

# VMware View- Sicherheit

View 5.0

View Manager 5.0

View Composer 2.7

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter <http://www.vmware.com/de/support/pubs>.

DE-000575-00

**vmware**<sup>®</sup>

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

<http://www.vmware.com/de/support/pubs/>

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

Copyright © 2011 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch Urheberrechtsgesetze, internationale Verträge und mindestens eines der unter <http://www.vmware.com/go/patents-de> aufgeführten Patente geschützt.

VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

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

**VMware Global, Inc.**  
Zweigniederlassung Deutschland  
Freisinger Str. 3  
85716 Unterschleißheim/Lohhof  
Germany  
Tel.: +49 (0) 89 3706 17000  
Fax: +49 (0) 89 3706 17333  
[www.vmware.com/de](http://www.vmware.com/de)

# Inhalt

|                                               |    |
|-----------------------------------------------|----|
| VMware View-Sicherheit                        | 5  |
| VMware View-Sicherheitsreferenz               | 7  |
| VMware View-Konten                            | 8  |
| VMware View-Sicherheitseinstellungen          | 9  |
| VMware View-Ressourcen                        | 18 |
| VMware View-Protokolldateien                  | 19 |
| TCP- und UDP-Ports von VMware View            | 21 |
| Dienste auf einem View Connection Server-Host | 26 |
| Dienste auf einem Sicherheitsserver           | 27 |
| Dienste auf einem View Transfer Server-Host   | 27 |
| Index                                         | 29 |



# VMware View-Sicherheit

---

*VMware View-Sicherheit* stellt eine umfassende Referenz zu allen Sicherheitsfunktionen von VMware View™ dar.

- Erforderliche Anmeldekonto für das System und die Datenbank.
- Sicherheitsrelevante Konfigurationsoptionen und Einstellungen.
- Zu schützende Ressourcen, z. B. sicherheitsrelevante Konfigurationsdateien und Kennwörter, sowie die empfohlenen Zugriffskontrollen für sicheren Betrieb.
- Speicherort von Protokolldateien und deren Zweck.
- Externe Schnittstellen, Ports und Dienste die für den ordnungsgemäßen Betrieb von VMware View geöffnet oder aktiviert sein müssen.

## Zielgruppe

Diese Informationen richten sich an IT-Entscheider, -Architekten, -Administratoren und andere Benutzer, die sich mit den Sicherheitskomponenten von VMware View vertraut machen möchten. Dieses Referenzhandbuch sollte in Verbindung mit dem *VMware View Hardening Guide* und anderer VMware View-Dokumentation verwendet werden.



# VMware View-Sicherheitsreferenz

---

Wenn Sie eine sichere View-Umgebung konfigurieren, können Sie in vielen Bereichen Einstellungen ändern und Anpassungen vornehmen, um Ihre Systeme zu schützen.

- [VMware View-Konten](#) auf Seite 8  
Sie müssen System- und Datenbankkonten einrichten, um die Komponenten von VMware View zu verwalten.
- [VMware View-Sicherheitseinstellungen](#) auf Seite 9  
VMware View enthält verschiedene Einstellungen, die Sie verwenden können, um die Sicherheit der Konfiguration anzupassen. Sie können mit View Administrator auf diese Einstellungen zugreifen, indem Sie Gruppenprofile bearbeiten bzw. das Dienstprogramm „ADSI Edit“ verwenden.
- [VMware View-Ressourcen](#) auf Seite 18  
VMware View enthält verschiedene Konfigurationsdateien und ähnliche Ressourcen, die geschützt werden müssen.
- [VMware View-Protokolldateien](#) auf Seite 19  
Die VMware View-Software erstellt Protokolldateien, mit denen die Installation und der Betrieb der View-Komponenten aufgezeichnet werden.
- [TCP- und UDP-Ports von VMware View](#) auf Seite 21  
View verwendet TCP- und UDP-Ports für den Netzwerkzugriff zwischen seinen Komponenten. Möglicherweise müssen Sie eine Firewall neu konfigurieren, um den Zugriff auf die entsprechenden Ports zuzulassen.
- [Dienste auf einem View Connection Server-Host](#) auf Seite 26  
Der Betrieb von View Manager hängt von verschiedenen Diensten ab, die auf einem View Connection Server-Host ausgeführt werden. Wenn Sie den Betrieb dieser Dienste anpassen möchten, müssen Sie sich zunächst mit ihnen vertraut machen.
- [Dienste auf einem Sicherheitsserver](#) auf Seite 27  
Der Betrieb von View Manager hängt von verschiedenen Diensten ab, die auf einem Sicherheitsserver ausgeführt werden. Wenn Sie den Betrieb dieser Dienste anpassen möchten, müssen Sie sich zunächst mit ihnen vertraut machen.
- [Dienste auf einem View Transfer Server-Host](#) auf Seite 27  
Die Übertragungsvorgänge für lokale Desktops hängen von Diensten ab, die auf einem View Transfer Server-Host ausgeführt werden. Wenn Sie den Betrieb dieser Dienste anpassen möchten, müssen Sie sich zunächst mit ihnen vertraut machen.

## VMware View-Konten

Sie müssen System- und Datenbankkonten einrichten, um die Komponenten von VMware View zu verwalten.

**Tabelle 1.** VMware View-Systemkonten

| VMware View-Komponente                                              | Erforderliche Konten                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View Client                                                         | Konfigurieren Sie in Active Directory Benutzerkonten für die Benutzer, die Zugriff auf View-Desktops haben. Die Benutzerkonten müssen Mitglieder der Gruppe der Remote-Desktop-Benutzer sein, aber die Konten erfordern keine View Administrator-Berechtigungen.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| View Client with Local Mode                                         | Konfigurieren Sie in Active Directory Benutzerkonten für die Benutzer, die Zugriff auf View-Desktops im lokalen Modus haben. Die Benutzerkonten erfordern keine View Administrator-Berechtigungen.<br>Als standardmäßige Vorgehensweise für Desktops wird empfohlen, auf jedem View-Desktop, der im lokalen Modus verwendet werden soll, ein eindeutiges Passwort für das lokale Administratorkonto zu erstellen.                                                                                                                                                                                                                                                                                    |
| vCenter Server                                                      | Konfigurieren Sie in Active Directory ein Benutzerkonto, das über die Berechtigung verfügt, die Vorgänge in vCenter Server auszuführen, die erforderlich sind, um View Manager zu unterstützen.<br>Weitere Informationen über die erforderlichen Berechtigungen finden Sie im Dokument <i>Installation von VMware View</i> .                                                                                                                                                                                                                                                                                                                                                                         |
| View Composer                                                       | Erstellen Sie in Active Directory ein Benutzerkonto, das mit View Composer verwendet werden soll. Dieses Konto ist für View Composer erforderlich, um Linked-Clone-Desktops zur Active Directory-Domäne hinzuzufügen.<br>Das Benutzerkonto sollte kein View-Administratorkonto sein. Erteilen Sie diesem Konto die Mindestberechtigungen, die zum Erstellen und Entfernen von Computerobjekten in einem festgelegten Active Directory-Container erforderlich sind. Beispielsweise sind die Berechtigungen eines Domänenadministrators nicht für das Konto erforderlich.<br>Weitere Informationen über die erforderlichen Berechtigungen finden Sie im Dokument <i>Installation von VMware View</i> . |
| View Connection Server, Sicherheitsserver oder View Transfer Server | Anfänglich sind alle Benutzer, die Mitglieder der lokalen Administratorengruppe (BUILTIN\Administrators) auf dem View Connection Server-Computer sind, zur Anmeldung an View Administrator berechtigt.<br>In View Administrator können Sie <b>[View Configuration (View-Konfiguration)] &gt; [Administrators (Administratoren)]</b> verwenden, um die Liste der View-Administratoren zu ändern.<br>Weitere Informationen zu den erforderlichen Berechtigungen finden Sie im Dokument <i>Verwaltung von VMware View</i> .                                                                                                                                                                             |

**Tabelle 2.** VMware View-Datenbankkonten

| VMware View-Komponente                                  | Erforderliche Konten                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View Composer-Datenbank                                 | Eine SQL Server- oder Oracle-Datenbank speichert die View Composer-Daten. Sie können ein Administratorkonto für die Datenbank erstellen, die Sie dem View Composer-Benutzerkonto zuweisen können.<br>Informationen zum Einrichten einer View Composer-Datenbank finden Sie im Dokument <i>Installation von VMware View</i> .         |
| Von View Connection Server verwendete Ereignisdatenbank | Eine SQL Server- oder Oracle-Datenbank speichert die View-Ereignisdaten. Sie erstellen ein Administratorkonto für die Datenbank, das View Administrator zum Zugriff auf die Ereignisdaten verwenden kann.<br>Informationen zum Einrichten einer View Composer-Datenbank finden Sie im Dokument <i>Installation von VMware View</i> . |



Um das Risiko von Sicherheitsgefährdungen zu mindern, unternehmen Sie Folgendes:

- Konfigurieren Sie View-Datenbanken auf Servern, die von anderen von Ihrem Unternehmen verwendeten Datenbankservern getrennt sind.
- Gewähren Sie einem einzelnen Benutzerkonto nicht das Recht, auf mehrere Datenbanken zuzugreifen.
- Konfigurieren Sie separate Konten für den Zugriff auf die View Composer- und Ereignisdatenbanken.

## VMware View-Sicherheitseinstellungen

VMware View enthält verschiedene Einstellungen, die Sie verwenden können, um die Sicherheit der Konfiguration anzupassen. Sie können mit View Administrator auf diese Einstellungen zugreifen, indem Sie Gruppenprofile bearbeiten bzw. das Dienstprogramm „ADSI Edit“ verwenden.

### Sicherheitsbezogene globale Einstellungen in View Administrator

Sicherheitsbezogene globale Einstellungen für Clientsitzungen und -verbindungen sind verfügbar unter **[View Configuration (View-Konfiguration)] > [Global Settings (Globale Einstellungen)]** in View Administrator.

**Tabelle 3.** Sicherheitsbezogene globale Einstellungen

| Einstellung                                                                                                                                        | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Disable Single Sign-On for Local Mode operations (SSO für Vorgänge im lokalen Modus deaktivieren)]                                                | Legt fest, ob die einmalige Anmeldung aktiviert ist, wenn Benutzer sich an ihren lokalen Desktops anmelden.<br>Diese Einstellung ist standardmäßig deaktiviert.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| [Enable automatic status updates (Automatische Status-Updates aktivieren)]                                                                         | Bestimmt, ob View Manager regelmäßig den globalen Statusbereich und das Dashboard in View Administrator aktualisiert. Wenn Sie diese Einstellung aktivieren, wird für im Leerlauf befindliche Sitzungen aller Benutzer, die an View Administrator angemeldet sind, keine Zeitüberschreitung ausgelöst.<br>Diese Einstellung ist standardmäßig deaktiviert.                                                                                                                                                                                                                                                                                                                |
| [Message security mode (Sicherheitsmodus für Nachrichten)]                                                                                         | Legt fest, ob zwischen den View Manager-Komponenten übermittelte JMS-Nachrichten signiert und überprüft werden.<br>Wenn für diese Einstellung <b>[Disabled (Deaktiviert)]</b> festgelegt ist, ist der Sicherheitsmodus für Nachrichten deaktiviert.<br>Wenn für diese Einstellung <b>[Enabled (Aktiviert)]</b> festgelegt ist, lehnen View-Komponenten nicht signierte Nachrichten ab.<br>Wenn für diese Einstellung <b>[Mixed (Gemischt)]</b> festgelegt ist, ist der Sicherheitsmodus für Nachrichten aktiviert, wird aber für View-Komponenten, die älter als View Manager 3.0 sind, nicht erzwungen.<br>Die Standardeinstellung ist <b>[Disabled (Deaktiviert)]</b> . |
| [Reauthenticate Secure tunnel connections after network interruption (Sichere Tunnelverbindungen nach Netzwerkunterbrechung neu authentifizieren)] | Legt fest, ob die Benutzeranmeldeinformationen nach einer Netzwerkunterbrechung neu authentifiziert werden müssen, wenn View Client-Instanzen sichere Tunnelverbindungen zu View-Desktops verwenden.<br>Diese Einstellung ist standardmäßig aktiviert.                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Tabelle 3.** Sicherheitsbezogene globale Einstellungen (Fortsetzung)

| Einstellung                                                                                                                  | Beschreibung                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Require SSL for client connections and View Administrator (SSL für Clientverbindungen und View Administrator erforderlich)] | Legt fest, ob ein sicherer SSL-Kommunikationskanal zwischen View Connection Server und View-Desktop-Clients sowie zwischen View Connection Server und Clients mit Zugriff auf View Administrator verwendet wird.<br>Diese Einstellung ist standardmäßig aktiviert. |
| [Session timeout (Zeitüberschreitung der Sitzung)]                                                                           | Legt fest, wie lange ein Benutzer eine Sitzung geöffnet lassen kann, nachdem er sich an View Connection Server angemeldet hat.<br>Der Standardwert lautet 600 Minuten.                                                                                             |

Weitere Informationen zu diesen Einstellungen und deren Auswirkungen auf die Sicherheit finden Sie im Dokument *Verwaltung von VMware View*.

## Sicherheitsbezogene Servereinstellungen in View Administrator

Sicherheitsbezogene Servereinstellungen sind verfügbar unter **[View Configuration (View-Konfiguration)]** > **[Server]** in View Administrator.

**Tabelle 4.** Sicherheitsbezogene Servereinstellungen

| Einstellung                                                                                                                        | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Verbinden über SSL]                                                                                                               | Nach entsprechender Aktivierung kommuniziert View über SSL-Verschlüsselung mit einem vCenter Server.<br>Diese Einstellung ist standardmäßig aktiviert.                                                                                                                                                                                                                                                                                                                                      |
| [Use PCoIP Secure Gateway for PCoIP connections to desktop (PCoIP Secure Gateway für PCoIP-Verbindungen zu dem Desktop verwenden)] | Falls aktiviert, stellt View Client eine weitere sichere Verbindung zum View Connection Server- oder Sicherheitsserverhost her, wenn Benutzer sich über das PCoIP-Anzeigeprotokoll mit einem View-Desktop verbinden.<br>Wenn diese Einstellung deaktiviert ist, wird die Desktop-Sitzung direkt zwischen dem Clientsystem und der View-Desktop-VM unter Umgehung des View Connection Servers oder des Sicherheitsserverhosts aufgebaut.<br>Diese Einstellung ist standardmäßig deaktiviert. |
| [Use secure tunnel connection to desktop (Sichere Tunnelverbindung zum Desktop verwenden)]                                         | Wenn Benutzer eine Verbindung zu einem View-Desktop herstellen und diese Einstellung aktiviert ist, baut View Client eine weitere HTTPS-Verbindung zu dem View Connection Server oder Sicherheitsserverhost auf.<br>Wenn diese Einstellung deaktiviert ist, wird die Desktop-Sitzung direkt zwischen dem Clientsystem und der View-Desktop-VM unter Umgehung des View Connection Servers oder des Sicherheitsserverhosts aufgebaut.<br>Diese Einstellung ist standardmäßig aktiviert.       |
| [Use secure tunnel connection for Local Mode operations (Sichere Tunnelverbindung für Vorgänge im lokalen Modus verwenden)]        | Wenn diese aktiviert ist, verwenden lokale Desktops Tunnelverbindungen. Netzwerkdatenverkehr wird durch View Connection Server oder einen Sicherheitsserver (sofern konfiguriert) geleitet.<br>Wenn diese Einstellung deaktiviert ist, werden Übertragungsvorgänge direkt zwischen lokalen Desktops und den zugehörigen Remote-Desktops im Rechenzentrum ausgeführt.<br>Diese Einstellung ist standardmäßig deaktiviert.                                                                    |

**Tabelle 4.** Sicherheitsbezogene Servereinstellungen (Fortsetzung)

| Einstellung                                                                                                             | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Use SSL for Local Mode operations (SSL für Vorgänge im lokalen Modus verwenden)]                                       | Wenn diese Einstellung aktiviert ist, wird für die Kommunikation und Datenübertragungen zwischen Clientcomputern und dem Rechenzentrum die SSL-Verschlüsselung verwendet. Zu diesen Vorgängen zählen das Ein- und Auschecken von Desktops sowie das Replizieren von Daten von Clientcomputern in das Rechenzentrum, nicht jedoch die Übertragung von View Composer-Basis-Images.<br>Diese Einstellung ist standardmäßig deaktiviert. |
| [Use SSL when provisioning desktops in Local Mode (SSL bei der Bereitstellung von Desktops im lokalen Modus verwenden)] | Wenn diese Einstellung aktiviert ist, wird bei Übertragungen der View Composer-Basis-Image-Dateien aus dem Transfer Server-Repository auf Clientcomputer die SSL-Verschlüsselung verwendet.<br>Diese Einstellung ist standardmäßig deaktiviert.                                                                                                                                                                                      |

Weitere Informationen zu diesen Einstellungen und deren Auswirkungen auf die Sicherheit finden Sie im Dokument *Verwaltung von VMware View*.

## Sicherheitsbezogene Einstellungen in der View Agent-Konfigurationsvorlage

Sicherheitsbezogene Einstellungen werden in der ADM-Vorlagendatei für View Agent (`vdm_agent.adm`) bereitgestellt. Falls nicht anders angegeben, enthalten die Einstellungen nur eine Einstellung „Computer Configuration (Computerkonfiguration)“.

Sicherheitseinstellungen werden in der Registrierung auf dem Gastcomputer unter `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\Configuration` gespeichert.

**Tabelle 5.** Sicherheitsbezogene Einstellungen in der View Agent-Konfigurationsvorlage

| Einstellung                                                           | Registry Value Name (Registrierungswertname)                          | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AllowDirectRDP                                                        | AllowDirectRDP                                                        | Legt fest, ob Nicht-View Clients über RDP eine direkte Verbindung mit View-Desktops herstellen können. Ist diese Einstellung deaktiviert, lässt View Agent nur View-verwaltete Verbindungen über View Client zu.<br><b>WICHTIG</b> Damit View ordnungsgemäß funktioniert, muss der Windows Terminal Services-Dienst auf dem Gastbetriebssystem jedes Desktops ausgeführt werden. Sie können diese Einstellung verwenden, um Benutzer davon abzuhalten, direkte RDP-Verbindungen zu ihren Desktops herzustellen.<br>Diese Einstellung ist standardmäßig aktiviert. |
| AllowSingleSignon (Einmalige Anmeldung (Single Sign-On) zulassen)     | AllowSingleSignon (Einmalige Anmeldung (Single Sign-On) zulassen)     | 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 View Client herstellen. Ist diese Einstellung deaktiviert, müssen sich die Benutzer beim Herstellen einer Remote-Verbindung erneut authentifizieren.<br>Diese Einstellung ist standardmäßig aktiviert.                                                                                       |
| CommandsToRunOnConnect (Befehle, die beim Verbinden auszuführen sind) | CommandsToRunOnConnect (Befehle, die beim Verbinden auszuführen sind) | Gibt eine Liste mit Befehlen oder Befehlskripten an, die bei der ersten Verbindungsherstellung ausgeführt werden. Standardmäßig ist keine Liste angegeben.                                                                                                                                                                                                                                                                                                                                                                                                        |

**Tabelle 5.** Sicherheitsbezogene Einstellungen in der View Agent-Konfigurationsvorlage (Fortsetzung)

| Einstellung                                                             | Registry Value Name (Registrierungswertname)                            | Beschreibung                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CommandsToRunOnReconnect (Befehle, die beim Verbinden auszuführen sind) | CommandsToRunOnReconnect (Befehle, die beim Verbinden auszuführen sind) | Gibt eine Liste mit Befehlen oder Befehlskripten an, die ausgeführt werden, wenn eine Sitzung nach einer Verbindungstrennung wiederhergestellt wird.<br>Standardmäßig ist keine Liste angegeben.                                                                           |
| ConnectionTicketTimeout (Verbindungsticket abgelaufen)                  | VdmConnectionTicketTimeout                                              | Gibt die Gültigkeitsdauer des View-Verbindungstickets in Sekunden an.<br>Wenn diese Einstellung nicht konfiguriert ist, beträgt die standardmäßige Dauer bis zur Zeitüberschreitung 120 Sekunden.                                                                          |
| CredentialFilterExceptions (CredentialFilter-Ausnahmen)                 | CredentialFilterExceptions (CredentialFilter-Ausnahmen)                 | 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.<br>Standardmäßig ist keine Liste angegeben. |

Weitere Informationen zu diesen Einstellungen und deren Auswirkungen auf die Sicherheit finden Sie im Dokument *Verwaltung von VMware View*.

## Sicherheitseinstellungen in der View Client-Konfigurationsvorlage

Sicherheitsbezogene Einstellungen werden in der ADM-Vorlagendatei für View Client (`vdm_client.adm`) bereitgestellt. Falls nicht anders angegeben, enthalten die Einstellungen nur eine Einstellung „Computer Configuration (Computerkonfiguration)“. Wenn eine Benutzerkonfigurationseinstellung verfügbar ist und Sie einen Wert dafür definieren, setzt diese die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Sicherheitseinstellungen werden in der Registrierung auf dem Hostcomputer unter `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\Configuration` gespeichert.

**Tabelle 6.** Sicherheitseinstellungen in der View Client-Konfigurationsvorlage

| Einstellung                                                                                  | Registry Value Name (Registrierungswertname) | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allow command line credentials (Benutzeranmeldeinformationen von der Befehlszeile ausführen) | AllowCmdLineCredentials                      | Legt fest, ob Benutzeranmeldeinformationen mit View Client-Befehlszeilenoptionen bereitgestellt werden können. Wenn diese Einstellung aktiviert ist, stehen die Optionen <code>smartCardPIN</code> und <code>password</code> nicht zur Verfügung, wenn Benutzer View Client von der Befehlszeile ausführen.<br>Diese Einstellung ist standardmäßig aktiviert.                                                                                                                                                                                                                                                                                                                               |
| Brokers Trusted For Delegation                                                               | BrokersTrustedForDelegation                  | Gibt die View Connection Server-Instanzen an, welche die Benutzeridentitäts- und Anmeldeinformationen akzeptieren, die bei Aktivierung des Kontrollkästchens <b>[Log in as current user (Anmelden als aktueller Benutzer)]</b> übergeben werden. Wenn Sie keine View Connection Server-Instanzen angeben, akzeptieren alle View Connection Server-Instanzen diese Informationen.<br>Verwenden Sie zum Hinzufügen einer View Connection Server-Instanz eines der folgenden Formate: <ul style="list-style-type: none"> <li>■ <code>domain\system\$</code></li> <li>■ <code>system\$@domain.com</code></li> <li>■ Service Principal Name (SPN) des View Connection Server-Dienstes</li> </ul> |

**Tabelle 6.** Sicherheitseinstellungen in der View Client-Konfigurationsvorlage (Fortsetzung)

| Einstellung                                                    | Registry Value Name<br>(Registrierungswert-<br>name) | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate verification mode<br>(Zertifikatüberprüfungsmodus) | CertCheckMode                                        | <p>Konfiguriert die Ebene der Zertifikatüberprüfung, die durch View Client durchgeführt wird. Es stehen folgende Modi zur Auswahl:</p> <ul style="list-style-type: none"> <li>■ <b>No Security (Keine Sicherheit).</b> View führt keine Überprüfung durch.</li> <li>■ <b>Warn But Allow (Warnen, aber zulassen).</b> Wenn die folgenden Serverzertifikatprobleme auftreten, wird eine Warnung angezeigt, aber der Benutzer kann mit der Verbindungsherstellung mit View Connection Server fortfahren: <ul style="list-style-type: none"> <li>■ Von View wird ein selbstsigniertes Zertifikat bereitgestellt. In diesem Fall ist es akzeptabel, wenn der Zertifikatname nicht mit dem Namen des View Connection Servers übereinstimmt, der in View Client vom Benutzer angegeben wurde.</li> <li>■ Ein überprüfbares Zertifikat, das in Ihrer Bereitstellung konfiguriert wurde, ist abgelaufen oder noch nicht gültig.</li> </ul> </li> </ul> |

**Tabelle 6.** Sicherheitseinstellungen in der View Client-Konfigurationsvorlage (Fortsetzung)

| Einstellung | Registry Value Name<br>(Registrierungswert-<br>name) | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             |                                                      | <p>Wenn andere Zertifikatfehlerbedingungen vorliegen, zeigt View ein Fehlerdialogfeld an und verhindert, dass der Benutzer eine Verbindung mit View Connection Server herstellt.</p> <p>Warn But Allow (Warnen, aber zulassen) ist der Standardwert.</p> <ul style="list-style-type: none"> <li>■ Full Security (Volle Sicherheit). Wenn ein beliebiger Zertifikatfehler auftritt, kann der Benutzer keine Verbindung mit View Connection Server herstellen. View zeigt dem Benutzer die Zertifikatfehler an.</li> </ul> <p>Damit View Client das Zertifikat überhaupt überprüft, müssen Sie die globale Einstellung <b>[Require SSL for client connections and View Administrator (SSL für Clientverbindungen und View Administrator erforderlich)]</b> in View Administrator auswählen.</p> <p>Wenn diese Gruppenrichtlinieneinstellung konfiguriert ist, können die Benutzer den ausgewählten Modus für die Zertifikatüberprüfung in View Client sehen, ihn aber nicht konfigurieren. Das Dialogfeld für die SSL-Konfiguration informiert die Benutzer darüber, dass der Administrator die Einstellung gesperrt hat.</p> <p>Wenn diese Einstellung nicht konfiguriert oder deaktiviert wurde, können View Client-Benutzer SSL konfigurieren und einen Modus für die Zertifikatüberprüfung auswählen.</p> <p>Wenn Sie diese Einstellung bei Windows-Clients nicht als Gruppenrichtlinie konfigurieren möchten, können Sie die Zertifikatüberprüfung auch durch Hinzufügen des Wertnamens CertCheckMode zum folgenden Registrierungsschlüssel auf dem Clientcomputer aktivieren:</p> <p>HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security</p> <p>Verwenden Sie die folgenden Werte im Registrierungsschlüssel:</p> <ul style="list-style-type: none"> <li>■ 0 implementiert No Security (Keine Sicherheit).</li> <li>■ 1 implementiert Warn But Allow (Warnen, aber zulassen).</li> <li>■ 2 implementiert Full Security (Volle Sicherheit).</li> </ul> <p>Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung CertCheckMode im Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor der Registrierungsschlüsseleinstellung.</p> |

**Tabelle 6.** Sicherheitseinstellungen in der View Client-Konfigurationsvorlage (Fortsetzung)

| Einstellung                                                                                                                   | Registry Value Name<br>(Registrierungswert-<br>name) | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default value of the 'Log in as current user' checkbox (Standardwert des Kontrollkästchens 'Anmelden als aktueller Benutzer') | LogInAsCurrentUse                                    | <p>Gibt den Standardwert des Kontrollkästchens <b>[Log in as current user (Anmelden als aktueller Benutzer)]</b> im Dialogfeld für die View Client-Verbindung an.</p> <p>Diese Einstellung setzt den Standardwert außer Kraft, der während der View Client-Installation angegeben wurde.</p> <p>Wenn ein Benutzer View Client von der Befehlszeile ausführt und die Option <code>LogInAsCurrentUser</code> angibt, überschreibt der eingegebene Wert diese Einstellung.</p> <p>Wenn das Kontrollkästchen <b>[Log in as current user (Anmelden als aktueller Benutzer)]</b> aktiviert ist, werden die Identität und die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem verwendet, an die View Connection Server-Instanz und schließlich an den View-Desktop übergeben. Ist das Kontrollkästchen deaktiviert, müssen Benutzer Identitäts- und Anmeldeinformationen mehrere Male eingeben, bevor Sie auf einen View-Desktop zugreifen können.</p> <p>Zusätzlich zur Computerkonfigurationseinstellung ist eine Benutzerkonfigurationseinstellung verfügbar.</p> <p>Diese Einstellungen sind standardmäßig deaktiviert.</p> |
| Display option to Log in as current user (Option zum Anmelden als aktueller Benutzer anzeigen)                                | LogInAsCurrentUser_Display                           | <p>Legt fest, ob das Kontrollkästchen <b>[Log in as current user (Anmelden als aktueller Benutzer)]</b> im Dialogfeld für die View Client-Verbindung angezeigt wird.</p> <p>Bei Anzeige des Kontrollkästchens können Benutzer die Option aktivieren oder deaktivieren oder den zugehörigen Standardwert außer Kraft setzen. Wird das Kontrollkästchen ausgeblendet, können Benutzer den Standardwert im Dialogfeld für die View Client-Verbindung nicht ändern.</p> <p>Sie können den Standardwert für <b>[Log in as current user (Anmelden als aktueller Benutzer)]</b> über die Richtlinieneinstellung <code>Default value of the 'Log in as current user' checkbox</code> (Standardwert des Kontrollkästchens 'Anmelden als aktueller Benutzer') festlegen.</p> <p>Zusätzlich zur Computerkonfigurationseinstellung ist eine Benutzerkonfigurationseinstellung verfügbar.</p> <p>Diese Einstellungen sind standardmäßig aktiviert.</p>                                                                                                                                                                                                             |
| Enable jump list integration (Integration der Sprungliste aktivieren)                                                         | EnableJumplist                                       | <p>Legt fest, ob eine Sprungliste im View Client-Symbol in der Taskleiste von Windows 7 oder höheren Systemen angezeigt werden soll. Über die Sprungliste können sich Benutzer mit zuletzt verwendeten View Connection Server-Instanzen und View-Desktops verbinden.</p> <p>Wenn View Client gemeinsam verwendet wird, können Benutzern die Namen zuletzt verwendeter Desktops angezeigt werden. Die Sprungliste können Sie deaktivieren, indem Sie diese Einstellung deaktivieren.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Enable Single Sign-On for smart card authentication (Aktivieren von Single Sign-On für die Smartcard-Authentifizierung)       | EnableSmartCardSSO                                   | <p>Legt fest, ob für die Smartcard-Authentifizierung das Single Sign-On (SSO) aktiviert ist. Ist SSO aktiviert, speichert View Client die verschlüsselte Smartcard-PIN im temporären Arbeitsspeicher, bevor sie an View Connection Server gesendet wird. Ist SSO deaktiviert, zeigt View Client kein benutzerdefiniertes PIN-Dialogfeld an.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Tabelle 6.** Sicherheitseinstellungen in der View Client-Konfigurationsvorlage (Fortsetzung)

| <b>Einstellung</b>                                                                                                                                  | <b>Registry Value Name<br/>(Registrierungswert-<br/>name)</b> | <b>Beschreibung</b>                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ignore bad SSL certificate date received from the server (Vom Server erhaltenes SSL Zertifikat mit ungültigen Datumswerten ignorieren)              | IgnoreCertDateInvalid                                         | Legt fest, ob Fehler in Zusammenhang mit ungültigen Datumswerten für das Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn ein Server ein abgelaufenes Zertifikat sendet.<br><br>Diese Einstellung ist standardmäßig aktiviert.<br>Diese Einstellung gilt nur für View 4.6 und frühere Releases.                                                                                                                    |
| Ignore certificate revocation problems (Fehler in Zusammenhang mit einem gesperrten Serverzertifikat ignorieren)                                    | IgnoreRevocation                                              | Legt fest, ob Fehler in Zusammenhang mit einem gesperrten Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn der Server ein Zertifikat sendet, das gesperrt wurde, und der Client den Sperrstatus eines Zertifikats nicht überprüfen kann.<br><br>Diese Einstellung ist standardmäßig deaktiviert.<br>Diese Einstellung gilt nur für View 4.6 und frühere Releases.                                                  |
| Ignore incorrect SSL certificate common name (host name field) (Fehler in Zusammenhang mit falschen allgemeinen Namen im SSL-Zertifikat ignorieren) | IgnoreCertCnInvalid                                           | Legt fest, ob Fehler in Zusammenhang mit falschen allgemeinen Namen im Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn der allgemeine Name des Zertifikats nicht mit dem Hostnamen des Servers übereinstimmt, der das Zertifikat sendet.<br><br>Diese Einstellung ist standardmäßig deaktiviert.<br>Diese Einstellung gilt nur für View 4.6 und frühere Releases.                                                 |
| Ignore incorrect usage problems (Fehler in Zusammenhang mit einer falschen Verwendung ignorieren)                                                   | IgnoreWrongUsage                                              | Legt fest, ob Fehler in Zusammenhang mit einer falschen Verwendung des Serverzertifikats ignoriert werden. Diese Fehler treten auf, wenn das vom Server gesendete Zertifikat für einen anderen Zweck als die Überprüfung der Absenderidentität und zum Verschlüsseln der Serverkommunikation gedacht ist.<br><br>Diese Einstellung ist standardmäßig deaktiviert.<br>Diese Einstellung gilt nur für View 4.6 und frühere Releases. |
| Ignore unknown certificate authority problems (Fehler in Zusammenhang mit einer unbekanntenen Zertifizierungsstelle ignorieren)                     | IgnoreUnknownCa                                               | Legt fest, ob bestimmte Fehler in Zusammenhang mit einer unbekanntenen Zertifizierungsstelle im Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn das vom Server gesendete Zertifikat durch eine nicht vertrauenswürdige Drittanbieter-Zertifizierungsstelle signiert wurde.<br><br>Diese Einstellung ist standardmäßig deaktiviert.<br>Diese Einstellung gilt nur für View 4.6 und frühere Releases.               |

Weitere Informationen zu diesen Einstellungen und deren Auswirkungen auf die Sicherheit finden Sie im Dokument *Verwaltung von VMware View*.

## Sicherheitsbezogene Einstellungen im Abschnitt „Scripting Definitions (Skriptdefinitionen)“ der View Client-Konfigurationsvorlage

Sicherheitsbezogene Einstellungen werden im Abschnitt „Scripting Definitions (Skriptdefinitionen)“ der ADM-Vorlagendatei für View Client (`vdm_client.adm`) bereitgestellt. Falls nicht anders angegeben, enthalten die Einstellungen 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.



Einstellungen für Skriptdefinitionen werden in der Registrierung auf dem Hostcomputer unter HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client gespeichert.

**Tabelle 7.** Sicherheitsbezogene Einstellungen im Abschnitt „Scripting Definitions (Skriptdefinitionen)“

| Einstellung                                                                                                                                  | Registry Value Name<br>(Registrierungswert-<br>name) | Beschreibung                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connect all USB devices to the desktop on launch (Alle USB-Geräte mit dem Desktop verbinden, wenn dieser gestartet wird)                     | connectUSBOnStart-up                                 | Legt fest, ob alle der verfügbaren USB-Geräte auf dem Clientsystem mit dem Desktop verbunden werden, wenn dieser gestartet wird.<br>Diese Einstellung ist standardmäßig deaktiviert.               |
| Connect all USB devices to the desktop when they are plugged in (Alle USB-Geräte mit dem Desktop verbinden, wenn diese angeschlossen werden) | connectUSBOnInsert                                   | Legt fest, ob USB-Geräte mit dem Desktop verbunden werden, wenn die Geräte an das Clientsystem angeschlossen werden.<br>Diese Einstellung ist standardmäßig deaktiviert.                           |
| Logon Password (Passwort für Anmeldung)                                                                                                      | Password                                             | Legt das von View Client während der Anmeldung verwendete Kennwort fest. Das Kennwort wird von Active Directory im Textformat gespeichert.<br>Diese Einstellung ist standardmäßig nicht definiert. |

Weitere Informationen zu diesen Einstellungen und deren Auswirkungen auf die Sicherheit finden Sie im Dokument *Verwaltung von VMware View*.

## Sicherheitsbezogene Einstellungen in View LDAP

Sicherheitsbezogene Einstellungen werden in View LDAP im Objektpfad `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` bereitgestellt. Sie können das Dienstprogramm „ADSI Edit“ zum Ändern des Wertes dieser Einstellungen auf einer View Connection Server-Instanz verwenden. Die Änderung wird automatisch auf alle anderen View Connection Server-Instanzen in einer Gruppe übernommen.

**Tabelle 8.** Sicherheitsbezogene Einstellungen in View LDAP

| Name/Wert-Paar                     | Attribut                      | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [cs-allowunencryptedstart-session] | pae-NameValuePair             | <p>Ermöglicht die Verwendung von statischem Schlüsselschutz für SSO bei Desktops, die sich nicht in einer vertrauenswürdigen Domäne befinden, bei der SSPI-Datenaustausch (Security Support Provider Interface) unterstützt wird. Vom statischen Schlüsselschutz ist bekannt, dass er im Vergleich zu SSPI relativ unsicher ist.</p> <p>Wenn diese Einstellung auf <b>[0]</b> gesetzt wird, ist der statische Schlüsselschutz nicht zulässig. Diese Einstellung ist geeignet, wenn sich alle Desktops in vertrauenswürdigen Domänen befinden. Wenn beim SSPI-Datenaustausch Fehler auftreten, wird die Sitzung nicht gestartet.</p> <p>Wenn diese Einstellung auf <b>[1]</b> gesetzt wird, kann der statische Schlüsselschutz verwendet werden, wenn es beim SSPI-Datenaustausch zu Fehlern kommt. Diese Einstellung ist geeignet, wenn sich einige Desktops nicht in vertrauenswürdigen Domänen befinden.</p> <p>Die Standardeinstellung ist <b>[1]</b>.</p> |
|                                    | pae-OVDIKeyCipher             | <p>Gibt die Verschlüsselungsmethode an, die von View Connection Server zum Verschlüsseln der virtuellen Festplattendatei (.vmdk) verwendet wird, wenn Benutzer einen lokalen Desktop ein- und auschecken.</p> <p>Sie können den Wert für die Verschlüsselungsmethode auf <b>[AES-128]</b>, <b>[AES-192]</b> oder <b>[AES-256]</b> festlegen.</p> <p>Der Standardwert lautet <b>[AES-128]</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                    | pae-SSOCredentialCacheTimeout | <p>Das Zeitüberschreitungslimit für die einmalige Anmeldung (Single Sign-On, SSO) in Minuten, nachdem die SSO-Anmeldinformationen eines Benutzers ungültig werden.</p> <p>Der Standardwert lautet <b>[15]</b>.</p> <p>Ein Wert von <b>[-1]</b> bedeutet, dass kein SSO-Zeitüberschreitungslimit festgelegt ist.</p> <p>Mit dem Wert <b>[0]</b> wird die einmalige Anmeldung (SSO) deaktiviert.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## VMware View-Ressourcen

VMware View enthält verschiedene Konfigurationsdateien und ähnliche Ressourcen, die geschützt werden müssen.

**Tabelle 9.** View Connection Server- und Sicherheitsserver-Ressourcen

| Resource (Ressource)   | Standort                                                                                                                                                                                                                  | Schutz                                                                                  |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| LDAP-Einstellungen     | Nicht anwendbar.                                                                                                                                                                                                          | LDAP-Daten werden automatisch als Teil der rollenbasierten Zugriffskontrolle geschützt. |
| LDAP-Sicherungsdateien | <p>&lt;Laufwerksbuchstabe&gt;:\Programdata\VMWare\VDM\backups (Windows Server 2008)</p> <p>&lt;Laufwerksbuchstabe&gt;:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMWare\VDM\backups (Windows Server 2003)</p> | Geschützt durch die Zugriffskontrolle.                                                  |

**Tabelle 9.** View Connection Server- und Sicherheitsserver-Ressourcen (Fortsetzung)

| Resource (Ressource)                                | Standort                                                                                                                                         | Schutz                                                                                                                                                                            |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| locked.properties<br>(Zertifikateigenschaftendatei) | <i>Installationsverzeichnis</i> \VMware\VMware View\Server\sslgateway\conf                                                                       | Kann durch die Zugriffskontrolle geschützt werden. Stellen Sie sicher, dass die Datei vor dem Zugriff durch Benutzer geschützt ist, die nicht den View-Administratoren angehören. |
| Protokolldateien                                    | %ALLUSERSPROFILE%\Anwendungsdaten\VMware\VDM\logs<br><Laufwerksbuchstabe>:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs | Geschützt durch die Zugriffskontrolle.                                                                                                                                            |
| web.xml<br>(Tomcat-Konfigurationsdatei)             | <i>Installationsverzeichnis</i> \VMware View\Server\broker\web apps\ROOT\Web INF                                                                 | Geschützt durch die Zugriffskontrolle.                                                                                                                                            |

**Tabelle 10.** View Transfer Server-Ressourcen

| Resource (Ressource)                       | Standort                                                                                                                                                                                                                                                            | Schutz                                                                                                                                                                            |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| httpd.conf<br>(Apache-Konfigurationsdatei) | <i>Installationsverzeichnis</i> \VMware\VMware View\Server\httpd\conf                                                                                                                                                                                               | Kann durch die Zugriffskontrolle geschützt werden. Stellen Sie sicher, dass die Datei vor dem Zugriff durch Benutzer geschützt ist, die nicht den View-Administratoren angehören. |
| Protokolldateien                           | <Laufwerksbuchstabe>:\ProgramData\VMware\VDM\logs<br>(Windows Server 2008 R2)<br>%ALLUSERSPROFILE%\Anwendungsdaten\VMware\VDM\logs<br>(Windows Server 2003 und Windows Server 2003 R2)<br><Laufwerksbuchstabe>:\Programme\Apache Group\Apache2\logs (Apache-Server) | Geschützt durch die Zugriffskontrolle.                                                                                                                                            |

## VMware View-Protokolldateien

Die VMware View-Software erstellt Protokolldateien, mit denen die Installation und der Betrieb der View-Komponenten aufgezeichnet werden.

**HINWEIS** VMware View-Protokolldateien werden vom VMware-Support verwendet. VMware empfiehlt das Konfigurieren und Verwenden der Ereignisdatenbank zur Überwachung von View. Weitere Informationen hierzu finden Sie in den Dokumenten *Installation von VMware View* und *Integration von VMware View*.

**Tabelle 11.** VMware View-Protokolldateien

| <b>VMware View-Komponente</b>                    | <b>Dateipfad und andere Informationen</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alle Komponenten (Installationsprotokolldateien) | %TEMP%\vminst.log_Datum_Zeitstempel<br>%TEMP%\vmmsi.log_Datum_Zeitstempel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| View Agent                                       | Windows XP-Gastbetriebssystem:<br><Laufwerksbuchstabe>:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\Logs<br>Windows Vista- und Windows 7-Gastbetriebssystem:<br><Laufwerksbuchstabe>:\ProgramData\VMware\VDM\Logs<br>Wenn eine User Data Disk (UDD) konfiguriert ist, stimmt der <Laufwerksbuchstabe> möglicherweise mit der UDD überein.<br>Die Protokolle für PCoIP heißen pcoip_agent*.log und pcoip_server*.log.                                                                                                                             |
| View-Anwendungen                                 | View Event Database, konfiguriert auf einem SQL Server- oder Oracle-Datenbankserver.<br>Windows-Anwendungsereignisprotokolle. Standardmäßig deaktiviert.                                                                                                                                                                                                                                                                                                                                                                                                              |
| View Client mit lokalem Modus                    | Windows XP-Hostbetriebssystem:<br>C:\Dokumente und Einstellungen\%Benutzername%\Lokale Einstellungen\Anwendungsdaten\VMware\VDM\Logs\<br>Windows Vista- und Windows 7-Hostbetriebssystem:<br>C:\Benutzer\%Benutzername%\AppData\VMware\VDM\Logs\<br>                                                                                                                                                                                                                                                                                                                  |
| View Composer                                    | %Systemlaufwerk%\Windows\Temp\vmware-viewcomposer-ga-new.log auf dem verknüpften Klon-Desktop.<br>Das View Composer-Protokoll enthält Informationen über die Ausführung von QuickPrep- und Sysprep-Skripts. Das Protokoll zeichnet die Start- und Endzeit der Skriptausführung sowie alle Ausgabe- oder Fehlermeldungen auf.                                                                                                                                                                                                                                          |
| View Connection Server oder Sicherheitsserver    | %ALLUSERSPROFILE%\Anwendungsdaten\VMware\VDM\logs\*.txt auf dem Server.<br><Laufwerksbuchstabe>:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs\*.txt auf dem Server.<br>Das Protokollverzeichnis ist in den Protokollkonfigurationseinstellungen der ADM-Vorlagendatei für die allgemeine View-Konfiguration (vdm_common.adm) konfigurierbar.<br>PCoIP Secure Gateway-Protokolle werden in Dateien namens SecurityGateway_*.log im Unterverzeichnis PCoIP Secure Gateway des Protokollverzeichnisses auf einem Sicherheitsserver geschrieben. |
| View-Dienste                                     | View Event Database, konfiguriert auf einem SQL Server- oder Oracle-Datenbankserver.<br>Windows-Systemereignisprotokolle.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| View Transfer Server                             | Windows Server 2008 R2:<br><Laufwerksbuchstabe>:\ProgramData\VMware\VDM\logs\*.txt<br>Windows Server 2003 und Windows Server 2003 R2:<br>%ALLUSERSPROFILE%\Anwendungsdaten\VMware\VDM\logs\*.txt<br>Apache Server:<br><Laufwerksbuchstabe>:\Programme\Apache Group\Apache2\logs\error.log                                                                                                                                                                                                                                                                             |

## TCP- und UDP-Ports von VMware View

View verwendet TCP- und UDP-Ports für den Netzwerkzugriff zwischen seinen Komponenten. Möglicherweise müssen Sie eine Firewall neu konfigurieren, um den Zugriff auf die entsprechenden Ports zuzulassen.

**Tabelle 12.** Von View verwendete TCP- und UDP-Ports mit Ausnahme des lokalen Modus

| Quelle                     | Port                                                      | Ziel                         | Port                                                      | Protokoll | Beschreibung                                                                      |
|----------------------------|-----------------------------------------------------------|------------------------------|-----------------------------------------------------------|-----------|-----------------------------------------------------------------------------------|
| Sicherheitsserver          | 4172                                                      | View Agent 4.5 oder früher   | 50002 (kann durch eine Gruppenrichtlinie geändert werden) | UDP       | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway verwendet wird.                |
| Sicherheitsserver          | 4172                                                      | View Agent 4.6 oder höher    | 4172                                                      | UDP       | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway verwendet wird.                |
| Sicherheitsserver          | 4172                                                      | View Client 4.5 oder früher  | 50002 (kann nicht geändert werden)                        | UDP       | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway verwendet wird.                |
| Sicherheitsserver          | 4172                                                      | View Client 4.6 oder höher   | 4172                                                      | UDP       | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway verwendet wird.                |
| Sicherheitsserver          | *                                                         | View Connection Server       | 4001                                                      | TCP       | JMS-Datenverkehr.                                                                 |
| Sicherheitsserver          | *                                                         | View Connection Server       | 8009                                                      | TCP       | AJP13-weitergeleiteter Webdatenverkehr.                                           |
| Sicherheitsserver          | *                                                         | View-Desktop                 | 3389                                                      | TCP       | Microsoft RDP-Datenverkehr an View-Desktops.                                      |
| Sicherheitsserver          | *                                                         | View-Desktop                 | 9427                                                      | TCP       | Wyse MMR-Umleitung.                                                               |
| Sicherheitsserver          | *                                                         | View-Desktop                 | 32111                                                     | TCP       | USB-Umleitung.                                                                    |
| Sicherheitsserver          | *                                                         | View-Desktop 4.5 oder früher | 50002 (kann durch eine Gruppenrichtlinie geändert werden) | TCP       | PCoIP (HTTPS), wenn PCoIP Secure Gateway verwendet wird.                          |
| Sicherheitsserver          | *                                                         | View-Desktop 4.6 oder höher  | 4172                                                      | TCP       | PCoIP (HTTPS), wenn PCoIP Secure Gateway verwendet wird.                          |
| View Agent 4.5 oder früher | 50002 (kann durch eine Gruppenrichtlinie geändert werden) | View Client 4.5 oder früher  | 50002 (kann nicht geändert werden)                        | UDP       | PCoIP (AES-128-GCM oder SALSA20), wenn PCoIP Secure Gateway nicht verwendet wird. |
| View Agent 4.5 oder früher | 50002 (kann durch eine Gruppenrichtlinie geändert werden) | View Client 4.6 oder höher   | 4172                                                      | UDP       | PCoIP (AES-128-GCM oder SALSA20), wenn PCoIP Secure Gateway nicht verwendet wird. |
| View Agent 4.6 oder höher  | 4172                                                      | View Client 4.5 oder früher  | 50002 (kann nicht geändert werden)                        | UDP       | PCoIP (AES-128-GCM oder SALSA20), wenn PCoIP Secure Gateway nicht verwendet wird. |

**Tabelle 12.** Von View verwendete TCP- und UDP-Ports mit Ausnahme des lokalen Modus (Fortsetzung)

| Quelle                      | Port                                                      | Ziel                                          | Port                                                      | Proto-<br>koll | Beschreibung                                                                                                      |
|-----------------------------|-----------------------------------------------------------|-----------------------------------------------|-----------------------------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------|
| View Agent 4.6 oder höher   | 4172                                                      | View Client 4.6 oder höher                    | 4172                                                      | UDP            | PCoIP (AES-128-GCM oder SALSA20), wenn PCoIP Secure Gateway nicht verwendet wird.                                 |
| View Agent 4.5 oder früher  | 50002 (kann durch eine Gruppenrichtlinie geändert werden) | View Connection Server oder Sicherheitsserver | 4172                                                      | UDP            | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway verwendet wird.                                                |
| View Agent 4.6 oder höher   | 4172                                                      | View Connection Server oder Sicherheitsserver | 4172                                                      | UDP            | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway verwendet wird.                                                |
| View Client                 | *                                                         | View Connection Server oder Sicherheitsserver | 80                                                        | TCP            | HTTP-Zugriff, wenn SSL für Clientverbindungen deaktiviert ist.                                                    |
| View Client                 | *                                                         | View Connection Server oder Sicherheitsserver | 443                                                       | TCP            | HTTPS-Zugriff, wenn SSL für Clientverbindungen aktiviert ist.                                                     |
| View Client                 | *                                                         | View Connection Server oder Sicherheitsserver | 4172                                                      | TCP            | PCoIP (HTTPS), wenn PCoIP Secure Gateway verwendet wird.                                                          |
| View Client                 | *                                                         | View-Desktop                                  | 3389                                                      | TCP            | Microsoft RDP-Datenverkehr an View-Desktops, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden. |
| View Client                 | *                                                         | View-Desktop                                  | 9427                                                      | TCP            | Wyse MMR-Umleitung, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden.                          |
| View Client                 | *                                                         | View-Desktop                                  | 32111                                                     | TCP            | USB-Umleitung, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden.                               |
| View Client 4.5 oder früher | *                                                         | View Agent 4.5 oder früher                    | 50002 (kann durch eine Gruppenrichtlinie geändert werden) | TCP            | PCoIP (HTTPS), wenn PCoIP Secure Gateway nicht verwendet wird.                                                    |
| View Client 4.5 oder früher | 50002 (kann nicht geändert werden)                        | View Agent 4.5 oder früher                    | 50002 (kann durch eine Gruppenrichtlinie geändert werden) | UDP            | PCoIP (AES-28-GCM oder SALSA20), wenn PCoIP Secure Gateway nicht verwendet wird.                                  |
| View Client 4.5 oder früher | *                                                         | View Agent 4.6 oder höher                     | 4172                                                      | TCP            | PCoIP (HTTPS), wenn PCoIP Secure Gateway nicht verwendet wird.                                                    |
| View Client 4.5 oder früher | 50002 (kann nicht geändert werden)                        | View Agent 4.6 oder höher                     | 4172                                                      | UDP            | PCoIP (AES-28-GCM oder SALSA20), wenn PCoIP Secure Gateway nicht verwendet wird.                                  |

**Tabelle 12.** Von View verwendete TCP- und UDP-Ports mit Ausnahme des lokalen Modus (Fortsetzung)

| Quelle                      | Port                               | Ziel                                          | Port                                                      | Proto-<br>koll | Beschreibung                                                                                       |
|-----------------------------|------------------------------------|-----------------------------------------------|-----------------------------------------------------------|----------------|----------------------------------------------------------------------------------------------------|
| View Client 4.5 oder früher | 50002 (kann nicht geändert werden) | View Connection Server oder Sicherheitsserver | 4172                                                      | UDP            | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway verwendet wird.                                 |
| View Client 4.6 oder höher  | *                                  | View Agent 4.5 oder früher                    | 50002 (kann durch eine Gruppenrichtlinie geändert werden) | TCP            | PCoIP (HTTPS), wenn PCoIP Secure Gateway nicht verwendet wird.                                     |
| View Client 4.6 oder höher  | 4172                               | View Agent 4.5 oder früher                    | 50002 (kann durch eine Gruppenrichtlinie geändert werden) | UDP            | PCoIP (AES-28-GCM oder SALSA20), wenn PCoIP Secure Gateway nicht verwendet wird.                   |
| View Client 4.6 oder höher  | *                                  | View Agent 4.6 oder höher                     | 4172                                                      | TCP            | PCoIP (HTTPS), wenn PCoIP Secure Gateway nicht verwendet wird.                                     |
| View Client 4.6 oder höher  | 4172                               | View Agent 4.6 oder höher                     | 4172                                                      | UDP            | PCoIP (AES-28-GCM oder SALSA20), wenn PCoIP Secure Gateway nicht verwendet wird.                   |
| View Client 4.6 oder höher  | 4172                               | View Connection Server oder Sicherheitsserver | 4172                                                      | UDP            | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway verwendet wird.                                 |
| View Connection Server      | *                                  | vCenter Server oder View Composer             | 80                                                        | TCP            | SOAP-Nachrichten, wenn SSL für den Zugriff auf vCenter Server oder View Composer deaktiviert ist.  |
| View Connection Server      | *                                  | vCenter Server oder View Composer             | 443                                                       | TCP            | SOAP-Nachrichten, wenn SSL für den Zugriff auf vCenter Server oder View Composer aktiviert ist.    |
| View Connection Server      | 4172                               | View Agent 4.5 oder früher                    | 50002 (kann durch eine Gruppenrichtlinie geändert werden) | UDP            | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway über den View Connection Server verwendet wird. |
| View Connection Server      | 4172                               | View Agent 4.6 oder höher                     | 4172                                                      | UDP            | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway über den View Connection Server verwendet wird. |
| View Connection Server      | 4172                               | View Client 4.5 oder früher                   | 50002 (kann nicht geändert werden)                        | UDP            | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway über den View Connection Server verwendet wird. |
| View Connection Server      | 4172                               | View Client 4.6 oder höher                    | 4172                                                      | UDP            | PCoIP (nur AES-128-GCM), wenn PCoIP Secure Gateway über den View Connection Server verwendet wird. |

**Tabelle 12.** Von View verwendete TCP- und UDP-Ports mit Ausnahme des lokalen Modus (Fortsetzung)

| Quelle                 | Port | Ziel                             | Port  | Proto-<br>koll | Beschreibung                                                                                                                                                                                                          |
|------------------------|------|----------------------------------|-------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View Connection Server | *    | View Connection Server           | 4100  | TCP            | JMS-Datenverkehr zwischen Routern.                                                                                                                                                                                    |
| View Connection Server | *    | View-Desktop                     | 3389  | TCP            | Microsoft RDP-Datenverkehr an View-Desktops, wenn Tunnelverbindungen über den View Connection Server verwendet werden.                                                                                                |
| View Connection Server | *    | View-Desktop                     | 4172  | TCP            | PCoIP (HTTPS), wenn PCoIP Secure Gateway über den View Connection Server verwendet wird.                                                                                                                              |
| View Connection Server | *    | View-Desktop                     | 9427  | TCP            | Wyse MMR-Umleitung, wenn Tunnelverbindungen über den View Connection Server verwendet werden.                                                                                                                         |
| View Connection Server | *    | View-Desktop                     | 32111 | TCP            | USB-Umleitung, wenn Tunnelverbindungen über den View Connection Server verwendet werden.                                                                                                                              |
| View-Desktop           | *    | View Connection Server-Instanzen | 4001  | TCP            | JMS-Datenverkehr.                                                                                                                                                                                                     |
| View Composer-Dienst   | *    | ESXi-Host                        | 902   | TCP            | Wird verwendet, wenn View Composer Linked-Clone-Festplatten anpasst. Dazu gehören interne Festplatten von View Composer und, falls diese angegeben werden, persistente Festplatten und SDD (System-Disposable Disks). |

Die Funktion „Local Mode (Lokaler Modus)“ erfordert von Ihnen, eine zusätzliche Anzahl Ports zu öffnen, damit sie ordnungsgemäß ausgeführt werden kann.



**Tabelle 13.** Vom lokalen Modus verwendete TCP- und UDP-Ports

| Quelle                             | Port | Ziel                 | Port | Proto-<br>koll | Beschreibung                                                                                                                                                                                                    |
|------------------------------------|------|----------------------|------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sicherheitsserver                  | *    | View Transfer Server | 80   | TCP            | View-Desktop-Downlo-<br>ad und -Datenreplikati-<br>on, wenn Tunnelverbin-<br>dungen verwendet wer-<br>den und SSL für Vorgän-<br>ge des lokalen Modus<br>deaktiviert ist.                                       |
| Sicherheitsserver                  | *    | View Transfer Server | 443  | TCP            | View-Desktop-Downlo-<br>ad und -Datenreplikati-<br>on, wenn Tunnelverbin-<br>dungen verwendet wer-<br>den und SSL für Vorgän-<br>ge des lokalen Modus<br>aktiviert ist.                                         |
| View Client mit lo-<br>kalem Modus | *    | View Transfer Server | 80   | TCP            | View-Desktop-Downlo-<br>ad und -Datenreplikati-<br>on, wenn direkte Ver-<br>bindungen statt Tunnel-<br>verbindungen verwen-<br>det werden und SSL für<br>Vorgänge des lokalen<br>Modus deaktiviert ist.         |
| View Client mit lo-<br>kalem Modus | *    | View Transfer Server | 443  | TCP            | View-Desktop-Downlo-<br>ad und -Datenreplikati-<br>on, wenn direkte Ver-<br>bindungen statt Tunnel-<br>verbindungen verwen-<br>det werden und SSL für<br>Vorgänge des lokalen<br>Modus aktiviert ist.           |
| View Connection<br>Server          | *    | ESX-Host             | 902  | TCP            | Wird beim Auschecken<br>lokaler Desktops ver-<br>wendet.                                                                                                                                                        |
| View Connection<br>Server          | *    | View Transfer Server | 80   | TCP            | View-Desktop-Downlo-<br>ad und -Datenreplikati-<br>on, wenn Tunnelverbin-<br>dungen über den View<br>Connection Server ver-<br>wendet werden und SSL<br>für Vorgänge des loka-<br>len Modus deaktiviert<br>ist. |
| View Connection<br>Server          | *    | View Transfer Server | 443  | TCP            | View-Desktop-Downlo-<br>ad und -Datenreplikati-<br>on, wenn Tunnelverbin-<br>dungen über den View<br>Connection Server ver-<br>wendet werden und SSL<br>für Vorgänge des loka-<br>len Modus aktiviert ist.      |

**Tabelle 13.** Vom lokalen Modus verwendete TCP- und UDP-Ports (Fortsetzung)

| Quelle                 | Port | Ziel                 | Port | Proto-<br>koll | Beschreibung                                                      |
|------------------------|------|----------------------|------|----------------|-------------------------------------------------------------------|
| View Connection Server | *    | View Transfer Server | 4001 | TCP            | JMS-Datenverkehr zur Unterstützung des lokalen Modus.             |
| View Transfer Server   | *    | ESX-Host             | 902  | TCP            | Veröffentlichung von View Composer-Paketen für den lokalen Modus. |

## Dienste auf einem View Connection Server-Host

Der Betrieb von View Manager hängt von verschiedenen Diensten ab, die auf einem View Connection Server-Host ausgeführt werden. Wenn Sie den Betrieb dieser Dienste anpassen möchten, müssen Sie sich zunächst mit ihnen vertraut machen.

**Tabelle 14.** View Connection Server-Hostdienste

| Dienstname                                 | Starttyp                      | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VMware View Connection Server              | Automatisch                   | Stellt Verbindungs-Broker-Dienste bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework-, Nachrichtenbus-, Sicherheits-Gateway- und Webdienste gestartet oder beendet. Dieser Dienst führt keinen Start des VMware VDMS-Dienstes oder des VMware View-Skripthostdienstes durch bzw. beendet diese Dienste nicht. |
| VMware View-Framework-Komponente           | Manuell                       | Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework für View Manager bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden.                                                                                                                                                                                                                                        |
| VMware View-Nachrichtenbuskomponente       | Manuell                       | Stellt Dienste für die Nachrichtenübermittlung zwischen View Manager-Komponenten bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden.                                                                                                                                                                                                                                                  |
| VMware View, PCoIP Secure Gateway          | Manuell                       | Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu View Connection Server über ein PCoIP Secure Gateway herstellen.                                                                                                                                                                                                                                 |
| VMware View-Skripthost                     | Automatisch (falls aktiviert) | Bietet Unterstützung für Drittanbieterskripts, die beim Löschen von virtuellen Maschinen ausgeführt werden. Dieser Dienst ist standardmäßig deaktiviert. Sie sollten diesen Dienst aktivieren, wenn Sie Skripts ausführen möchten.                                                                                                                                                                                            |
| VMware View-Sicherheits-Gateway-Komponente | Manuell                       | Stellt sichere Tunneldienste für View Manager bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden.                                                                                                                                                                                                                                                                                     |
| VMware View-Webkomponente                  | Manuell                       | Stellt Webdienste für View Manager bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden.                                                                                                                                                                                                                                                                                                |
| VMwareVDMS                                 | Automatisch                   | Stellt LDAP-Verzeichnisdienste für View Manager bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden. Dieser Dienst muss auch bei Upgrades von VMware View ausgeführt werden, um die ordnungsgemäße Migration vorhandener Daten zu gewährleisten.                                                                                                                                       |

## Dienste auf einem Sicherheitsserver

Der Betrieb von View Manager hängt von verschiedenen Diensten ab, die auf einem Sicherheitsserver ausgeführt werden. Wenn Sie den Betrieb dieser Dienste anpassen möchten, müssen Sie sich zunächst mit ihnen vertraut machen.

**Tabelle 15.** Dienste auf einem Sicherheitsserver

| Dienstname                                 | Starttyp    | Beschreibung                                                                                                                                                                                                                                                        |
|--------------------------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VMware View Security Server                | Automatisch | Stellt Sicherheitsserverdienste bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion eines Sicherheitsservers ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework- und Sicherheits-Gateway-Dienste gestartet oder beendet. |
| VMware View-Framework-Komponente           | Manuell     | Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion eines Sicherheitsservers ausgeführt werden.                                                                                       |
| VMware View, PCoIP Secure Gateway          | Manuell     | Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu einem Sicherheitsserver über ein PCoIP Secure Gateway herstellen.                                                                      |
| VMware View-Sicherheits-Gateway-Komponente | Manuell     | Stellt sichere Tunneldienste bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion eines Sicherheitsservers ausgeführt werden.                                                                                                                                    |

## Dienste auf einem View Transfer Server-Host

Die Übertragungsvorgänge für lokale Desktops hängen von Diensten ab, die auf einem View Transfer Server-Host ausgeführt werden. Wenn Sie den Betrieb dieser Dienste anpassen möchten, müssen Sie sich zunächst mit ihnen vertraut machen.

Sämtliche der Dienste, die mit View Transfer Server installiert werden, müssen ausgeführt werden, um den ordnungsgemäßen Betrieb lokaler Desktops in View Manager zu gewährleisten.

**Tabelle 16.** View Transfer Server-Hostdienste

| Dienstname                                   | Starttyp    | Beschreibung                                                                                                                                                                                                                           |
|----------------------------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VMware View Transfer Server                  | Automatisch | Stellt Dienste zur Koordination der View Transfer Server-bezogenen Dienste bereit. Wenn Sie diesen Dienst starten oder beenden, werden auch der View Transfer Server-Steuerungsdienst und der Framework-Dienst gestartet oder beendet. |
| VMware View Transfer Server-Steuerungsdienst | Manuell     | Stellt Verwaltungsfunktionen für View Transfer Server bereit und sorgt für die Kommunikation mit View Connection Server.                                                                                                               |
| VMware View-Framework-Komponente             | Manuell     | Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework für View Manager bereit.                                                                                                                                     |
| Apache2.2-Dienst                             | Automatisch | Stellt Datenübertragungsfunktionen für Clientcomputer bereit, die View-Desktops im lokalen Modus ausführen.<br>Der Apache2.2-Dienst wird gestartet, wenn Sie View Transfer Server zu View Manager hinzufügen.                          |



# Index

## A

ADM-Vorlagendateien, sicherheitsbezogene Einstellungen **9**

## C

Connection Server-Dienst **26**

## D

Dienste

Sicherheitsserver, Hosts **27**

View Connection Server-Hosts **26**

View Transfer Server-Hosts **27**

## F

Firewall-Einstellungen **21**

Framework-Komponente, Dienst **26, 27**

## K

Konten **8**

## N

Nachrichtenbuskomponente, Dienst **26**

## P

Protokolldateien **19**

## R

Ressourcen **18**

## S

Servereinstellungen, sicherheitsbezogen **9**

Sicherheits-Gateway-Komponente, Dienst **26, 27**

Sicherheitseinstellungen, Global **9**

Sicherheitsserver, Dienste **27**

Sicherheitsserver, Dienst **27**

Sicherheitsübersicht **5**

Skriphost, Dienst **26**

## T

TCP-Ports **21**

Transfer Server-Dienst **27**

Transfer Server-Steuerungsdienst **27**

## U

UDP-Ports **21**

## V

View Connection Server, Dienste **26**

View Transfer Server-Verwaltung, Dienste auf einem View Transfer Server-Host **27**

View-Sicherheit **7**

VMwareVDMDS-Dienst **26**

## W

Webkomponente, Dienst **26**

