation zwischen der View Agent- und Connection Server-Instanz möglich ist)
- Provisioning error occurred on Pool Desktop-ID because of a networking problem with a View Agent (Bereitstellungsfehler für Pool *Desktop-ID* aufgrund eines Netzwerkproblems mit einer View Agent-Instanz)
- Unable to launch from Pool *Desktop-ID* for user *Anzeigename\_des\_Benutzers*: Failed to connect to Machine *Name\_der\_Maschine* using Protokoll (Starten aus Pool *Desktop-ID* für Benutzer *Anzeigename\_des\_Benutzers* nicht möglich: Verbindung zu Maschine *Name\_der\_Maschine* konnte unter Verwendung von *Protokoll* nicht hergestellt werden)

## Ursache

Bei der Konnektivität zwischen einem Computer und einer View-Verbindungsserver-Instanz können aus verschiedenen Gründen Probleme auftreten.

- Lookup-Fehler auf dem Computer für den DNS-Namen des View-Verbindungsserver-Hosts.
- Die Ports für die JMS-, RDP- oder AJP13-Kommunikation werden durch Firewall-Regeln blockiert.
- Ein Ausfall des JMS-Routers auf dem View-Verbindungsserver-Host.

## Lösung

- ◆ Geben Sie an einer Eingabeaufforderung auf dem Computer den Befehl `nslookup` ein.

```
nslookup CS_FQDN
```

*CS-FQDN* ist der vollqualifizierte Domänenname (FQDN) des View-Verbindungsserver-Hosts. Wenn der Befehl die IP-Adresse des View-Verbindungsserver-Hosts nicht zurückgibt, korrigieren Sie die DNS-Konfiguration mithilfe der allgemeinen Verfahren zur Behandlung von Netzwerkproblemen.

- ◆ Stellen Sie an einer Eingabeaufforderung auf dem Computer sicher, dass TCP-Port 4001 ordnungsgemäß funktioniert. Dieser Port wird von der View Agent-Instanz für die JMS-Kommunikation mit dem View-Verbindungsserver-Host verwendet. Geben Sie zu diesem Zweck den `telnet`-Befehl ein.

```
telnet CS_FQDN 4001
```

Wenn die `telnet`-Verbindung hergestellt wird, funktioniert die Netzwerkkonnektivität für JMS ordnungsgemäß.

- ◆ Wenn ein Sicherheitsserver in der DMZ bereitgestellt wird, stellen Sie sicher, dass in der inneren Firewall Ausnahmeregeln konfiguriert sind, um RDP-Konnektivität zwischen dem Sicherheitsserver und virtuellen Maschinen an TCP-Port 3389 zuzulassen.
- ◆ Wenn sichere Verbindungen umgangen werden, stellen Sie sicher, dass die Firewall-Regeln Folgendes zulassen: Clients können eine direkte RDP-Verbindung mit der virtuellen Maschine an TCP-Port 3389 oder eine direkte PCoIP-Verbindung mit der virtuellen Maschine an TCP-Port 4172 und UDP-Port 4172 herstellen.
- ◆ Stellen Sie sicher, dass in der inneren Firewall Ausnahmeregeln konfiguriert sind, um Verbindungen zwischen jeder Sicherheitsserver-Instanz und dem zugehörigen View-Verbindungsserver-Host an TCP-Port 4001 (JMS) und TCP-Port 8009 (AJP13) zuzulassen.

## Verbindungsprobleme aufgrund einer falschen Zuweisung von IP-Adressen zu geklonten Computern

Möglicherweise kann keine Verbindung zu geklonten Computern hergestellt werden, wenn diese über statische IP-Adressen verfügen.

### Problem

Horizon Client kann nicht verwendet werden, um eine Verbindung mit geklonten Computern herzustellen.

### Ursache

Geklonte Computer sind fälschlicherweise für die Verwendung einer statischen IP-Adresse konfiguriert. Diese Computer sollten die IP-Adressen jedoch über DHCP abrufen.

### Lösung

- 1 Stellen Sie sicher, dass die Vorlage für einen Desktop-Pool auf vCenter Server für die Verwendung von DHCP konfiguriert ist, um IP-Adressen für Computer zuzuweisen.
- 2 Klonen Sie in vSphere Web Client eine virtuelle Maschine manuell aus dem Desktop-Pool und stellen Sie sicher, dass die IP-Adresse ordnungsgemäß über DHCP abgerufen wird.

## Fehlerbehebung bei Problemen mit der USB-Umleitung

Bei der USB-Umleitung in Horizon Client können verschiedene Probleme auftreten.

### Problem

Bei der USB-Umleitung in Horizon Client werden lokale Geräte nicht auf dem Remote-Desktop verfügbar gemacht oder einige Geräte werden für die Umleitung in Horizon Client nicht als verfügbar angezeigt.

## Ursache

Im Folgenden sind mögliche Ursachen aufgeführt, aufgrund derer die USB-Umleitung nicht ordnungsgemäß oder wie erwartet ausgeführt werden kann.

- Das Gerät ist ein Verbund-USB-Gerät und eines der enthaltenen Geräte wird standardmäßig gesperrt. Beispielsweise wird ein Diktiergerät mit einer Maus standardmäßig gesperrt, da Mauszeigergeräte standardmäßig gesperrt werden. Informationen zum Umgehen dieses Problems finden Sie unter [Konfigurieren der Gerätesplittingrichtlinieneinstellungen für Composite USB-Geräte](#).
- Die USB-Umleitung wird für Windows 2008-Systeme oder für sitzungsbasierte Remote-Desktops mit RDS-Host nicht unterstützt.
- Die Umleitung wird für Webcams nicht unterstützt.
- Die Umleitung von USB-Audiogeräten ist vom Netzwerkstatus abhängig und daher nicht zuverlässig. Manche Geräte erfordern auch im Ruhezustand einen hohen Datendurchsatz.
- Die USB-Umleitung wird für Startgeräte nicht unterstützt. Wenn Sie Horizon Client auf einem Windows-System ausführen, das von einem USB-Gerät startet, und Sie dieses Gerät auf den Remote-Desktop umleiten, reagiert das lokale Betriebssystem möglicherweise nicht oder kann nicht verwendet werden. Siehe <http://kb.vmware.com/kb/1021409>.
- Standardmäßig ermöglicht Ihnen Horizon Client für Windows nicht, Taste, Maus, Smartcard und Audio-Ausgangsgeräte zur Umleitung auszuwählen. Siehe <http://kb.vmware.com/kb/1011600>.
- RDP bietet keine Unterstützung für die Umleitung von USB-Eingabegeräten für die Konsolensitzung oder für Smartcard-Leser. Siehe <http://kb.vmware.com/kb/1011600>.
- Windows Mobile-Gerätecenter kann die Umleitung von USB-Geräten für RDP-Sitzungen verhindern. Siehe <http://kb.vmware.com/kb/1019205>.
- Für einige USB-Eingabegeräte müssen Sie die virtuelle Maschine so konfigurieren, dass die Position des Mauszeigers aktualisiert wird. Siehe <http://kb.vmware.com/kb/1022076>.
- Einige Audiogeräte erfordern möglicherweise Änderungen an Richtlinieneinstellungen oder Registrierungseinstellungen. Siehe <http://kb.vmware.com/kb/1023868>.
- Netzwerklatenz kann zu einer langsamen Geräteinteraktion führen. Zudem ist es möglich, dass Anwendungen nicht zu reagieren scheinen, da sie für die Interaktion mit lokalen Geräten konzipiert sind. Bei USB-Festplattenlaufwerken mit sehr hoher Kapazität kann es einige Minuten dauern, bis diese im Windows Explorer angezeigt werden.
- USB-Flashkarten, die mit dem FAT32-Dateisystem formatiert sind, werden langsam geladen. Siehe <http://kb.vmware.com/kb/1022836>.
- Ein Prozess oder Dienst auf dem lokalen System hat das Gerät geöffnet, bevor Sie sich mit dem Remote-Desktop verbunden haben.
- Ein umgeleitetes USB-Gerät arbeitet nicht mehr, wenn Sie eine Desktop-Sitzung wiederherstellen – selbst wenn der Desktop anzeigt, dass das Gerät verfügbar ist.
- Die USB-Umleitung ist in View Administrator deaktiviert.

- Fehlende oder deaktivierte Treiber für die USB-Umleitung auf dem Gast.

### Lösung

- ◆ Verwenden Sie, wenn möglich, PCoIP anstelle von RDP als Desktop-Protokoll.
- ◆ Wenn ein umgeleitetes Gerät weiterhin nicht verfügbar ist oder nach einer vorübergehenden Verbindungstrennung nicht mehr arbeitet, entfernen Sie das Gerät, schließen Sie es wieder an, und führen Sie erneut eine Umleitung durch.
- ◆ Wechseln Sie in View Administrator zu **Richtlinien > Globale Richtlinien** und prüfen Sie, ob USB-Zugriff unter „View-Richtlinien“ auf **Zulassen** gesetzt ist.
- ◆ Überprüfen Sie das Protokoll auf dem Gast auf Einträge der Klasse `ws_vhub` und das Protokoll auf dem Client auf Einträge der Klasse `vmware-view-usbd`.

Einträge dieser Klassen werden in die Protokolle geschrieben, wenn es sich bei einem Benutzer nicht um einen Administrator handelt oder wenn die Treiber für die USB-Umleitung nicht installiert sind oder nicht ordnungsgemäß funktionieren. Informationen zum Speicherort dieser Protokolldateien finden Sie unter [Verwenden von Protokolldateien für die Fehlerbehebung und das Bestimmen von USB-Geräte-IDs](#).

- ◆ Öffnen Sie auf dem Gast den Geräte-Manager, erweitern Sie die USB-Controller und installieren Sie die Treiber VMware View Virtual USB Host Controller und VMware View Virtual USB Hub erneut, wenn diese Treiber nicht vorhanden sind, bzw. aktivieren Sie die Treiber, wenn diese deaktiviert sind.

## Fehlerbehebung von GINA-Problemen auf Windows XP-Computern

Auf Windows XP-Computern können bei der Verkettung von VMware View GINA-dll-Dateien (Graphical Identification and Authentication Dynamic Link Library) Probleme auftreten.

### Problem

Auf Windows XP-Computern können die folgenden Probleme auftreten:

- Der Computer startet nicht
- Beim Start oder Herunterfahren eines Computers wird der folgende Fehler angezeigt: Cannot start gina.dll module (GINA-dll-Modul kann nicht gestartet werden). A required component is missing (Es fehlt eine erforderliche Komponente): gina.dll. Please install the application again (gina.dll. Installieren Sie die Anwendung erneut).
- Beim Start eines Computers wird eine unerwartete Anmeldeaufforderung angezeigt
- Sie können sich nicht beim Computer anmelden

### Ursache

Probleme beim Start und bei der Anmeldung können auf Windows XP-Computern auftreten, wenn die View GINA-dll-Dateien nicht korrekt mit den Drittanbieter-GINAs verkettet werden, die sich eventuell auf den virtuellen Maschinen befinden.

Um sicherzustellen, dass die GINA korrekt verkettet wurde, müssen Sie die GINA WinLogon als View-GINA konfigurieren und dafür sorgen, dass vdmGinaChainDLL erstellt wurde und die Drittanbieter-GINAs enthält.

Wenn Sie keine Software installiert haben, die Verkettungen zu einer anderen GINA herstellt, ist msgina.dll als Standard eingestellt und befindet sich unter %systemroot%\system32\msgina.dll auf der virtuellen Maschine.

## Lösung

- 1 Melden Sie sich bei der übergeordneten virtuellen Maschine, der virtuellen Vorlagenmaschine oder beim View-Computer an.
- 2 Klicken Sie auf **Start > Ausführen**, geben Sie **Regedit** ein und drücken Sie auf die Eingabetaste.
- 3 Navigieren Sie zum folgenden Windows-Registrierungsschlüssel:  
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon\GinaDLL
- 4 Stellen Sie sicher, dass der Schlüssel GinaDLL den folgenden Wert aufweist:  
*Installationsverzeichnis\VMware\VMware View\Agent\bin\wsgina.dll*  
*Installationsverzeichnis* ist der Pfad, unter dem Sie View Agent installiert haben.
- 5 Ist der Zeichenfolgewert vdmGinaChainDLL nicht vorhanden, müssen Sie diesen erstellen.
  - a Navigieren Sie zum folgenden Registrierungsschlüssel:  
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\Current Version
  - b Erstellen Sie den Schlüssel vdmGinaChainDLL.
- 6 Legen Sie die dll-Namen der Drittanbieter-GINA im Schlüssel vdmGinaChainDLL ab.
- 7 Falls danach immer noch Probleme bei den Windows XP-Computern auftreten, sollten Sie sicherstellen, dass keine herstellerspezifischen GINA-Schlüssel in der Registrierung geladen werden.  
  
Beim Laden von Drittanbieter-GINA-Schlüsseln ruft die verkettende GINA eventuell immer noch die Standard-GINA msgina auf. Manche Netzwerkmanagement- und Sicherheitssoftware-Produkte legen ihre GINA-Ersatz-dlls in ihren eigenen Installationsverzeichnissen ab, zum Beispiel unter Registrierungspfaden wie diesem:  
  
HKEY\_LOKALE\_MASCHINE\Software\Anbieter-ID\_oder\_-Name\GINA-Schlüsselreferenz\GINA-\_Ladebefehle = msgina  
  
Entfernen Sie diese GINA-Schlüssel aus dem herstellerspezifischen Speicherort und legen Sie sie im Schlüssel vdmGinaChainDLL ab.

## Verwalten von Maschinen und Richtlinien für nicht berechtigte Benutzer

Sie können die Maschinen von Benutzern anzeigen, deren Berechtigungen entfernt wurden. Zudem können Sie die Richtlinien anzeigen, die auf nicht berechtigte Benutzer angewendet werden.

Ein Benutzer ohne Berechtigung hat möglicherweise die Organisation verlassen oder das Konto wurde für einen längeren Zeitraum gesperrt. Diese Benutzer verfügen über eine zugewiesene Maschine, sind jedoch nicht länger zur Verwendung des Maschinen-Pools berechtigt.

Sie können auch den Befehl `vdmadmin` mit der Option `-O` oder `-P` verwenden, um nicht berechtigte Maschinen und Richtlinien anzuzeigen. Weitere Informationen finden Sie im Dokument *Administration von View*.

#### Verfahren

- 1 Wählen Sie in View Administrator **Ressourcen > Maschinen** aus.
- 2 Wählen Sie **Weitere Befehle > Computer nicht berechtigter Benutzer anzeigen** aus.
- 3 Entfernen Sie die Maschinenzuweisungen für nicht berechtigte Benutzer.
- 4 Wählen Sie je nach Bedarf **Weitere Befehle > Computer nicht berechtigter Benutzer anzeigen** oder **Weitere Befehle > Nicht berechtigte Richtlinien anzeigen**.
- 5 Ändern oder entfernen Sie die Richtlinien, die auf nicht berechtigte Benutzer angewendet 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>