

View-Sicherheit

VMware Horizon 6 6.0



vmware®

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

<https://docs.vmware.com/de/>

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

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

Inhalt

View-Sicherheit 4

1 View-Sicherheitsreferenz 5

View-Konten 6

View-Sicherheitseinstellungen 7

View-Ressourcen 16

View-Protokolldateien 17

View-TCP- und UDP-Ports 18

Hinweise und Vorsichtsmaßnahmen für die von View verwendeten TCP- und UDP-Ports 21

Dienste auf einem View-Verbindungsserver-Host 22

Dienste auf einem Sicherheitsserver 22

Konfigurieren von Sicherheitsprotokollen und Cipher Suites auf einer View-Verbindungsserver-Instanz oder einem Sicherheitsserver 23

Standardmäßige globale Richtlinien für Sicherheitsprotokolle und Cipher Suites 23

Aktualisierung von JCE-Richtliniendateien zur Unterstützung hochverschlüsselter Cipher Suites 24

Konfigurieren globaler Akzeptanz- und Vorschlagsrichtlinien 24

Konfigurieren der Akzeptanzrichtlinien auf einzelnen View Servern 26

IETF-Standards 27

Perfect Forward Secrecy 28

View-Sicherheit

View-Sicherheit stellt eine umfassende Referenz zu allen Sicherheitsfunktionen von VMware Horizon (mit 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 View geöffnet oder aktiviert sein müssen.

Zielgruppe

Diese Informationen richten sich an IT-Entscheidungsträger, -Architekten, -Administratoren und andere Benutzer, die sich mit den Sicherheitskomponenten von View vertraut machen möchten.

View-Sicherheitsreferenz

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

- [View-Konten](#)

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

- [View-Sicherheitseinstellungen](#)

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.

- [View-Ressourcen](#)

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

- [View-Protokolldateien](#)

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

- [View-TCP- und UDP-Ports](#)

View verwendet TCP- und UDP-Ports für den Netzwerkzugriff zwischen seinen Komponenten.

- [Dienste auf einem View-Verbindungsserver-Host](#)

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

- [Dienste auf einem Sicherheitsserver](#)

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

- [Konfigurieren von Sicherheitsprotokollen und Cipher Suites auf einer View-Verbindungsserver-Instanz oder einem Sicherheitsserver](#)

Sie können die Sicherheitsprotokolle und Cipher Suites konfigurieren, die von View-Verbindungsserver-Instanzen akzeptiert werden. Sie können eine globale Akzeptanzrichtlinie festlegen, die für alle View-Verbindungsserver-Instanzen in einer replizierten Gruppe gilt, oder Sie können eine Akzeptanzrichtlinie für einzelne View-Verbindungsserver-Instanzen und Sicherheitsserver festlegen.

View-Konten

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

Tabelle 1-1. View-Systemkonten

View-Komponente	Erforderliche Konten
Horizon Client	Konfigurieren Sie in Active Directory Benutzerkonten für die Benutzer, die Zugriff auf Remote-Desktops und -Anwendungen haben. Die Benutzerkonten müssen Mitglieder der Gruppe der Remote-Desktop-Benutzer sein, aber die Konten erfordern keine View Administrator-Berechtigungen.
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 zu unterstützen. Weitere Informationen über die erforderlichen Berechtigungen finden Sie im Dokument <i>Installation von 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. 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 <i>Installation von View</i> .
View-Verbindungsserver oder Sicherheitsserver	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-Konfiguration > Administratoren verwenden, um die Liste der View-Administratoren zu ändern. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie im Dokument <i>Verwaltung von View</i> .

Tabelle 1-2. View-Datenbankkonten

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 <i>Installation von View</i> .
Von View-Verbindungsserver 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 <i>Installation von 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.

View-Sicherheitseinstellungen

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 in View Administrator unter **View-Konfiguration > Globale Einstellungen** verfügbar.

Tabelle 1-3. Sicherheitsbezogene globale Einstellungen

Einstellung	Beschreibung
Kennwort für die Datenwiederherstellung ändern	<p>Das Kennwort ist erforderlich, wenn Sie die View LDAP-Konfiguration aus einem verschlüsselten Backup wiederherstellen.</p> <p>Wenn Sie View-Verbindungsserver Version 5.1 oder höher installieren, geben Sie ein Kennwort für die Datenwiederherstellung an. Nach der Installation können Sie dieses Kennwort in View Administrator ändern.</p> <p>Wenn Sie View-Verbindungsserver sichern, wird die View LDAP-Konfiguration in Form verschlüsselter LDIF-Daten exportiert. Sie müssen das Kennwort für die Datenwiederherstellung angeben, um das verschlüsselte Backup mit dem Dienstprogramm <code>vdmimport</code> wiederherzustellen. Das Kennwort muss 1 bis 128 Zeichen umfassen. Befolgen Sie die empfohlenen Vorgehensweisen Ihrer Organisation für das Generieren sicherer Kennwörter.</p>
Sicherheitsmodus für Nachrichten	<p>Legt fest, ob zwischen den View-Komponenten übermittelte JMS-Nachrichten signiert und überprüft werden.</p> <p>Wenn für diese Einstellung Deaktiviert festgelegt ist, ist der Sicherheitsmodus für Nachrichten deaktiviert.</p> <p>Wenn für diese Einstellung Aktiviert festgelegt ist, lehnen View-Komponenten nicht signierte Nachrichten ab.</p> <p>Wenn für diese Einstellung 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 Aktiviert.</p>
Sichere Tunnelverbindungen nach Netzwerkunterbrechung neu authentifizieren	<p>Legt fest, ob die Anmeldedaten nach einer Netzwerkunterbrechung neu authentifiziert werden müssen, wenn Horizon Clients sichere Tunnelverbindungen zu View-Desktops und -Anwendungen verwenden.</p> <p>Diese Einstellung bietet erhöhte Sicherheit. Wenn beispielsweise ein Laptop gestohlen und in ein anderes Netzwerk bewegt wurde, kann der Benutzer nicht automatisch Zugang zu View-Desktops und -Anwendungen erlangen, da die Netzwerkverbindung vorübergehend unterbrochen wurde. Diese Einstellung ist standardmäßig aktiviert.</p>
Trennung der Benutzer erzwingen	<p>Trennt alle Desktops und Anwendungen, nachdem die angegebene Anzahl von Minuten seit der Anmeldung des Benutzers bei View vergangen ist. Alle Desktops und Anwendungen werden gleichzeitig getrennt, unabhängig davon, wann der Benutzer sie geöffnet hat.</p> <p>Der Standardwert lautet 600 Minuten.</p>

Einstellung	Beschreibung
<p>Für Clients, die Anwendungen unterstützen.</p> <p>Sobald der Benutzer nicht mehr mit Tastatur und Maus arbeitet, werden die Verbindungen zu Anwendungen getrennt und die SSO-Anmeldeinformationen verworfen.</p>	<p>Schützt Anwendungssitzungen, wenn auf dem Client-Gerät keine Tastatur- oder Mausektivitäten stattfinden. Bei Festlegung auf Nach ... Minuten trennt View nach Ablauf der angegebenen Anzahl von Minuten ohne Benutzeraktivität sämtliche Anwendungssitzungen und verwirft die SSO-Anmeldeinformationen. Desktop-Sitzungen werden getrennt. Benutzer müssen sich erneut anmelden, um eine Verbindung zu den getrennten Anwendungen wiederherzustellen, oder einen neuen Desktop bzw. eine neue Anwendung starten.</p> <p>Bei der Einstellung Nie trennt View in keinem Fall Anwendungen oder verwirft SSO-Anmeldeinformationen aufgrund von Benutzerinaktivität.</p> <p>Die Standardeinstellung ist Nie.</p>
<p>Andere Clients. SSO-Anmeldeinformationen verwerfen</p>	<p>Verwirft die SSO-Anmeldeinformationen nach einem bestimmten Zeitraum. Diese Einstellung gilt für Clients, die die Remote-Ausführung von Anwendungen nicht unterstützen. Bei Festlegung von Nach ... Minuten müssen sich die Benutzer nach Ablauf der angegebenen Anzahl von Minuten nach der Anmeldung bei View erneut anmelden, um eine Verbindung zu einem Desktop herzustellen, unabhängig von den Benutzeraktivitäten auf dem Client-Gerät.</p> <p>Die Standardeinstellung ist Nach 15 Minuten.</p>
<p>IPSec für Sicherheitsserver-Kombination aktivieren</p>	<p>Bestimmt, ob Internet Protocol Security (IPSec) für Verbindungen zwischen Sicherheitsservern und View-Verbindungsserver-Instanzen verwendet wird.</p> <p>Standardmäßig ist IPSec für Sicherheitsserver-Verbindungen aktiviert.</p>
<p>Zeitüberschreitung für View Administrator-Sitzung</p>	<p>Bestimmt, wie lange eine View Administrator-Sitzung im Leerlauf bleibt, bevor die Sitzung abläuft.</p> <p>Wichtig Wenn Sie den Zeitüberschreitungswert für die View Administrator-Sitzung auf eine hohe Minutenzahl einstellen, steigt das Risiko, dass View Administrator unautorisiert genutzt werden könnte. Seien Sie vorsichtig, wenn Sie zulassen, dass eine Sitzung lange Zeit im Leerlauf bleibt.</p> <p>Standardmäßig beträgt die Zeitüberschreitung für die View Administrator-Sitzung 30 Minuten. Sie können eine Sitzungszeitüberschreitung von 1 bis 4.320 Minuten festlegen.</p>

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

Hinweis Für alle Horizon Client-Verbindungen und View Administrator-Verbindungen mit View ist SSL erforderlich. Wenn Ihre View-Bereitstellung Lastausgleichsmodule oder andere Zwischenserver mit Client-Verbindung verwendet, können Sie SSL darauf verlagern und dann Nicht-SSL-Verbindungen auf einzelnen View-Verbindungsserver-Instanzen und Sicherheitsservern konfigurieren. Weitere Informationen finden Sie unter „Verschieben von SSL-Verbindungen auf Zwischenserver“ im Dokument *Verwaltung von View*.

Sicherheitsbezogene Servereinstellungen in View Administrator

Sicherheitsbezogene Servereinstellungen sind in View Administrator unter **View-Konfiguration > Server** verfügbar.

Tabelle 1-4. Sicherheitsbezogene Servereinstellungen

Einstellung	Beschreibung
PCoIP Secure Gateway für PCoIP-Verbindungen zum Computer verwenden	<p>Bestimmt, ob Horizon Client eine weitere sichere Verbindung zum View-Verbindungsserver- oder Sicherheitsserverhost herstellt, wenn Benutzer sich über das PCoIP-Anzeigeprotokoll mit View-Desktops und -Anwendungen verbinden.</p> <p>Wenn diese Einstellung deaktiviert ist, wird die Desktop- bzw. Anwendungssitzung direkt zwischen dem Client und dem View-Desktop oder Remote-Desktop-Dienste-Hosts unter Umgehung des View-Verbindungsserver- bzw. Sicherheitsserverhosts aufgebaut.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>
Sichere Tunnelverbindung zum Computer verwenden	<p>Bestimmt, ob Horizon Client eine zweite HTTPS-Verbindung mit dem View-Verbindungsserver- oder Sicherheitsserverhost aufbaut, wenn Benutzer sich mit einem View-Desktop bzw. mit einer View-Anwendung verbinden.</p> <p>Wenn diese Einstellung deaktiviert ist, wird die Desktop- bzw. Anwendungssitzung direkt zwischen dem Client und dem View-Desktop oder Remote-Desktop-Dienste-Hosts unter Umgehung des View-Verbindungsserver- bzw. Sicherheitsserverhosts aufgebaut.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
Verwenden Sie Blast Secure Gateway für den HTML Access auf den Computer	<p>Legt fest, ob Clients, die einen Webbrowser für den Zugriff auf Desktops verwenden, Blast Secure Gateway zum Herstellen einer sicheren Verbindung zum View-Verbindungsserver verwenden.</p> <p>Wenn die Option nicht aktiviert ist, stellen Webbrowser direkte Verbindungen zu View-Desktops her und umgehen dabei den View-Verbindungsserver.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>

Weitere Informationen zu diesen Einstellungen und ihren Auswirkungen auf die Sicherheit finden Sie im Dokument *Verwaltung von 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 „Computerkonfiguration“.

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

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

Einstellung	Registrierungswertname	Beschreibung
AllowDirectRDP	AllowDirectRDP	<p>Legt fest, ob Nicht-Horizon Clients über RDP eine direkte Verbindung mit View-Desktops herstellen können. Ist diese Einstellung deaktiviert, lässt View Agent nur View-verwaltete Verbindungen über Horizon Client zu.</p> <p>Standardmäßig können Sie RDP verwenden, um eine Verbindung zur virtuellen Maschine von außerhalb von View herzustellen, während ein Benutzer bei einer View-Desktopsitzung angemeldet ist. Die RDP-Verbindung beendet die View-Desktopsitzung und die nicht gespeicherten Daten und Einstellungen des View-Benutzers gehen u. U. verloren. Der View-Benutzer kann sich erst dann am Desktop anmelden, wenn die externe RDP-Verbindung beendet wurde. Deaktivieren Sie die Einstellung AllowDirectRDP, um diese Situation zu vermeiden.</p> <hr/> <p>Wichtig Damit View ordnungsgemäß funktioniert, müssen die Windows-Remote-Desktop-Dienste auf dem Gastbetriebssystem jedes Desktops ausgeführt werden. Sie können diese Einstellung verwenden, um Benutzer davon abzuhalten, direkte RDP-Verbindungen zu ihren Desktops herzustellen.</p> <hr/> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
AllowSingleSignon	AllowSingleSignon	<p>Legt fest, ob zur Verbindungsherstellung mit Desktops und Anwendungen die einmalige Anmeldung (Single Sign-On, SSO) zulässig ist. Bei Aktivierung dieser Einstellung werden Benutzer nur dann zur Eingabe ihrer Anmeldeinformationen aufgefordert, wenn sie eine Verbindung mit Horizon Client herstellen. Ist diese Einstellung deaktiviert, müssen sich die Benutzer beim Herstellen einer Remote-Verbindung erneut authentifizieren.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p>
CommandsToRunOnConnect	CommandsToRunOnConnect	<p>Gibt eine Liste mit Befehlen oder Befehlsskripten an, die bei der ersten Verbindungsherstellung ausgeführt werden.</p> <p>Standardmäßig ist keine Liste angegeben.</p>
CommandsToRunOnReconnect	CommandsToRunOnReconnect	<p>Gibt eine Liste mit Befehlen oder Befehlsskripten an, die ausgeführt werden, wenn eine Sitzung nach einer Verbindungstrennung wiederhergestellt wird.</p> <p>Standardmäßig ist keine Liste angegeben.</p>
CommandsToRunOnDisconnect	CommandsToRunOnDisconnect	<p>Gibt eine Liste mit Befehlen oder Befehlsskripten an, die ausgeführt werden, wenn eine Sitzung getrennt wird.</p> <p>Standardmäßig ist keine Liste angegeben.</p>
ConnectionTicketTimeout	VdmConnectionTicketTimeout	<p>Gibt die Gültigkeitsdauer des View-Verbindungstickets in Sekunden an.</p> <p>Wenn diese Einstellung nicht konfiguriert ist, beträgt die standardmäßige Dauer bis zur Zeitüberschreitung 120 Sekunden.</p>
CredentialFilterExceptions	CredentialFilterExceptions	<p>Gibt die ausführbaren Dateien an, die nicht zum Laden des CredentialFilter-Agenten berechtigt sind. Dateinamen dürfen weder einen Pfad noch ein Suffix enthalten. Verwenden Sie ein Semikolon zum Trennen mehrerer Dateinamen.</p> <p>Standardmäßig ist keine Liste angegeben.</p>

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

Sicherheitseinstellungen in der Horizon Client-Konfigurationsvorlage

Sicherheitsbezogene Einstellungen werden in der ADM-Vorlagendatei für Horizon Client (`vdm_client.adm`) bereitgestellt. Falls nicht anders angegeben, enthalten die Einstellungen nur eine Einstellung „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\VMware, Inc.\VMware VDM\Client\Configuration` gespeichert.

Tabelle 1-6. Sicherheitseinstellungen in der Horizon Client-Konfigurationsvorlage

Einstellung	Registrierungswertname	Beschreibung
Allow command line credentials	AllowCmdLineCredentials	Legt fest, ob Anmeldedaten mit Horizon 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 Horizon 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 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: <ul style="list-style-type: none"> ■ <code>domain\system\$</code> ■ <code>system\$@domain.com</code> ■ Service Principal Name (SPN) des View-Verbindungsserver-Dienstes

Einstellung	Registrierungswertname	Beschreibung
Certificate verification mode	CertCheckMode	<p>Konfiguriert die Ebene der Zertifikatüberprüfung, die durch Horizon Client durchgeführt wird. Es stehen folgende Modi zur Auswahl:</p> <ul style="list-style-type: none"> ■ Keine Sicherheit. View führt keine Überprüfung durch. ■ Warnen, aber zulassen. Wenn die folgenden Serverzertifikatprobleme auftreten, wird eine Warnung angezeigt, aber der Benutzer kann mit der Verbindungsherstellung mit View-Verbindungsserver fortfahren: <ul style="list-style-type: none"> ■ 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 Horizon Client vom Benutzer angegeben wurde. ■ Die Zertifikatsprüfung ist auf einem Zero-Client nicht möglich, da der Trust Store leer ist. <p>Wenn andere Zertifikatfehlerbedingungen vorliegen, zeigt View ein Fehlerdialogfeld an und verhindert, dass der Benutzer eine Verbindung mit View-Verbindungsserver herstellt.</p> <ul style="list-style-type: none"> ■ Volle Sicherheit. Wenn ein beliebiger Zertifikatfehler auftritt, kann der Benutzer keine Verbindung mit View-Verbindungsserver herstellen. View zeigt dem Benutzer die Zertifikatfehler an. <p>Der Standardwert lautet Warnen, aber zulassen.</p> <hr/> <p>Wichtig Der Standardwert von Warnen, aber zulassen dient der Erleichterung der Bereitstellung und dem Testen in einer Vorproduktionsumgebung. Für den Produktionseinsatz wird nur Volle Sicherheit empfohlen.</p> <hr/> <p>Wenn diese Gruppenrichtlinieneinstellung konfiguriert ist, können die Benutzer den ausgewählten Modus für die Zertifikatüberprüfung in Horizon Client sehen, die Einstellung jedoch 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 Horizon 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"> ■ 0 implementiert Keine Sicherheit. ■ 1 implementiert Warnen, aber zulassen. ■ 2 implementiert Volle Sicherheit. <p>Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung CertCheckMode im Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor der Registrierungsschlüsseleinstellung.</p>

Einstellung	Registrierungswertname	Beschreibung
Default value of the 'Log in as current user' checkbox	LogInAsCurrentUser	<p>Gibt den Standardwert des Kontrollkästchens Anmelden als aktueller Benutzer im Dialogfeld für die Horizon Client-Verbindung an.</p> <p>Diese Einstellung setzt den Standardwert außer Kraft, der während der Horizon Client-Installation angegeben wurde.</p> <p>Wenn ein Benutzer Horizon Client von der Befehlszeile ausführt und die Option <code>LogInAsCurrentUser</code> angibt, überschreibt der eingegebene Wert diese Einstellung.</p> <p>Wenn das Kontrollkästchen Anmelden als aktueller Benutzer aktiviert ist, werden die Identität und die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung beim Clientsystem verwendet, an die View-Verbindungsserver-Instanz und schließlich an den View-Desktop oder an die View-Anwendung übergeben. Ist das Kontrollkästchen deaktiviert, müssen Benutzer Identitäts- und Anmeldeinformationen mehrere Male eingeben, bevor sie auf einen View-Desktop oder auf eine View-Anwendung 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	LogInAsCurrentUser_Display	<p>Legt fest, ob das Log in as current user check box is visible on the Horizon Client connection dialog box.</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 Horizon Client-Verbindung nicht ändern.</p> <p>Sie können den Standardwert für Anmelden als aktueller Benutzer über die Richtlinieneinstellung 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	EnableJumplist	<p>Legt fest, ob eine Sprungliste im Horizon Client icon on the taskbar of Windows 7 and later systems. Über die Sprungliste können sich Benutzer mit zuletzt verwendeten View-Verbindungsserver-Instanzen und View-Desktops sowie -Anwendungen verbinden.</p> <p>Wenn Horizon Client gemeinsam verwendet wird, können Benutzern die Namen zuletzt verwendeter Desktops und Anwendungen 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	EnableSmartCardSSO	<p>Legt fest, ob für die Smartcard-Authentifizierung das Single Sign-On (SSO) aktiviert ist. Ist SSO aktiviert, speichert Horizon Client die verschlüsselte Smartcard-PIN im temporären Arbeitsspeicher, bevor sie an den View-Verbindungsserver gesendet wird. Ist SSO deaktiviert, zeigt Horizon Client kein benutzerdefiniertes PIN-Dialogfeld an.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p>

Einstellung	Registrierungswertname	Beschreibung
Ignore bad SSL certificate date received from the server	IgnoreCertDateInvalid	<p>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.</p> <p>Diese Einstellung ist standardmäßig aktiviert.</p> <p>Diese Einstellung gilt nur für View 4.6 und frühere Releases.</p>
Ignore certificate revocation problems	IgnoreRevocation	<p>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.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p> <p>Diese Einstellung gilt nur für View 4.6 und frühere Releases.</p>
Ignore incorrect SSL certificate common name (host name field)	IgnoreCertCnInvalid	<p>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.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p> <p>Diese Einstellung gilt nur für View 4.6 und frühere Releases.</p>
Ignore incorrect usage problems	IgnoreWrongUsage	<p>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.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p> <p>Diese Einstellung gilt nur für View 4.6 und frühere Releases.</p>
Ignore unknown certificate authority problems	IgnoreUnknownCa	<p>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.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p> <p>Diese Einstellung gilt nur für View 4.6 und frühere Releases.</p>
EnableTicketSSL Auth	EnableTicketSSLAuth	<p>Aktiviert den SSL-verschlüsselten Framework-Kanal. Diese Einstellung kann die folgenden Werte enthalten:</p> <ul style="list-style-type: none"> ■ Aktivieren: Aktivieren Sie SSL und ermöglichen Sie das Zurücksetzen auf Desktops ohne SSL-Unterstützung. ■ Deaktivieren: Deaktivieren Sie SSL. ■ Erzwingen: Aktivieren Sie SSL und verweigern Sie das Herstellen einer Verbindung zu Desktops ohne SSL-Unterstützung. <p>Der Standardwert lautet Aktivieren.</p>
SSLCipherList	SSLCipherList	<p>Konfiguriert die Verschlüsselungsliste, um die Verwendung bestimmter kryptografischer Algorithmen und Protokolle zu beschränken, bevor eine verschlüsselte SSL-Verbindung hergestellt wird.</p> <p>Der Standardwert lautet „SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH“. Dies bedeutet: SSL v3.0, TLS v1.0 und TLS v1.1 sind aktiviert (SSL v2.0 und TLS v1.2 sind deaktiviert).</p>

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

Sicherheitsbezogene Einstellungen im Abschnitt „Skriptdefinitionen“ der Horizon Client-Konfigurationsvorlage

Sicherheitsbezogene Einstellungen werden im Abschnitt „Skriptdefinitionen“ der ADM-Vorlagendatei für Horizon 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 „Skriptdefinitionen“

Einstellung	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	Password	Legt das von Horizon 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 ihren Auswirkungen auf die Sicherheit finden Sie im Dokument *Verwaltung von 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-allowunencryptedsession	paenNameValuePair	<p>Dieses Attribut steuert, ob eine sichere Verbindung zwischen einer View-Verbindungsserver-Instanz und einem Desktop notwendig ist, wenn eine Remotebenutzer-Sitzung gestartet wird.</p> <p>Wenn View Agent 5.1 oder höher auf einem Desktop-Computer installiert ist, hat dieses Attribut keine Auswirkung, und es ist immer eine sichere Verbindung erforderlich. Wenn ein View Agent installiert ist, der älter als View 5.1 ist, kann keine sichere Verbindung hergestellt werden, sofern der Desktop-Computer nicht einer Domäne mit einer bidirektionalen Vertrauensbeziehung zur Domäne der View-Verbindungsserver-Instanz angehört. In diesem Fall ist das Attribut wichtig, um zu bestimmen, ob eine Remotebenutzer-Sitzung ohne eine sichere Verbindung gestartet werden kann.</p> <p>In allen Fällen werden Anmeldedaten und Autorisierungstickets durch einen statischen Schlüssel geschützt. Eine sichere Verbindung bietet einen weiteren Vertrauensschutz durch Verwendung dynamischer Schlüssel.</p> <p>Bei der Einstellung 0 wird keine Remotebenutzer-Sitzung gestartet, wenn keine sichere Verbindung hergestellt werden kann. Diese Einstellung eignet sich, wenn sich alle Desktops in vertrauenswürdigen Domänen befinden oder wenn auf allen Desktops View Agent 5.1 oder höher installiert ist.</p> <p>Bei der Einstellung 1 kann eine Remotebenutzer-Sitzung auch dann gestartet werden, wenn keine sichere Verbindung hergestellt werden kann. Diese Einstellung eignet sich, wenn auf einigen Desktops ältere View Agents installiert sind und sich diese nicht in vertrauenswürdigen Domänen befinden.</p> <p>Die Standardeinstellung ist</p> <p>1.</p>

View-Ressourcen

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

Tabelle 1-9. View-Verbindungsserver- und Sicherheitsserver-Ressourcen

Resource (Ressource)	Speicherort	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.

Resource (Ressource)	Speicherort	Schutz
Protokolldateien	Siehe View-Protokolldateien	Geschützt durch die Zugriffskontrolle.
web.xml (Tomcat-Konfigurationsdatei)	<i>Installationsverzeichnis</i> \VMware View\Server \broker\web apps\ROOT\Web INF	Geschützt durch die Zugriffskontrolle.

View-Protokolldateien

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

Hinweis View-Protokolldateien sind für die Verwendung durch den VMware Support bestimmt. VMware empfiehlt das Konfigurieren und Verwenden der Ereignisdatenbank zur Überwachung von View. Weitere Informationen hierzu finden Sie in den Dokumenten *Installation von View* und *Integration von View*.

Tabelle 1-10. View-Protokolldateien

View-Komponente	Dateipfad und andere Informationen
Alle Komponenten (Installationsprotokolldateien)	%TEMP%\vminst.log_ Datum _ Zeitstempel %TEMP%\vmmsi.log_ Datum _ Zeitstempel
View Agent	<p>Windows XP-Gastbetriebssystem:</p> <p><Laufwerksbuchstabe>:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs</p> <p>Windows Vista-, Windows 7- und Windows 8-Gastbetriebssystem:</p> <p><Laufwerksbuchstabe>:\ProgramData\VMware\VDM\logs</p> <p>Um auf View-Protokolldateien zugreifen zu können, die unter <Laufwerksbuchstabe>:\ProgramData\VMware\VDM\logs gespeichert sind, müssen Sie die Protokolle aus einem Programm mit erweiterten Administratorberechtigungen öffnen. Klicken Sie mit der rechten Maustaste auf die Programmdatei und wählen Sie Als Administrator ausführen.</p> <p>Wenn eine User Data Disk (UDD) konfiguriert ist, stimmt der <Laufwerksbuchstabe> möglicherweise mit der UDD überein.</p> <p>Die Protokolle für PCoIP heißen pcoip_agent*.log und pcoip_server*.log.</p>
View-Anwendungen	<p>View Event Database, konfiguriert auf einem SQL Server- oder Oracle-Datenbankserver.</p> <p>Windows-Anwendungseignisprotokolle. Standardmäßig deaktiviert.</p>
View Composer	<p>%Systemlaufwerk%\Windows\Temp\vmware-viewcomposer-ga-new.log auf dem verknüpften Klon-Desktop.</p> <p>Das View Composer-Protokoll enthält Informationen über die Ausführung von QuickPrep- und Sysprep-Skripts. Das Protokoll zeichnet den Start und das Ende der Skriptausführung sowie Ausgabe- oder Fehlermeldungen auf.</p>

View-Komponente	Dateipfad und andere Informationen
View-Verbindungsserver oder Sicherheitsserver	<p><Laufwerksbuchstabe>:\ProgramData\VMware\VDM\logs.</p> <p>Das Protokollverzeichnis ist in den Protokollkonfigurationseinstellungen der ADM-Vorlagendatei für die allgemeine View-Konfiguration (vdm_common.adm) konfigurierbar.</p> <p>PCoIP Secure Gateway-Protokolle werden in Dateien namens SecurityGateway_*.log im Unterverzeichnis PCoIP Secure Gateway des Protokollverzeichnisses auf einem Sicherheitsserver geschrieben.</p>
View-Dienste	<p>View Event Database, konfiguriert auf einem SQL Server- oder Oracle-Datenbankserver.</p> <p>Windows-Systemereignisprotokolle.</p>

View-TCP- und UDP-Ports

View verwendet TCP- und UDP-Ports für den Netzwerkzugriff zwischen seinen Komponenten.

Während der Installation kann View optional Windows-Firewall-Regeln konfigurieren, um die Ports zu öffnen, die standardmäßig verwendet werden. Wenn Sie die Standard-Ports nach der Installation ändern, müssen Sie die Windows-Firewall-Regeln manuell neu konfigurieren, um Zugriff auf die aktualisierten Ports zu erlauben. Weitere Informationen finden Sie unter „Ersetzen von Standard-Ports für View-Dienste“ im Dokument *Installation von View*.

Tabelle 1-11. Von View verwendete TCP- und UDP-Ports

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
Sicherheitsserver	55000	View Agent	4172	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.
Sicherheitsserver	4172	Horizon Client	50001	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-weitergeleiteter Webdatenverkehr, falls nicht IPsec verwendet wird.
Sicherheitsserver	*	View-Verbindungsserver	*	ESP	AJP13-weitergeleiteter Webdatenverkehr, wenn IPsec ohne NAT verwendet wird.
Sicherheitsserver	4500	View-Verbindungsserver	4500	UDP	AJP13-weitergeleiteter Webdatenverkehr, wenn IPsec über 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	4172	TCP	PCoIP (HTTPS), wenn PCoIP Secure Gateway verwendet wird.
Sicherheitsserver	*	View-Desktop	22443	TCP	HTML Access.

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
View Agent	4172	Horizon Client	50001	UDP	PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird.
View Agent	4172	View-Verbindungsserver oder Sicherheitsserver	55000	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.
Horizon Client	*	View-Verbindungsserver oder Sicherheitsserver	80	TCP	<p>SSL (HTTPS-Zugriff) ist standardmäßig für Clientverbindungen aktiviert, in bestimmten Fällen kann jedoch Port 80 (HTTP-Zugriff) verwendet werden. Siehe</p> <p>Hinweise und Vorsichtsmaßnahmen für die von View verwendeten TCP- und UDP-Ports.</p>
Horizon Client	*	View-Sicherheitsserver	443	TCP	<p>HTTPS-Zugriff. Port 443 ist für Clientverbindungen standardmäßig aktiviert. Port 443 kann geändert werden.</p> <p>Beim Versuch, über HTTP eine Verbindung mit Port 80 herzustellen, wird die Verbindung standardmäßig an Port 443 umgeleitet. Port 80 kann jedoch für Clientverbindungen verwendet werden, wenn SSL auf einen Zwischenserver verschoben wird. Wenn der HTTPS-Port geändert wurde, können Sie die Umleitungsregel neu konfigurieren. Siehe Hinweise und Vorsichtsmaßnahmen für die von View verwendeten TCP- und UDP-Ports.</p>
Horizon Client	*	View-Verbindungsserver	443	TCP	<p>HTTPS-Zugriff. Port 443 ist für Clientverbindungen standardmäßig aktiviert. Port 443 kann geändert werden.</p> <p>Beim Versuch, eine Clientverbindung mit Port 80 herzustellen, wird die Verbindung standardmäßig an Port 443 umgeleitet. Port 80 kann jedoch für Clientverbindungen verwendet werden, wenn SSL auf einen Zwischenserver verschoben wird. Beim Versuch, über Port 80 eine Verbindung mit View Administrator herzustellen, findet keine Umleitung statt. Verbindungen mit View Administrator müssen über HTTPS hergestellt werden.</p> <p>Sie können eine HTTP-Umleitung verhindern und erzwingen, dass Clients HTTPS verwenden. Siehe Hinweise und Vorsichtsmaßnahmen für die von View verwendeten TCP- und UDP-Ports.</p>
Horizon Client	*	View-Verbindungsserver oder Sicherheitsserver	4172	TCP	PCoIP (HTTPS), wenn PCoIP Secure Gateway verwendet wird.
Horizon Client	*	View-Desktop	3389	TCP	Microsoft RDP-Datenverkehr an View-Desktops, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden.

Quelle	Port	Ziel	Port	Protokoll	Beschreibung
Horizon Client	*	View-Desktop	9427	TCP	Wyse MMR-Umleitung, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden.
Horizon Client	*	View-Desktop	32111	TCP	USB-Umleitung, wenn direkte Verbindungen statt Tunnelverbindungen verwendet werden.
Horizon Client	*	View Agent	4172	TCP	PCoIP (HTTPS), wenn PCoIP Secure Gateway nicht verwendet wird.
Horizon Client	50001	View Agent	4172	UDP	PCoIP, wenn PCoIP Secure Gateway nicht verwendet wird.
Horizon Client	50001	View-Verbindungsserver oder Sicherheitsserver	4172	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway verwendet wird.
Webbrowser	*	Sicherheitsserver	8443	TCP	HTML Access.
View-Verbindungsserver	*	View-Verbindungsserver	48080	TCP	Zur internen Kommunikation zwischen Komponenten von View-Verbindungsserver.
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	55000	View Agent	4172	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway über den View-Verbindungsserver verwendet wird.
View-Verbindungsserver	4172	Horizon Client	50001	UDP	PCoIP (nicht SALSA20), wenn PCoIP Secure Gateway über den View-Verbindungsserver verwendet wird.
View-Verbindungsserver	*	View-Verbindungsserver	4100	TCP	JMS-Datenverkehr zwischen Routern.
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.
View-Verbindungsserver	*	View-Verbindungsserver	8472	TCP	Für podübergreifende Kommunikation in der Cloud-Pod-Architektur
View-Verbindungsserver	*	View-Verbindungsserver	22389	TCP	Für globale LDAP-Replizierung in der Cloud-Pod-Architektur
View-Verbindungsserver	*	View-Verbindungsserver	22636	TCP	Für sichere globale LDAP-Replizierung in der Cloud-Pod-Architektur

Quelle	Port	Ziel	Port	Protokoll	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. Dazu gehören interne Festplatten von View Composer und, falls diese angegeben werden, persistente Festplatten und SDD (System-Disposable Disks).

Hinweise und Vorsichtsmaßnahmen für die von View verwendeten TCP- und UDP-Ports

Beim Versuch, eine Verbindung über HTTP herzustellen, wird im Hintergrund eine Umleitung an HTTPS durchgeführt. Die einzige Ausnahme stellen Verbindungsversuche mit View Administrator dar. Bei neueren View-Clients ist keine HTTP-Umleitung erforderlich, da diese Clients standardmäßig HTTPS verwenden. Wenn Benutzer jedoch eine Verbindung mit einem Webbrowser herstellen (z. B. zum Herunterladen von View Client), ist diese Option jedoch nützlich.

Das Problem der HTTP-Umleitung ist, dass es sich nicht um ein sicheres Protokoll handelt. Wenn sich ein Benutzer nicht angewöhnt, **https://** in der Adresszeile einzugeben, kann ein Angreifer über den Webbrowser schädliche Software installieren oder Anmeldeinformationen ausspähen. Dies ist selbst dann möglich, wenn die erwartete Seite ordnungsgemäß angezeigt wird.

Hinweis Eine HTTP-Umleitung ist für externe Verbindungen nur dann möglich, wenn Sie Ihre externe Firewall für das Zulassen von eingehendem Datenverkehr an TCP-Port 80 konfigurieren.

Beim Versuch, über HTTP eine Verbindung mit View Administrator herzustellen, findet keine Umleitung statt. Stattdessen wird in einer Fehlermeldung angezeigt, dass Sie HTTPS verwenden müssen.

Informationen zum Verhindern der Umleitung für alle HTTP-Verbindungsversuche finden Sie unter „Verhindern der HTTP-Umleitung für Clientverbindungen zum Verbindungsserver“ im Dokument *Installation von View*.

Verbindungen mit Port 80 einer View-Verbindungsserver-Instanz oder eines Sicherheitsservers sind auch dann möglich, wenn Sie SSL-Clientverbindungen auf ein Zwischengerät verschieben. Siehe „Verschieben von SSL-Verbindungen auf Zwischenserver“ im Dokument *Verwaltung von VMware Horizon View*.

Informationen zum Zulassen der HTTP-Umleitung, wenn die SSL-Portnummer geändert wurde, finden Sie unter „Ändern der Portnummer für die HTTP-Umleitung zum Verbindungsserver“ im Dokument *Installation von View*.

Hinweis Die UDP-Portnummer, die von Clients für PCoIP verwendet wird, kann sich ändern. Wenn Port 50001 verwendet wird, wählt der Client Port 50002 aus. Wenn Port 50002 verwendet wird, wählt der Client Port 50003 aus usw. Sie müssen die Firewall mit der Option BELIEBIG konfigurieren, wobei 50001 in der Tabelle aufgeführt sein muss.

Dienste auf einem View-Verbindungsserver-Host

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

Tabelle 1-12. View-Verbindungsserver-Hostdienste

Dienstname	Starttyp	Beschreibung
VMware Horizon View Blast Secure Gateway	Automatisch	Stellt sichere HTML Access-Dienste bereit. Dieser Dienst muss ausgeführt werden, wenn Clients die Verbindung zu View-Verbindungsserver über den HTML Access Secure Gateway herstellen.
VMware Horizon View- Verbindungsserver	Automatisch	Stellt Verbindungs-Broker-Dienste bereit. Dieser Dienst muss immer ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework-, Nachrichtenbus-, Sicherheits-Gateway- und Webdienste gestartet oder beendet. Dieser Dienst führt keinen Start des VMware VDMDS-Dienstes oder des VMware Horizon View-Skripthostdienstes durch bzw. beendet diese Dienste nicht.
VMware Horizon View Framework- Komponente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View Message Bus- Komponente	Manuell	Stellt Dienste für die Nachrichtenübermittlung zwischen den View-Komponenten bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View PCoIP Secure Gateway	Manuell	Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu View-Verbindungsserver über ein PCoIP Secure Gateway herstellen.
VMware Horizon View-Skripthost	Deaktiviert	Bietet Unterstützung für Drittanbieterskripts, die beim Löschen von virtuellen Maschinen ausgeführt werden. Dieser Dienst ist standardmäßig deaktiviert. Sie sollten diesen Dienst aktivieren, wenn Sie Skripts ausführen möchten.
VMware Horizon View Security Gateway- Komponente	Manuell	Stellt gängige Gateway-Dienste bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View Web- Komponente	Manuell	Stellt Webdienste bereit. Dieser Dienst muss immer ausgeführt werden.
VMwareVDMDS	Automatisch	Stellt LDAP-Verzeichnisdienste bereit. Dieser Dienst muss immer ausgeführt werden. Während Upgrade-Vorgängen von View stellt dieser Dienst sicher, dass vorhandene Daten korrekt migriert werden.

Dienste auf einem Sicherheitsserver

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

Tabelle 1-13. Dienste auf einem Sicherheitsserver

Dienstname	Starttyp	Beschreibung
VMware Horizon View Blast Secure Gateway	Automatisch	Stellt sichere HTML Access-Dienste bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu diesem Sicherheitsserver über ein HTML Access Secure Gateway herstellen.
VMware Horizon View- Sicherheitsserver	Automatisch	Stellt Sicherheitsserverdienste bereit. Dieser Dienst muss immer ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework- und Sicherheits-Gateway-Dienste gestartet oder beendet.
VMware Horizon View Framework- Komponente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework bereit. Dieser Dienst muss immer ausgeführt werden.
VMware Horizon View PCoIP Secure Gateway	Manuell	Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu diesem Sicherheitsserver über ein PCoIP Secure Gateway herstellen.
VMware Horizon View Security Gateway- Komponente	Manuell	Stellt gängige Gateway-Dienste bereit. Dieser Dienst muss immer ausgeführt werden.

Konfigurieren von Sicherheitsprotokollen und Cipher Suites auf einer View-Verbindungsserver-Instanz oder einem Sicherheitsserver

Sie können die Sicherheitsprotokolle und Cipher Suites konfigurieren, die von View-Verbindungsserver-Instanzen akzeptiert werden. Sie können eine globale Akzeptanzrichtlinie festlegen, die für alle View-Verbindungsserver-Instanzen in einer replizierten Gruppe gilt, oder Sie können eine Akzeptanzrichtlinie für einzelne View-Verbindungsserver-Instanzen und Sicherheitsserver festlegen.

Sie können auch die Sicherheitsprotokolle und Cipher Suites konfigurieren, die View-Verbindungsserver-Instanzen vorschlagen, wenn eine Verbindung zu vCenter Server und View Composer hergestellt wird. Sie können eine globale Vorschlagsrichtlinie festlegen, die für alle View-Verbindungsserver-Instanzen in einer replizierten Gruppe gilt. Sie können keine einzelnen Instanzen definieren, um eine globale Vorschlagsrichtlinie nicht anzuwenden.

Die Standardrichtlinien und die Vorgehensweisen für das Konfigurieren von Richtlinien haben sich in View 5.2 geändert. Informationen zu früheren View-Versionen finden Sie im VMware Knowledge Base-Artikel 1021466 unter <http://kb.vmware.com/kb/1021466>.

Standardmäßige globale Richtlinien für Sicherheitsprotokolle und Cipher Suites

Bestimmte Sicherheitsprotokolle und Cipher Suites werden in View 5.2 und neueren Versionen standardmäßig bereitgestellt. Die globalen Akzeptanz- und Vorschlagsrichtlinien sind standardmäßig sehr ähnlich.

Tabelle 1-14. Standardmäßige globale Richtlinien

Standardmäßige Sicherheitsprotokolle	Standardmäßige Cipher Suites
■ TLS 1.1	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
■ TLS 1.0	■ TLS_DHE_DSS_WITH_AES_128_CBC_SHA
■ SSLv2Hello (nur Akzeptanzrichtlinie)	■ TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	■ TLS_RSA_WITH_AES_128_CBC_SHA
	■ SSL_RSA_WITH_RC4_128_SHA

Sie können die Standardrichtlinien auf folgende Weise ändern.

- Wenn alle Clients, die eine Verbindung herstellen, TLS 1.1 unterstützen, können Sie TLS 1.0 und SSLv2Hello aus der Akzeptanzrichtlinie entfernen.
- Sie können TLS 1.2 zur Akzeptanz- und Vorschlagsrichtlinie hinzufügen. Dann wird TLS 1.2 ausgewählt, wenn TLS 1.2 am anderen Ende der Verbindung unterstützt wird.
- Wenn alle Clients, die eine Verbindung herstellen, AES Cipher Suites unterstützen, können Sie SSL_RSA_WITH_RC4_128_SHA aus der Akzeptanzrichtlinie entfernen.

Aktualisierung von JCE-Richtliniendateien zur Unterstützung hochverschlüsselter Cipher Suites

Sie können für mehr Sicherheit hochverschlüsselte Cipher Suites hinzufügen, müssen aber erst die Richtliniendateien `local_policy.jar` und `US_export_policy.jar` für JRE 7 auf jeder View-Verbindungsserver-Instanz und jedem Sicherheitsserver aktualisieren. Sie aktualisieren diese Richtliniendateien, indem Sie „Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7“ von der Oracle Java SE Download-Website herunterladen.

Wenn Sie hochverschlüsselte Cipher Suites in die Liste aufnehmen und die Richtliniendateien nicht ersetzen, können Sie den VMware Horizon View-Verbindungsserver-Dienst nicht neu starten.

Die Richtliniendateien befinden sich im Verzeichnis `C:\Programme\VMware\VMware View\Server\jre\lib\security`.

Weitere Informationen zum Herunterladen von „JCE Unlimited Strength Jurisdiction Policy Files 7“ finden Sie auf der Oracle Java SE Download-Website: <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

Nachdem Sie die Richtliniendateien aktualisiert haben, müssen Sie Backups der Dateien erstellen. Wenn Sie die View-Verbindungsserver-Instanz oder den Sicherheitsserver aktualisiert haben, werden womöglich alle Änderungen, die Sie an diesen Dateien vorgenommen haben, überschrieben, und Sie müssen die Dateien aus dem Backup wiederherstellen.

Konfigurieren globaler Akzeptanz- und Vorschlagsrichtlinien

Die standardmäßigen globalen Akzeptanz- und Vorschlagsrichtlinien werden in den View LDAP-Attributen festgelegt. Diese Richtlinien gelten für alle View-Verbindungsserver-Instanzen in einer replizierten Gruppe. Sie können View LDAP auf einer beliebigen View-Verbindungsserver-Instanz bearbeiten, um eine globale Richtlinie zu ändern.

Jede Richtlinie ist ein einwertiges Attribut an folgendem View LDAP-Ort:
cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int

In View LDAP definierte globale Akzeptanz- und Vorschlagsrichtlinien

Sie können die View LDAP-Attribute bearbeiten, die die globalen Akzeptanz- und Vorschlagsrichtlinien definieren.

Globale Akzeptanzrichtlinien

Das folgende Attribut führt Sicherheitsprotokolle auf. Sie müssen die Liste sortieren, indem Sie das neueste Protokoll an den Anfang stellen:

```
pae-ServerSSLSecureProtocols = "\LIST:TLSv1.1,TLSv1"
```

Das folgende Attribut führt die Cipher Suites auf. Die Reihenfolge der Cipher Suites ist unwichtig. Dieses Beispiel zeigt eine verkürzte Liste:

```
pae-ServerSSLCipherSuites = "\LIST:TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_
WITH_AES_128_CBC_SHA"
```

Globale Vorschlagsrichtlinien

Das folgende Attribut führt Sicherheitsprotokolle auf. Sie müssen die Liste sortieren, indem Sie das neueste Protokoll an den Anfang stellen:

```
pae-ClientSSLSecureProtocols = "\LIST:TLSv1.1,TLSv1"
```

Das folgende Attribut führt die Cipher Suites auf. Diese Liste sollte in der gewünschten Reihenfolge sortiert sein. Stellen Sie die bevorzugte Cipher Suite an den Anfang der Liste und sortieren Sie die restlichen Cipher Suites nach Ihrer Präferenz. Dieses Beispiel zeigt eine verkürzte Liste:

```
pae-ClientSSLCipherSuites = "\LIST:TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_
WITH_AES_128_CBC_SHA"
```

Ändern der globalen Akzeptanz- und Vorschlagsrichtlinien

Mit dem Dienstprogramm ADSI-Editor können Sie die View LDAP-Attribute bearbeiten, um die globalen Akzeptanz- und Vorschlagsrichtlinien für Sicherheitsprotokolle und Cipher Suites zu ändern.

Voraussetzungen

- Machen Sie sich mit den View LDAP-Attributen vertraut, die die Akzeptanz- und Vorschlagsrichtlinien definieren. Siehe [In View LDAP definierte globale Akzeptanz- und Vorschlagsrichtlinien](#).
- Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogrammes ADSI-Editor mit Ihrer Windows Server-Betriebssystemversion.

Verfahren

- 1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem View-Verbindungsserver-Computer.

- 2 Wählen Sie im Konsolenbaum **Verbinden mit**.
- 3 Geben Sie im Textfeld **Definierten Namen oder Namenskontext auswählen bzw. eintippen** den definierten Namen **DC=vdi**, **DC=vmware**, **DC=int** ein.
- 4 Wählen Sie im Textfeld **Domäne oder Server auswählen bzw. eintippen** **localhost:389** oder den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) des View-Verbindungsserver-Computers gefolgt von Port 389 aus bzw. geben Sie dies ein.

Beispiel: **localhost:389** oder **mycomputer.mydomain.com:389**
- 5 Erweitern Sie den Baum vom ADSI-Editor, erweitern Sie **OU=Properties**, wählen Sie **OU=Global** und wählen Sie **OU=Common** im rechten Fensterbereich aus.
- 6 Wählen Sie beim Objekt **CN=Common, OU=Global, OU=Properties** jedes Attribut aus, das Sie ändern möchten, und geben Sie die neue Liste von Sicherheitsprotokollen oder Cipher Suites ein.
- 7 Starten Sie den VMware Horizon View-Verbindungsserver-Dienst neu.

Konfigurieren der Akzeptanzrichtlinien auf einzelnen View Servern

Zur Angabe einer lokalen Akzeptanzrichtlinie auf einer einzelnen View-Verbindungsserver-Instanz oder einem einzelnen Sicherheitsserver müssen Sie Eigenschaften zur Datei `locked.properties` hinzufügen. Wenn die Datei `locked.properties` noch nicht auf dem View Server vorhanden ist, müssen Sie diese erstellen.

Sie müssen einen Eintrag `secureProtocols.n` für jedes Sicherheitsprotokoll hinzufügen, das Sie konfigurieren möchten. Verwenden Sie die folgende Syntax: `secureProtocols.n=security protocol`.

Sie fügen einen Eintrag `enabledCipherSuite.n` für jede Cipher Suite hinzu, die Sie konfigurieren möchten. Verwenden Sie die folgende Syntax: `enabledCipherSuite.n=cipher suite`.

Die Variable *n* ist eine Ganzzahl, die Sie in aufsteigender Folge (1, 2, 3) an jeden Eintragstyp anhängen.

Vergewissern Sie sich, dass die Einträge in der Datei `locked.properties` die korrekte Syntax aufweisen und dass die Namen der Cipher Suites und Sicherheitsprotokolle korrekt geschrieben sind. Jegliche Fehler in der Datei können dazu führen, dass der Austausch zwischen Client und Server fehlschlägt.

Verfahren

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

Beispiel: `install_directory\VMware\VMware View\Server\sslgateway\conf\`
- 2 Fügen Sie die Einträge `secureProtocols.n` und `enabledCipherSuite.n` hinzu, einschließlich der verknüpften Sicherheitsprotokolle und Cipher Suites.
- 3 Speichern Sie die Datei `locked.properties`.
- 4 Starten Sie den VMware Horizon View-Verbindungsserver- oder VMware Horizon View-Sicherheitsserver-Dienst neu, damit die Änderungen wirksam werden.

Beispiel: Standard-Akzeptanzrichtlinien auf einem einzelnen Server

Das folgende Beispiel zeigt die Einträge in der Datei `locked.properties`, die zur Angabe der Standardrichtlinien benötigt werden:

```
# The following list should be ordered with the latest protocol first:

secureProtocols.1=TLSv1.1
secureProtocols.2=TLSv1
secureProtocols.3=SSLv2Hello

# This setting must be the latest protocol given in the list above:

preferredSecureProtocol=TLSv1.1

# The order of the following list is unimportant:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.2=TLS_DHE_DSS_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_DHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.4=TLS_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.5=SSL_RSA_WITH_RC4_128_SHA
```

IETF-Standards

View-Verbindungsserver und -Sicherheitsserver entsprechen bestimmten Internet Engineering Task Force (IETF)-Standards.

- Transport Layer Security (TLS) von RFC 5746 – Die Anzeige-Erweiterung der Neuverhandlung, auch als sichere Neuverhandlung bezeichnet, ist standardmäßig aktiviert.
- HTTP Strict Transport Security (HSTS) von RFC 6797, auch als Transportsicherheit bezeichnet, ist standardmäßig aktiviert.
- HTTP Header Field X-Frame-Optionen von RFC 7034, auch als Zähler-Clickjacking bezeichnet, sind standardmäßig deaktiviert. Sie können sie aktivieren, indem Sie die Eingabe `x-frame-options=<options>` zur Datei `locked.properties` hinzufügen. Weitere Informationen zum Hinzufügen von Eigenschaften zur Datei `locked.properties` finden Sie unter [Konfigurieren der Akzeptanzrichtlinien auf einzelnen View Servern](#). Der Parameter `<options>` kann einen der folgenden Werte enthalten, bei denen die Groß-/Kleinschreibung berücksichtigt wird:
 - OFF -Das Zähler-Clickjacking deaktivieren (Standardeinstellung).
 - DENY -Keine Frames verwenden.
 - SAMEORIGIN -Keine fremden Frames verwenden.
 - ALLOW-FROM <URL> -Keine fremden Frames verwenden außer <URL>, wobei <URL> einen zusätzlichen vertrauenswürdigen Ursprung angibt.

Weitere Informationen zu RFC 7034 finden Sie unter <http://tools.ietf.org/html/rfc7034>.

Hinweis Das Zähler-Clickjacking verhindert den ordnungsgemäßen Einsatz von HTML Access, wenn ein standardmäßig deaktiviertes Blast Secure Gateway (BSG) verwendet wird.

Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) stellt sicher, dass die Kompromittierung einer SSL-Sitzung nicht die Kompromittierung von anderen SSL-Sitzungen bedeutet, die dasselbe Serverzertifikat verwenden. Es handelt sich um eine Eigenschaft von Verschlüsselungssammlungen mit DHE in deren Namen. Von den fünf Verschlüsselungssammlungen, die wir standardmäßig aktivieren, haben drei diese Eigenschaft. Der Nachteil von PFD ist die geringere Leistung, so dass ein Gleichgewicht gefunden werden muss.

View unterstützt DHE-DSS, DHE-RSA und ECDHE-RSA-Verschlüsselungssammlungen. Die ersten beiden können in Verbindung mit Standard-DSS- oder RSA-Zertifikaten aktiviert werden. ECDHE-RSA bietet eine bessere Leistung, benötigt aber ein ECC-Zertifikat, das mit einem RSA-Schlüssel signiert ist. Fordern Sie von einer Zertifizierungsstelle kein ECC-Zertifikat an, das mit einem EC-Schlüssel signiert ist, da View dies nicht verwenden kann.