Diese Hinweise bitte lesen! Das Setup von View wird damit einfacher!

Lesen Sie diese Hinweise in einer der folgenden Sprachen:
Français Deutsch 简体中文 日本語 한국어

Nach den von uns in View 5.1 und späteren Versionen vorgenommenen Änderungen unterscheidet sich die Konfiguration der View-Komponenten in mancher Hinsicht gegenüber früheren Versionen. Mithilfe dieser Hinweise können Sie etwaige Schwierigkeiten bei der Installation von View 5.1 oder einer späteren Version bzw. beim Upgrade auf View 5.1 oder eine spätere Version vermeiden.

Hinweis: Wenn Sie das Upgrade von View 5.1 oder einer späteren Version aus vornehmen, sollten Sie diese Konfigurationsschritte bereits durchgeführt haben. Prüfen Sie Ihr View-Setup mithilfe dieser Hinweise.

1) Ein Downgrade von einem View 5.1-Verbindungsserver oder einer späteren Version auf vorherige Versionen ist nicht möglich.

In View 5.1 oder einer späteren Version ist die View LDAP-Konfiguration verschlüsselt und kann nicht von früheren View-Versionen verwendet werden.

- Nach dem Upgrade einer View-Verbindungsserver-Instanz auf View 5.1 oder eine spätere Version kann für diese Instanz kein Downgrade auf eine frühere Version durchgeführt werden.
- Nach dem Upgrade aller View-Verbindungsserver-Instanzen in einer replizierten Gruppe ist es nicht möglich, eine weitere Instanz mit einer älteren View-Version hinzuzufügen.

Hinweis: Downgrades wurden nie unterstützt, funktionierten jedoch in vorherigen Versionen. Dies ist nun nicht mehr der Fall.

2) vCenter Server- und View Composer-Hosts benötigen gültige SSL-Zertifikate.

- *Beste Vorgehensweise*: Stellen Sie sicher, dass vCenter Server und View Composer über Zertifikate von einer Zertifizierungsstelle verfügen:
    - Installieren Sie ein von einer Zertifizierungsstelle signiertes SSL-Zertifikat auf dem Windows Server, auf dem der vCenter Server installiert ist.
    - Verfahren Sie ebenso für View Composer. Wenn Sie View Composer und vCenter Server auf demselben Host installieren, können diese dasselbe Zertifikat verwenden. Sie müssen das Zertifikat jedoch für jede Komponente separat konfigurieren.

      * Wenn Sie vor der Installation von View Composer ein Zertifikat installieren, können Sie Ihr Zertifikat während der View Composer-Installation auswählen.

      * Wenn Sie das Standardzertifikat zu einem späteren Zeitpunkt ersetzen, führen Sie den Befehl *SviConfig ReplaceCertificate* aus, um das neue Zertifikat an den von View Composer verwendeten Port zu binden.
    - Stellen Sie sicher, dass die Zertifizierungsstelle für die neuen Zertifikate sowie sämtliche übergeordnete Zertifizierungsstellen von allen Windows-Servern mit installierter View-Verbindungsserver-Instanz als vertrauenswürdig eingestuft werden.

- *Alternative*: Akzeptieren Sie nach dem Hinzufügen von vCenter Server und View Composer zu View den Fingerabdruck des Standardzertifikats für View Composer, indem Sie in View Administrator auf **Überprüfen** klicken. Verfahren Sie ebenso für vCenter Server.

Weitere Informationen: Siehe „Konfigurieren von SSL-Zertifikaten für View Servers“ im Handbuch zur *View-Installation*.

3) Sicherheitsserver- und View-Verbindungsserver-Hosts benötigen gültige SSL-Zertifikate.

- *Beste Vorgehensweise*: Öffnen Sie nach der Installation einer View-Verbindungsserver-Instanz bzw. eines Sicherheitsservers auf einem Windows Server-Host den Windows Server-Zertifikatspeicher und führen Sie die folgenden Schritte durch:
    - Importieren Sie ein von einer Zertifizierungsstelle signiertes und von Ihren Clients überprüfbares SSL-Zertifikat.
    - Stellen Sie sicher, dass die gesamte Zertifikatskette, einschließlich Zwischenzertifikaten und Stammzertifikat, installiert wird.
    - Stellen Sie sicher, dass das Zertifikat über einen privaten Schlüssel verfügt, und markieren Sie diesen Schlüssel als exportierbar.
    - Konfigurieren Sie den Anzeigenamen des Zertifikats als *vdm*.
- *Alternative*: Lassen Sie vom View Server-Installationsprogramm ein Standardzertifikat im Windows Server-Zertifikatspeicher erstellen. Das Zertifikat ist selbstsigniert und wird in View Administrator als ungültig angezeigt.
- *Upgrade auf View 5.1 oder eine spätere Version*: Wenn Ihre ursprünglichen View Server bereits über von einer Zertifizierungsstelle signierte SSL-Zertifikate verfügen, sind keine weiteren Schritte Ihrerseits erforderlich. Während des Upgrades importiert View Ihre Zertifikate in den Windows Server-Zertifikatspeicher.

  Wenn Ihre ursprünglichen View Server über Standardzertifikate verfügen, aktualisieren Sie Ihre View Server und befolgen Sie die oben unter *Beste Vorgehensweise* beschriebenen Schritte.

Weitere Informationen: Siehe „Konfigurieren von SSL-Zertifikaten für View Servers“ im Handbuch zur *View-Installation*.

4) Zertifikate für vCenter Server, View Composer und View Server müssen Zertifikatssperrlisten (CRLs) enthalten.

View validiert Zertifikate ohne Zertifikatssperrliste nicht.

- *Beste Vorgehensweise*: Führen Sie bei Bedarf die folgenden Schritte durch:
    - Fügen Sie Ihrem Zertifikat eine Zertifikatssperrliste hinzu.
    - Importieren Sie das aktualisierte Zertifikat in den Windows-Zertifkatspeicher auf dem vCenter Server-, View Composer- und View Server-Host.

- *Alternative*: Ändern Sie die Registrierungseinstellungen, die die Überprüfung der Zertifikatssperrliste steuern.

Weitere Informationen: Siehe „Konfigurieren der Zertifikatssperrüberprüfung bei Serverzertifikaten“ im Handbuch zur *View-Installation*.

Hinweis: Wenn Ihre Firma Proxy-Einstellungen für den Internetzugriff verwendet, müssen Sie möglicherweise Ihre View-Verbindungsserver-Computer konfigurieren, um sie nutzen zu können. Mit diesem Schritt wird sichergestellt, dass die Server auf Zertifikatssperrüberprüfungs-Sites im Internet zugreifen können. Sie können Microsoft *Netshell*-Befehle verwenden, um die Proxy-Einstellungen zum View-Verbindungsserver zu importieren.

5) Auf Sicherheitsserver- und View-Verbindungsserver-Hosts muss die Windows-Firewall mit erweiterter Sicherheit aktiviert sein.

Standardmäßig steuern IPsec-Regeln die Verbindungen zwischen dem View-Sicherheitsserver und dem View-Verbindungsserver und erfordern die Aktivierung einer Windows-Firewall mit erweiterter Sicherheit.

- *Beste Vorgehensweise*: Legen Sie für die Windows-Firewall mit erweiterter Sicherheit die Option **Ein** fest, bevor Sie die View Server installieren. Stellen Sie sicher, dass die Windows-Firewall für alle aktiven Profile auf **Ein** gestellt ist. Empfehlung: Wählen Sie die Option **Ein** am besten für *alle* Profile aus.

- *Alternative*: Öffnen Sie vor der Installation von Sicherheitsservern View Administrator und deaktivieren Sie die globale Einstellung *IPSec für Sicherheitsserververbindungen verwenden*, indem Sie die Option **Nein** einstellen. (Dies wird nicht empfohlen.)

6) Back-End-Firewalls müssen zur Unterstützung von IPsec eingerichtet sein.

Wenn zwischen Sicherheitsservern und View-Verbindungsserver-Instanzen eine Back-End-Firewall vorhanden ist, müssen Sie Firewall-Regeln konfigurieren, damit die Verbindungen funktionieren.

Weitere Informationen: Siehe „Konfigurieren einer Back-End-Firewall zur Unterstützung von IPsec“ im Handbuch zur *View-Installation*.

7) View Client-Instanzen müssen HTTPS für View-Verbindungen verwenden.

View-Verbindungsserver-Instanzen und Sicherheitsserver verwenden SSL für Clientverbindungen.

- Wenn sich View Client-Instanzen über ein zwischengeschaltetes Gerät mit SSL-Offloading-Funktion verbinden, müssen Sie das SSL-Zertifikat des zwischengeschalteten Geräts auf dem View-Verbindungsserver oder auf dem Sicherheitsserver installieren.

- Die Verbindung muss über HTTPS erfolgen, unabhängig davon, ob sich eine View Client-Instanz über ein zwischengeschaltetes Gerät, beispielsweise ein Lastenausgleichsmodul, verbindet. Wenn Sie ein zwischengeschaltetes Gerät verwenden und die Verbindung zwischen dem zwischengeschalteten Gerät und dem View Server über HTTP erfolgen soll (SSL-Offloading), dann konfigurieren Sie die Datei *locked.properties* auf dem View Server.

- Ältere View Client-Versionen, bei denen HTTPS abgewählt werden kann, erhalten einen Fehler, wenn Benutzer HTTP auswählen. Bisher wurden die Benutzer im Hintergrund an HTTPS umgeleitet. Clients, die keine SSL-Verbindungen herstellen können, ist es nicht möglich, sich mit View zu verbinden.

Weitere Informationen: Siehe „Offloading von SSL-Verbindungen auf Zwischenserver“ im Handbuch zur *Verwaltung von View*.

8) Für verschlüsselte und bereinigte View-Sicherungen sind neue Schritte zur Wiederherstellung erforderlich.

Standardmäßig sind Sicherungen von View 5.1 oder späteren Versionen verschlüsselt. Es ist auch möglich, View-Sicherungen zu bereinigen (Kennwörter und andere vertrauliche Daten aus den Sicherungsdaten ausschließen) oder in Form einfachen Texts zu sichern (nicht empfohlen).

- Um eine verschlüsselte Sicherung wiederherzustellen, müssen Sie zunächst die Daten entschlüsseln. Sie müssen das Kennwort für die Datenwiederherstellung verwenden, das Sie während der Installation vom View-Verbindungsserver festgelegt haben.

- Stellen Sie keine bereinigten Sicherungen wieder her. Daten wie Kennwörter fehlen dann in Ihrer View LDAP-Konfiguration. View-Komponenten funktionieren ohne diese Daten nicht einwandfrei. Um die normale Funktionsweise wiederherzustellen, müssen Sie mithilfe von View Administrator alle Kennwörter und andere fehlende Datenelemente manuell zurücksetzen.

Weitere Informationen: Siehe „Sichern und Wiederherstellen von View-Konfigurationsdaten“ im Handbuch zur *Verwaltung von View*.

9) Vor dem Upgrade oder der Neuinstallation eines View 5.1-Sicherheitsservers oder einer späteren Version müssen Sie die entsprechenden IPsec-Regeln von der kombinierten View-Verbindungsserver-Instanz entfernen, damit neue Regeln festgelegt werden können.

- Wählen Sie in View Administrator den Sicherheitsserver aus und klicken Sie auf **Weitere Befehle > Auf Upgrade oder Neuinstallation vorbereiten**.

  Hinweis: Sie müssen einen Sicherheitsserver nicht aus View entfernen, bevor Sie den Server aktualisieren oder neu installieren.

Weitere Informationen: Siehe „Vorbereiten eines Upgrades oder einer Neuinstallation eines Sicherheitsservers“ im Handbuch zur *View-Installation*.