Dell Security Management Server Virtual

Schnellstart- und Installationshandbuch v10.2.5

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

2019 - 06

Rev. A01

Inhaltsverzeichnis

1

Erste Schritte

Die Schnellstartanleitung ist für erfahrenere Anwender konzipiert, die DDP Dell Server schnell einrichten und starten möchten. Im Allgemeinen empfiehlt Dell, zuerst Dell Server zu installieren, gefolgt von der Installation der Clients.

Detailliertere Anweisungen finden Sie im Installationshandbuch für Security Management Server Virtual.

Weitere Informationen zu den Voraussetzungen von Dell Server finden Sie unter Security Management Server Virtual – Voraussetzungen, Voraussetzungen für die Verwaltungskonsole und Proxy-Modus-Voraussetzungen.

Informationen zum Aktualisieren eines vorhandenen Dell Server, siehe Aktualisierung von Security Management Server Virtual.

Installation

1 Navigieren Sie zum Verzeichnis, wo die Dell Data Security-Dateien gespeichert werden, und doppelklicken Sie, um in VMware Security Management Server Virtual **v10.x.x Build x.ova** zu importieren.

> **ANMERKUNG: OVA ist jetzt mit SHA256 signiert und kann innerhalb des VMware Thick Clients nicht importiert werden. Informationen finden Sie unter https://kb.vmware.com/s/article/2151537.**

2 Schalten Sie Security Management Server Virtual an.

3 Befolgen Sie die Anweisungen auf dem Bildschirm.

Konfiguration

Bevor Sie Benutzer aktivieren, müssen Sie folgende Konfigurationsaufgaben am Security Management Server Virtual-Terminal ausführen:

- SMTP-Einstellungen konfigurieren
- Import eines bestehenden Zertifikats oder Registrierung eines neuen Serverzertifikats
- Aktualisierung von Security Management Server Virtual
- Installieren Sie einen FTP-Client, der SFTP an Port 22 unterstützt und richten Sie Dateiübertragung (FTP)-Benutzer ein.

  Wenn Ihr Unternehmen über externe Geräte verfügt, siehe Proxy-Modus installieren und konfigurieren.

Öffnen der Verwaltungskonsole

Öffnen Sie die Verwaltungskonsole unter dieser Adresse: https://server.domain.com:8443/webui/

Die Standard-Anmeldeinformationen lauten **superadmin/changeit**.

Eine Liste der unterstützten Webbrowser finden Sie unter Voraussetzungen für die Verwaltungskonsole.

Administrative Aufgaben

Wenn Sie die Verwaltungskonsole noch nicht gestartet haben, tun Sie dies jetzt. Die Standard-Anmeldeinformationen lauten **superadmin/changeit**.

Dell empfiehlt, Administratorrollen so bald wie möglich zuzuweisen. Um diese Aufgabe jetzt abzuschließen, siehe Dell Administratorrolle zuweisen.

Klicken Sie auf „?“ in der oberen rechten Ecke der Verwaltungskonsole, um *AdminHelp* zu starten. Die Seite „*Erste Schritte*“ wird angezeigt. Klicken Sie auf **Domänen hinzufügen**.

Für Ihre Organisation wurden grundlegende Richtlinien festgelegt, aber je nach Ihren Anforderungen sollten diese wie folgt geändert werden (für alle Aktivierungen sind Lizenzen und Berechtigungen erforderlich):

- Richtlinienbasierte Verschlüsselung wird mit Verschlüsselung durch einen allgemeinen Schlüssel aktiviert.
- Computer mit selbstverschlüsselnden Laufwerken werden verschlüsselt.
- BitLocker Management ist nicht aktiviert
- Advanced Threat Prevention ist nicht aktiviert
- Der Bedrohungsschutz ist deaktiviert.
- Externe Medien werden nicht verschlüsselt.
- Ports werden nicht durch die Portsteuerung verwaltet.
- Geräte, auf denen die vollständige Datenträgerverschlüsselung installiert ist, werden nicht verschlüsselt.
- Data Guardian ist deaktiviert.

Im Hilfethema *Richtlinien verwalten* der AdminHelp finden Sie Anweisungen zum Navigieren zu Technologiegruppen und Richtlinienbeschreibungen.

Die Ersten Schritte sind damit abgeschlossen.

2

Detailliertes Installationshandbuch

Dieses Installationshandbuch soll weniger erfahrenen Benutzern bei der Installation und Konfiguration von Security Management Server Virtual. Im Allgemeinen empfiehlt Dell, zuerst Security Management Server Virtual zu installieren, gefolgt von der Installation der Clients.

Informationen zum Aktualisieren einer vorhandenen Security Management Server Virtual, siehe Aktualisierung von Security Management Server Virtual.

Info über Security Management Server Virtual

Mit der Verwaltungskonsole können Administratoren den Status der Endpunkte, die Richtliniendurchsetzung und den Schutz für das gesamte Unternehmen überwachen. Der Proxy-Modus bietet eine Front-End-DMZ-Modus-Option für die Verwendung mit Security Management Server Virtual.

Security Management Server Virtual verfügt über die folgenden Funktionen:

- Zentrale Verwaltung von bis zu 3,500 Geräten
- Erstellung und Verwaltung rollenbasierter Sicherheitsrichtlinien
- Gerätewiederherstellung durch einen Administrator
- Aufteilung administrativer Aufgaben
- Automatische Verteilung von Sicherheitsrichtlinien
- Vertrauenswürdige Kommunikation zwischen Komponenten
- Generierung eindeutiger Verschlüsselungsschlüssel und automatische, sichere Schlüsselhinterlegung
- Zentrale Compliance-Prüfverfahren und -Berichterstellung
- Automatische Erzeugung von selbstsignierten Zertifikaten

Kontaktaufnahme mit dem Dell ProSupport

Telefonischen Support rund um die Uhr für Ihr Dell Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

Zusätzlich steht Ihnen unser Online-Support für Dell Produkte unter dell.com/support zur Verfügung. Der Online-Support enthält Treiber, Handbücher, technische Ratgeber, FAQs und eine Beschreibung festgestellter Probleme.

Halten Sie bei Ihrem Anruf Ihre Service-Tag-Nummer oder Ihren Express-Servicecode bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

Telefonnummern außerhalb der Vereinigten Staaten finden Sie unter Dell ProSupport – Internationale Telefonnummern.

Anforderungen

Security Management Server Virtual

Hardware

Der empfohlene Speicherplatz für Security Management Server Virtual ist 80 GB.

Virtuelle Umgebung

Security Management Server Virtual v10.2.5 wurde mit den folgenden Virtualisierungsumgebungen validiert.

Dell unterstützt derzeit das Hosten von Dell Security Management Server oder Dell Security Management Server Virtual innerhalb einer in der Cloud gehosteten Infrastructure-as-a-Service (IaaS)-Umgebung, wie z. B. Amazon Web Services, Azure und mehrere andere Anbieter. Der Support für diese Umgebungen ist nur auf die Funktionalität der Anwendungsserver beschränkt, die innerhalb dieser Virtual Machines gehostet werden; die Verwaltung und Sicherheit von diesen Virtual Machines liegen in der Verantwortung des Administrators der IaaS-Lösung.

Zusätzliche Anforderungen an die Infrastruktur (Active Directory sowie SQL Server für Dell Security Management Server) sind immer noch erforderlich für die ordnungsgemäße Funktion.

Virtuelle Umgebungen

- VMware Workstation 12.5
  - 64-Bit-CPU erforderlich
  - 8 GB RAM erforderlich
  - 80 GB Festplattenspeicherplatz
  - Hostcomputer mindestens mit Doppelkern
  - Unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Weitere Informationen finden Sie unter https://kb.vmware.com/s/article/1003746
- VMware Workstation 14.0
  - 64-Bit-CPU erforderlich
  - 8 GB RAM erforderlich
  - 80 GB Festplattenspeicherplatz
  - Hostcomputer mindestens mit Doppelkern
  - Unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Weitere Informationen finden Sie unter https://kb.vmware.com/s/article/1003746
- VMware Workstation 14.1
  - 64-Bit-CPU erforderlich
  - 8 GB RAM erforderlich
  - 80 GB Festplattenspeicherplatz
  - Hostcomputer mindestens mit Doppelkern
  - Unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Weitere Informationen finden Sie unter https://kb.vmware.com/s/article/1003746
- VMware ESXi 6.5
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM erforderlich
  - 80 GB Festplattenspeicherplatz
  - Ein Betriebssystem ist nicht erforderlich
  - Unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme.
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen

- Weitere Informationen finden Sie unter https://kb.vmware.com/s/article/1003746

- VMware ESXi 6.0
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM erforderlich
  - 80 GB Festplattenspeicherplatz
  - Ein Betriebssystem ist nicht erforderlich
  - Unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme.
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Weitere Informationen finden Sie unter https://kb.vmware.com/s/article/1003746

- VMware ESXi 5.5
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM erforderlich
  - 80 GB Festplattenspeicherplatz
  - Ein Betriebssystem ist nicht erforderlich
  - Unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme.
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Weitere Informationen finden Sie unter https://kb.vmware.com/s/article/1003746

- Hyper-V-Server (Vollständige oder Core-Installation)
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM erforderlich
  - 80 GB Festplattenspeicherplatz
  - Ein Betriebssystem ist nicht erforderlich
  - Die Hardware muss die Mindestanforderungen für Hyper-V erfüllen.
  - Muss als virtuelle Maschine der 1. Generation ausgeführt werden.

ANMERKUNG: Zu Informationen zum Einrichten von Hyper-V befolgen Sie die Anweisungen für Endpunkt-Betriebssysteme: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v oder für Server-Betriebssysteme: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.

Management Console

Internet-Browser

ANMERKUNG:
Der Browser muss Cookies akzeptieren.

Die folgende Tabelle führt unterstützte Internet-Browser auf.

Internet-Browser

- Internet Explorer 11.x oder höher
- Internet Explorer 41.x oder höher
- Google Chrome 46.x oder höher

<1>Proxy-Modus</1>

Hardware

In der folgenden Tabelle werden die *Hardware-Mindestanforderungen* aufgelistet:

Prozessor

Moderne Dual-Core-CPU (1,5 Ghz +)

RAM

2 GB dedizierter RAM mindestens/4 GB dedizierter RAM empfohlen

Freier Speicherplatz

1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher)

Netzwerkkarte

Netzwerkschnittstellenkarte 10/100/1000

Sonstiges

IPv4, IPv6 oder eine Kombination aus IPv4 und IPv6 werden unterstützt.

Software

Die folgende Tabelle enthält genauere Informationen zu der Software, die zur Installation des Proxy-Modus-Servers erforderlich ist.

Voraussetzungen
• **Windows Installer 4.0 oder höher** Auf dem für die Installation vorgesehenen Server muss Windows Installer 4.0 oder eine spätere Version installiert sein.
• **Microsoft Visual C++ 2010 Redistributable Package** Wenn sie nicht installiert ist, installiert der Installer sie für Sie.
• **Microsoft .NET Framework Version 4.5.2** Für .NET Framework Version 4.5.2 hat Microsoft Sicherheitsupdates veröffentlicht.

ANMERKUNG:

Universal Account Control (UAC) muss deaktiviert sein, wenn die Installation in einem geschützten Verzeichnis stattfindet. Nach der Deaktivierung des UAC, muss der Server neu gestartet werden, damit diese Änderungen in Kraft treten.

Registrierungspfad für Windows Server: HKLM\SOFTWARE\Dell.

In der folgenden Tabelle sind die Anforderungen an die Software für den Proxy-Modus-Server aufgelistet.

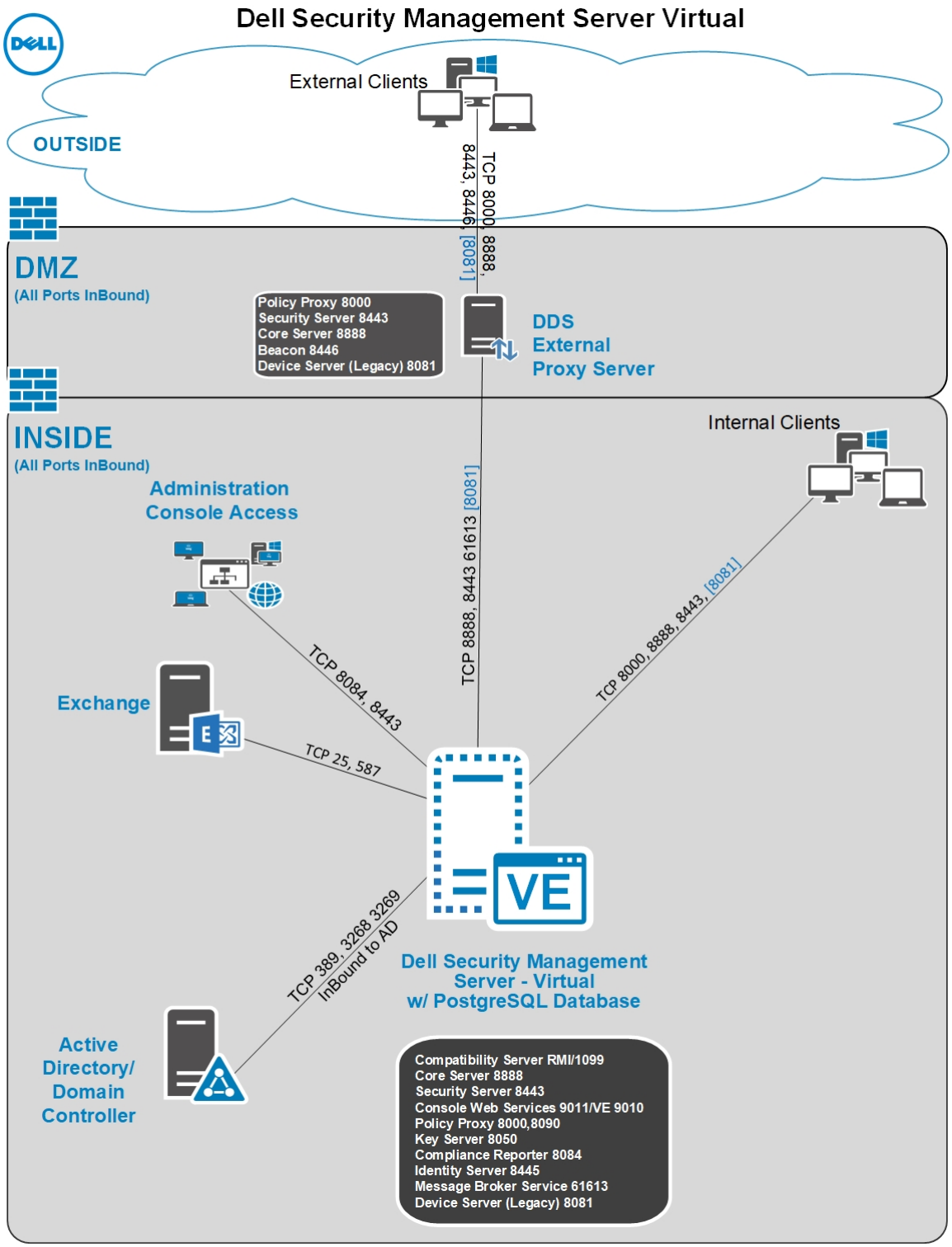
Betriebssystem
· **Windows Server 2019** - Standard Edition - Datacenter Edition
· **Windows Server 2016** - Standard Edition - Datacenter Edition
· **Windows Server 2012 R2** - Standard Edition - Datacenter Edition
· **LDAP-Repository** - Active Directory 2008 R2 - Active Directory 2012 R2 - Active Directory 2016

Architektur-Design von Security Management Server Virtual

Die Dell Encryption-Lösungen Endpoint Security Suite Enterprise und Data Guardian sind basierend auf der Anzahl an Endpunkten zur Verschlüsselung in Ihrer Organisation hochgradig skalierbare Produkte.

Architekturkomponenten

Im Folgenden ist eine einfache Bereitstellung für Dell Security Management Server Virtual beschrieben.



Herunterladen und Installieren der OVA-Datei

Bei der Erstinstallation wird Security Management Server Virtual als OVA-Datei bereitgestellt. Das Open Virtual Application-Format wird zur Bereitstellung von Software für die Ausführung auf virtuellen Maschinen verwendet. Die OVA-Datei steht unter www.dell.com/support auf den Produkt-Supportseiten der folgenden Dell Data Security-Produkte bereit:

- Verschlüsselung

- Endpoint Security Suite Enterprise
- Data Guardian

So laden Sie die OVA-Datei herunter:

1 Navigieren Sie zur Seite *Treiber und Downloads* für das oben aufgeführte Produkt.
2 Klicken Sie auf **Treiber und Downloads**.
3 Wählen Sie die entsprechende VMware ESXi-Version.
4 Laden Sie das entsprechende Paket herunter.

So installieren Sie die OVA-Datei:

Stellen Sie vor Beginn sicher, dass alle Anforderungen an die Systeme und die virtuelle Umgebung erfüllt sind.

1 Suchen Sie auf dem Dell Installationsmedium *Security Management Server Virtual v9.x.x.x Build x.ova* und doppelklicken Sie darauf, um die Datei in VMware zu importieren.

> **ANMERKUNG: Bei Verwendung von Hyper-V anstelle von VMware befolgen Sie die Anweisungen für Windows 10 https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/. Bei serverbasierten Betriebssystemen befolgen Sie die Anweisungen: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server. Wenn Sie ESXi anstelle von VMware verwenden, befolgen Sie diese Anweisungen:https://kb.vmware.com/s/article/2109708.**

2 Befolgen Sie die Anweisungen auf dem Bildschirm.

> **ANMERKUNG: Wenn der Import bei der Verwendung von VMware fehlschlägt, ist der Webclient der empfohlene Pfad zum Importieren der OVA-Datei. Weitere Informationen finden Sie unter https://kb.vmware.com/s/article/2151537.**

3 Schalten Sie Security Management Server Virtual an.
4 Wählen Sie die Sprache für die Lizenzvereinbarung aus und wählen Sie dann **EULA anzeigen** aus.
5 Lesen Sie die Vereinbarung durch und wählen Sie **EULA akzeptieren**.
6 Falls eine Aktualisierung verfügbar ist, klicken Sie auf **Annehmen**.
7 Wählen Sie **Verbundener Modus** oder **Getrennten Modus**.

> **ANMERKUNG:**
> Wenn Sie **Getrennter Modus** auswählen, kann der Modus nicht mehr in den verbundenen Modus geändert werden.
>
> Der getrennte Modus isoliert Dell Server aus dem Internet und einem ungesicherten LAN oder anderen Netzwerk. Alle Aktualisierungen müssen manuell durchgeführt werden. Weitere Informationen über den getrennten Modus und die Richtlinien finden Sie in der *AdminHelp*.

8 Geben Sie in *delluser-Kennwort einstellen* das aktuelle (Standard-)Passwort **delluser** und dann ein eindeutiges Kennwort ein. Wiederholen Sie es und wählen Sie **Anwenden** aus.

Passwörter müssen folgende Elemente enthalten:

- Mindestens 8 Zeichen
- Mindestens 1 Großbuchstaben
- Mindestens 1 Ziffer
- Mindestens 1 Sonderzeichen

> **ANMERKUNG: Es ist möglich, das Standardkennwort beizubehalten, indem Sie Abbrechen auswählen oder auf der Tastatur die Escape-Taste drücken.**

9 Wählen Sie **Schließen**, um das Fenster „Hostname konfigurieren“ aufzurufen.
10 Verwenden Sie in *Hostname konfigurieren* die Zurücktaste, um den Standardhostnamen zu entfernen. Geben Sie einen eindeutigen Hostnamen ein und wählen Sie **OK** aus.

11 Wählen Sie in *Netzwerkeinstellungen konfigurieren* eine der nachstehenden Optionen aus und wählen Sie dann **OK** aus.

- (Standard) DHCP verwenden (IPv4)
- (Empfohlen) Drücken Sie in *DHCP verwenden* die Leertaste, um das X zu entfernen, und geben Sie manuell die zutreffenden folgenden Adressen ein:

  Statische IP-Adresse

  Netzwerkmaske

  Standard-Gateway

  DNS-Server 1

  DNS-Server 2

  DNS-Server 3

  Für eine statische Konfiguration kann entweder IPv6 oder IPv4 gewählt werden.
- **ANMERKUNG: Bei Verwendung einer statischen IP-Adresse müssen Sie auch einen Host-Eintrag auf dem DNS-Server erstellen.**

12 Wenn Sie aufgefordert werden, die Zeitzone zu bestätigen, wählen Sie **OK** aus.

13 Wenn die Nachricht angibt, dass die erste Startkonfiguration abgeschlossen ist, wählen Sie **OK** aus.

14 SMTP-Einstellungen konfigurieren

15 Ein bestehendes Zertifikat importieren oder ein neues Serverzertifikat registrieren

16 Aktualisierung von Security Management Server Virtual.

17 Installieren Sie einen FTP-Client, der SFTP an Port 22 unterstützt und richten Sie Dateiübertragung (FTP)-Benutzer ein.

Die Installationsaufgaben für Security Management Server Virtual wurden abgeschlossen.

Öffnen der Verwaltungskonsole

Öffnen Sie die Verwaltungskonsole unter dieser Adresse: https://server.domain.com:8443/webui/

Die Standard-Anmeldeinformationen lauten **superadmin/changeit**.

Eine Liste der unterstützten Webbrowser finden Sie unter Voraussetzungen für die Verwaltungskonsole.

Proxy-Modus installieren und konfigurieren

Proxy-Modus bietet eine Front-End-Option (DMZ-Modus) für die Verwendung mit demDell Server. Wenn Sie Dell-Komponenten in Ihre DMZ implementieren möchten, vergewissern Sie sich, dass sie ausreichend vor Angriffen geschützt sind.

ANMERKUNG: Der Beacon-Dienst wird im Rahmen dieser Installation zur Unterstützung des Data Guardian-Rückrufsignals installiert. Dieser fügt zu jeder durch Data Guardian geschützten Datei beim Zulassen oder Erzwingen von geschützten Office-Dokumenten in der Umgebung ein Rückrufsignal hinzu. Dies ermöglicht die Kommunikation zwischen jedem Gerät an jedem Standort und dem Dell Front-End-Server. Stellen Sie vor Verwendung des Rückrufsignals sicher, dass die erforderliche Netzwerksicherheit konfiguriert ist.

Für diese Installation benötigen Sie den vollständig qualifizierten Hostnamen des DMZ-Servers.

1 Wechseln Sie auf dem Dell Installationsmedium in das Security Management Server-Verzeichnis. **Entpacken** Sie (NICHT kopieren/einfügen oder ziehen) Security Management Server-x64 im Stammverzeichnis des Servers, auf dem Sie Security Management Server Virtual installieren möchten. ***Kopieren/Einfügen oder Ziehen führt zu Fehlern und einer nicht erfolgreichen Installation.***

2 Doppelklicken Sie auf **setup.exe**.

3 Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.

4 Wenn die Voraussetzungen noch nicht installiert wurden, wird eine Meldung angezeigt, die Sie darüber informiert, welche Voraussetzungen installiert werden Klicken Sie auf **Installieren**.

5 Klicken Sie im Dialogfeld „Willkommen“ auf **Weiter**.

6 Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen und klicken Sie auf **Weiter**.

7 Geben Sie den 32-stelligen Produktschlüssel ein und klicken Sie dann auf **Weiter**. Der Produktschlüssel befindet sich in der Datei EnterpriseServerInstallKey.ini.

8 Wählen Sie **Front-End-Installation** aus, und klicken Sie dann auf **Weiter**.

9 Klicken Sie zur Installation des Front-End-Servers im Standardverzeichnis C:\Programme\Dell auf **Weiter**. Klicken Sie anderenfalls auf **Ändern**, um einen anderen Speicherort auszuwählen; klicken Sie anschließend auf **Weiter**.

10 Sie können aus verschiedenen digitalen Zertifikatstypen auswählen.

ANMERKUNG: Es wird dringend empfohlen, ein digitales Zertifikat einer vertrauenswürdigen Zertifizierungsstelle zu verwenden.

Wählen Sie entweder Option „a“ oder „b“ unten aus:

a Um ein vorhandenes Zertifikat zu verwenden, das Sie bei einer Zertifizierungsstelle erworben haben, wählen Sie **Vorhandenes Zertifikat importieren** aus, und klicken Sie dann auf **Weiter**.

b Wählen Sie zum Erstellen eines selbstsignierten Zertifikats **Ein selbstsigniertes Zertifikat erstellen und in den Schlüsselspeicher importieren und klicken Sie auf Weiter.**

Geben Sie im Dialogfeld *Selbstsigniertes Zertifikat erstellen* die folgenden Informationen ein:

Vollständiger Computername (Beispiel: computername.domain.com)

Organisation

Organisationseinheit (Beispiel: Sicherheit)

Ort

Bundesstaat (vollständiger Name)

Land: Abkürzung aus zwei Buchstaben

Klicken Sie auf **Weiter**.

ANMERKUNG: Das Zertifikat läuft standardmäßig in zehn Jahren ab.

11 Geben Sie im Dialogfeld *Front-End-Server-Setup* den vollständigen Hostnamen oder DNS-Alias des Back-End-Servers ein, wählen Sie **Dell Security Management Server** aus und klicken Sie auf **Weiter**.

12 Über das Dialogfeld *Front-End-Server-Installationseinrichtung* können Sie Hostnamen und Ports anzeigen oder bearbeiten.

- Klicken Sie zum Übernehmen der Standard-Hostnamen und -Ports im Dialogfeld *Front-End-Server-Installationseinrichtung* auf **Weiter**.
- Klicken Sie zum Anzeigen oder Bearbeiten von Hostnamen im Dialogfeld *Front-End-Server-Setup* auf **Hostnamen bearbeiten**. Bearbeiten Sie Hostnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen.

ANMERKUNG:
Im Hostnamen darf kein Unterstrich (_) enthalten sein.

Heben Sie die Auswahl eines Proxys nur dann auf, wenn Sie sicher sind, dass Sie ihn nicht für die Installation konfigurieren wollen. Wenn Sie die Auswahl eines Proxys in diesem Dialogfeld aufheben, wird er nicht installiert.

Klicken Sie anschließend auf **OK**.

- Klicken Sie zum Anzeigen oder Bearbeiten von Ports im Dialogfeld *Front-End-Server-Setup* entweder auf **Externe Ports bearbeiten** oder **Interne Ports bearbeiten**. Bearbeiten Sie Portnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen.

Wenn Sie die Auswahl eines Proxys im Dialogfeld *Front-End-Hostnamen bearbeiten* aufheben, wird sein Port in den Dialogfeldern für Externe Ports und Interne Ports nicht angezeigt.

Klicken Sie anschließend auf **OK**.

13 Klicken Sie im Dialogfeld *Bereit zur Installation des Programms* auf **Installieren**.

14 Wenn die Installation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.

– Grundlegende Terminal-Konfigurationsaufgaben

Die grundlegenden Konfigurationsaufgaben werden über das Hauptmenü aufgerufen.

System-Dashboard prüfen

Um den Status der Dell Server-Dienste zu prüfen, wählen Sie aus dem Hauptmenü **System-Dashboard** aus.

Das Widget *Systeminformationen* zeigt die aktuelle Version, den Hostnamen, die IP-Adresse sowie die Auslastung von CPU, Speicher und Laufwerk an.

Das Widget *Versionsverlauf* zeigt versionierte Änderungen am Datenbankschema an. Die Daten stammen aus der Tabelle „Informationen“ und sind nach Zeit sortiert, wobei die aktuellste Version oben ist.

Die folgende Tabelle zeigt die einzelnen Dienste und deren Funktion im Widget *Dienststatus* an.

Name	Beschreibung
Message Broker	Enterprise Server-Bus
Identity Server	Verarbeitet Authentifizierungsanforderungen für die Domäne.
Compatibility Server	Ein Dienst für die Verwaltung der Unternehmensarchitektur.
Security Server	Stellt den Mechanismus für die Steuerung von Befehlen und die Kommunikation mit Active Directory bereit.
Compliance Reporter	Bietet eine umfassende Übersicht über die Umgebung für die Durchführung von Prüfverfahren und die Erstellung von Berichten über die Regelkonformität.
Core Server	Ein Dienst für die Verwaltung der Unternehmensarchitektur. Dieser Dienst handhabt auch alle Aktivierungs-, Richtlinien- und Inventarerfassungen bei „Agenten“-basierten Geräten.
Core Server HA (Hohe Verfügbarkeit)	Ein High-Availability-Dienst, der beim Verwalten der Enterprise-Architektur eine höhere Sicherheit und Leistung von HTTPS-Verbindungen ermöglicht.
Inventory Server	Verarbeitet die Bestandswarteschlange.
Forensics Server	Bietet Web-Services für die forensische API.
Policy Proxy	Stellt einen netzwerkbasierten Kommunikationsweg bereit, über den Aktualisierungen der Sicherheitsrichtlinien und der Bestandsdaten übermittelt werden.

Dienste werden überwacht und bei Bedarf automatisch neu gestartet.

ANMERKUNG: Wenn der Datenbankanpassungsvorgang fehlschlägt, werden die Server in den Status „Fehler bei der Ausführung“ versetzt. Zur Überprüfung der Datenbankanpassung wählen Sie im Hauptmenü die Option „Protokolle anzeigen“ aus.

Hostnamen ändern

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von Security Management Server Virtual ist nicht erforderlich.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **Hostname** aus.
2 Verwenden Sie die Zurück-Taste, um den bestehenden -Hostnamen zu entfernen, ersetzen Sie ihn durch einen neuen Hostnamen und wählen Sie **OK**.

Ändern der Netzwerkeinstellungen

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von Security Management Server Virtual ist nicht erforderlich.

1 Wählen Sie aus dem Menü *Grundkonfiguration* das **Netzwerk** aus.
2 Wählen Sie auf dem Bildschirm *Netzwerkeinstellungen konfigurieren* eine der nachstehenden Optionen aus und wählen Sie dann **OK** aus.
   - (Standard) DHCP verwenden (IPv4).
   - (Empfohlen) Drücken Sie in *DHCP verwenden* die Leertaste, um das X zu entfernen, und geben Sie manuell die zutreffenden folgenden Adressen ein:

     Statische IP-Adresse

     Netzwerkmaske

     Standard-Gateway

     DNS-Server 1

     DNS-Server 2

     DNS-Server 3

     Für eine statische Konfiguration kann entweder IPv6 oder IPv4 gewählt werden.

     ANMERKUNG:
     Bei Verwendung einer statischen IP-Adresse müssen Sie einen Host-Eintrag auf dem DNS-Server erstellen.

DMZ-Serverunterstützung festlegen

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von Security Management Server Virtual ist nicht erforderlich.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **DMZ-Serverunterstützung** aus.
2 Geben Sie mithilfe der Leertaste ein **X** in das Feld „DMZ-Serverunterstützung aktivieren“ ein.
3 Geben Sie den vollständig qualifizierten Domänennamen des DMZ-Servers ein und wählen Sie **OK** aus.

ANMERKUNG: Zum Nutzen eines DMZ-Servers beachten Sie die Installationsanweisungen für einen Proxy-Server oben: Proxy-Modus installieren und konfigurieren.

Ändern der Zeitzone

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von Security Management Server Virtual ist nicht erforderlich.

1 Wählen Sie aus dem Menü *Grundkonfiguration* die **Zeitzone** aus.
2 Verwenden Sie auf dem Bildschirm *Zeitzone* die Pfeiltasten, um Ihre Zeitzone hervorzuheben und wählen Sie dann **Eingabe** aus.

Aktualisierung von Security Management Server Virtual

Weitere Informationen zu bestimmten Aktualisierungen finden Sie in den *Technischen Tipps für Security Management Server Virtual* unter dell.com/support. Um die Version und das Installationsdatum einer Aktualisierung anzuzeigen, die bereits angewendet wird, überprüfen Sie das *System-Dashboard*.

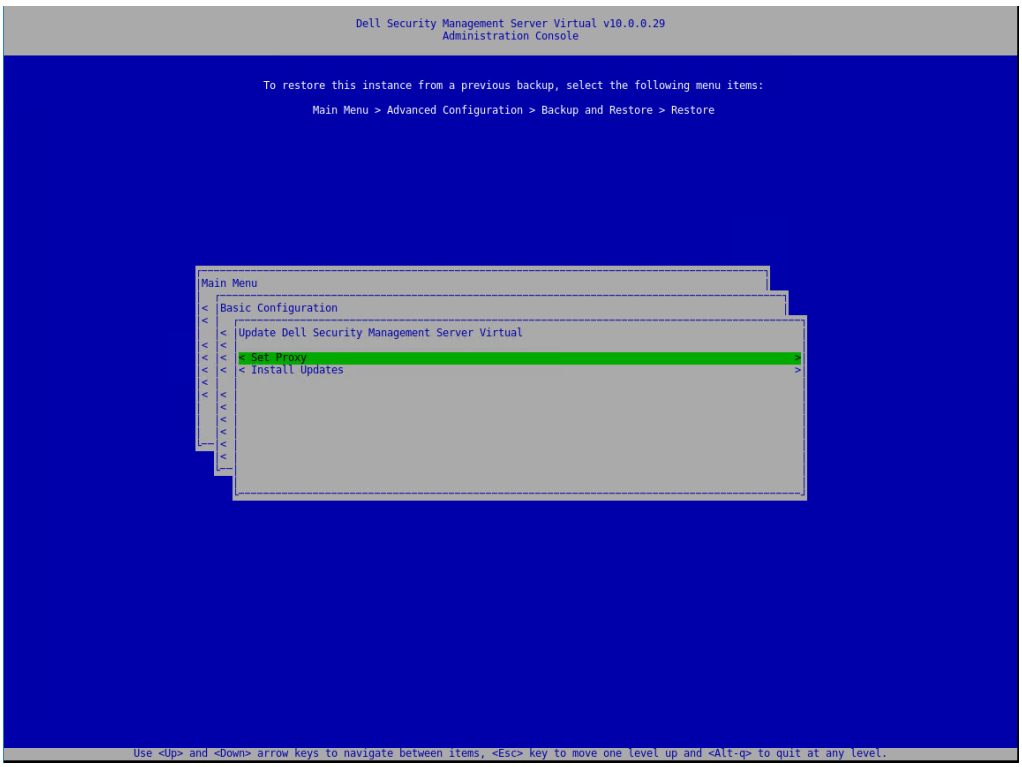
Anweisungen zum Erhalten von E-Mail-Benachrichtigungen, wenn Dell Server-Aktualisierungen verfügbar sind finden Sie unter SMTP-Einstellungen konfigurieren.

Wenn Richtlinienänderungen vorgenommen, jedoch nicht in der Verwaltungskonsole bestätigt wurden, übernehmen Sie vor der Dell Server-Aktualisierung die Richtlinienänderungen:

1 Melden Sie sich als Dell Administrator bei der Verwaltungskonsole an.
2 Klicken Sie im linken Menü auf **Verwaltung** > **Bestätigen**.
3 Geben Sie in das Kommentarfeld eine Beschreibung der Änderung ein.
4 Klicken Sie auf **Richtlinien bestätigen**.
5 Melden Sie sich nach Abschluss der Bestätigung von der Verwaltungskonsole ab.

Aktualisierung von Security Management Server Virtual (verbundener Modus)

1 Dell empfiehlt, eine regelmäßige Sicherung durchzuführen. Stellen Sie vor der Aktualisierung sicher, dass der Sicherungsprozess ordnungsgemäß funktioniert hat. Siehe Sichern und wiederherstellen.
2 Wählen Sie aus dem Menü **Basiskonfiguration Aktualisierung von Dell Security Management Server Virtual**.



ANMERKUNG: Die Versionsnummer unterscheidet sich möglicherweise vom beigefügten Bildschirmausschnitt.

3 Wählen Sie die gewünschte Aktion aus:

- Proxy-Einstellungen festlegen – Wählen Sie diese Option aus, um die Proxy-Einstellungen zum Herunterladen von Aktualisierungen festzulegen.

  Drücken Sie im Bildschirm *Proxy-Einstellungen konfigurieren* auf die Leertaste, um ein **X** in *Proxy verwenden* einzugeben. Geben Sie HTTPS und HTTP ein. Falls Firewall-Authentifizierung erforderlich ist, drücken Sie die Leertaste, um ein **X** in „Authentifizierung erforderlich“ einzugeben. Geben Sie den Benutzernamen und Ihr Kennwort ein und wählen Sie **OK**.

  ANMERKUNG: Diese Proxy-Einstellungsoption aktualisiert nun die Proxy-Einstellungen für die verschiedenen Java-basierten Anwendungen für das Abrufen von On-the-Box-Lizenzen sowie zur Kommunikation mit Endpoint Security Suite Enterprise-SaaS und der Dell/Credant Back-End-Infrastruktur.

- Bei der Auswahl von **Updates installieren** fragt der Security Management Server Virtual die integrierten standardmäßigen Ubuntu-Repositories und dist.ddspproduction.com, das benutzerdefinierte Dell Repository mit Anwendungsaktualisierungen ab.

  ANMERKUNG: Dell fragt dist.ddspproduction.com über Port 443 und Port 80 für alle Ubuntu-Aktualisierungen ab. Alle verfügbaren Aktualisierungen werden heruntergeladen. Die Proxy-Einstellungen, die in "Proxy festlegen" definiert sind, werden für die Port 443- und Port 80-Verbindungen zum Herunterladen verwendet.

Aktualisierung von Security Management Server Virtual (getrennter Modus)

1 Dell empfiehlt, eine regelmäßige Sicherung durchzuführen. Stellen Sie vor der Aktualisierung sicher, dass der Sicherungsprozess ordnungsgemäß funktioniert hat. Siehe Sichern und wiederherstellen.

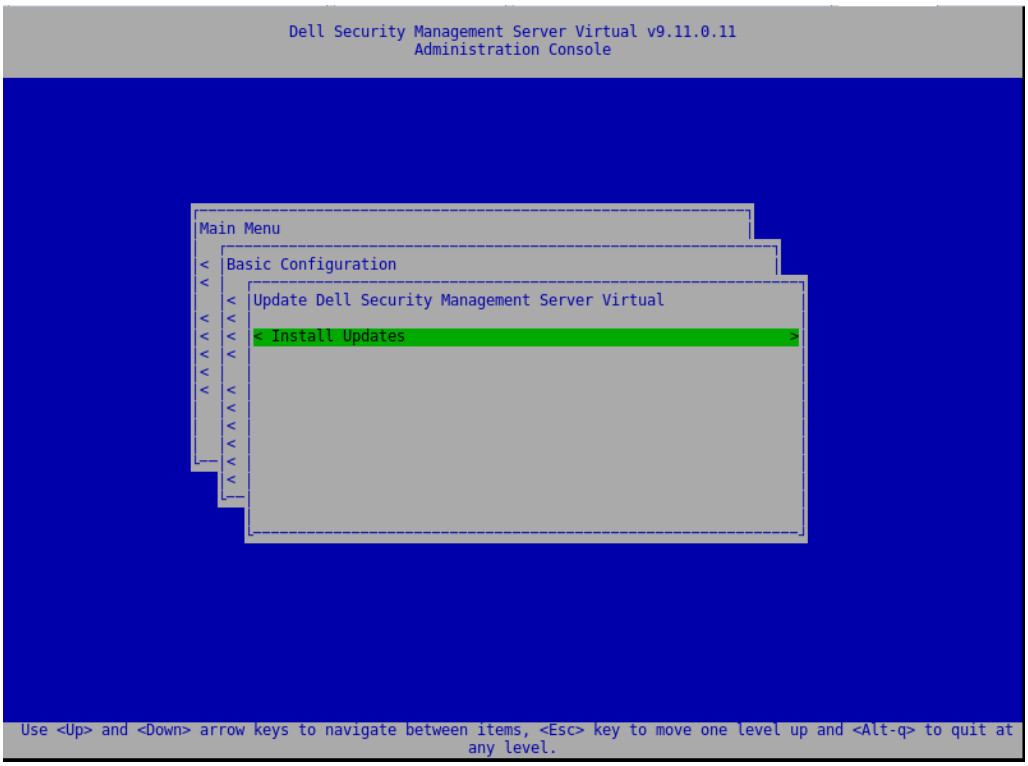
2 Rufen Sie die .deb-Datei ab, die die neueste Dell Server-Aktualisierung von Dell ProSupport enthält.

3 Speichern Sie die .deb-Datei im Ordner „/Aktualisierungen“ auf dem sicheren FTP-Server des Dell Server.

  Stellen Sie sicher, dass der FTP-Client SFTP an Port 22 unterstützt und ein FTP-Benutzer eingerichtet wird. Siehe File Transfer (FTP)-Benutzer einrichten.

4 Wählen Sie aus dem Menü **Grundkonfiguration Aktualisierung von Security Management Server Virtual**.

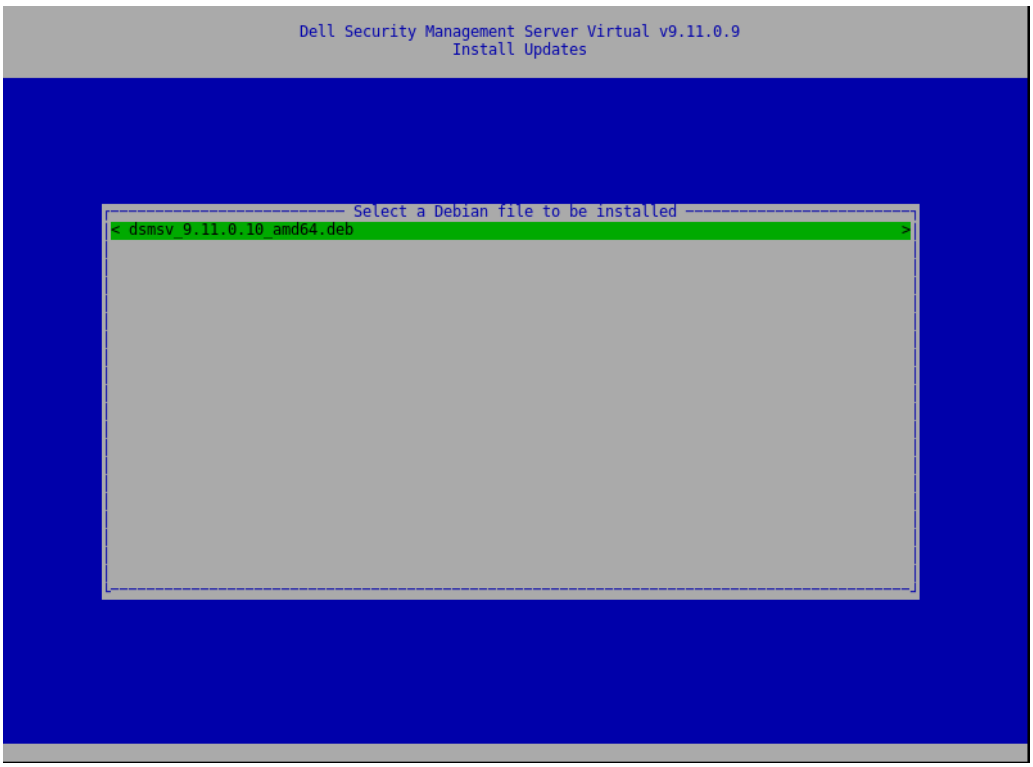
5 Wählen Sie **Aktualisierungen installieren** und drücken Sie **Eingabe**.



ANMERKUNG: Die Versionsnummer unterscheidet sich möglicherweise vom beigefügten Bildschirmausschnitt.

Wenn die .deb-Datei nicht angezeigt wird, stellen Sie sicher, dass die .deb-Datei am richtigen Speicherort gespeichert ist.

6 Wählen Sie die .deb Aktualisierungsdatei aus, die Sie installieren möchten und drücken Sie **Eingabe**.



ANMERKUNG: Die Versionsnummer unterscheidet sich möglicherweise vom beigefügten Bildschirmausschnitt.

Benutzerkennwörter ändern

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von Security Management Server Virtual ist nicht erforderlich.

Sie können die Passwörter für die folgenden Benutzer ändern:

- delluser (Terminal-Administrator) – Dieser Benutzer hat Zugriff auf das Terminal und die Menüs von Dell Server.
- dellconsole (Shell-Zugriff) – Dieser Benutzer hat Zugriff auf die Shell von Dell Server. Shell-Zugriff steht für einen Netzwerkadministrator zur Verfügung, um die Netzwerkkonnektivität zu überprüfen und allfällige Probleme zu beheben.
- dellsupport (Dell ProSupport Administrator) – Dieser Benutzer hat „sudo"-Rechte und sollte sparsam genutzt werden. Sie kontrollieren das Kennwort für dieses Konto aus Sicherheitsgründen.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **Benutzerpasswörter ändern** aus.

2 Wählen Sie auf dem Bildschirm *Benutzerpasswörter ändern* das zu ändernde Benutzerpasswort aus und wählen Sie dann **Eingabe** aus.

3 Geben Sie auf dem Bildschirm *Passwort einstellen* das aktuelle Passwort ein. Dann geben Sie das neue Passwort ein, wiederholen Sie es zur Bestätigung und wählen dann **OK** aus.

Passwörter müssen folgende Elemente enthalten:

- Mindestens 8 Zeichen
- Mindestens 1 Großbuchstaben
- Mindestens 1 Ziffer
- Mindestens 1 Sonderzeichen

ANMERKUNG:
Um verschiedene Benutzerkonten auszuwählen, drücken Sie zum Anzeigen der Auswahlliste die Leertaste auf der Tastatur.

Festlegen von Secure File Transfer (SFTP)-Benutzern

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von Security Management Server Virtual ist nicht erforderlich.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **SFTP** aus.

2 Drücken Sie zum Hinzufügen eines SFTP-Benutzers und zum Festlegen eines Kennworts im *SFTP*-Bildschirm die **Eingabetaste** oder in *Status* für den Benutzer die Nach-unten-Taste. Durch Drücken der Leertaste wird die Option zum Aktualisieren oder Löschen eines vorhandenen Benutzers angezeigt. Zum Deaktivieren eines SFTP-Benutzers wählen Sie nach der Auswahl des Benutzers **Löschen** und dann **Ja** auf dem SFTP-Bestätigungsbildschirm aus.

3 Geben Sie einen Benutzernamen und ein Kennwort für den SFTP-Benutzer ein.

Passwörter müssen folgende Elemente enthalten:

- Mindestens 8 Zeichen
- Mindestens 1 Großbuchstaben
- Mindestens 1 Ziffer
- Mindestens 1 Sonderzeichen

4 Wenn Sie mit der Eingabe der SFTP-Benutzer fertig sind, wählen Sie **Anwenden** aus.

Aktivierung von SSH

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von Security Management Server Virtual ist nicht erforderlich.

Sie können SSH für die Support-Administrator Anmeldung, Shell-Zugang und die Terminal-Befehlszeilenschnittstelle aktivieren.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **SSH** aus.
2 Markieren Sie den Benutzer, für den Sie SSH aktivieren möchten und drücken Sie die Leertaste, um ein **X** einzugeben und wählen Sie **OK** aus.

Dienste starten oder beenden

Führen Sie diese Aufgabe nur bei Bedarf aus.

1 Um alle Dienste gleichzeitig hoch- oder herunterzufahren, wählen Sie aus dem Menü *Grundkonfiguration* entweder **Anwendung starten** oder **Anwendung beenden** aus.
2 Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie **Ja**.

ANMERKUNG:
Es kann bis zu zwei Minuten dauern, bis der Serverstatus geändert wird.

Neustart des Geräts

Führen Sie diese Aufgabe nur bei Bedarf aus.

1 Wählen Sie aus dem Menü *Grundkonfiguration* **Gerät neu starten** aus.
2 Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie **Ja**.
3 Nach dem Neustart melden Sie sich bei Security Management Server Virtual an.

Herunterfahren des Geräts

Führen Sie diese Aufgabe nur bei Bedarf aus.

1 Scrollen Sie im Menü *Grundkonfiguration* nach unten und wählen Sie **Gerät herunterfahren** aus.
2 Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie **Ja**.
3 Nach dem Neustart melden Sie sich bei Security Management Server Virtual an.

Erweiterte Terminal-Konfigurationsaufgaben

Die erweiterten Konfigurationsaufgaben werden über das Hauptmenü aufgerufen.

Konfigurieren des Protokollrotators

ANMERKUNG: Die nachfolgenden Anweisungen definieren die Protokollrotation für Anwendungen in Dell Security Management Server Virtual, die eine Protokollrotation unterstützen.

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von Security Management Server Virtual ist nicht erforderlich.

Standardmäßig ist die tägliche Protokollrotation aktiviert. Um die Standard-Protokollrotation zu ändern, wählen Sie aus dem Menü *Erweiterte Konfiguration* **Protokollrotations-Konfiguration** aus.

Um die Protokollrotation zu deaktivieren, verwenden Sie die Leertaste, um ein **X** in „Keine Rotation“ einzugeben, und wählen Sie dann **OK**.

Führen Sie zur Aktivierung des Protokollrotators die folgenden Schritte aus:

1 Um tägliche, wöchentliche oder monatliche Rotation zu aktivieren, geben Sie mit der Leertaste ein **X** in das entsprechende Feld ein. Wählen Sie für wöchentliche Rotation den entsprechenden Wochentag über das Drop-down-Menü aus. Geben Sie für monatliche Rotation den gewünschten Tag des Monats ein.

2 Geben Sie eine Uhrzeit für die Rotation in *Protokollrotationszeit* ein.

3 Wählen Sie **OK**.

Sichern und wiederherstellen

Sicherungen können jederzeit konfiguriert oder durchgeführt werden und sind nicht erforderlich, um Security Management Server Virtual verwenden zu können. Dell empfiehlt, einen regelmäßigen Sicherungsprozess zu konfigurieren. Weitere Informationen finden Sie unter http://www.dell.com/support/article/us/en/19/sln304943/how-to-back-up-and-restore-dell-security-management-server-virtual-dell-data-protection-virtual-edition?lang=en

Wenn bei einem Speichern auf dem Dell Server die Festplattenkapazität auf 90 % steht, werden keinen neuen Sicherungen gespeichert. Wenn E-Mail-Benachrichtigungen konfiguriert wurden, erhalten Sie eine Benachrichtigung per E-Mail, dass der Speicherplatz auf der Festplatte nicht mehr ausreicht.

ANMERKUNG:
Um Speicherplatz von Festplattenpartitionen einzusparen und das automatische Löschen von Sicherungen zu verhindern, entfernen Sie unnötige Sicherungen aus dem Speicher.

Sicherungen werden standardmäßig täglich ausgeführt. Dell empfiehlt, Sicherungen auf einem externen sicheren FTP-Server mit einer Häufigkeit zu speichern, die die Anforderungen der Organisation für Sicherungen und eine angemessene Nutzung von Speicherplatz erfüllt.

Zur Konfiguration eines Sicherungsplans wählen Sie aus dem Menü *Erweiterte Konfiguration* **Sicherung und Wiederherstellung > Konfiguration** aus und gehen folgendermaßen vor:

1 Zur Aktivierung täglicher, wöchentlicher oder monatlicher Sicherungen geben Sie mithilfe der Leertaste ein **X** in das entsprechende Feld ein. Geben Sie bei der wöchentlichen oder monatlichen Sicherung den entsprechenden Tag der Woche oder des Monats als Zahl ein, wobei Montag = 1 ist. Um die Sicherungen zu deaktivieren, geben Sie mithilfe der Leertaste ein **X** in *Keine Sicherungen* ein und wählen Sie dann **OK**.

2 Geben Sie eine Uhrzeit für die Sicherung in *Sicherungszeit* ein.

3 Wählen Sie **OK**.

Um eine sofortige Sicherung durchzuführen, wählen Sie im Menü *Erweiterte Konfiguration* **Sicherung und Wiederherstellung > Jetzt sichern** aus. Wenn „Sicherung bestätigen“ angezeigt wird, wählen Sie **OK**.

ANMERKUNG:
Bevor Sie eine Wiederherstellung beginnen, müssen alle Dell Server-Services laufen. Serverstatus prüfen. Wenn nicht alle Dienste laufen, starten Sie die Dienste neu. Weitere Informationen finden Sie unter Dienste starten oder beenden. Beginnen Sie die Wiederherstellung ***nur***, wenn ***alle*** Dienste laufen.

Zur Wiederherstellung einer Sicherungsdatei wählen Sie aus dem Menü *Erweiterte Konfiguration* die Optionen **Sicherung und Wiederherstellung > Wiederherstellen** und dann die gewünschte wiederherzustellende Sicherungsdatei aus. Wählen Sie auf dem Bestätigungsbildschirm **Ja** aus.

Die Sicherung wird nach dem Neustart wiederhergestellt.

Sicherungen auf einem sicheren FTP-Server speichern

Um Sicherungen auf einem FTP-Server zu speichern, muss der FTP-Client SFTP auf Port 22 unterstützen.

Entsprechend den Sicherungsanforderungen der Organisation können Sicherungen auf die folgende Arten heruntergeladen werden:

- Manuell
- Durch automatisches Skript
- Durch die zugelassene Sicherungslösung der Organisation

Um Sicherungen mithilfe der Sicherungslösung der Organisation herunterzuladen, können Sie detaillierte Anweisungen vom Anbieter Ihrer Sicherungslösung erhalten.

ANMERKUNG:
Dell Server beruht auf Linux Debian Ubuntu x64.

Melden Sie sich beim Dell Server als „dellsupport“ an und verwenden Sie den Befehl `sudo` zum Konfigurieren Ihrer Sicherungslösung:

`sudo` <Anleitungen vom Anbieter der Sicherungslösung>

Sicherungsinhalte der folgenden Ordner:

/backup (erforderlich)

/certificates (dringend empfohlen)

/support (optional)

Wenn der sudo-Vorgang läuft, geben Sie **Beenden** ein und drücken Sie die **Eingabetaste** bis die Anmeldeaufforderung erscheint.

SMTP-Einstellungen konfigurieren

Wenn Sie E-Mail-Benachrichtigungen empfangen **oder** Data Guardian verwenden möchten, befolgen Sie die Schritte in diesem Abschnitt zur Konfiguration der SMTP-Einstellungen. Per E-Mail-Benachrichtigung werden die Empfänger auf Serverstatus-Fehler von Dell Server, Kennwort-Aktualisierungen, neue Aktualisierungen für Dell Server und Probleme mit Client-Lizenzen aufmerksam gemacht.

Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

Führen Sie zur Konfiguration von SMTP-Einstellungen die folgenden Schritte aus:

1 Wählen Sie aus dem Menü *Erweiterte Konfiguration* die Option **E-Mail-Benachrichtigungen** aus.
2 Um E-Mail-Warnungen zu aktivieren, drücken Sie auf dem Bildschirm „E-Mail-Benachrichtigungen“ die Leertaste, um ein **X** in *E-Mail-Warnungen aktivieren* einzugeben.
3 Geben Sie den vollständigen Domänennamen des SMTP-Servers ein.
4 Geben Sie den SMTP-Port ein.
5 Geben Sie den SMTP-Benutzer ein.
6 Geben Sie das SMTP-Passwort ein.
7 Geben Sie in *Benachrichtigungen senden von* das E-Mail-Konto an, von dem die E-Mail-Benachrichtigungen gesendet werden sollen.
8 Geben Sie in *Serverstatus senden an* das E-Mail-Konto an, von dem Serverstatus-Benachrichtigungen gesendet werden sollen. Trennen Sie Empfänger durch Komma oder Semikolon.
9 Geben Sie in *Kennwortänderungen senden an* ein E-Mail-Konto an, um Kennwortänderungsbenachrichtigungen zu senden.
10 Geben Sie in *Softwareupdates senden an* ein E-Mail-Konto an, um Softwareupdate-Benachrichtigungen zu senden.
11 Drücken Sie zum Aktivieren von Erinnerungen in *Dienste-Erinnerungsalarm* die Leertaste, um ein **X** zu setzen, und legen Sie anschließend das Erinnerungsintervall in Minuten fest. Nach dem Senden einer Benachrichtigung zu einem Problem in Zusammenhang mit dem Systemzustand wird nach Verstreichen des Erinnerungsintervalls ein Dienste-Erinnerungsalarm ausgelöst und der Host bzw. Dienst verbleibt im gleichen Zustand.
12 Wählen Sie zum Aktivieren von Berichten von Benachrichtigungen im Feld *Zusammenfassungsbericht* das gewünschte Intervall aus (Täglich, Wöchentlich oder Monatlich), und drücken Sie dann auf die Leertaste, um ein **X** in das Feld zu setzen.

13 Wählen Sie **OK**.

Import eines bestehenden Zertifikats oder Registrierung eines neuen Serverzertifikats

Sie können ein bestehendes Zertifikat importieren oder eine Zertifikatsanforderung über Security Management Server Virtual erstellen.

Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

Import eines bestehenden Zertifikats

1 Exportieren Sie das bestehende Zertifikat mit der vollständigen Zertifikatkette aus dem Schlüsselspeicher.

> **ANMERKUNG: Bewahren Sie das Export-Kennwort auf. Sie müssen es eingeben, wenn Sie das Zertifikat in Security Management Server Virtual importieren.**

2 Speichern Sie auf dem FTP-Server von Dell Server das Zertifikat unter **/certificates**.

3 Wählen Sie aus dem Menü *Erweiterte Konfiguration* **Server-Zertifikate** aus.

4 Wählen Sie **Bestehendes Zertifikat importieren** aus.

5 Wählen Sie die auf Dell Server zu installierende Zertifikatdatei aus.

6 Geben Sie auf Aufforderung das Zertifikat-Export-Passwort ein und wählen Sie dann **OK**.

7 Nach Abschluss des Imports wählen Sie **OK** aus.

> **ANMERKUNG: Weitere Informationen finden Sie unter http://www.dell.com/support/article/us/en/19/sln302996/dell-data-protection-virtual-edition-dell-security-management-server-virtual-manual-csr-creation-and-certificate-import?lang=en**

Registrierung eines neuen Serverzertifikats

1 Wählen Sie aus dem Menü *Erweiterte Konfiguration* **Server-Zertifikate** aus.

2 Wählen Sie **Neues Server-Zertifikat** aus.

3 Wählen Sie **Zertifikatanforderung erstellen** aus.

4 Füllen Sie die Felder unter *Zertifikatanforderung erstellen* aus:

- Name des Landes: Zweistelliger Ländercode.
- *Bundesstaat bzw. Bundesland*: Geben Sie den Namen des Bundesstaats oder -landes ohne Abkürzungen ein (Beispiel: Bayern).
- *Ort/Stadt*. Geben Sie den entsprechenden Wert ein (z. B. Dallas).
- *Organisation*: Geben Sie den entsprechenden Wert ein (Beispiel: Dell).
- *Organisationseinheit*: Geben Sie den entsprechenden Wert ein (Beispiel: Sicherheit).
- *Allgemeiner Name:* Geben Sie den vollständig qualifizierten Domänennamen von Dell Server ein. Zum vollständigen Namen gehören der Hostname und der Domänenname (Beispiel: server.domäne.com).
- *E-Mail-ID:* Geben Sie die E-Mail-Adresse ein, an die Ihr CSR gesendet wird.

5 Befolgen Sie Ihr Organisationsverfahren zum Erwerb eines SSL-Serverzertifikats bei einer Zertifizierungsstelle. Senden Sie den Inhalt der Zertifikatanforderungsdatei zum Signieren.

6 Wenn Sie das signierte Zertifikat erhalten haben, exportieren Sie es als .p7b-Datei und laden Sie die vollständige Zertifikatkette im .der-Format herunter.

7 Erstellen Sie Sicherungskopien des Zertifikats und der vollständigen Zertifikatkette.

8 Laden Sie die Zertifikatsdatei und die vollständige Vertrauenskette auf den FTP-Server von Dell Server herunter.

9 Wählen Sie aus dem Menü *Erweiterte Konfiguration* **Server-Zertifikate** aus.

10 Wählen Sie **Neues Server-Zertifikat** aus.

11 Wählen Sie `Zertifikateintragung abschließen` aus.

12 Wählen Sie die auf Dell Server zu installierende Zertifikatdatei aus.

13 Geben Sie bei entsprechender Aufforderung das Zertifikatkennwort ein: **changeit**.

Um die Vertrauensvalidierung auf Windows-basierten Encryption-Clients zu aktivieren, siehe Manager-Vertrauenskettenprüfung aktivieren.

Erstellen und Installieren eines selbstsignierten Zertifikats

ANMERKUNG: Die standardmäßig erzeugten selbstsignierte Zertifikate werden für zehn Jahre erzeugt.

1 Im Menü *Erweiterte Konfiguration* von Dell Server wählen Sie **Server-Zertifikate**.

2 Wählen Sie **Erstellen und Installieren eines selbstsignierten Zertifikats** aus.

3 Um zu bestätigen, dass Sie das vorinstallierte Zertifikat mit einem neuen Zertifikat ersetzen möchten, klicken Sie auf **Ja**.

4 Geben Sie das Zertifikatkennwort ein: **changeit**.

5 Wählen Sie nach der Installation des neuen Zertifikats **OK** aus, und warten Sie bis die Dienste neu starten.

Die Services werden automatisch neu gestartet.

Datenbankzugriff aktivieren

Diese Aufgabe kann jederzeit durchgeführt werden. Die Verwendung von Security Management Server Virtual ist nicht erforderlich.

ANMERKUNG: Dell empfiehlt, den Zugriff auf die Datenbank nur bei Bedarf zu aktivieren und ihn zu deaktivieren, sobald Sie den Vorgang abgeschlossen haben.

1 Wählen Sie aus dem Menü *Erweiterte Konfiguration* **Datenbankzugriff** aus.

2 Geben Sie mithilfe der Leertaste ein **X** in „Datenbankzugriff aktivieren“ ein und wählen Sie dann **OK** aus. Wenn das Datenbankpasswort noch nicht konfiguriert wurde, wird eine Aufforderung für das Datenbankpasswort angezeigt.

3 Geben Sie das Datenbankpasswort ein.

4 Geben Sie das Datenbankpasswort erneut ein.

Dell Data Security Anwendungskomponenten werden automatisch gestoppt.

Terminal-Sprache einstellen oder ändern

Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

1 Wählen Sie im Hauptmenü **Sprache einstellen** aus.

2 Wählen Sie mithilfe der Pfeiltasten die gewünschte Sprache aus.

Anzeigen von Protokollen

Wenn Sie die folgenden Protokolle prüfen möchten, wählen Sie im Hauptmenü **Protokolle anzeigen** aus.

- Systemprotokolle
  - Syslog-Protokoll
  - E-Mail-Protokoll
  - Autorisierungsprotokoll (SSH)
  - Postgres-Protokoll
  - Überwachungsprotokoll

- Serverprotokolle
  - Message Broker
  - Identity Server
  - Compatibility Server
  - Security Server
  - Compliance Reporter
  - Core Server
  - Core Server HA
  - Inventory Server
  - Forensics Server
  - Policy Proxy
- Administration Console
  - pybackup.log
  - pyconsole.log
  - pydatabase.log
  - update.log
- Protokoll der Datenbankanpassung

ANMERKUNG: So navigieren Sie durch diesen Bildschirm:

- Um zum Ende des Protokolls zu springen, halten Sie die rechte Alt-Taste gedrückt und drücken Sie dann die Taste „/“ auf der Tastatur.
- Zum Beenden des Protokolls halten Sie die linke Strg-Taste gedrückt und drücken Sie „x“ auf der Tastatur.
- Pfeiltasten ermöglichen die Navigation.
- Mit Bild nach oben und Bild nach unten können Seiten nach oben und nach unten geblättert werden.
- Mit der Leertaste werden die Protokolle um eine Seite vorgeblättert.

Öffnen der Befehlszeilenschnittstelle

Zum Öffnen der Befehlszeilenschnittstelle wählen Sie im Hauptmenü **Shell starten** aus.

Wenn Sie die Befehlszeilenschnittstelle verlassen möchten, geben Sie **Beenden** ein und drücken dann die **Eingabetaste**.

Erstellen eines Systemmomentaufnahme-Protokolls

Wenn Sie ein System-Schnappschuss-Protokoll für Dell ProSupport erstellen möchten, wählen Sie aus dem Hauptmenü **Support-Tools** aus.

1 Wählen Sie im Menü *Support-Tools* **System Schnappschuss-Protokoll erstellen** aus.
2 Wenn angezeigt wird, dass die Datei erstellt wurde, wählen Sie **OK** aus.

3

Wartung von

Entfernen Sie unnötige Sicherungen von Security Management Server Virtual.

Nur die letzten zehn Sicherungskopien werden erhalten. Wenn der freie Speicherplatz auf der Partition zehn Prozent oder weniger beträgt, werden keine Sicherungskopien mehr gespeichert. In diesem Fall erhalten Sie eine Benachrichtigung per E-Mail, dass der Speicherplatz auf der Festplatte nicht mehr ausreicht.

4

Fehlerbehebung

Wenn ein Fehler auftritt und Sie die E-Mail-Benachrichtigungen konfiguriert haben, erhalten Sie eine Benachrichtigung per E-Mail. Führen Sie je nach den Informationen in der E-Mail-Benachrichtigung die folgenden Schritte aus:

1 Überprüfen der verfügbaren Protokolldateien.

2 Bei Bedarf Neustart der Dienste. Eine empfohlene Vorgehensweise besteht darin, die Dienste jedes Mal neu zu starten, wenn eine Veränderung der Einstellungen vorgenommen wird.

3 Systemmomentaufnahme-Protokoll erstellen.

4 Kontaktieren Sie den Dell ProSupport. Weitere Informationen finden Sie unter Dell ProSupport kontaktieren.

5

Konfiguration nach der Installation

Nach der Installation müssen einige Komponenten Ihrer Umgebung möglicherweise konfiguriert werden. Dies hängt von der Dell Data Security-Lösung ab, die Ihre Organisation verwendet.

Nach der Installation von Security Management Server Virtual müssen die folgenden Standardeinstellungen angepasst werden:

- Ändern Sie das Back-End-Server-Kennwort an folgendem Speicherort:

  `C:\Program Files\Dell\Enterprise Edition\Message Broker\conf\application.properties`

- Ändern Sie das Kennwort für jeden Front-End-Server in Ihrer Umgebung an folgendem Speicherort:

  `C:\Program Files\DELL\Enterprise Edition\Beac\conf\application.properties`

Das Kennwort wird wie folgt angezeigt: `proxy-server.password=ENC(<texthere>)`

So ändern Sie das Kennwort:

1 Wählen Sie: `ENC(<texthere>)`

2 Ändern Sie den ausgewählten Text zu: `CLR(<newpasswordhere>)`

Nach einem Serviceneustart ändert sich die angepasste Zeile von `CLR` zu `ENC` und das Kennwort ist verschlüsselt.

HINWEIS: Der Proxy-Server-Benutzername wird möglicherweise auch geändert, dieser muss jedoch mit der application.properties-Datei des Nachrichtenbroker und allen aktiven Front-End-Servern übereinstimmen.

Konfiguration für Data Guardian

Um den Dell Server zur Unterstützung von Data Guardian zu konfigurieren, setzen Sie in der Verwaltungskonsole eine oder beide Richtlinien auf **Ein**: *Geschützte Office-Dokumente* und *Cloud-Verschlüsselung*.

Informationen zur Installation des Data Guardian-Clients finden Sie im *Data Guardian-Administratorhandbuch* oder im *Data Guardian-Benutzerhandbuch*. Es wird Administratoren empfohlen, SMTP zu aktivieren, damit Dell Data Guardian E-Mails an externe Benutzer senden und das Key-Management für Ersteller vereinfacht werden kann.

Manager-Vertrauenskettenprüfung überprüfen

Wenn ein selbstsigniertes Zertifikat auf Security Management Server Virtual für SED oder BitLocker Manager verwendet wird, muss die SSL-/TLS-Vertrauensprüfung auf dem Client-Computer ***deaktiviert*** bleiben. Vor dem Aktivieren der SSL/TLS-Vertrauensprüfung auf dem Client müssen die folgenden Voraussetzungen erfüllt sein:

- Ein durch eine Stammzertifizierungsstelle, wie beispielsweise Ensign oder Verisign signiertes Zertifikat muss auf den Dell Server importiert werden. Siehe Import eines bestehenden Zertifikats oder Registrierung eines neuen Serverzertifikats.
- Die vollständige Vertrauenskette des Zertifikats muss im Microsoft Keystore des Client-Computers gespeichert werden.

Um die SSL/TLS-Trust-Validierung auf dem Clientcomputer zu deaktivieren, ändern Sie den Wert des folgenden Registry-Eintrags in 1:

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

DisableSSLCertTrust=REG_DWORD (32-Bit):1

6

Administratoraufgaben für die Verwaltungskonsole

Dell Administratorrolle zuweisen

1 Melden Sie sich als Administrator von Security Management Server Virtual an der Verwaltungskonsole an: https://server.domain.com:8443/webui/. Die Standard-Anmeldeinformationen lauten **superadmin/changeit**.

2 Klicken Sie im linken Bereich auf **Bestückung** > **Domänen**.

3 Klicken Sie auf eine Domäne, der ein Benutzer hinzugefügt werden soll.

4 Klicken Sie auf der Seite „Domänendetails“ auf die Registerkarte **Mitglieder**.

5 Klicken Sie auf **Benutzer hinzufügen**.

6 Geben Sie einen Filter ein, um den Benutzernamen nach allgemeinem Namen, UPN (Universal Principal Name) oder SAM-Kontonamen zu suchen. Der Platzhalter ist *.

Auf dem Unternehmensverzeichnisserver muss für jeden Benutzer ein allgemeiner Name, ein UPN (Universal Principal Name) und ein SAM-Kontoname definiert sein. Wenn ein Benutzer einer Domäne oder Gruppe angehört, aber nicht in der Liste der Domänen- oder Gruppenmitglieder im Management angezeigt wird, überprüfen Sie, ob alle drei Namen für diesen Benutzer auf dem Unternehmensverzeichnisserver korrekt definiert sind.

Bei der Abfrage wird automatisch zunächst nach dem allgemeinen Namen, dann nach dem UPN und dann nach dem SAM-Kontonamen gesucht, bis ein Treffer gefunden wurde.

7 Wählen Sie die Benutzer, die Sie zur Domäne hinzufügen möchten, aus der *Verzeichnisbenutzerliste* aus. Verwenden Sie <Umschalt><Klick> oder <Strg><Klick>, um mehrere Benutzer auszuwählen.

8 Klicken Sie auf **Hinzufügen**.

9 Klicken Sie in der Menüleiste auf die Registerkarte **Details und Aktionen** des angegebenen Benutzers.

10 Scrollen Sie durch die Menüleiste und wählen Sie die Registerkarte **Admin**.

11 Wählen Sie die Administratorrollen aus, die Sie diesem Benutzer zuweisen möchten.

12 Klicken Sie auf **Speichern**.

Mit Dell Administratorrolle anmelden

1 Melden Sie sich bei der Verwaltungskonsole ab.

2 Melden Sie sich mit den Anmeldeinformationen eines Domänenbenutzers bei der Verwaltungskonsole an.

Klicken Sie auf „?“ in der oberen rechten Ecke der Verwaltungskonsole, um *AdminHelp* zu starten. Die Seite *Erste Schritte* wird angezeigt. Klicken Sie auf **Domänen hinzufügen**.

Für Ihre Organisation wurden grundlegende Richtlinien festgelegt, diese sollten aber entsprechend Ihren Anforderungen wie folgt geändert werden (für alle Aktivierungen sind Lizenzen und Berechtigungen erforderlich):

- Richtlinienbasierte Verschlüsselung wird mit Verschlüsselung durch einen allgemeinen Schlüssel aktiviert.
- Computer mit selbstverschlüsselnden Laufwerken werden verschlüsselt.
- BitLocker Management ist nicht aktiviert
- Advanced Threat Prevention ist nicht aktiviert
- Der Bedrohungsschutz ist deaktiviert.
- Externe Medien werden nicht verschlüsselt.

- Ports werden nicht durch die Portsteuerung verwaltet.
- Geräte, auf denen die vollständige Datenträgerverschlüsselung installiert ist, werden nicht verschlüsselt.
- Data Guardian ist deaktiviert.

Im AdminHelp-Thema *Richtlinien verwalten* finden Sie Beschreibungen der Richtlinien.

Richtlinien bestätigen

Wenn die Installation abgeschlossen ist, bestätigen Sie die Richtlinien.

Um Richtlinien nach der Installation oder später, nachdem die Richtlinienänderungen gespeichert sind, zu bestätigen, führen Sie die folgenden Schritte aus:

1 Klicken Sie im linken Fensterbereich auf **Verwaltung** > **Festlegen**.
2 Geben Sie in *Anmerkung* eine Beschreibung der Änderung ein.
3 Klicken Sie auf **Richtlinien bestätigen**.

7

Ports

In der folgenden Tabelle werden die einzelnen Komponenten mit ihren Funktionen aufgeführt.

Name	Standardport	Beschreibung
ACL-Dienst	TCP/ 8006	Verwaltet verschiedene Berechtigungen und Gruppenzugriffe für verschiedene Dell Sicherheitsprodukte.
Compliance Reporter	HTTP(S)/ 8084	Bietet eine umfassende Übersicht über die Umgebung für die Durchführung von Prüfverfahren und die Erstellung von Berichten über die Regelkonformität.
Management Console	HTTPS/ 8443	Verwaltungskonsole und Befehlszentrale für die gesamte Unternehmensimplementierung.
Core Server	HTTPS/ 8887 (geschlossen)	Verwaltet den Richtlinienablauf, Lizenzen und die Registrierung für die Preboot-Authentifizierung, SED-Verwaltung, BitLocker Manager, Threat Protection und Advanced Threat Prevention. Verarbeitet Bestandslistendaten zur Verwendung durch den Compliance Reporter und die Verwaltungskonsole. Sammelt und speichert Authentifizierungsdaten Steuert den rollenbasierten Zugriff.
Core Server HA (Hohe Verfügbarkeit)	HTTPS/ 8888	Ein High-Availability-Dienst, der eine höhere Sicherheit und Leistung von HTTPS-Verbindungen mit der Verwaltungskonsole, Preboot-Authentifizierung, SED-Verwaltung, FDE, BitLocker Manager, Threat Protection und Advanced Threat Prevention ermöglicht.
Security Server	HTTPS/ 8443	Kommuniziert mit dem Policy Proxy; verwaltet Abrufungen von Forensic Keys, Aktivierungen von Clients, Data Guardian Produkte und die SED-PBA-Kommunikation.
Compatibility Server	TCP/ 1099 (geschlossen)	Ein Dienst für die Verwaltung der Unternehmensarchitektur. Sammelt und speichert anfängliche Bestandslistendaten während der Aktivierung und Richtliniendaten während Migrationen. Verarbeitet Daten auf Grundlage von Benutzergruppen.
Message Broker-Service	TCP/ 61616 (geschlossen) und STOMP/ 61613 (geschlossen, oder - sofern für DMZ konfiguriert - geöffnet)	Handhabt die Kommunikation zwischen Diensten von Dell Server. Stellt durch den Compatibility Server für Policy-Proxy-Warteschlangen erzeugte Richtlinieninformationen bereit.

Name	Standardport	Beschreibung
Identity Server	8445 (geschlossen)	Handhabt Domänen-Authentifizierungsanfragen, einschließlich der Authentifizierung für SED Management.
Forensics Server	HTTPS/ 8448	Ermöglicht es Administratoren mit entsprechenden Berechtigungen, Verschlüsselungsschlüssel von der Verwaltungskonsole zur Verwendung beim Entsperren von Daten oder Entschlüsselungsaufgaben zu erhalten. Erforderlich für forensische API.
Inventory Server	8887	Verarbeitet die Bestandswarteschlange.
Policy Proxy	TCP/ 8000	Stellt einen netzwerkbasierten Kommunikationsweg bereit, über den Aktualisierungen der Sicherheitsrichtlinien und der Bestandsdaten übermittelt werden. Erforderlich für Encryption Enterprise (Windows und Mac)
Postgres	TCP/ 5432	Lokale Datenbank, die für Ereignisdaten verwendet wird.
LDAP	389/636, 3268/3269 RPC – 135, 49125+	Port 389 - Dieser Port wird für die Anforderung von Informationen aus dem lokalen Domänencontroller verwendet. LDAP-Anfragen, die an Port 389 gesandt wurden, können nur zur Suche nach Objekten innerhalb der Startdomäne des globalen Katalogs verwendet werden. Die anfordernde Anwendung kann jedoch alle Attribute für diese Objekte ermitteln. Eine Anfrage an Port 389 könnte beispielsweise zur Ermittlung des Departements eines Benutzers verwendet werden. Port 3268 – Dieser Port wird für Abfragen verwendet, die spezifisch für den globalen Katalog vorgesehen ist. LDAP-Anfragen, die an Port 3268 gesandt wurden, können zur Suche nach Objekten im ganzen Wald verwendet werden. Es können jedoch nur die Attribute zurückgegeben werden, die zur Replikation im globalen Katalog markiert sind. Das Departement eines Benutzers kann beispielsweise nicht unter Verwendung von Pport 3268 zurückgegeben werden, da dieses Attribut nicht in den globalen Katalog repliziert wurde.
Client-Authentifizierung	HTTPS/ 8449	Ermöglicht Client-Servern die Authentifizierung bei Dell Server. Erforderlich für Server Encryption
Callback-Signal	HTTP/TCP 8446	Bei einem Front-End-Server kann in jede geschützte Office-Datei ein Rückrufsignal eingefügt werden, wenn Data Guardian im geschützten Office-Modus ausgeführt wird.