VMware View-Sicherheit

View 5.1
View Manager 5.1
View Composer 3.0

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-000732-00

vmware®

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

http://www.vmware.com/de/support/

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
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

Inhalt

VMware View-Sicherheit 5

1 VMware View-Sicherheitsreferenz 7
- VMware View-Konten 8
- VMware View-Sicherheitseinstellungen 9
- VMware View-Ressourcen 20
- VMware View-Protokolldateien 20
- TCP- und UDP-Ports von VMware View 22
- 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 Anmeldekonten 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 1

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 20

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

- VMware View-Protokolldateien auf Seite 20

  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 22

  View verwendet TCP- und UDP-Ports für den Netzwerkzugriff zwischen seinen Komponenten. Sie müssen eventuell die Firewall neu konfigurieren, damit der Zugriff auf die richtigen Ports möglich ist.

- 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 1-1. 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. 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. Weitere Informationen über die erforderlichen Berechtigungen finden Sie im Dokument *Installation von VMware View*.
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. 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. Weitere Informationen über die erforderlichen Berechtigungen finden Sie im Dokument *Installation von VMware View*.
View Connection Server, Sicherheitsserver oder View Transfer Server	Wenn Sie View installieren, können Sie auswählen, welche Mitglieder der lokalen Administratorengruppe (`BUILTIN\Administrators`) berechtigt sind, sich bei View Administrator anzumelden. In View Administrator können Sie **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** verwenden, um die Liste der View-Administratoren zu ändern. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie im Dokument *Verwaltung von VMware View*.

Tabelle 1-2. 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. Informationen zum Einrichten einer View Composer-Datenbank finden Sie im Dokument *Installation von VMware View*.
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. Informationen zum Einrichten einer View Composer-Datenbank finden Sie im Dokument *Installation von VMware View*.

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 1-3. Sicherheitsbezogene globale Einstellungen

Einstellung	Beschreibung
[Change data recovery password (Kennwort für die Datenwiederherstellung ändern)]	Das Kennwort ist erforderlich, wenn die View LDAP-Konfiguration aus einer verschlüsselten Sicherung wiederhergestellt wird. Beim Installieren vom View-Verbindungsserver Version 5.1 oder höher legen Sie ein Kennwort für die Datenwiederherstellung fest. Nach der Installation können Sie dieses Kennwort in View Administrator ändern. Wenn Sie den View-Verbindungsserver sichern, wird die View LDAP-Konfiguration in Form von verschlüsselten LDIF-Daten exportiert. Um die verschlüsselte Sicherung mit dem Dienstprogramm `vdmimport` wiederherzustellen, müssen Sie das Kennwort für die Datenwiederherstellung angeben. Das Kennwort muss 1 bis 128 Zeichen umfassen. Befolgen Sie die empfohlenen Vorgehensweisen Ihrer Organisation zum Generieren sicherer Kennwörter.
[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. Diese Einstellung ist standardmäßig deaktiviert.
[Enable automatic status updates (Automatische Status-Updates aktivieren)]	Legt fest, ob View Manager die globale Statusanzeige im oberen linken Bereich von View Administrator wird mit einem Intervall von wenigen Minuten aktualisiert. Die Dashboard-Seite von View Administrator wird ebenfalls mit einem Intervall von wenigen Minuten aktualisiert. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 1-3. Sicherheitsbezogene globale Einstellungen (Fortsetzung)

Einstellung	Beschreibung
[Message security mode (Sicherheitsmodus für Nachrichten)]	Legt fest, ob zwischen den View Manager-Komponenten übermittelte JMS-Nachrichten signiert und überprüft werden. Wenn für diese Einstellung **[Disabled (Deaktiviert)]** festgelegt ist, ist der Sicherheitsmodus für Nachrichten deaktiviert. Wenn für diese Einstellung **[Enabled (Aktiviert)]** festgelegt ist, lehnen View-Komponenten nicht signierte Nachrichten ab. Wenn für diese Einstellung **[Mixed (Gemischt)]** festgelegt ist, ist der Sicherheitsmodus für Nachrichten aktiviert, wird aber für View-Komponenten, die älter als View Manager 3.0 sind, nicht erzwungen. Die Standardeinstellung für neue Installationen ist **[Enabled (Aktiviert)]** .
[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. Diese Einstellung erhöht die Sicherheit. Wenn beispielsweise ein Laptop gestohlen wurde und mit einem anderen Netzwerk verbunden wird, kann sich der Benutzer nicht automatisch Zugriff auf den Remotedesktop verschaffen, da die Netzwerkverbindung vorübergehend unterbrochen wurde. Diese Einstellung ist standardmäßig aktiviert.
[Session timeout (Zeitüberschreitung der Sitzung)]	Legt fest, wie lange ein Benutzer eine Sitzung geöffnet lassen kann, nachdem er sich am View-Verbindungsserver angemeldet hat. Der Standardwert lautet 600 Minuten.
[Use IPSec for Security Server connections (IPSec für Sicherheitsserververbindungen verwenden)]	Legt fest, ob Internet Protocol Security (IPsec) für Verbindungen zwischen Sicherheitsservern und View-Verbindungsserver-Instanzen verwendet wird. Standardmäßig ist IPsec für Sicherheitsserververbindungen aktiviert.
[View Administrator session timeout (Zeitüberschreitung der View Administrator-Sitzung)]	Legt fest, wie lange eine sich im Leerlauf befindliche View Administrator-Sitzung andauert, bevor es zu einer Zeitüberschreitung der Sitzung kommt. **WICHTIG** Wenn unter „View Administrator session timeout (Zeitüberschreitung der View Administrator-Sitzung)“ ein hoher Minutenwert eingestellt wird, erhöht sich das Risiko, dass View Administrator unbefugterweise verwendet wird. Gehen Sie mit Bedacht vor, wenn Sie zulassen, dass sich eine Sitzung über einen längeren Zeitraum im Leerlauf befinden darf. Standardmäßig ist unter „View Administrator session timeout (Zeitüberschreitung der View Administrator-Sitzung)“ ein Wert von 30 Minuten angegeben. Sie können als Zeitüberschreitung für die Sitzung einen Wert zwischen 1 und 4230 Minuten festlegen.

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

Hinweis SSL ist für alle View Client- und View Administrator-Verbindungen mit View erforderlich. Wenn Ihre View-Bereitstellung Lastausgleichsmodule oder andere clientorientierte Zwischenserver verwendet, können Sie ein entsprechendes SSL-Offloading durchführen und anschließend Nicht-SSL-Verbindungen auf einzelnen View-Verbindungsserver-Instanzen und Sicherheitsservern konfigurieren. Weitere Informationen finden Sie unter „Offloading von SSL-Verbindungen auf Zwischenserver“ im Dokument *Verwaltung von VMware View*.

Sicherheitsbezogene Servereinstellungen in View Administrator

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

Tabelle 1-4. Sicherheitsbezogene Servereinstellungen

Einstellung	Beschreibung
[Use PCoIP Secure Gateway for PCoIP connections to desktop (PCoIP Secure Gateway für PCoIP-Verbindungen zu dem Desktop verwenden)]	Legt fest, ob View Client eine weitere sichere Verbindung zum View-Verbindungsserver- oder Sicherheitsserverhost herstellt, wenn Benutzer sich über das PCoIP-Anzeigeprotokoll mit einem View-Desktop verbinden. Wenn diese Einstellung deaktiviert ist, wird die Desktop-Sitzung direkt zwischen dem Clientsystem und der View-Desktop-VM unter Umgehung des View-Verbindungsserver- oder des Sicherheitsserverhosts aufgebaut. Diese Einstellung ist standardmäßig deaktiviert.
[Use secure tunnel connection to desktop (Sichere Tunnelverbindung zum Desktop verwenden)]	Legt fest, ob View Client eine zweite HTTPS-Verbindung zum View-Verbindungsserver- oder Sicherheitsserverhost aufbaut, wenn Benutzer eine Verbindung zu einem View-Desktop herstellen und diese Einstellung aktiviert ist. Wenn diese Einstellung deaktiviert ist, wird die Desktop-Sitzung direkt zwischen dem Clientsystem und der View-Desktop-VM unter Umgehung des View-Verbindungsserver- oder des Sicherheitsserverhosts aufgebaut. Diese Einstellung ist standardmäßig aktiviert.
[Use secure tunnel connection for Local Mode operations (Sichere Tunnelverbindung für Vorgänge im lokalen Modus verwenden)]	Legt fest, ob lokale Desktops Tunnelverbindungen verwenden. Wenn diese Einstellung aktiviert ist, wird der Netzwerkdatenverkehr durch den View-Verbindungsserver oder einen Sicherheitsserver (sofern konfiguriert) geleitet. Wenn diese Einstellung deaktiviert ist, finden Datenübertragungen direkt zwischen lokalen Desktops und dem View-Übertragungsserver statt. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 1-4. Sicherheitsbezogene Servereinstellungen (Fortsetzung)

Einstellung	Beschreibung
[Use SSL for Local Mode operations (SSL für Vorgänge im lokalen Modus verwenden)]	Legt fest, ob für die Kommunikation und Datenübertragungen zwischen Clientcomputern und dem Rechenzentrum die SSL-Verschlüsselung verwendet wird. 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. Diese Vorgänge umfassen Verbindungen zwischen Clientcomputern und dem View-Übertragungsserver. Diese Einstellung ist standardmäßig aktiviert.
[Use SSL when provisioning desktops in Local Mode (SSL bei der Bereitstellung von Desktops im lokalen Modus verwenden)]	Legt fest, ob bei Übertragungen der View Composer-Basis-Image-Dateien aus dem Übertragungsserver-Repository auf Clientcomputer die SSL-Verschlüsselung verwendet wird. Diese Vorgänge umfassen Verbindungen zwischen Clientcomputern und dem View-Übertragungsserver. Diese Einstellung ist standardmäßig aktiviert.

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 1-5. Sicherheitsbezogene Einstellungen in der View Agent-Konfigurationsvorlage

Einstellung	Registry Value Name (Registrierungswertname)	Beschreibung
`AllowDirectRDP (Direkte RDP-Verbindung zulassen)`	`AllowDirectRDP (Direkte RDP-Verbindung zulassen)`	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. **Wichtig** 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. Diese Einstellung ist standardmäßig aktiviert.
`AllowSingleSignon`	`AllowSingleSignon`	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. Diese Einstellung ist standardmäßig aktiviert.
`CommandsToRunOnConnect`	`CommandsToRunOnConnect`	Gibt eine Liste mit Befehlen oder Befehlsskripts an, die bei der ersten Verbindungsherstellung ausgeführt werden. Standardmäßig ist keine Liste angegeben.

Tabelle 1-5. Sicherheitsbezogene Einstellungen in der View Agent-Konfigurationsvorlage (Fortsetzung)

Einstellung	Registry Value Name (Registrierungswertname)	Beschreibung
CommandsToRunOnReconnect	CommandsToRunOnReconnect	Gibt eine Liste mit Befehlen oder Befehlsskripts an, die ausgeführt werden, wenn eine Sitzung nach einer Verbindungstrennung wiederhergestellt wird. Standardmäßig ist keine Liste angegeben.
ConnectionTicketTimeout	VdmConnectionTicketTimeout	Gibt die Gültigkeitsdauer des View-Verbindungstickets in Sekunden an. Wenn diese Einstellung nicht konfiguriert ist, beträgt die standardmäßige Dauer bis zur Zeitüberschreitung 120 Sekunden.
CredentialFilterExceptions	CredentialFilterExceptions	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. 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 1-6. 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 `smartCardPIN` und `password` nicht zur Verfügung, wenn Benutzer View Client von der Befehlszeile ausführen. Diese Einstellung ist standardmäßig aktiviert.
Brokers Trusted For Delegation	BrokersTrustedForDelegation	Gibt die View-Verbindungsserver-Instanzen an, welche die Benutzeridentitäts- und Anmeldeinformationen akzeptieren, die bei Aktivierung des Kontrollkästchens **[Log in as current user (Anmelden als aktueller Benutzer)]** übergeben werden. Wenn Sie keine View-Verbindungsserver-Instanzen angeben, akzeptieren alle View-Verbindungsserver-Instanzen diese Informationen. Verwenden Sie zum Hinzufügen einer View-Verbindungsserver-Instanz eines der folgenden Formate: ■ **`domain\system$`** ■ **`system$@domain.com`** ■ Service Principal Name (SPN) des View-Verbindungsserver-Dienstes

Tabelle 1-6. Sicherheitseinstellungen in der View Client-Konfigurationsvorlage (Fortsetzung)

Einstellung	Registry Value Name (Registrierungswertname)	Beschreibung
`Certificate verification mode (Zertifikatüberprüfungsmodus)`	`CertCheckMode`	Konfiguriert die Ebene der Zertifikatüberprüfung, die durch View Client durchgeführt wird. Es stehen folgende Modi zur Auswahl: ■ `No Security (Keine Sicherheit)`. View führt keine Überprüfung durch. ■ `Warn But Allow (Warnen, aber zulassen)`. Wenn die folgenden Serverzertifikatprobleme auftreten, wird eine Warnung angezeigt, aber der Benutzer kann mit der Verbindungsherstellung mit dem View-Verbindungsserver fortfahren: ■ Von View wird ein selbstsigniertes Zertifikat bereitgestellt. In diesem Fall ist es akzeptabel, wenn der Zertifikatname nicht mit dem Namen des View-Verbindungsservers übereinstimmt, der in View Client vom Benutzer angegeben wurde. ■ Ein überprüfbares Zertifikat, das in Ihrer Bereitstellung konfiguriert wurde, ist abgelaufen oder noch nicht gültig.

Tabelle 1-6. Sicherheitseinstellungen in der View Client-Konfigurationsvorlage (Fortsetzung)

Einstellung	Registry Value Name (Registrierungswertname)	Beschreibung
		Wenn andere Zertifikatfehlerbedingungen vorliegen, zeigt View ein Fehlerdialogfeld an und verhindert, dass der Benutzer eine Verbindung mit dem View-Verbindungsserver herstellt. `Warn But Allow (Warnen, aber zulassen)` ist der Standardwert. ■ `Full Security (Volle Sicherheit)`. Wenn ein beliebiger Zertifikatfehler auftritt, kann der Benutzer keine Verbindung mit dem View-Verbindungsserver herstellen. View zeigt dem Benutzer die Zertifikatfehler an. 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. Wenn diese Einstellung nicht konfiguriert oder deaktiviert wurde, können View Client-Benutzer SSL konfigurieren und einen Modus für die Zertifikatüberprüfung auswählen. Damit ein View Server die von einem View Client bereitgestellten Zertifikate überprüfen kann, muss der View Client HTTPS-Verbindungen zum View-Verbindungsserver- oder Sicherheitsserverhost herstellen. Die Zertifikatüberprüfung wird beim SSL-Offloading auf ein zwischengeschaltetes Gerät, das HTTP-Verbindungen zum View-Verbindungsserver- oder Sicherheitsserverhost herstellt, nicht unterstützt. 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: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security` Verwenden Sie die folgenden Werte im Registrierungsschlüssel: ■ **`0`** implementiert `Keine Sicherheit`. ■ **`1`** implementiert `Warnen, aber zulassen`. ■ **`2`** implementiert `Volle Sicherheit`. Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung `CertCheckMode` im Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor der Registrierungsschlüsseleinstellung.

Tabelle 1-6. Sicherheitseinstellungen in der View Client-Konfigurationsvorlage (Fortsetzung)

Einstellung	Registry Value Name (Registrierungswertname)	Beschreibung
`Default value of the 'Log in as current user' checkbox`	`LogInAsCurrentUse`	Gibt den Standardwert des Kontrollkästchens **[Log in as current user (Anmelden als aktueller Benutzer)]** im Dialogfeld für die View Client-Verbindung an. Diese Einstellung setzt den Standardwert außer Kraft, der während der View Client-Installation angegeben wurde. Wenn ein Benutzer View Client von der Befehlszeile ausführt und die Option `logInAsCurrentUser` angibt, überschreibt der eingegebene Wert diese Einstellung. Wenn das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** aktiviert ist, werden die Identität und die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem verwendet, an die View-Verbindungsserver-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. Zusätzlich zur Computerkonfigurationseinstellung ist eine Benutzerkonfigurationseinstellung verfügbar. Diese Einstellungen sind standardmäßig deaktiviert.
`Display option to Log in as current user`	`LogInAsCurrentU-ser_Display`	Legt fest, ob das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** im Dialogfeld für die View Client-Verbindung angezeigt wird. 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. Sie können den Standardwert für **[Log in as current user (Anmelden als aktueller Benutzer)]** über die Richtlinieneinstellung `Default value of the 'Log in as current user' checkbox (Standardwert des Kontrollkästchens 'Anmelden als aktueller Benutzer')` festlegen. Zusätzlich zur Computerkonfigurationseinstellung ist eine Benutzerkonfigurationseinstellung verfügbar. Diese Einstellungen sind standardmäßig aktiviert.
`Enable jump list integration`	`EnableJumplist`	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-Verbindungsserver-Instanzen und View-Desktops verbinden. 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. Diese Einstellung ist standardmäßig aktiviert.
`Enable Single Sign-On for smart card authentication`	`EnableSmartCardSSO`	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 den View-Verbindungsserver gesendet wird. Ist SSO deaktiviert, zeigt View Client kein benutzerdefiniertes PIN-Dialogfeld an. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 1-6. Sicherheitseinstellungen in der View Client-Konfigurationsvorlage (Fortsetzung)

Einstellung	Registry Value Name (Registrierungswertname)	Beschreibung
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. Diese Einstellung ist standardmäßig aktiviert. Diese Einstellung gilt nur für View 4.6 und frühere Releases.
Ignore certificate revocation problems	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. Diese Einstellung ist standardmäßig deaktiviert. 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. Diese Einstellung ist standardmäßig deaktiviert. Diese Einstellung gilt nur für View 4.6 und frühere Releases.
Ignore incorrect usage problems	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. Diese Einstellung ist standardmäßig deaktiviert. Diese Einstellung gilt nur für View 4.6 und frühere Releases.
Ignore unknown certificate authority problems	IgnoreUnknownCa	Legt fest, ob bestimmte Fehler in Zusammenhang mit einer unbekannten Zertifizierungsstelle im Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn das vom Server gesendete Zertifikat durch eine nicht vertrauenswürdige Drittanbieter-Zertifizierungsstelle signiert wurde. Diese Einstellung ist standardmäßig deaktiviert. 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 1-7. Sicherheitsbezogene Einstellungen im Abschnitt „Scripting Definitions (Skriptdefinitionen)“

Einstellung	Registry Value Name (Registrierungswertname)	Beschreibung
`Connect all USB devices to the desktop on launch`	`connectUSBOnStartup`	Legt fest, ob alle der verfügbaren USB-Geräte auf dem Clientsystem mit dem Desktop verbunden werden, wenn dieser gestartet wird. Diese Einstellung ist standardmäßig deaktiviert.
`Connect all USB devices to the desktop when they are plugged in`	`connectUSBOnInsert`	Legt fest, ob USB-Geräte mit dem Desktop verbunden werden, wenn die Geräte an das Clientsystem angeschlossen werden. Diese Einstellung ist standardmäßig deaktiviert.
`Logon Password (Passwort für Anmeldung)`	`Kennwort`	Legt das von View Client während der Anmeldung verwendete Kennwort fest. Das Kennwort wird von Active Directory im Textformat gespeichert. 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-Verbindungsserver-Instanz verwenden. Die Änderung wird automatisch auf alle anderen View-Verbindungsserver-Instanzen in einer Gruppe übernommen.

Tabelle 1-8. Sicherheitsbezogene Einstellungen in View LDAP

Name/Wert-Paar	Attribut	Beschreibung
[cs-allowunencryptedstart-session]	`pae-NameValuePair`	Dieses Attribut steuert, ob eine sichere Verbindung zwischen einer View-Verbindungsserver-Instanz und einem Desktop erforderlich ist, wenn eine Remote-Benutzersitzung gestartet wird. Wenn View Agent 5.1 oder höher auf einem Desktop-Computer installiert ist, hat dieses Attribut keinerlei Auswirkung und eine sichere Verbindung ist immer erforderlich. Wenn ein älterer View Agent als View 5.1 installiert ist, kann keine sichere Verbindung hergestellt werden, wenn der Desktop-Computer kein Mitglied einer Domäne mit bidirektionaler Vertrauensstellung zur Domäne der View-Verbindungsserver-Instanz ist. In diesem Fall ist das Attribut zur Bestimmung dafür wichtig, ob eine Remote-Benutzersitzung ohne eine sichere Verbindung gestartet werden kann. In jedem Fall werden Benutzeranmeldeinformationen und Autorisierungstickets durch einen statischen Schlüsselschutz geschützt. Eine sichere Verbindung sorgt mithilfe von dynamischen Schlüsseln für eine zusätzliche Vertraulichkeitsgewährleistung. Ist sie auf **[0]** eingestellt, kann keine Remote-Benutzersitzung gestartet werden, wenn keine sichere Verbindung hergestellt werden kann. Diese Einstellung ist geeignet, wenn sich alle Desktops in vertrauenswürdigen Domänen befinden oder wenn auf allen Desktops View Agent 5.1 oder höher installiert ist. Ist sie auf **[1]** eingestellt, kann sogar dann eine Remote-Benutzersitzung gestartet werden, wenn keine sichere Verbindung hergestellt werden kann. Diese Einstellung eignet sich, wenn auf einigen Desktops ältere View Agent-Instanzen installiert sind und wenn sich einige Desktops nicht in vertrauenswürdigen Domänen befinden. Die Standardeinstellung ist **[1]** .
	`pae-OVDIKeyCipher`	Gibt die Verschlüsselungsmethode an, die vom View-Verbindungsserver zum Verschlüsseln der virtuellen Festplattendatei (`.vmdk`) verwendet wird, wenn Benutzer einen lokalen Desktop ein- und auschecken. Sie können den Wert für die Verschlüsselungsmethode auf **[AES-128]** , **[AES-192]** oder **[AES-256]** festlegen. Der Standardwert lautet **[AES-128]** .
	`pae-SSOCredentialCacheTimeout`	Das Zeitüberschreitungslimit für die einmalige Anmeldung (Single Sign-On, SSO) in Minuten, nachdem die SSO-Anmeldeinformationen eines Benutzers ungültig werden. Der Standardwert lautet **[15]** . Ein Wert von **[-1]** bedeutet, dass kein SSO-Zeitüberschreitungslimit festgelegt ist. Mit dem Wert **[0]** wird die einmalige Anmeldung (SSO) deaktiviert.

VMware View-Ressourcen

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

Tabelle 1-9. 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	*<Laufwerksbuchstabe>*:\Programdata\VMWare\VDM\backups (Windows Server 2008)	Geschützt durch die Zugriffskontrolle.
locked.properties (Zertifikateigenschaftendatei)	*Installationsverzeichnis*\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 *<Laufwerksbuchstabe>*:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs	Geschützt durch die Zugriffskontrolle.
web.xml (Tomcat-Konfigurationsdatei)	*Installationsverzeichnis*\VMware View\Server\broker\web apps\ROOT\Web INF	Geschützt durch die Zugriffskontrolle.

Tabelle 1-10. View Transfer Server-Ressourcen

Resource (Ressource)	Standort	Schutz
httpd.conf (Apache-Konfigurationsdatei)	*Installationsverzeichnis*\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 (Windows Server 2008 R2) *<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 1-11. VMware View-Protokolldateien

VMware View-Komponente	Dateipfad und andere Informationen
Alle Komponenten (Installationsprotokolldateien)	*%TEMP%*\vminst.log_*Datum_Zeitstempel* *%TEMP%*\vmmsi.log_*Datum_Zeitstempel*
View Agent	Windows XP-Gastbetriebssystem: *<Laufwerksbuchstabe>*:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs Windows Vista- und Windows 7-Gastbetriebssystem: *<Laufwerksbuchstabe>*:\ProgramData\VMware\VDM\logs Wenn eine User Data Disk (UDD) konfiguriert ist, stimmt der *<Laufwerksbuchstabe>* möglicherweise mit der UDD überein. 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. Windows-Anwendungsereignisprotokolle. Standardmäßig deaktiviert.
View Client with Local Mode	Windows XP-Hostbetriebssystem: C:\Dokumente und Einstellungen*%Benutzername%*\Lokale Einstellungen\Anwendungsdaten\VMware\VDM\Logs\ Windows Vista- und Windows 7-Hostbetriebssystem: C:\Benutzer*%Benutzername%*\AppData\Local\VMware\VDM\Logs\
View Composer	*%Systemlaufwerk%*\Windows\Temp\vmware-viewcomposer-ga-new.log auf dem verknüpften Klon-Desktop. 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-Verbindungsserver oder Sicherheitsserver	*%ALLUSERSPROFILE%*\Anwendungsdaten\VMware\VDM\logs*.txt auf dem Server. *<Laufwerksbuchstabe>*:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs*.txt auf dem Server. Das Protokollverzeichnis ist in den Protokollkonfigurationseinstellungen der ADM-Vorlagendatei für die allgemeine View-Konfiguration (vdm_common.adm) konfigurierbar. 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. Windows-Systemereignisprotokolle.
View-Übertragungsserver	Windows Server 2008 R2: *<Laufwerksbuchstabe>*:\ProgramData\VMware\VDM\logs*.txt Apache Server: *<Laufwerksbuchstabe>*:\Program Files\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. Sie müssen eventuell die Firewall neu konfigurieren, damit der Zugriff auf die richtigen Ports möglich ist.

Tabelle 1-12. Von View verwendete TCP- und UDP-Ports mit Ausnahme des lokalen Modus

Quelle	Port	Ziel	Port	Proto-koll	Beschreibung
Sicherheitsserver	*	View Agent 4.5 oder früher	50002 (kann durch eine Gruppenrichtlinie geändert werden)	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.
Sicherheitsserver	*	View Agent 4.6 oder höher	4172	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.
Sicherheitsserver	4172	View Client	*	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.
Sicherheitsserver	500	View-Verbindungsserver	500	UDP	IPsec-Aushandlungsverkehr.
Sicherheitsserver	*	View-Verbindungsserver	4001	TCP	JMS-Datenverkehr.
Sicherheitsserver	*	View-Verbindungsserver	8009	TCP	AJP13-umgeleiteter Webverkehr, wenn IPsec oder NAT nicht verwendet werden.
Sicherheitsserver	4500	View-Verbindungsserver	4500	UDP	AJP13-umgeleiteter Webdatenverkehr, wenn IPsec durch ein NAT-Gerät verwendet wird.
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	*	UDP	PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird.
View Agent 4.6 oder höher	4172	View Client	*	UDP	PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird.

Tabelle 1-12. Von View verwendete TCP- und UDP-Ports mit Ausnahme des lokalen Modus (Fortsetzung)

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
View Agent 4.5 oder früher	50002 (kann durch eine Gruppenrichtlinie geändert werden)	View-Verbindungsserver oder Sicherheitsserver	*	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.
View Agent 4.6 oder höher	4172	View-Verbindungsserver oder Sicherheitsserver	*	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.
View Client	*	View-Verbindungsserver oder Sicherheitsserver	80	TCP	HTTP-Zugriff, wenn SSL für Clientverbindungen deaktiviert ist.
View Client	*	View-Verbindungsserver oder Sicherheitsserver	443	TCP	HTTPS-Zugriff, wenn SSL für Clientverbindungen aktiviert ist.
View Client	*	View-Verbindungsserver 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	*	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	*	View Agent 4.5 oder früher	50002 (kann durch eine Gruppenrichtlinie geändert werden)	UDP	PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird.
View Client	*	View Agent 4.6 oder höher	4172	TCP	PCoIP (HTTPS), wenn PCoIP Secure Gateway nicht verwendet wird.
View Client	*	View Agent 4.6 oder höher	4172	UDP	PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird.
View Client	*	View-Verbindungsserver oder Sicherheitsserver	4172	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.

Tabelle 1-12. Von View verwendete TCP- und UDP-Ports mit Ausnahme des lokalen Modus (Fortsetzung)

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
View-Verbindungsserver	*	vCenter Server oder View Composer	80	TCP	SOAP-Nachrichten, wenn SSL für den Zugriff auf vCenter Server oder View Composer deaktiviert ist.
View-Verbindungsserver	*	vCenter Server oder View Composer	443	TCP	SOAP-Nachrichten, wenn SSL für den Zugriff auf vCenter Server oder View Composer aktiviert ist.
View-Verbindungsserver	*	View Agent 4.5 oder früher	50002 (kann durch eine Gruppenrichtlinie geändert werden)	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway über den View-Verbindungsserver verwendet wird.
View-Verbindungsserver	*	View Agent 4.6 oder höher	4172	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway über den View-Verbindungsserver verwendet wird.
View-Verbindungsserver	4172	View Client	*	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway über den View-Verbindungsserver verwendet wird.
View-Verbindungsserver	*	View-Verbindungsserver	4100	TCP	JMS-routerinterner Datenverkehr.
View-Verbindungsserver	*	View-Desktop	3389	TCP	Microsoft RDP-Datenverkehr an View-Desktops, wenn Tunnelverbindungen über den View-Verbindungsserver verwendet werden.
View-Verbindungsserver	*	View-Desktop	4172	TCP	PCoIP (HTTPS), wenn PCoIP Secure Gateway über den View-Verbindungsserver verwendet wird.
View-Verbindungsserver	*	View-Desktop	9427	TCP	Wyse MMR-Umleitung, wenn Tunnelverbindungen über den View-Verbindungsserver verwendet werden.
View-Verbindungsserver	*	View-Desktop	32111	TCP	USB-Umleitung, wenn Tunnelverbindungen über den View-Verbindungsserver verwendet werden.

Tabelle 1-12. Von View verwendete TCP- und UDP-Ports mit Ausnahme des lokalen Modus (Fortsetzung)

Quelle	Port	Ziel	Port	Proto-koll	Beschreibung
View-Desktop	*	View-Verbindungsserver-Instanzen	4001	TCP	JMS-Datenverkehr.
View Composer-Dienst	*	ESXi-Host	902	TCP	Wird verwendet, wenn View Composer Linked-Clone-Festplatten anpasst, einschließlich View Composer-interner Festplatten 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 1-13. Vom lokalen Modus verwendete TCP- und UDP-Ports

Quelle	Port	Ziel	Port	Proto-koll	Beschreibung
Sicherheitsserver	*	View-Übertragungsserver	80	TCP	Auschecken und Einchecken des lokalen Desktops und Replikation, wenn Tunnelverbindungen verwendet werden und SSL für Vorgänge des lokalen Modus deaktiviert ist.
Sicherheitsserver	*	View-Übertragungsserver	443	TCP	Auschecken und Einchecken des lokalen Desktops und Replikation, wenn Tunnelverbindungen verwendet werden und SSL für Vorgänge des lokalen Modus aktiviert ist.
View Client with Local Mode	*	View-Übertragungsserver	80	TCP	Auschecken und Einchecken des lokalen Desktops und Replikation, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden und SSL für Vorgänge des lokalen Modus deaktiviert ist.
View Client with Local Mode	*	View-Übertragungsserver	443	TCP	Auschecken und Einchecken des lokalen Desktops und Replikation, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden und SSL für Vorgänge des lokalen Modus aktiviert ist.

Tabelle 1-13. Vom lokalen Modus verwendete TCP- und UDP-Ports (Fortsetzung)

Quelle	Port	Ziel	Port	Proto-koll	Beschreibung
View-Verbin-dungsserver	*	ESX-Host	902	TCP	Auschecken und Einchecken des lokalen Desktops und Replikation.
View-Verbin-dungsserver	*	View-Übertragungsser-ver	80	TCP	Auschecken und Einchecken des lokalen Desktops und Replikation, wenn Tunnelverbindungen über den View-Verbindungsserver verwendet werden und SSL für Vorgänge des lokalen Modus deaktiviert ist.
View-Verbin-dungsserver	*	View-Übertragungsser-ver	443	TCP	Auschecken und Einchecken des lokalen Desktops und Replikation, wenn Tunnelverbindungen über den View-Verbindungsserver verwendet werden und SSL für Vorgänge des lokalen Modus aktiviert ist.
View-Übertra-gungsserver	*	View-Verbindungsser-ver	4001	TCP	JMS-Datenverkehr zur Unterstützung des lokalen Modus.
View-Übertra-gungsserver	*	ESX-Host	902	TCP	Veröffentlichung von View Composer-Paketen für den lokalen Modus.
View-Übertra-gungsserver	*	Server, der die Übertra-gungsserver-Reposito-ry-Netzwerkfreigabe hostet	445	UDP	Konfigurieren und Veröffentlichen von View Composer-Paketen auf der Übertragungsser-ver-Repository-Netz-werkfreigabe.

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 1-14. View Connection Server-Hostdienste

Dienstname	Starttyp	Beschreibung
VMware View Con-nection Server	Automa-tisch	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 VDMDS-Dienstes oder des VMware View-Skripthostdienstes durch bzw. beendet diese Dienste nicht.
VMware View-Fra-mework-Kompo-nente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework für View Manager bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden.

Tabelle 1-14. View Connection Server-Hostdienste (Fortsetzung)

Dienstname	Starttyp	Beschreibung
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.
VMwareVDMDS	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 1-15. 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 1-16. 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. 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 **22**

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

K

Konten **8**

N

Nachrichtenbuskomponente, Dienst **26**

P

Protokolldateien **20**

R

Ressourcen **20**

S

security settings (Sicherheitseinstellungen), Global **9**

Servereinstellungen. sicherheitsbezogen **9**

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

Sicherheitsserver, Dienste **27**

Sicherheitsserver, Dienst **27**

Sicherheitsübersicht **5**

Skripthost, Dienst **26**

T

TCP-Ports **22**

Transfer Server-Dienst **27**

Transfer Server-Steuerungsdienst **27**

U

UDP-Ports **22**

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**