Dell Data Protection

Enterprise Server-Installations- und Migrationshandbuch
Version 9.7

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.

Enterprise Server-Installations- und Migrationshandbuch

2017 - 04

Rev. A01

Inhaltsverzeichnis

1 Einführung in Dell Enterprise Server 5
Info über Dell Enterprise Server 5
Kontaktaufnahme mit dem Dell ProSupport 5

2 Dell Enterprise Server-Anforderungen und -Architektur 6
Anforderungen für Dell Enterprise Server 6
Voraussetzungen für Dell Enterprise Server 6
Dell Enterprise Server-Hardware 6
Software für Dell Enterprise Server 7
Unterstützte Sprachen für Dell Enterprise Server 9
Dell Enterprise Server Architektur 10

3 Vorinstallationskonfiguration 15
Konfiguration 15

4 Installation oder Upgrade/Migraton 21
Vor der Installation, Aktualisierung oder Migration 21
Neue Installation 22
Back-End-Server und neue Datenbank installieren 22
Back-End-Server mit vorhandener Datenbank installieren 26
Front-End-Server installieren 30
Aktualisierung und Migration 32
Vor der Aktualisierung oder Migration 32
Back-End-Server-Aktualisierung/Migration 34
Front-End-Server Aktualisierung/Migration 36
Installation im getrennten Modus 37
Enterprise Server im getrennten Modus installieren 40
Dell Enterprise Server deinstallieren 40

5 Konfiguration nach der Installation 41
EAS-Management installieren und konfigurieren 41
Installation des EAS-Geräte-Managers 41
Installation des EAS-Postfach-Managers 42
Verwendung des EAS-Konfigurationsprogramms 42
Einstellungen für EAS-Management konfigurieren 43
Dell Security Server im DMZ-Modus konfigurieren 43
Verwenden von Keytool für den Import des DMZ-Domänenzertifikats 43
Ändern der Datei „application.properties“ 44
APNs-Eintragung 44
Serverkonfigurationstool 45
Neue oder aktualisierte Zertifikate hinzufügen 46
Dell Manager-Zertifikat importieren 48
Identitätszertifikat importieren 49

Einstellungen für Server SSL-Zertifikat oder Mobile Edition konfigurieren..... 50
SMTP-Einstellungen für Data Guardian oder E-Mail-Services konfigurieren.....50
Datenbankname, Speicherort oder Anmeldeinformationen ändern.....51
Datenbank migrieren.....52

6 Administrative Aufgaben.....53
Dell Administratorrolle zuweisen..... 53
Mit Dell Administratorrolle anmelden.....53
Hochladen der Client-Zugriffslizenz.....53
Richtlinien bestätigen..... 53
Dell Compliance Reporter konfigurieren.....54
SQL-Authentifizierung mit Compliance Reporter konfigurieren.....54
Windows-Authentifizierung mit Compliance Reporter konfigurieren.....54
Ausführen von Sicherungen..... 55
Enterprise Server-Sicherungen.....55
SQL Server-Sicherungen.....55
PostgreSQL Server-Sicherungen..... 55

7 Beschreibung der Dell Komponenten.....56

8 Bewährte Verfahren für SQL Server..... 59

9 Zertifikate.....60
Erstellen eines selbstsignierten Zertifikats und Generieren einer Zertifikatssignieranforderung.....60
Neue Key-Paare und selbstsignierte Zertifikate erstellen..... 60
Signierte Zertifikate von einer Zertifizierungsstelle anfordern..... 61
Stammzertifikate importieren.....62
Beispielmethode zur Anforderung eines Zertifikats.....62
Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.....63
Vertrauenswürdiges, signiertes Zertifikat zum Security Server hinzufügen, wenn ein nicht vertrauenswürdiges Zertifikat für SSL verwendet wurde.....64

Einführung in Dell Enterprise Server

Info über Dell Enterprise Server

Der Enterprise Server ist die Sicherheitsverwaltungskomponente der Dell-Lösung. Mit der Remote-Verwaltungskonsole können Administratoren den Status der Endpunkte, die Richtliniendurchsetzung und den Schutz für das gesamte Unternehmen überwachen.

Der Enterprise Server hat die folgenden Funktionen:

- Zentralisierte Verwaltung von 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

Kontaktaufnahme mit dem Dell ProSupport

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

Zusätzlich steht Ihnen unser Online-Support für Dell Data Protection-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 Ihren Service Code 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.

2

Dell Enterprise Server-Anforderungen und -Architektur

In diesem Kapitel werden die Hardware- und Softwareanforderungen und Architektur-Design-Empfehlungen für Dell Data Protection-Implementierung erläutert.

Anforderungen für Dell Enterprise Server

Für die Komponenten von Dell Enterprise Server gelten neben der über das Dell Installationsmedium bereitgestellten Software zusätzliche Hard- und Softwareanforderungen. Vergewissern Sie sich, dass die Installationsumgebung diese Anforderungen erfüllt, bevor Sie mit der Installation, einem Upgrade oder einer Migration von Aufgaben fortfahren.

Bevor Sie die Installation beginnen, stellen Sie sicher, dass alle Patches und Aktualisierungen auf den Servern, die zur Installation verwendet werden, angewendet wurden.

Voraussetzungen für Dell Enterprise Server

Die folgende Tabelle führt die Software auf, die auf dem System vorhanden sein muss, damit Dell Enterprise Server installiert werden kann. Links und Anweisungen zur Installation dieser Voraussetzungen finden Sie unter Vorinstallationskonfiguration.

Alle anwendbare Softwareelemente müssen vor Anfang der Installation installiert werden, außer wenn angegeben wird, dass das Installationsprogramm das Element installiert. Andernfalls schlägt die Installation fehl.

Dell Enterprise Server-Hardware

Voraussetzungen

- **Visual C++ 2010 Redistributable-Paket**

  Wenn sie nicht installiert ist, installiert der Installer sie für Sie.
- **Visual C++ 2013 Redistributable-Paket**

  Wenn sie nicht installiert ist, installiert der Installer sie für Sie.
- **Visual C++ 2015 Redistributable-Paket**

  Wenn sie nicht installiert ist, installiert der Installer sie für Sie.
- **.NET Framework Version 3.5 SP1**
- **.NET Framework Version 4.5**

  Für .NET Framework Version 4,5 wurden von Microsoft Sicherheitsupdates veröffentlicht.
- **SQL Native Client 2012**

  Wenn Sie SQL Server 2012 oder SQL Server 2016 verwenden.

Wenn sie nicht installiert ist, installiert der Installer sie für Sie.

In der folgenden Tabelle sind die *Mindestanforderungen* an die Hardware für Dell Enterprise Server aufgelistet. Zusätzliche Informationen zur Skalierung basierend auf der Größe Ihrer Bereitstellung finden Sie unter Dell Enterprise Server-Architektur.

Hardwareanforderungen

Prozessor

Moderner Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

Moderner Quad-Kern-CPU (mit mindestens 2 GHz) für Einzelserver-Konfiguration

RAM

Mindestens 8 GB, je nach Konfiguration

16 GB für Einzelserver-Konfiguration

Freier Speicherplatz

ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher)

Mindestens 20 GB freier Festplattenspeicher (plus virtueller Auslagerungsspeicher) für Einzelserver-Konfiguration

Netzwerkkarte

Netzwerkschnittstellenkarte 10/100/1000

Sonstiges

TCP/IPv4 installiert und aktiviert

Software für Dell Enterprise Server

In der folgenden Tabelle sind die Software-Anforderungen für den Dell Enterprise Server und Proxy Server enthalten.

ANMERKUNG: UAC muss vor der Installation deaktiviert werden. Der Server muss neu gestartet werden, damit diese Änderung in Kraft tritt. Auf Windows Server 2012 R2 und Windows Server 2016 deaktiviert das Installationsprogramm UAC.

ANMERKUNG: Registrierungspfade für Dell Policy Proxy (sofern installiert): HKLM\SOFTWARE\Wow6432Node\Dell

ANMERKUNG: Registrierungspfad für Windows Server: HKLM\SOFTWARE\Dell

Dell Enterprise Server – Back-End-Server und Front-End-Server

- **Windows Server 2008 R2 SP0 bis SP1 64-Bit**
  - Standard Edition
  - Enterprise Edition
- **Windows Server 2008 SP2 64-Bit**
  - Standard Edition
  - Enterprise Edition

- **Windows Server 2012 R2**

  - Standard Edition

  - Datacenter Edition
- **Windows Server 2016**

  - Standard Edition

  - Datacenter Edition

Exchange ActiveSync-Server

Wenn Sie Mobile Edition verwenden möchten, werden die folgenden Exchange ActiveSync-Server unterstützt. Diese Komponente wird auf Ihrem Front-End-Exchange-Server installiert.

- Exchange ActiveSync 12.0 – eine Komponente von Exchange Server 2007
- Exchange ActiveSync 12.1 – eine Komponente von Exchange Server 2007 SP1
- Exchange ActiveSync 14.0 – eine Komponente von Exchange Server 2010
- Exchange ActiveSync 14.1 – eine Komponente von Exchange Server 2010 SP1

Microsoft Message Queuing (MSMQ) muss auf dem Exchange-Server installiert/konfiguriert sein.

LDAP-Repository

- Active Directory 2008
- Active Directory 2008 R2
- Active Directory 2012

Empfohlene virtuelle Umgebungen für Komponenten von Dell Enterprise Server

Dell Enterprise Server kann optional in einer virtuellen Umgebung installiert werden. Nur die folgenden Umgebungen werden empfohlen.

Dell Enterprise Server v9.7 wurde mit Hyper-V-Server (vollständige oder Core-Installation) und als Rolle in Windows Server 2012 R2 oder Windows Server 2016 validiert.

- Hyper-V-Server (vollständige oder Core-Installation)
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Ein Betriebssystem ist nicht erforderlich
  - Die Hardware muss die Mindestanforderungen für Hyper-V erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Muss als virtueller Computer der ersten Generation ausgeführt werden
  - Weitere Informationen finden Sie unter https://technet.microsoft.com/en-us/library/hh923062.aspx

Dell Enterprise Server v9.7 wurde mit VMware ESXi 5.5 und VMWare ESXi 6.0 validiert. Stellen Sie sicher, dass alle Patches und Aktualisierungen umgehend auf VMWare ESXi angewendet werden, um möglichen Anfälligkeiten vorzubeugen.

ANMERKUNG: Beim Ausführen von VMware ESXi und Windows Server 2012 R2 oder Windows Server 2016 werden VMXNET3 Ethernet-Adapter empfohlen.

- VMware ESXi 5.5
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen

- Ein Betriebssystem ist nicht erforderlich
- Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
- Die Hardware muss die Mindestanforderungen für VMware erfüllen
- Mindestens 4 GB RAM für dedizierte Bildressource
- Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-55/index.jsp

- VMware ESXi 6.0
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Ein Betriebssystem ist nicht erforderlich
  - Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-60/index.jsp

ANMERKUNG: Die SQL Server-Datenbank, auf der Dell Enterprise Server gehostet wird, sollte auf einem anderen Computer ausgeführt werden.

Datenbank

- **SQL Server 2008 und SQL Server 2008 R2 –** Standard Edition/Enterprise Edition
- **SQL Server 2008 SP4 (mit KB3045311) –** Standard Edition/Enterprise Edition
- **SQL Server 2012 –** Standard Edition/Business Intelligence/Enterprise Edition
- **SQL Server 2014 –** Standard Edition/Business Intelligence/Enterprise Edition
- **SQL Server 2016 –** Standard Edition/Enterprise Edition

ANMERKUNG: Der Einsatz von Express Editionen in Produktionsumgebungen wird nicht unterstützt. Express Editionen werden möglicherweise nur für Machbarkeitsnachweise und Bewertungen verwendet.

Dell Data Protection Remote Management Console und Compliance Reporter

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

ANMERKUNG: Ihr Browser muss Cookies akzeptieren.

Unterstützte Sprachen für Dell Enterprise Server

Die Remote Management Console ist Multilingual User Interface (MUI)-konform und unterstützt folgende Sprachen:

Sprachunterstützung	
EN: Englisch	JA: Japanisch
ES: Spanisch	KO: Koreanisch
FR: Französisch	PT-BR: Portugiesisch, Brasilien
IT: Italienisch	PT-PT: Portugiesisch, Portugal
DE: Deutsch	

Dell Enterprise Server Architektur

Die Dell Lösungen Verschlüsselung, Endpoint Security Suite, Endpoint Security Suite Enterprise und Data Guardian sind hoch skalierbare Produkte, die auf die Größe Ihrer Organisation und die Anzahl der für die Verschlüsselung angezielten Endpunkte skaliert werden. Dieser Abschnitt enthält Richtlinien zur Skalierung der Architektur für 5.000 bis 60.000 Endpunkte.

ANMERKUNG: Falls die Organisation mehr als 50.000 Endpunkte hat, bitten Sie den ProSupport von Dell um Hilfe.

ANMERKUNG:

Jede der in den einzelnen Abschnitten aufgeführte Komponenten enthält die minimalen Hardwarespezifikationen, die zur optimalen Leistung in den meisten Umgebungen erforderlich sind. Wenn die notwendingen Ressourcen diesen Komponenten nicht zugeordnet wurden, kann dies dazu führen, dass die Leistung abfällt oder funktionelle Probleme mit der Anwendung auftreten.

Bis zu 5.000 Endpunkte

Diese Architektur ist für die meisten kleinen bis mittelgroßen Geschäfte mit 1 bis 5.000 Endpunkten geeignet. Alle Dell Enterprise-Serverkomponenten können auf einem einzelnen Server installiert werden. Optional kann ein Frontend-Server zur Veröffentlichung von Richtlinien und/oder zur Aktivierung von Endpunkten übers Internet im DMZ platziert werden.

Architekturkomponenten

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64-Bit/Windows Server 2008 SP2 64-Bit – Standard oder Enterprise Edition

Windows Server 2012 R2 – Standard oder Datacenter Edition

Windows Server 2016 – Standard oder Datacenter Edition

Einzelserver-Konfiguration

16 GB, 20 GB oder mehr freier Festplattenspeicher (plus virtueller Auslagerungsspeicher); moderner Quad-Kern-CPU (mit mindestens 2 GHz)

Serverkonfiguration bei Verwendung mit einem Front-End-Server

Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

Externer Dell-Frontend-Server

Windows Server 2008 R2 SP0-SP1 64-Bit/Windows Server 2008 SP2 64-Bit – Standard oder Enterprise Edition

Windows Server 2012 R2 – Standard oder Datacenter Edition

Windows Server 2016 – Standard oder Datacenter Edition

Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

SQL-Server

SQL Server 2008, SQL Server 2008 R2 und SQL Server 2008 SP4 (mit KB3045311) Standard Edition/Enterprise Edition

Microsoft SQL Server 2012 Standard Edition/Business Intelligence/Enterprise Edition

Microsoft SQL Server 2014 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2016 Standard Edition/Enterprise Edition

5.000 - 20.000 Endpunkte

Diese Architektur ist für Umgebungen mit 5.000 bis 20.000 Endpunkten geeignet. Ein Frontend-Server wird hinzugefügt, um die zusätzliche Last zu verteilen, und soll ungefähr 15.000 bis 20.000 Endpunkte handhaben. Optional kann ein Frontend-Server zur Veröffentlichung von Richtlinien und/oder zur Aktivierung von Endpunkten übers Internet im DMZ platziert werden.

Architekturkomponenten

Dell Enterprise Server

Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

Interner Dell-Front-End-Server (1) und Externer Dell-Front-End-Server (1)

Windows Server 2008 R2 SP0-SP1 64-Bit/Windows Server 2008 SP2 64-Bit – Standard oder Enterprise Edition

Windows Server 2012 R2 – Standard oder Datacenter Edition

Windows Server 2016 – Standard oder Datacenter Edition

Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

SQL-Server

SQL Server 2008, SQL Server 2008 R2 und SQL Server 2008 SP4 (mit KB3045311) Standard Edition/Enterprise Edition

Microsoft SQL Server 2012 Standard Edition/Business Intelligence/Enterprise Edition

Microsoft SQL Server 2014 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2016 Standard Edition/Enterprise Edition

20.000 - 40.000 Endpunkte

Diese Architektur ist für Umgebungen mit 20.000 bis 40.000 Endpunkten geeignet. Ein zusätzlicher Frontend-Server wird zur Verteilung der zusätzlichen Last hinzugefügt. Jeder Frontend-Server soll etwa 15.000 bis 20.000 Endpunkte handhaben. Optional kann ein Frontend-Server zur Aktivierung von Endpunkten und/oder Veröffentlichung von Richtlinien an Endpunkte übers Internet im DMZ platziert werden.

Architekturkomponenten

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64-Bit/Windows Server 2008 SP2 64-Bit – Standard oder Enterprise Edition

Windows Server 2012 R2 – Standard oder Datacenter Edition

Windows Server 2016 – Standard oder Datacenter Edition

Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

Interne Dell-Front-End-Server (2) und Externer Dell-Front-End-Server (1)

Windows Server 2008 R2 SP0-SP1 64-Bit/Windows Server 2008 SP2 64-Bit – Standard oder Enterprise Edition

Windows Server 2012 R2 – Standard oder Datacenter Edition

Windows Server 2016 – Standard oder Datacenter Edition

Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

SQL-Server

SQL Server 2008, SQL Server 2008 R2 und SQL Server 2008 SP4 (mit KB3045311) Standard Edition/Enterprise Edition

Microsoft SQL Server 2012 Standard Edition/Business Intelligence/Enterprise Edition

Microsoft SQL Server 2014 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2016 Standard Edition/Enterprise Edition

40.000 - 60.000 Endpunkte

Diese Architektur ist für Umgebungen mit 40.000 bis 60.000 Endpunkten geeignet. Ein zusätzlicher Frontend-Server wird zur Verteilung der zusätzlichen Last hinzugefügt. Jeder Frontend-Server soll etwa 15.000 bis 20.000 Endpunkte handhaben. Optional kann ein Frontend-Server zur Aktivierung von Endpunkten und/oder Veröffentlichung von Richtlinien an Endpunkte übers Internet im DMZ platziert werden.

ANMERKUNG:
Falls die Organisation mehr als 50.000 Endpunkte hat, bitten Sie den ProSupport von Dell um Hilfe.

Architekturkomponenten

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64-Bit/Windows Server 2008 SP2 64-Bit – Standard oder Enterprise Edition

Windows Server 2012 R2 – Standard oder Datacenter Edition

Windows Server 2016 – Standard oder Datacenter Edition

Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

Interne Dell-Front-End-Server (2) und Externer Dell-Front-End-Server (1)

Windows Server 2008 R2 SP0-SP1 64-Bit/Windows Server 2008 SP2 64-Bit – Standard oder Enterprise Edition

Windows Server 2012 R2 – Standard oder Datacenter Edition

Windows Server 2016 – Standard oder Datacenter Edition

Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

SQL-Server

SQL Server 2008, SQL Server 2008 R2 und SQL Server 2008 SP4 (mit KB3045311) Standard Edition/Enterprise Edition

Microsoft SQL Server 2012 Standard Edition/Business Intelligence/Enterprise Edition

Microsoft SQL Server 2014 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2016 Standard Edition/Enterprise Edition

Überlegungen für hohe Verfügbarkeit

Diese Architektur beschreibt eine höchst verfügbare Architektur, die bis zu 60.000 Endpunkte unterstützt. Es wurden auch zwei Dell Enterprise Server in einer aktiven/passiven Konfiguration eingerichtet. Um ein Failover auf den zweiten Dell Enterprise Server auszuführen, halten Sie die Dienste auf dem Primärknoten an und weisen das DNS-Alias (CNAME) auf den zweiten Knoten. Starten Sie die Dienste auf dem zweiten Knoten, und starten Sie die Remote Management-Konsole, um sicherzustellen, dass die Anwendung ordnungsgemäß läuft. Die Dienste auf dem zweiten (passiven) Knoten sollten als "Manuell" konfiguriert sein, um zu vermeiden, dass diese Dienste während einer regulären Wartung und Patching unabsichtlich gestartet werden.

Eine Organisation kann auch einen SQL Cluster-Datenbankserver haben. In dieser Konfiguration sollte der Dell Enterprise Server so konfiguriert sein, dass er den Cluster-IP- oder Hostnamen verwendet.

ANMERKUNG:
Die Datenbankreplikation wird nicht unterstützt.

Der Client-Datenverkehr wird über drei interne Frontend-Server verteilt. Optional können Frontend-Server auch zur Aktivierung von Endpunkten und/oder Veröffentlichung von Richtlinien an Endpunkte übers Internet im DMZ platziert werden.

Virtualisierung

Dell Enterprise Server kann optional in einer virtuellen Umgebung installiert werden. Nur die folgenden Umgebungen werden empfohlen.

Dell Enterprise Server v9.7 wurde mit Hyper-V-Server (vollständige oder Core-Installation) und als Rolle in Windows Server 2012 R2 oder Windows Server 2016 validiert.

- Hyper-V-Server (vollständige oder Core-Installation)
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Ein Betriebssystem ist nicht erforderlich
  - Die Hardware muss die Mindestanforderungen für Hyper-V erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Muss als virtueller Computer der ersten Generation ausgeführt werden
  - Weitere Informationen finden Sie unter https://technet.microsoft.com/en-us/library/hh923062.aspx

Dell Enterprise Server v9.7 wurde mit VMware ESXi 5.5 und VMWare ESXi 6.0 validiert. Stellen Sie sicher, dass alle Patches und Aktualisierungen umgehend auf VMWare ESXi angewendet werden, um möglichen Anfälligkeiten vorzubeugen.

ANMERKUNG: Beim Ausführen von VMware ESXi und Windows Server 2012 R2 oder Windows Server 2016 werden VMXNET3 Ethernet-Adapter empfohlen.

- VMware ESXi 5.5
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Ein Betriebssystem ist nicht erforderlich
  - Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-55/index.jsp
- VMware ESXi 6.0
  - 64-Bit x86 CPU erforderlich

- Hostcomputer mindestens mit Doppelkern
- Mindestens 8 GB RAM empfohlen
- Ein Betriebssystem ist nicht erforderlich
- Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
- Die Hardware muss die Mindestanforderungen für VMware erfüllen
- Mindestens 4 GB RAM für dedizierte Bildressource
- Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-60/index.jsp

ANMERKUNG: Die SQL Server-Datenbank, auf der Dell Enterprise Server gehostet wird, sollte auf einem anderen Computer ausgeführt werden.

SQL-Server

In größeren Umgebungen wird empfohlen, dass der SQL-Datenbankserver auf einem redundanten System ausgeführt wird, wie z. B. einem SQL-Cluster, um die Verfügbarkeit und Datenkontinuität sicherzustellen. Es wird auch empfohlen, täglich eine vollständige Sicherung mit aktivierter Transaktionsprotokollierung auszuführen, um sicherzustellen, dass neu durch Benutzer-/Geräteaktivierung generierte Schlüssel wiederherstellbar sind.

Aufgaben zur Datenbankwartung sollten den Neuaufbau aller Datenbankindizes und das Sammeln von Statistik einschließen.

3

Vorinstallationskonfiguration

Lesen Sie vor Beginn die *Technischen Tipps für Enterprise Server*, um sich über aktuelle Lösungen oder bekannte Probleme in Verbindung mit Dell Enterprise Server zu informieren.

Die Vorinstallationskonfiguration der Server, auf denen Sie Dell Enterprise Server installieren möchten, ist sehr wichtig. Sehen Sie sich diesen Abschnitt genau an, um sicherzustellen, dass Dell Enterprise Server fehlerfrei installiert wird.

Konfiguration

1 Deaktivieren Sie, falls aktiviert, die verstärkte Sicherheitskonfiguration für Internet Explorer (ESC). Fügen Sie die Server-URL den vertrauenswürdigen Sites in den Sicherheitsoptionen des Browsers hinzu. Starten Sie den Server neu.

2 Öffnen Sie die folgenden Ports für die einzelnen Komponenten:

Intern:

Active Directory-Kommunikation: TCP/389

E-Mail-Kommunikation (optional): 25

An Frontend (falls nötig):

Kommunikation zwischen externem Dell Policy Proxy und Dell Message Broker: TCP/61616 und STOMP/61613

Kommunikation mit Back-End Dell Security Server: HTTPS/8443

Kommunikation mit Back-End Dell Core Server: HTTPS/8888 and 9000

Kommunikation mit RMI-Ports - 1099

Kommunikation mit Back-End Dell Device Server: HTTP(S)/8443 – Falls Sie einen Dell Enterprise Server ab Version 7.7 verwenden. Falls Ihr Dell Enterprise Server eine Version vor v7.7, HTTP(S)/8081 ist.

Beacon-Server: HTTP/8446 (bei Verwendung von Data Guardian)

Extern (falls nötig):

SQL-Datenbank: TCP/1433

Remote Management Console: HTTPS/8443

LDAP: TCP/389/636 (lokaler Domänencontroller), TCP/3268/3269 (globaler Katalog), TCP/135/49125+ (RPC)

Dell Compatibility Server: TCP/1099

Dell Compliance Reporter: HTTP(S)/8084 (wird bei der Installation automatisch konfiguriert)

Dell Identity Server: HTTPS/8445

Dell Core Server: HTTPS/8888 und 9000 (8888 wird bei der Installation automatisch konfiguriert)

Dell Device Server: HTTP(S)/8443 (ab Dell Enterprise Server 7.7) oder HTTP(S)/8081 (Dell Enterprise Server vor Version 7.7)

Dell Schlüssel-Server: TCP/8050

Dell Policy Proxy: TCP/8000

Dell Security Server: HTTPS/8443

Clientauthentifizierung: HTTPS/8449 (falls die Server-Verschlüsselung verwendet wird)

Client-Kommunikation, wenn Advanced Threat Prevention verwendet wird: HTTPS/TCP/443

ANMERKUNG:
Wenn für Ihre Enterprise Edition Clients werksseitige Berechtigungen vorliegen oder Sie Lizenzen erwerben, aktivieren Sie diese Berechtigungen durch das Einrichten eines Gruppenrichtlinienobjekts auf dem Domänencontroller (das darf nicht der Server sein, auf dem Enterprise Edition ausgeführt wird). Achten Sie bitte darauf, dass der ausgehende Port 443 für die Kommunikation mit dem Server verfügbar ist. Falls der Port 443 (aus irgendeinem Grund) gesperrt ist, funktioniert die Berechtigungsfunktion nicht. Weitere Informationen finden Sie im Enterprise Edition-Handbuch für erweiterte Installation.

Dell Datenbank erstellen

3 Wenn Sie noch keine SQL-Datenbank für Dell Enterprise Server konfiguriert haben, erstellt das Installationsprogramm die Datenbank während der Installation für Sie. Falls Sie lieber eine Datenbank einrichten, bevor Sie Dell Enterprise Server installieren, befolgen Sie die folgenden Anweisungen zur Erstellung der SQL-Datenbank und des SQL-Benutzers im SQL Management Studio. ***Diese Anleitungen sind optional, weil das Installationsprogramm eine Datenbank für Sie erstellt, falls noch keine vorhanden ist.***

Folgen Sie bei der Installation von Dell Enterprise Server den Anleitungen unter Back-End-Server mit vorhandener Datenbank installieren.

Der Dell Enterprise Server ist für die SQL- und Windows-Authentifizierung ausgelegt. Das Standardauthentifizierungsverfahren ist die SQL-Authentifizierung.

Erstellen Sie nach dem Anlegen der Datenbank einen Datenbankbenutzer mit db_owner-Rechten. Ein Benutzer mit db_owner-Rechten kann Berechtigungen zuweisen, die Datenbank sichern und wiederherstellen, Objekte erstellen und löschen sowie Benutzerkonten und -rollen uneingeschränkt verwalten. Stellen Sie außerdem sicher, dass ein solcher Benutzer Berechtigungen zum Ausführen der gespeicherten Verfahren hat.

Bei Verwendung einer nicht standardmäßiger SQL Server-Instanz und nach der Installation des Dell Enterprise Servers müssen Sie auf der Registerkarte „Datenbank“ des Serverkonfigurationstools den dynamischen Port der Instanz angeben. Weitere Informationen finden Sie unter Serverkonfigurationstool. Alternativ dazu aktivieren Sie den SQL Server Browser-Service und stellen Sie sicher, dass UDP-Port 1434 geöffnet ist. Weitere Informationen finden Sie unter https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

Falls entweder die SQL-Datenbank oder SQL-Instanz mit einer nicht standardmäßigen Sortierreihenfolge konfiguriert wird, muss bei der nicht-standardmäßigen Sortierung die Groß- und Kleinschreibung nicht beachtet werden. Eine Liste der Sortierreihenfolgen und Groß- und Kleinschreibung finden Sie unter https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx.

Wählen Sie eine der folgenden Optionen zum Erstellen der SQL-Datenbank und des SQL-Benutzers in SQL Management Studio.

Unter Verwendung von Windows-Authentifizierung eine neue Windows SQL Server-Datenbank erstellen:

a Klicken Sie auf **Start** > **Alle Programme** > **Microsoft SQL Server** > **Management Studio**.

b Klicken Sie mit der rechten Maustaste auf den Ordner „Datenbanken“, und klicken Sie dann auf „Neue Datenbank“. Daraufhin wird das Dialogfeld „Datenbankeigenschaften“ angezeigt.

c Geben Sie den Datenbanknamen ein, und klicken Sie dann auf **OK**.

d Erweitern Sie den Ordner *Sicherheit*, und klicken Sie dann mit der rechten Maustaste auf **Anmeldungen**.

e Klicken Sie zur Erstellung eines Benutzers für die neue Datenbank auf **Neue Anmeldung**.

f Geben Sie einen Benutzernamen in das Feld *Name* ein.

g Wählen Sie die Authentifizierungsoption *Windows-Authentifizierung* aus.

h Wählen Sie **Benutzerzuweisung** aus, und markieren Sie dann die neue Datenbank.

i Wählen Sie die Datenbankrolle (db_owner) aus, und klicken Sie dann auf **OK**.

ODER

Unter Verwendung von SQL Server-Authentifizierung eine neue SQL Server-Datenbank erstellen:

a Klicken **Start** > **Alle Programe** > **Microsoft SQL Server** > **Management Studio**.

b Klicken Sie mit der rechten Maustaste auf den Ordner *Datenbanken*, und klicken Sie dann auf **Neue Datenbank**. Daraufhin wird das Dialogfeld *Datenbankeigenschaften* angezeigt.

c Geben Sie den Datenbanknamen ein, und klicken Sie dann auf **OK**.

d Erweitern Sie den Ordner *Sicherheit*, und klicken Sie dann mit der rechten Maustaste auf **Anmeldungen**.

e Klicken Sie zur Erstellung eines Benutzers für die neue Datenbank auf **Neue Anmeldung**.

f Geben Sie einen Benutzernamen in das Feld *Name* ein.

g Wählen Sie die Authentifizierungsoption *SQL Server-Authentifizierung* aus. Geben Sie das Kennwort ein und bestätigen Sie es.

h Heben Sie die Auswahl der Option **Ablauf des Passworts erzwingen** auf.

i Wählen Sie **Benutzerzuweisung** aus, und markieren Sie dann die neue Datenbank.

j Wählen Sie die Datenbankrolle (db_owner) aus, und klicken Sie dann auf **OK**.

Visual C++ 2010/2013/2015 Redistributable-Pakete installieren

4 *Falls noch nicht installiert*, installieren Sie die Visual C++ 2010, 2013 und 2015 Redistributable-Pakete. Sie können festlegen, dass diese Komponenten vom Enterprise Server-Installationsprogramm installiert werden.

Windows Server 2008 und Windows Server 2008 R2 – http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5555

Installieren von .NET Framework 4.5

5 *Falls noch nicht installiert*, installieren Sie .NET Framework 4.5.

Windows Server 2008 und Windows Server 2008 R2 – https://www.microsoft.com/en-us/download/details.aspx?id=42643

SQL Native Client 2012 installieren

6 *Wenn Sie SQL Server 2012 oder SQL Server 2016 verwenden* , installieren Sie SQL Native Client 2012. Sie können festlegen, dass diese Komponente vom Enterprise Server-Installationsprogramm installiert wird.

http://www.microsoft.com/en-us/download/details.aspx?id=35580

Konfigurieren der Microsoft-Zertifizierungsstelle (MSCEP)

Dieser Schritt muss auf Servern, die MSCEP ausführen, nur dann abgeschlossen werden, wenn Sie iOS mit Mobile Edition verwenden möchten.

7 Konfigurieren Sie MSCEP.

Windows Server 2008 R2 muss in der Enterprise Edition vorhanden sein. ***Bei Verwendung der Standard Edition kann die MSCEP-Rolle nicht installiert werden.***

a Öffnen Sie Server-Manager. Wählen Sie im Menü auf der linken Seite **Serverrollen** aus, und aktivieren Sie das Kontrollkästchen für die Option **Active Directory-Zertifikatsdienste**. Klicken Sie auf **Weiter**. Der Assistent zum Hinzufügen von Rollen führt Sie durch die nächsten Schritte.

Aktivieren Sie unter *AD-Zertifikatsdienste* > *Rollendienste* die Kontrollkästchen für die Rollendienste **Zertifikatstelle** und **Zertifizierungsstellen-Webregistrierung**. Wählen Sie die Option **Erforderliche Rollendienste für Webserver IIS hinzufügen** (nach Aufforderung) aus. Klicken Sie auf **Weiter**.

Wählen Sie unter *AD-Zertifikatsdienste* > *Setuptyp* die Option **Eigenständig** aus. Klicken Sie auf **Weiter**.

Wählen Sie unter *AD-Zertifikatsdienste* > *Zertifizierungsstellentyp* die Option **Untergeordnete Zertifizierungsstelle** aus. Klicken Sie auf **Weiter**.

Wählen Sie unter *AD-Zertifikatsdienste* > *Privater Schlüssel* die Option **Neuen privaten Schlüssel erstellen** aus. Klicken Sie auf **Weiter**.

Behalten Sie unter *AD-Zertifikatsdienste* > *Privater Schlüssel* > *Kryptografie* die Standardwerte für den **RSA#Softwareschlüsselspeicher-Anbieter** von Microsoft, **2048** und **SHA1** bei. Klicken Sie auf **Weiter**.

Behalten Sie unter *AD-Zertifikatsdienste* > *Privater Schlüssel* > *Name der Zertifizierungsstelle* die Standardwerte bei. Klicken Sie auf **Weiter**.

Wählen Sie unter *AD-Zertifikatsdienste* > *Privater Schlüssel* > *Zertifikatsanforderung* die Option **Zertifikatsanforderung an übergeordnete Zertifizierungsstelle senden** aus. Wählen Sie die Option **Durchsuchen nach: Name der Zertifizierungsstelle** aus. Navigieren Sie zur **übergeordneten Zertifizierungsstelle** und wählen Sie sie aus. Klicken Sie auf **Weiter**.

Behalten Sie unter *AD-Zertifikatdienste* > *Zertifikatdatenbank* die Standardwerte bei. Klicken Sie auf **Weiter**.

Klicken Sie unter *Webserver (IIS)* auf **Weiter**.

Behalten Sie unter *Webserver (IIS)* > *Rollendienste* die Standardwerte bei. Klicken Sie auf **Weiter**.

Klicken Sie unter *Bestätigung* auf **Installieren**.

Überprüfen Sie unter *Ergebnisse* die angezeigten Ergebnisse, und klicken Sie auf **Schließen**.

Wählen Sie unter *Server-Manager* > *Rollen* die Option **Rollendienste hinzufügen** unter *Active Directory-Zertifikatsdienste* aus.

Wenn das Fenster *Rollendienste auswählen* angezeigt wird, aktivieren Sie das Kontrollkästchen **Registrierungsdienst für Netzwerkgeräte.** Klicken Sie auf **Weiter**.

Fügen Sie das Benutzerkonto hinzu, das durch den *Registrierungsdienst für Netzwerkgeräte* bei der Autorisierung von Zertifikatsanfragen an die Benutzergruppe von IIS_IUSRS des lokalen Servers verwendet werden soll. Das Format lautet „Domäne\Benutzername“. Klicken Sie auf **OK**.

Wählen Sie in den Fenstern „Benutzerkonto angeben“ den Benutzer aus, den Sie gerade zur IIS_IUSRS-Gruppe hinzugefügt haben. Klicken Sie auf **Weiter**.

Behalten Sie im Fenster *Informationen zur Registrierungsstelle angeben* bei Bedarf die Standardwerte für *Erforderliche Informationen* und *Optionale Informationen hinzufügen* bei. Klicken Sie auf **Weiter**.

Behalten Sie im Fenster *Kryptografie für Registrierungsstelle konfigurieren* die Standardwerte bei. Klicken Sie auf **Weiter**.

Klicken Sie im Fenster *Installationsauswahl bestätigen* auf **Installieren**.

Überprüfen Sie im Fenster *Installationsergebnisse* die Ergebnisse, und klicken Sie dann auf **Schließen**.

Schließen Sie den Server-Manager.

b Ändern Sie den Registrierungsschlüssel wie folgt:

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

„EnforcePassword“=dword:00000000

c Öffnen Sie IIS-Manager. Navigieren Sie zu **\<ServerName > \Sites\Default Web Site\CertSrv\mscep_admin**.

Öffnen Sie *Authentifizierung*, und aktivieren Sie **Anonyme Authentifizierung**.

d Klicken Sie auf **Start** > **Ausführen**. Geben Sie *certsrv.msc* ein, und drücken Sie auf die **Eingabetaste**.

Wenn das Fenster *certsrv* angezeigt wird, klicken Sie mit der rechten Maustaste auf den Servernamen, wählen Sie **Eigenschaften** aus, und klicken Sie dann auf die Registerkarte ***Richtlinienmodul***.

Klicken Sie auf **Eigenschaften** und wählen Sie dann folgende Option aus: **Den Einstellungen der Zertifikatsvorlage folgen, falls zutreffend**. **Zertifikat ansonsten automatisch ausstellen.** Klicken Sie auf **OK**.

e Schließen Sie IIS-Manager.

f Starten Sie den Server neu. Öffnen Sie zur Überprüfung Internet Explorer, und geben Sie in die Adresszeile Folgendes ein:

http://server.domain.com/certsrv/mscep_admin/.

Ende des MSCEP Windows Server 2008 R2-Setups.

Windows Server 2012 R2 oder Windows Server 2016:

a Folgen Sie den Setup-Anweisungen im Artikel Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS).

b Ändern Sie den Registrierungsschlüssel wie folgt:

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

„EnforcePassword“=dword:00000000

c Öffnen Sie IIS-Manager. Wechseln Sie zu **<ServerName>\Sites\Default Web Site\CertSrv\mscep_admin**.

Öffnen Sie *Authentifizierung*, und aktivieren Sie **Anonyme Authentifizierung**.

d Klicken Sie auf **Start** > **Ausführen**. Geben Sie *certsrv.msc* ein, und drücken Sie auf die **Eingabetaste**.

Wenn das Fenster *certsrv* angezeigt wird, klicken Sie mit der rechten Maustaste auf den Servernamen, wählen Sie **Eigenschaften** aus, und klicken Sie dann auf die Registerkarte ***Richtlinienmodul***.

Klicken Sie auf **Eigenschaften** und wählen Sie dann die Option **Den Einstellungen der Zertifikatsvorlage folgen, falls zutreffend**. **Zertifikat ansonsten automatisch ausstellen.** Klicken Sie auf **OK**.

e Schließen Sie IIS-Manager.

f Starten Sie den Server neu. Öffnen Sie zur Überprüfung Internet Explorer, und geben Sie in die Adresszeile Folgendes ein:

http://server.domain.com/certsrv/mscep_admin/.

Ende des MSCEP Windows Server 2012 R2/Windows Server 2016-Setups.

Microsoft Message Queuing (MSMQ) installieren oder konfigurieren

Sie müssen diesen Schritt nur dann abschließen, wenn Sie Mobile Edition verwenden möchten. Er ist Voraussetzung für die Kommunikation zwischen dem EAS-Geräte-Manager und dem EAS Mailbox-Manager.

8 Auf Windows Server 2008 oder Windows Server 2008 R2 (auf dem Server, auf dem die Exchange-Umgebung gehostet wird): http://msdn.microsoft.com/en-us/library/aa967729.aspx

ODER

Auf Windows Server 2012 R2:

a Öffnen Sie Server-Manager.

b Navigieren Sie zu **Verwalten** > **Rollen und Funktionen hinzufügen**.

c Klicken Sie im Bildschirm „Vor der Installation“ auf **Weiter**.

d Wählen Sie **Rollenbasierte oder funktionsbasierte Installation** aus, und klicken Sie auf **Weiter**.

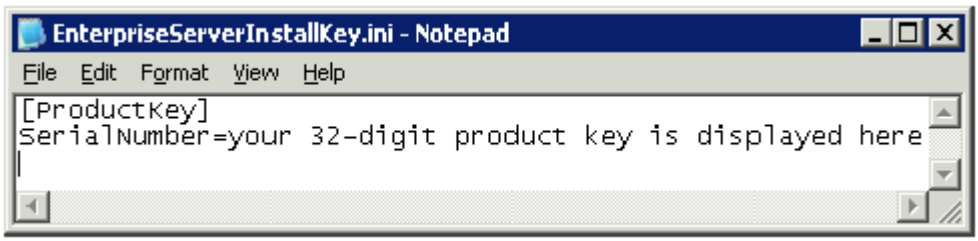
e Wählen Sie den Server aus, auf dem die Funktion installiert werden soll, und klicken Sie auf **Weiter**.

f Wählen Sie keine Serverrollen aus. Klicken Sie auf **Weiter**.

g Wählen Sie bei den Funktionen **Message Queuing** aus, und klicken Sie auf **Installieren**.

Optional

9 **Bei einer neuen Installation** – Kopieren Sie Ihren Produktschlüssel (der Name der Datei lautet *EnterpriseServerInstallKey.ini*) nach **C:\Windows**, um den Produktschlüssel mit 32 Zeichen automatisch in das Dell Enterprise Server-Installationsprogramm zu übertragen.



Die Vorinstallationskonfiguration des Servers ist abgeschlossen. Fahren Sie fort mit Installieren, Aktualisieren und Migrieren.

4

Installation oder Upgrade/Migraton

Das Kapitel enthält Anweisungen für folgende Aufgaben:

- Neue Installation – Ermöglicht die Installation eines neuen Dell Enterprise Servers.
- Aktualisierung/Migration – Ermöglicht die Aktualisierung von einem vorhandenen, funktionsfähigen Dell Enterprise Server ab Version 8.0.
- Dell Enterprise Server deinstallieren – Ermöglicht bei Bedarf das Entfernen der derzeitigen Installation.

  Falls Ihre Installation mehr als einen Hauptserver (Back-End-Server) enthalten muss, kontaktieren Sie Ihren Dell ProSupport-Mitarbeiter.

Vor der Installation, Aktualisierung oder Migration

Bevor Sie beginnen, stellen Sie sicher, dass die Schritte für die Vorinstallationskonfiguration durchgeführt wurden.

Lesen Sie die *Technischen Tipps für Enterprise Server*, um sich über aktuelle Lösungen oder bekannte Probleme hinsichtlich der Installation von Dell Enterprise Server zu informieren.

Falls User Account Control (UAC, Benutzerkontosteuerung) aktiviert ist, müssen Sie es deaktivieren. Auf Windows Server 2012 R2 deaktiviert das Installationsprogramm UAC. Der Server muss neu gestartet werden, damit diese Änderung in Kraft tritt.

Während der Installation benötigen Sie Ihre Windows oder SQL Anmeldeinformationen, um die Datenbank einrichten zu können. Wenn Sie sich für die Windows-Authentifizierung entscheiden, werden die Anmeldeinformationen des bereits angemeldeten Benutzers verwendet. Der Benutzer muss über Administratorrechte sowie über Rechte zum Erstellen und Verwalten der SQL Datenbank verfügen (Datenbank erstellen, Benutzer hinzufügen und Berechtigungen zuweisen). Bei einer SQL-Authentifizierung muss das Konto die gleichen Rechte aufweisen. Diese Anmeldeinformationen werden nur während der Installation verwendet. Das installierte Produkt verwendet nicht diese Anmeldeinformationen.

Des Weiteren müssen während der Installation die Service-Laufzeit-Anmeldeinformationen für Dell Dienste angegeben werden, um auf den SQL Server zugreifen und ihn verwenden zu können. Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: db_owner, public verfügen.

Wenn Sie sich unsicher sind in Bezug auf die Zugriffsberechtigungen oder die Konnektivität zur Datenbank, bitten Sie Ihren Datenbankadministrator um Auskunft, bevor Sie mit der Installation beginnen.

Dell empfiehlt, für die Dell Datenbank die bewährten Verfahren für Datenbanken zu verwenden und Dell Software in den Notfall-Wiederherstellungsplan Ihres Unternehmens einzubeziehen.

Wenn Sie Dell-Komponenten in Ihre DMZ implementieren möchten, vergewissern Sie sich, dass sie ausreichend vor Angriffen geschützt sind.

Für Produktionsumgebungen empfiehlt Dell dringend, die Installation von SQL Server auf einem dedizierten Server vorzunehmen.

Es ist ein bewährtes Verfahren, den Back-End Server vor der Installation und Konfiguration des Front-End-Servers zu installieren.

Die Installationsprotokolldateien befinden sich in diesem Verzeichnis: **C: \ProgramData\Dell\Dell Data Protection\Installationsprotokolle**

Neue Installation

Wählen Sie eine von zwei Optionen für die Back-End-Serverinstallation:

- Back-End-Server und neue Datenbank installieren – Ermöglicht die Installation eines neuen Dell Enterprise Servers und einer neuen Datenbank.
- Back-End-Server mit vorhandener Datenbank installieren – Ermöglicht die Installation eines neuen Dell Enterprise Servers und die Verbindung mit einer im Rahmen der Vorinstallationskonfiguration erstellten oder einer vorhandenen SQL-Datenbank ab Version 9.x, wenn die Schemaversion mit der zu installierenden Dell Enterprise Server-Version übereinstimmt. Eine Datenbank ab Version v8.x muss mit der neuesten Version des Serverkonfigurationstools auf das neueste Schema migriert werden. Anweisungen zur Datenbankmigration mit dem Serverkonfigurationstool finden Sie unter Datenbank migrieren. Um die neueste Version des Serverkonfigurationstools zu erhalten oder eine Datenbank vor Version 8.0 zu migrieren, wenden Sie sich bitte an Dell ProSupport.

ANMERKUNG:
Falls Sie über einen funktionsfähigen Dell Enterprise Server ab Version 8.x verfügen, lesen Sie die Anweisungen unter **Back-End-Server aktualisieren oder migrieren**

Falls Sie einen Front-End-Server installieren, führen Sie diese Installation vor der Installation des Back-End-Servers aus:

- Front-End-Server installieren – Ermöglicht die Installation eines Front-End-Servers zur Kommunikation mit dem Back-End-Server.

Back-End-Server und neue Datenbank installieren

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

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

3 Wählen Sie im Dialogfeld *InstallShield-Assistenten* die Sprache für die Installation aus, und klicken Sie dann 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 Falls Sie den optionalen Schritt 9 der Vorinstallationskonfiguration abgeschlossen haben, klicken Sie auf **Weiter**. Falls nicht, dann geben Sie den 32 Zeichen langen Produktschlüssel ein, und klicken Sie dann auf **Weiter**. Der Produktschlüssel befindet sich in der Datei *EnterpriseServerInstallKey.ini*.

8 Wählen Sie **Back-End-Installation** aus und klicken Sie auf **Weiter**.

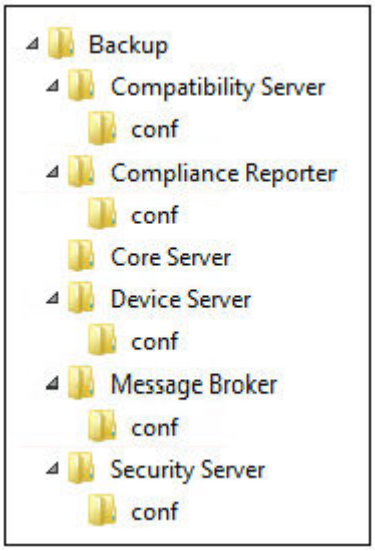
9 Klicken Sie zur Installation des Dell Enterprise Servers im Standardverzeichnis **C:\Programme\Dell** auf **Weiter**. Klicken Sie anderenfalls auf **Ändern**, um einen anderen Speicherort auszuwählen; klicken Sie anschließend auf **Weiter.**

10 Klicken Sie zur Auswahl eines Speicherorts für zu speichernde Konfigurations-Sicherungsdateien auf **Ändern**, navigieren Sie zum gewünschten Ordner und klicken Sie anschließend auf **Weiter**.

Dell empfiehlt die Auswahl eines Remote-Netzwerkspeicherortes oder eines externen Sicherungslaufwerks.

Nach der Installation müssen alle Änderungen an den Konfigurationsdateien, einschließlich Änderungen, die mit dem Serverkonfigurationstool vorgenommen werden, manuell in diesen Ordnern gesichert werden. Konfigurationsdateien sind ein wichtiger Bestandteil der gesamten Informationen, die für die manuelle Wiederherstellung des Servers verwendet werden.

ANMERKUNG: Die durch das Installationsprogramm während des Installationsschritts erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.



11 Sie können aus verschiedenen digitalen Zertifikatstypen auswählen. **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**.

Klicken Sie auf **Durchsuchen**, um den Pfad zum Zertifikat einzugeben.

Geben Sie das Passwort ein, das mit diesem Zertifikat verknüpft ist. Die Keystore-Datei muss „.p12“ oder „pfx“ sein. Anleitungen finden Sie unter Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

Klicken Sie auf **Weiter**.

> **ANMERKUNG:**
> Wenn Sie diese Einstellung verwenden möchten, muss das exportierte Zertifikat der Zertifizierungsstelle für den Import eine vollständige Vertrauenskette aufweisen. Wenn Sie nicht sicher sind, führen Sie den Export des Zertifikats der Zertifizierungsstelle erneut aus, und stellen Sie sicher, dass die folgenden Optionen im Assistenten für den Zertifikatsexport ausgewählt wurden:
>
> - Privater Informationsaustausch – PKCS#12 (.PFX)
> - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
> - Alle erweiterten Eigenschaften exportieren

ODER

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 einem Jahr ab.

12 Für die Server Encryption (SE, Serververschlüsselung) können Sie aus verschiedenen digitalen Zertifikattypen auswählen. 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**.

Klicken Sie auf **Durchsuchen**, um den Pfad zum Zertifikat einzugeben.

Geben Sie das Passwort ein, das mit diesem Zertifikat verknüpft ist. Die Keystore-Datei muss „.p12“ oder „pfx“ sein. Anleitungen finden Sie unter Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

Klicken Sie auf **Weiter**.

> **ANMERKUNG:**
> Wenn Sie diese Einstellung verwenden möchten, muss das exportierte Zertifikat der Zertifizierungsstelle für den Import eine vollständige Vertrauenskette aufweisen. Wenn Sie nicht sicher sind, führen Sie den Export des Zertifikats der Zertifizierungsstelle erneut aus, und stellen Sie sicher, dass die folgenden Optionen im Assistenten für den Zertifikatsexport ausgewählt wurden:
>
> - Privater Informationsaustausch – PKCS#12 (.PFX)
> - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
> - Alle erweiterten Eigenschaften exportieren

ODER

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 einem Jahr ab.

13 Über das Setup-Dialogfeld *Back-End-Server-Einrichtung* können Sie Hostnamen und Ports anzeigen oder bearbeiten.

- Klicken Sie zum Übernehmen der Standard-Hostnamen und -Ports im Dialogfeld *Back-End-Server-Installationseinrichtung* auf **Weiter**.
- Wenn Sie einen Front-End-Server verwenden, dann wählen Sie **Nutzt für die Kommunikation mit Clients intern in Ihrem Netzwerk oder extern in der DMZ den Front-End-Server** und geben Sie den Front-End-Sicherheitsserver-Hostnamen ein (zum Beispiel server.domain.com).

- Klicken Sie zum Anzeigen oder Bearbeiten von Hostnamen auf **Hostnamen bearbeiten**. Bearbeiten Sie Hostnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen.

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

  Klicken Sie anschließend auf **OK**.
- Klicken Sie zum Anzeigen oder Bearbeiten von Ports auf **Ports bearbeiten**. Bearbeiten Sie Portnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen. Klicken Sie anschließend auf **OK**.

14 Zum Erstellen einer neuen Datenbank gehen Sie wie folgt vor:

a Klicken Sie auf **Durchsuchen**, um den Server auszuwählen, auf dem die Datenbank installiert werden soll.

b Wählen Sie die Authentifizierungsmethode aus, die das Installationsprogramm zum Einrichten der Dell Data Protection-Datenbank verwenden soll. Nach der Installation verwendet das installierte Produkt nicht die hier angegebenen Anmeldeinformationen.

- **Anmeldeinformationen für die Windows-Authentifizierung des aktuellen Benutzers**

  Bei Auswahl der Option „Windows-Authentifizierung“ werden zur Authentifizierung dieselben Anmeldeinformationen verwendet wie bei der Anmeldung bei Windows (die Felder „Benutzername“ und „Kennwort“ sind nicht bearbeitbar). Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt.

  ODER

- **SQL-Server-Authentifizierung über die unten angegebenen Anmeldeinformationen**

  Bei Verwendung der SQL-Authentifizierung muss das verwendete SQL-Konto auf dem SQL-Server über Systemadministratorberechtigungen verfügen.

  Das Installationsprogramm muss sich anhand der folgenden Berechtigungen auf dem SQL Server authentifizieren: Datenbank erstellen, Benutzer hinzufügen, Berechtigungen zuweisen.

c Identifizierung des Datenbank-Katalogs:

Geben Sie den Namen für einen neuen Datenbank-Katalog ein. Sie werden im nächsten Dialogfeld zur Erstellung des neuen Katalogs aufgefordert.

d Klicken Sie auf **Weiter**.

e Bestätigen Sie, dass das Installationsprogramm eine Datenbank erstellen soll, indem Sie auf **Ja** klicken. Um zum vorherigen Bildschirm zurückzukehren und Änderungen vorzunehmen, klicken Sie auf **Nein**.

15 Wählen Sie die Authentifizierungsmethode für das zu verwendende Produkt aus. Dieser Schritt verbindet ein Konto mit dem Produkt.

- **Windows-Authentifizierung**

  Wählen Sie **Windows-Authentifizierung über die unten angegebenen Anmeldeinformationen** aus, geben Sie die Anmeldeinformationen für das zu verwendende Produkt ein, und klicken Sie auf **Weiter**.

  Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt. Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.

  Diese Anmeldeinformationen werden auch von den Dell Diensten verwendet, da sie mit dem Dell Enterprise Server funktionieren.

  ODER

- **SQL Server-Authentifizierung**

  Wählen Sie **SQL-Server-Authentifizierung über die unten angegebenen Anmeldeinformationen** aus, geben Sie die SQL-Server-Anmeldeinformationen für die Dell Dienste, die verwendet werden sollen, da sie mit dem Dell Enterprise Server funktionieren, und klicken Sie dann auf **Weiter.**

  Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.

16 Klicken Sie im Dialogfeld *Bereit zur Installation des Programms* auf **Installieren**.
Ein Fortschritts-Dialogfeld zeigt während des gesamten Installationsvorgangs den Status an.

17 Wenn die Installation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.
Die Back-End-Server Installationsaufgaben wurden abgeschlossen.

Die Dell Services werden am Ende der Installation neu gestartet. Es ist nicht erforderlich, den Server neu zu starten

Back-End-Server mit vorhandener Datenbank installieren

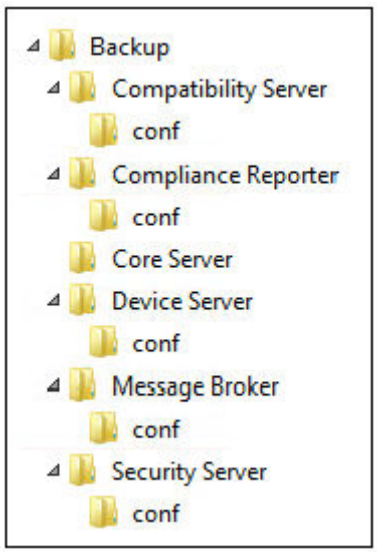
ANMERKUNG:
Falls Sie über einen funktionsfähigen Dell Enterprise Server ab v8.x verfügen, lesen Sie die Anweisungen unter „Back-End-Server-Aktualisierung/Migration“.

Sie können einen neuen Dell Enterprise Server installieren und diesen mit einer im Rahmen der Vorinstallationskonfiguration erstellten oder einer vorhandenen SQL-Datenbank ab Version 9.x verbinden, wenn die Schemaversion der zu installierenden Version von Dell Enterprise Server entspricht.

Eine Datenbank ab Version v8.x muss mit der neuesten Version des Serverkonfigurationstools auf das neueste Schema migriert werden. Anweisungen zur Datenbankmigration mit dem Serverkonfigurationstool finden Sie unter Datenbank migrieren. Um die neueste Version des Serverkonfigurationstools zu erhalten oder eine **Datenbank vor Version 8.0 zu migrieren**, wenden Sie sich bitte an Dell ProSupport.

Das Benutzerkonto, über das die Installation durchgeführt wird, muss über Datenbankbesitzerrechte für die SQL-Datenbank verfügen. Wenn Sie sich unsicher sind in Bezug auf die Zugriffsberechtigungen oder die Konnektivität zur Datenbank, bitten Sie Ihren Datenbankadministrator um Auskunft, bevor Sie mit der Installation beginnen.

Falls die vorhandene Datenbank zuvor mit Dell Enterprise Server installiert wurde, stellen Sie vor Beginn der Installation sicher, dass die Datenbank, Konfigurationsdateien und der secretKeyStore gesichert werden, auf den Sie von dem Server aus zugreifen können, auf dem Sie Dell Enterprise Server installieren. Der Zugriff auf diese Dateien ist für die Konfiguration von Dell Enterprise Server und der vorhandenen Datenbank erforderlich. Die durch das Installationsprogramm während der Installation erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.



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

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

3 Wählen Sie im Dialogfeld *InstallShield-Assistenten* die Sprache für die Installation aus, und klicken Sie dann 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 Falls Sie den optionalen Schritt 9 der Vorinstallationskonfiguration abgeschlossen haben, klicken Sie auf **Weiter**. Falls nicht, dann geben Sie den 32 Zeichen langen Produktschlüssel ein, und klicken Sie dann auf **Weiter**. Der Produktschlüssel befindet sich in der Datei *EnterpriseServerInstallKey.ini*.

8 Wählen Sie **Back-End-Installation** und **Wiederherstellungs-Installation** aus und klicken Sie auf **Weiter**.

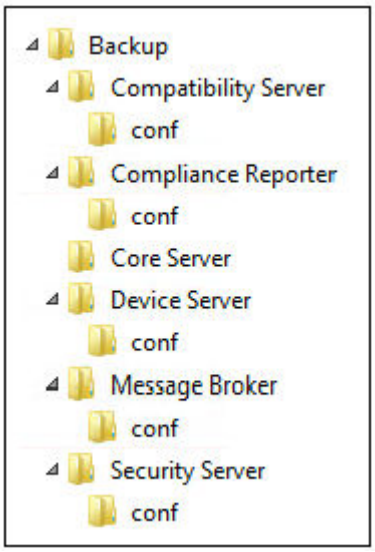
9 Klicken Sie zur Installation des Dell Enterprise Servers im Standardverzeichnis **C:\Programme\Dell** auf **Weiter**. Klicken Sie anderenfalls auf **Ändern**, um einen anderen Speicherort auszuwählen; klicken Sie anschließend auf **Weiter.**

10 Klicken Sie zur Auswahl eines Speicherorts für zu speichernde Konfigurations-Sicherungsdateien auf **Ändern**, navigieren Sie zum gewünschten Ordner und klicken Sie anschließend auf **Weiter**.

Dell empfiehlt die Auswahl eines Remote-Netzwerkspeicherortes oder eines externen Sicherungslaufwerks.

Nach der Installation müssen alle Änderungen an den Konfigurationsdateien, einschließlich Änderungen, die mit dem Serverkonfigurationstool vorgenommen werden, manuell in diesen Ordnern gesichert werden. Konfigurationsdateien sind ein wichtiger Bestandteil der gesamten Informationen, die für die manuelle Wiederherstellung des Servers verwendet werden.

ANMERKUNG: Die durch das Installationsprogramm während der Installation erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.



11 Sie können aus verschiedenen digitalen Zertifikatstypen auswählen. **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**.

Klicken Sie auf **Durchsuchen**, um den Pfad zum Zertifikat einzugeben.

Geben Sie das Passwort ein, das mit diesem Zertifikat verknüpft ist. Die Keystore-Datei muss „.p12“ oder „pfx“ sein. Anleitungen finden Sie unter Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

Klicken Sie auf **Weiter**.

ANMERKUNG:

Wenn Sie diese Einstellung verwenden möchten, muss das exportierte Zertifikat der Zertifizierungsstelle für den Import eine vollständige Vertrauenskette aufweisen. Wenn Sie nicht sicher sind, führen Sie den Export des Zertifikats der Zertifizierungsstelle erneut aus, und stellen Sie sicher, dass die folgenden Optionen im Assistenten für den Zertifikatsexport ausgewählt wurden:

- Privater Informationsaustausch – PKCS#12 (.PFX)
- Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Alle erweiterten Eigenschaften exportieren

ODER

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 einem Jahr ab.

12 Für die Server Encryption (SE, Serververschlüsselung) können Sie aus verschiedenen digitalen Zertifikattypen auswählen. 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**.

Klicken Sie auf **Durchsuchen**, um den Pfad zum Zertifikat einzugeben.

Geben Sie das Passwort ein, das mit diesem Zertifikat verknüpft ist. Die Keystore-Datei muss „.p12“ oder „pfx“ sein. Anleitungen finden Sie unter Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

Klicken Sie auf **Weiter**.

ANMERKUNG:

Wenn Sie diese Einstellung verwenden möchten, muss das exportierte Zertifikat der Zertifizierungsstelle für den Import eine vollständige Vertrauenskette aufweisen. Wenn Sie nicht sicher sind, führen Sie den Export des Zertifikats der Zertifizierungsstelle erneut aus, und stellen Sie sicher, dass die folgenden Optionen im Assistenten für den Zertifikatsexport ausgewählt wurden:

- Privater Informationsaustausch – PKCS#12 (.PFX)
- Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Alle erweiterten Eigenschaften exportieren

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 einem Jahr ab.**

13 Über das Setup-Dialogfeld *Back-End-Server-Einrichtung* können Sie Hostnamen und Ports anzeigen oder bearbeiten.

- Klicken Sie zum Übernehmen der Standard-Hostnamen und -Ports im Dialogfeld *Back-End-Server-Installationseinrichtung* auf **Weiter**.
- Wenn Sie einen Front-End-Server verwenden, dann wählen Sie **Nutzt für die Kommunikation mit Clients intern in Ihrem Netzwerk oder extern in der DMZ den Front-End-Server** und geben Sie den Front-End-Sicherheitsserver-Hostnamen ein (zum Beispiel server.domain.com).
- Klicken Sie zum Anzeigen oder Bearbeiten von Hostnamen auf **Hostnamen bearbeiten**. Bearbeiten Sie Hostnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen.

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

  Klicken Sie anschließend auf **OK**.
- Klicken Sie zum Anzeigen oder Bearbeiten von Ports auf **Ports bearbeiten**. Bearbeiten Sie Portnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen. Klicken Sie anschließend auf **OK**.

14 Geben Sie die Authentifizierungsmethode für das zu verwendende Installationsprogramm an.

a Klicken Sie auf **Durchsuchen**, um den Server auszuwählen, auf dem die Datenbank sich befindet.

b Wählen Sie den Authentifizierungstyp aus.

- **Anmeldeinformationen für die Windows-Authentifizierung des aktuellen Benutzers**

  Bei Auswahl der Option „Windows-Authentifizierung“ werden zur Authentifizierung dieselben Anmeldeinformationen verwendet wie bei der Anmeldung bei Windows (die Felder „Benutzername“ und „Kennwort“ sind nicht bearbeitbar). Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt.

  ODER

- **SQL-Server-Authentifizierung über die unten angegebenen Anmeldeinformationen**

  Bei Verwendung der SQL-Authentifizierung muss das verwendete SQL-Konto auf dem SQL-Server über Systemadministratorberechtigungen verfügen.

  Das Installationsprogramm muss sich anhand der folgenden Berechtigungen auf dem SQL Server authentifizieren: Datenbank erstellen, Benutzer hinzufügen, Berechtigungen zuweisen.

c Klicken Sie auf **Durchsuchen**, um nach dem Namen des vorhandenen Datenbank-Katalogs zu suchen.

d Klicken Sie auf **Weiter**.

15 Wählen Sie die Authentifizierungsmethode für das zu verwendende Produkt aus. Dies ist das Konto, das das Produkt für die Zusammenarbeit mit der Datenbank und den Dell Diensten verwendet.

- **Verwendung der Windows-Authentifizierung**

Wählen Sie **Windows-Authentifizierung über die unten angegebenen Anmeldeinformationen** aus, geben Sie die Anmeldeinformationen für das Konto ein, auf dem das Produkt verwendet werden kann, und klicken Sie auf **Weiter**.

Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt. Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.

ODER

- **Verwendung der SQL Server-Authentifizierung**

Wählen Sie **SQL-Server-Authentifizierung über die unten angegebenen Anmeldeinformationen**, geben Sie die SQL-Server-Anmeldeinformationen ein und klicken Sie auf **Weiter**.

Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.

Wenn das Installationsprogramm ein Problem mit der Datenbank erkennt, wird das Dialogfeld „Vorhandene Datenbank – Fehler“ angezeigt. Die Optionen in diesem Dialogfeld richten sich nach den jeweiligen Umständen:

- Das Datenbankschema stammt aus einer vorherigen Version. (Siehe Schritt a.)
- Die Datenbank weist bereits ein Datenbankschema auf, das mit der Version, die derzeit installiert wird, übereinstimmt. (Siehe Schritt b.)

a Wenn das Datenbankschema aus einer vorherigen Version stammt, wählen Sie **Installationsprogramm beenden** aus, **um diese Installation zu beenden**. Im nächsten Schritt müssen Sie die Datenbank sichern.

Die folgenden Optionen DÜRFEN nur mit Unterstützung durch den Dell ProSupport verwendet werden:

- Die Option **Diese Datenbank mit dem aktuellen Schema migrieren** wird verwendet, um eine gute Datenbank aus einer fehlerhaften Serverimplementierung wiederherzustellen. Diese Option verwendet die Wiederherstellungsdateien im Ordner „\Backup“, um die Verbindung zur Datenbank wiederherzustellen, und migriert anschließend die Datenbank mit dem aktuellen Schema. Diese Option sollte *erst* verwendet werden, nachdem Sie zunächst versucht haben, die korrekte Version von Enterprise Server neu zu installieren und anschließend das aktuelle Installationsprogramm für die Aktualisierung ausgeführt haben.
- Mit der Option **Fortfahren, ohne die Datenbank zu migrieren** werden die Enterprise Server-Dateien installiert, ohne die Datenbank zu konfigurieren. Die Datenbankkonfiguration muss später manuell über das Serverkonfigurationstool abgeschlossen werden. Außerdem sind weitere manuelle Änderungen erforderlich.

b Wenn das Datenbankschema bereits die aktuelle Schemaversion verwendet, jedoch nicht mit einem Dell Enterprise Server-Back-End verbunden ist, wird es als *Wiederherstellung* betrachtet. Das folgende Dialogfeld wird angezeigt:

- Wählen Sie **Wiederherstellungs-Installationsmodus** aus, um die Installation mit der ausgewählten Datenbank fortzusetzen.
- Wählen Sie **Neue Datenbank auswählen** aus, um eine andere Datenbank auszuwählen.
- Wählen Sie **Installationsprogramm beenden** aus, um diese Installation zu beenden.

c Klicken Sie auf **Weiter**.

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

Ein Fortschritts-Dialogfeld zeigt während des gesamten Installationsvorgangs den Status an.

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

Die Back-End-Server Installationsaufgaben wurden abgeschlossen.

Die Dell Services werden am Ende der Installation neu gestartet. Es ist nicht erforderlich, den Server neu zu starten

Front-End-Server installieren

Front-End-Server-Installation bietet eine Front-End-Option (z. B. DMZ-Modus) für die Verwendung mit Dell Enterprise 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 Ausführen des geschützten Office-Modus 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. Das Kontrollkästchen für die Richtlinie zur Aktivierung des Rückrufsignals ist standardmäßig aktiviert.

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

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

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

3 Wählen Sie im Dialogfeld *InstallShield-Assistenten* die Sprache für die Installation aus, und klicken Sie dann 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 Produktschlüssel ein.

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. **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**.

Klicken Sie auf **Durchsuchen**, um den Pfad zum Zertifikat einzugeben.

Geben Sie das Passwort ein, das mit diesem Zertifikat verknüpft ist. Die Keystore-Datei muss „.p12“ oder „pfx“ sein. Anleitungen finden Sie unter Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

Klicken Sie auf **Weiter**.

ANMERKUNG:

Wenn Sie diese Einstellung verwenden möchten, muss das exportierte Zertifikat der Zertifizierungsstelle für den Import eine vollständige Vertrauenskette aufweisen. Wenn Sie nicht sicher sind, führen Sie den Export des Zertifikats der Zertifizierungsstelle erneut aus, und stellen Sie sicher, dass die folgenden Optionen im Assistenten für den Zertifikatsexport ausgewählt wurden:

- Privater Informationsaustausch – PKCS#12 (.PFX)
- Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Alle erweiterten Eigenschaften exportieren

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 einem Jahr ab.**

11 Geben Sie im Dialogfeld *Front-End-Server-Setup* den vollständigen Hostnamen oder DNS-Alias des Back-End-Servers ein, wählen Sie **Enterprise Edition** 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**.
Ein Fortschritts-Dialogfeld zeigt während des gesamten Installationsvorgangs den Status an.

14 Wenn die Installation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.
Die Front-End-Server-Installationsaufgaben wurden abgeschlossen.

Aktualisierung und Migration

Sie können Dell Enterprise Server v8.0 und höher auf Dell Enterprise Server v9.x aktualisieren. Wenn Ihre Serverversion älter als v8.0 ist, müssen Sie zuerst auf v8.0 und anschließend auf v9.x aktualisieren.

Vor der Aktualisierung oder Migration

Stellen Sie vor Beginn sicher, dass die Vorinstallationskonfiguration abgeschlossen ist. Dies ist besonders wichtig, wenn Sie Mobile Edition bereitstellen möchten.

Lesen Sie die *Technischen Tipps für Enterprise Server*, um sich über aktuelle Lösungen oder bekannte Probleme hinsichtlich der Installation von Dell Enterprise Server zu informieren.

Das Benutzerkonto, über das die Installation durchgeführt wird, muss über Datenbankbesitzerrechte für die SQL-Datenbank verfügen. Wenn Sie sich unsicher sind in Bezug auf die Zugriffsberechtigungen oder die Konnektivität zur Datenbank, bitten Sie Ihren Datenbankadministrator um Auskunft, bevor Sie mit der Installation beginnen.

Dell empfiehlt, für die Dell Datenbank die bewährten Verfahren für Datenbanken zu verwenden und Dell Software in den Notfall-Wiederherstellungsplan Ihres Unternehmens einzubeziehen.

Wenn Sie Dell-Komponenten in Ihre DMZ implementieren möchten, vergewissern Sie sich, dass sie ausreichend vor Angriffen geschützt sind.

Für Produktionsumgebungen empfiehlt Dell, die Installation von SQL Server auf einem dedizierten Server vorzunehmen.

Zur vollständigen Umsetzung der Richtlinien empfehlen wir, sowohl Dell Enterprise Server als auch die Clients auf die neuesten Versionen zu aktualisieren.

Dell Enterprise Server v9.x unterstützt Folgendes:

- Enterprise Edition:
  - Windows-Clients v7.x/8.x
  - Mac-Clients v7.x/8.x
  - SED-Clients v8.x
  - Authentifizierung v8.x
  - BitLocker Manager v7.2x+ und v8.x
  - Data Guardian v1.x
- Endpoint Security Suite v1.x
- Endpoint Security Suite Enterprise v1.x
- Mobile Edition v7.x/v8.x
- Upgrade/Migration von Dell Enterprise Server v8.x oder späteren Versionen (Beim Migrieren von Dell Enterprise Server vor v8.x bitten Sie den Kundendienst um Hilfe.)

Beim Aktualisieren oder Migrieren von Dell Enterprise Server auf eine Version, die neu eingeführte Richtlinien enthält, müssen Sie nach der Aktualisierung oder Migration die aktualisierte Richtlinie bestätigen, damit anstelle der Standardwerte Ihre bevorzugten Richtlinieneinstellungen für die neuen Richtlinien implementiert werden.

Im Allgemeinen empfehlen wir als Aktualisierungspfad die Aktualisierung oder Migration von Dell Enterprise Server und seiner Komponenten, gefolgt von der Installation/Aktualisierung des Clients.

Richtlinienänderungen implementieren

1 Melden Sie sich als Dell Administrator bei der Remote Management Console 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 Remote-Verwaltungskonsole ab.

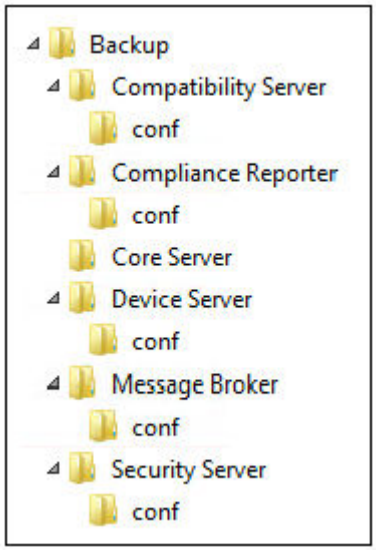
Stellen Sie sicher, dass die Dell Services ausgeführt werden

6 Klicken Sie im Windows-*Start*menü auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Nachdem *Services* geöffnet wurde, navigieren Sie zu den einzelnen Dell Diensten, und klicken Sie bei Bedarf auf **Service starten**.

Sichern der vorhandenen Installation

7 Sichern Sie die komplette vorhandene Installation an einem anderen Ort. Die Sicherung sollte die SQL Datenbank, secretKeyStore, und Konfigurationsdateien enthalten. Nach der Aktualisierung/Migration sind mehrere Dateien Ihrer bestehenden Installation erforderlich.

> **ANMERKUNG:**
> Die durch das Installationsprogramm während der Installation erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.



Back-End-Server-Aktualisierung/Migration

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

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

3 Wählen Sie im Dialogfeld *InstallShield-Assistenten* die Sprache für die Installation aus, und klicken Sie dann auf **OK**.

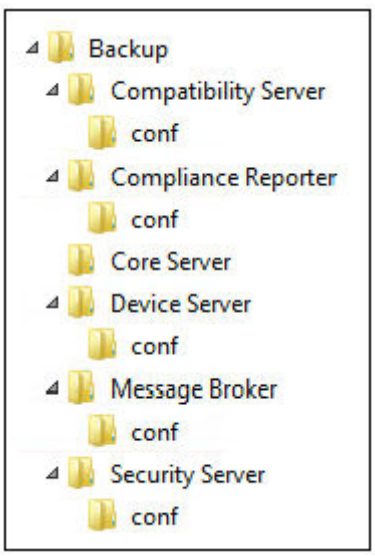
4 Klicken Sie im Dialogfeld *Willkommen* auf **Weiter**.

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

6 Klicken Sie zur Auswahl eines Speicherorts für zu speichernde Konfigurations-Sicherungsdateien auf **Ändern**, navigieren Sie zum gewünschten Ordner und klicken Sie anschließend auf **Weiter**.

Dell empfiehlt die Auswahl eines Remote-Netzwerkspeicherortes oder eines externen Sicherungslaufwerks.

Die durch das Installationsprogramm während der Installation erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.



7 Wenn das Installationsprogramm die vorhandene Datenbank ordnungsgemäß ermittelt, wird das Dialogfeld für Sie ausgefüllt.

Um die vorhandene Datenbank zu verbinden, geben Sie die zu verwendende Authentifizierungsmethode an. Nach der Installation verwendet das installierte Produkt nicht die hier angegebenen Anmeldeinformationen.

a Wählen Sie den Datenbankauthentifizierungstyp aus:

- **Anmeldeinformationen für die Windows-Authentifizierung des aktuellen Benutzers**

  Bei Auswahl der Option „Windows-Authentifizierung“ werden zur Authentifizierung dieselben Anmeldeinformationen verwendet wie bei der Anmeldung bei Windows (die Felder „Benutzername“ und „Kennwort“ sind nicht bearbeitbar).

  Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt. Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.

  ODER

- **SQL-Server-Authentifizierung über die unten angegebenen Anmeldeinformationen**

  Bei Verwendung der SQL-Authentifizierung muss das verwendete SQL-Konto auf dem SQL-Server über Systemadministratorberechtigungen verfügen.

  Das Installationsprogramm muss sich anhand der folgenden Berechtigungen auf dem SQL Server authentifizieren: Datenbank erstellen, Benutzer hinzufügen, Berechtigungen zuweisen.

b Klicken Sie auf **Weiter**.

8 Wenn das Dialogfenster für die Service-Laufzeit-Kontoangaben nicht automatisch ausgefüllt wird, geben Sie nach der Installation die Authentifizierungsmethode für das zu verwendende Produkt an.

a Wählen Sie den Authentifizierungstyp aus.

b Geben Sie den Benutzernamen und das Kennwort des Domänendienstkontos ein, das die Dell Dienste für den Zugriff auf den SQL-Server verwenden, und klicken Sie auf **Weiter**.

Das Benutzerkonto muss im Format DOMAIN\Username vorliegen und das Default Schema: dbo und Database Role Membership: dbo_owner, public aufweisen.

9 Falls die Datenbank noch nicht gesichert wurde, ***müssen*** Sie sie unbedingt sichern, bevor Sie mit der Installation fortfahren. ***Datenbankaktualisierung kann nicht rückgängig gemacht werden.*** Wählen Sie erst nach Sicherung der Datenbank **Ja**, **die Datenbank wurde gesichert** und klicken Sie auf **Weiter**.

10 Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

Ein Fortschritts-Dialogfeld zeigt während des gesamten Aktualisierungsvorgangs den Status an.

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

Die Dell Services werden am Ende der Migration neu gestartet. Es ist nicht erforderlich, den Server neu zu starten

Das Installationsprogramm führt die Schritte 12-13 für Sie aus. Es hat sich bewährt, diese Werte zu überprüfen, um sicherzustellen, dass die Änderungen ordnungsgemäß vorgenommen wurden.

12 Kopieren Sie nun von der Sicherungsinstallation <Compatibility Server install dir>\conf\secretKeyStore, und fügen Sie alles in der neuen Installation ein:

<Kompatibilitätsserver-Installationsverzeichnis>\conf\secretKeyStore

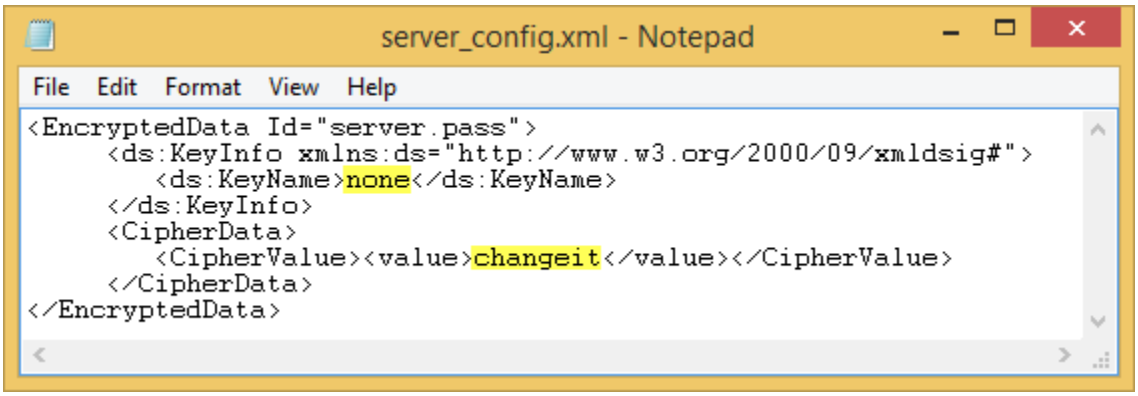
13 Öffnen Sie in der Neuinstallation <Kompatibilitätsserver-Installationsverzeichnis>\conf\server_config.xml, und ersetzen Sie den Wert für **server.pass** wie folgt durch den Wert der Sicherungsinstallation <Kompatibilitätsserver-Installationsverzeichnis>\conf \server_config.xml:

Anleitung für server.pass:

Wenn Sie das Passwort kennen, orientieren Sie sich an der Beispieldatei „server_config.xml“, und nehmen Sie die folgenden Änderungen vor:

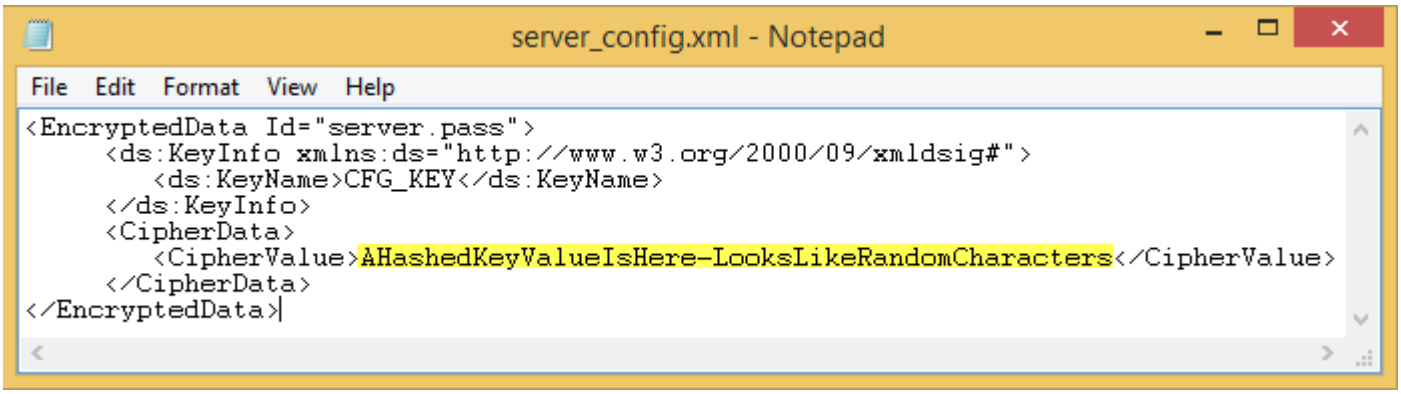
- Ändern Sie *KeyName* vom Wert **CFG_KEY** in den Wert **Keiner**.
- Geben Sie das Klartextpasswort ein, und schließen Sie es zwischen <value> </value> ein, in diesem Beispiel *<value>changeit</value>*.
- Beim Starten des Dell Enterprise Servers wird das Klartextpasswort verschlüsselt. Dieser Schlüsselwert ersetzt den Klartext.

Bekanntes Passwort:



Falls Sie das Passwort nicht kennen, schneiden Sie den Abschnitt in der gesicherten Datei „<Compatibility Server install dir>\conf \server_config.xml“ aus (vergleiche Abbildung 4-2), und fügen Sie ihn in den entsprechenden Abschnitt in der neuen Datei *server_config.xml* ein.

Unbekanntes Passwort:



Speichern und schließen Sie die Datei.

ANMERKUNG:
Versuchen Sie keinesfalls, das Passwort für den **Dell** Enterprise Server durch Bearbeiten des server.pass-Werts in der server_config.xml-Datei zu ändern. Wenn Sie diesen Wert ändern, können Sie nicht mehr auf die Datenbank zugreifen.

Die Back-End-Server Migrationsaufgaben wurden abgeschlossen.

Front-End-Server Aktualisierung/Migration

ANMERKUNG: Beginnend mit v9.5 wird der Beacon-Dienst als Teil dieses Upgrades unter Verwendung des standardmäßigen Hostnamen und Ports 8446 installiert. Der Beacon-Dienst unterstützt Data Guardian-Rückrufsignale. Dieser fügt zu jeder durch Data Guardian geschützten Datei beim Ausführen des geschützten Office-Modus ein Rückrufsignal hinzu. Dies ermöglicht die Kommunikation zwischen jedem Gerät an jedem Standort und dem Dell Front-End-Server. Das Kontrollkästchen für die Richtlinie zur Aktivierung des Rückrufsignals ist standardmäßig aktiviert. Stellen Sie vor Verwendung des Rückrufsignals sicher, dass die erforderliche Netzwerksicherheit konfiguriert ist.

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

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

3 Wählen Sie im Dialogfeld *InstallShield-Assistenten* die Sprache für die Installation aus, und klicken Sie dann 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 Klicken Sie im Dialogfeld *Bereit zur Installation des Programms* auf **Installieren**.

Ein Fortschritts-Dialogfeld zeigt während des gesamten Installationsvorgangs den Status an.

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

9 Richten Sie den Back-End-Server für die Kommunikation mit dem Front-End-Server ein.

a Wechseln Sie auf dem Back-End-Server zu <Security Server install dir>\conf\, und öffnen Sie die Datei „application.properties“.

b Suchen Sie „publicdns.server.host“, und legen Sie den Namen auf einen extern auflösbaren Hostnamen fest.

c Suchen Sie „publicdns.server.port“, und legen Sie den Port fest (die Standardeinstellungen lautet 8443).

Die Dell Services werden am Ende der Installation neu gestartet. Ein Neustart des Servers ist bis zum Abschluss der Konfigurationsaufgaben nach der Installation nicht erforderlich.

Installation im getrennten Modus

Der getrennte Modus isoliert Enterprise Server aus dem Internet und einem ungesicherten LAN oder anderen Netzwerk. Nachdem Enterprise Server im getrennten Modus installiert wurde, verbleibt er im getrennten Modus und kann nicht in den verbundenen Modus zurück geändert werden.

Enterprise Server wird im getrennten Modus an der Befehlszeile installiert.

Die folgende Tabelle zeigt die verfügbaren Switches.

Schalter	Erläuterung
/v	Gibt Variablen an die .msi-Datei innerhalb der *.exe-Datei weiter.
/s	Im Hintergrund

Die folgende Tabelle zeigt die verfügbaren Anzeigeoptionen.

Option	Erläuterung
/q	Kein Fortschrittsdialogfeld, führt nach Abschluss der Installation selbstständig einen Neustart durch
/qb	Dialogfeld mit der Schaltfläche **Abbrechen** fortführen
/qn	Keine Benutzeroberfläche

Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter. Diese Parameter können an der Befehlszeile angegeben oder aus einer Datei unter Verwendung der folgenden Eigenschaft aufgerufen werden:

```
INSTALL_VALUES_FILE=\"<file_path>\" "
```

Parameter
AGREE_TO_LICENSE=Yes – Der Wert muss „Yes“ (Ja) lauten.
PRODUCT_SN=xxxxx – Optional, wenn sich die Lizenzinformationen am standardmäßigen Ort befinden; andernfalls müssen Sie sie hier eingeben.
INSTALLDIR=<path> – Optional.

Parameter

BACKUPDIR=<path> – Dort werden die Wiederherstellungsdateien gespeichert.

ANMERKUNG: Die durch das Installationsprogramm während des Installationsschritts erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.

AIRGAP=1 – Zum Installieren von Enterprise Server im getrennten Modus muss der Wert „1“ lauten.

SSL_TYPE=n – Wobei n zum Importieren eines vorhandenen Zertifikats, das von einer CA-Zertifizierungsstelle erworben wurde, „1“ und zum Erstellen eines selbstsignierten Zertifikats „2“ lautet. Der Wert SSL_TYPE bestimmt, welche SSL-Eigenschaften erforderlich sind.

Mit SSL_TYPE=1 sind folgende Eigenschaften erforderlich:

SSL_CERT_PASSWORD=xxxxx

SSL_CERT_PATH=xxxxx

Mit SSL_TYPE=2 sind folgende Eigenschaften erforderlich:

SSL_CITYNAME

SSL_DOMAINNAME

SSL_ORGNAME

SSL_UNITNAME

SSL_COUNTRY – Optional, Standard = „US“

SSL_STATENAME

SSOS_TYPE=n – Wobei n zum Importieren eines vorhandenen Zertifikats, das von einer CA-Zertifizierungsstelle erworben wurde, „1“ und zum Erstellen eines selbstsignierten Zertifikats „2“ lautet. Der Wert SSOS_TYPE bestimmt, welche SSOS-Eigenschaften erforderlich sind.

Mit SSOS_TYPE=1 sind folgende Eigenschaften erforderlich:

SSOS_CERT_PASSWORD=xxxxx

SSOS_CERT_PATH=xxxxx

Mit SSOS_TYPE=2 sind folgende Eigenschaften erforderlich:

SSOS_CITYNAME

SSOS_DOMAINNAME

SSOS_ORGNAME

SSOS_UNITNAME

SSOS_COUNTRY – Optional, Standard = „US“

SSOS_STATENAME

DISPLAY_SQLSERVER – Dieser Wert wird analysiert, um Server-, Instanz- und Portinformationen zu erhalten.

Beispiel:

DISPLAY_SQLSERVER=SQL_server\Server_instance, Port

IS_AUTO_CREATE_SQLSERVER=FALSE – Optional. Der Standardwert ist FALSCH, was bedeutet, dass die Datenbank nicht erstellt wird. Die Datenbank muss bereits auf dem Server vorhanden sein.

Setzen Sie diesen Wert zum Erstellen einer neuen Datenbank auf WAHR.

Parameter

IS_SQLSERVER_AUTHENTICATION=0 – Optional. Der Standardwert ist 0 und gibt an, dass die Windows-Anmeldeinformationen für die Authentifizierung des aktuell angemeldeten Benutzers zur Authentifizierung des SQL-Servers genutzt werden. Wenn Sie die SQL-Authentifizierung verwenden möchten, setzen Sie diesen Wert auf 1.

ANMERKUNG: Das Installationsprogramm muss sich anhand der folgenden Berechtigungen auf dem SQL Server authentifizieren: Datenbank erstellen, Benutzer hinzufügen, Berechtigungen zuweisen. Die Anmeldeinformationen sind Installations-Anmeldeinformationen, nicht Laufzeit-Anmeldeinformationen.

Wenn die SQL-Authentifizierung verwendet wird, ist Folgendes erforderlich:

IS_SQLSERVER_USERNAME

IS_SQLSERVER_PASSWORD

EE_SQLSERVER_AUTHENTICATION – Erforderlich. Wählen Sie die Authentifizierungsmethode für das zu verwendende Produkt aus. Dieser Schritt verbindet ein Konto mit dem Produkt. Diese Anmeldeinformationen werden auch von den Dell Diensten verwendet, da sie mit dem Enterprise Server funktionieren. Um die Windows-Authentifizierung zu verwenden, setzen Sie den Wert auf 0. Um die SQL-Authentifizierung zu verwenden, setzen Sie den Wert auf 1.

ANMERKUNG: Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt. Das Benutzerkonto muss über die folgenden SQL Server-Berechtigungen verfügen Default Schema: dbo und Database Role Membership: db_owner, public.

SQL_EE_USERNAME – Erforderlich. Verwenden Sie mit Windows-Authentifizierung dieses Format: DOMÄNE\Benutzername. Geben Sie mit SQL-Authentifizierung den Benutzernamen an.

SQL_EE_PASSWORD – Erforderlich. Geben Sie das zum Windows- oder SQL-Benutzernamen gehörende Kennwort ein.

Wenn die SQL-Authentifizierung verwendet wird (EE_SQLSERVER_AUTHENTICATION= 1) ist Folgendes gültig:

RUNAS_KEYSERVER_USER – Verwenden Sie den Windows-Benutzernamen für Key Server „run as“ in diesem Format: Domäne \Benutzer. Dies muss ein Windows-Benutzerkonto sein.

RUNAS_KEYSERVER_PSWD – Windows-Kennwort für Windows-Benutzerkonto für Key Server "run as" festlegen.

SQL_ADD_LOGIN=T – Optional. Die Standardeinstellung ist Null (diese Art der Anmeldung ist nicht hinzugefügt worden). Wenn der Wert T eingestellt ist und der SQL_EE_USERNAME keine Anmeldung oder kein Benutzer für die Datenbank ist, versucht das Installationsprogramm die SQL-Anmeldeinformationen des Benutzers zur Authentifizierung hinzuzufügen und Berechtigungen festzulegen, damit die Anmeldedaten vom Produkt verwendet werden können.

Nachfolgend finden Sie Hostname-Parameter. Bearbeiten Sie Hostnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen. Das Format muss `server.domain.com` lauten.

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

CORESERVERHOST – Optional. Hostname des Core Servers.

RMIHOST – Optional. Hostname des Compatibility-Servers.

REPORTERHOST – Optional. Hostname des Compliance Reporter.

DEVICEHOST – Optional. Hostname des Geräteservers.

KEYSERVERHOST – Optional. Hostnamen des Key Servers.

TIGAHOST – Optional. Hostname des Sicherheitsservers.

SMTP_HOST – Optional. SMTP-Hostname.

ACTIVEMQHOST – Optional. Hostname des Message Broker.

Parameter
Im Folgenden finden Sie Portparameter. Bearbeiten Sie Portnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen SERVERPORT_CLIENTAUTH – Optional. REPORTERPORT – Optional. DEVICEPORT – Optional. KEYSERVERPORT – Optional. GKPORT – Optional. TIGAPORT – Optional. SMTP_PORT – Optional. ACTIVEMQ_TCP – Optional. ACTIVEMQ_STOMP – Optional.

Enterprise Server im getrennten Modus installieren

Im folgenden Beispiel wird Enterprise Server unter Verwendung von Installationparametern, die in der Datei `C:\mysetups\eeoptions.txt\" "` aufgeführt sind, installiert

```
Setup.exe /s /v"/qb INSTALL_VALUES_FILE=\"C:\mysetups\eeoptions.txt\" "
```

Dell Enterprise Server deinstallieren

1. Wechseln Sie auf dem Dell Installationsmedium in das Dell Enterprise Server-Verzeichnis. **Entpacken** (NICHT kopieren/einfügen oder ziehen) Sie Dell Enterprise Server-x64 im Stammverzeichnis des Servers, auf dem Sie Enterprise Server deinstallieren möchten. ***Kopieren/Einfügen oder Ziehen führt zu Fehlern und einer nicht erfolgreichen Installation.***
2. Doppelklicken Sie auf **setup.exe**.
3. Klicken Sie im Dialogfeld *Willkommen* auf **Weiter**.
4. Klicken Sie im Dialogfeld *Programm entfernen* auf **Entfernen**.
   Ein Fortschritts-Dialogfeld zeigt während des gesamten Deinstallationsvorgangs den Status an.
5. Wenn die Deinstallation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.

5

Konfiguration nach der Installation

Lesen Sie die *Technischen Tipps für Enterprise Server*, um sich über aktuelle Lösungen oder bekannte Probleme in Verbindung mit der Dell Enterprise Server-Konfiguration zu informieren.

Unabhängig davon, ob Sie Dell Enterprise Server zum ersten Mal installieren oder ob Sie eine Aktualisierung einer vorhandenen Installation durchführen, müssen Sie einige Komponenten Ihrer Umgebung konfigurieren.

EAS-Management installieren und konfigurieren

Dieser Abschnitt ist dann relevant, wenn Sie Mobile Edition verwenden möchten. Ist dies nicht der Fall, lassen Sie diesen Abschnitt aus, und fahren Sie mit Dell Security Server im DMZ-Modus konfigurieren fort.

Voraussetzungen

- Die Anmeldedaten für den EAS Mailbox Manager-Dienst müssen Berechtigungen zum Erstellen/Ändern der Exchange ActiveSync-Richtlinie, zur Zuweisung von Richtlinien an die Postfächer der Benutzer und zum Abfragen von Informationen über ActiveSync-Geräte umfassen.
- Das EAS-Konfigurationsdienstprogramm muss mit Administratorberechtigungen ausgeführt werden, um Dateien ändern und Dienste neu starten zu können.
- Es wird eine Netzwerkverbindung zum Dell Policy Proxy benötigt.
- Halten Sie den FQDN des Dell Policy Proxy bereit.
- Halten Sie die Port-Nummer des Dell Policy Proxy bereit.
- Microsoft Message Queuing (MSMQ) muss bereits auf dem Server installiert/konfiguriert sein, auf dem die Exchange-Umgebung gehostet wird. Ist dies nicht der Fall, lesen Sie den Abschnitt Microsoft Message Queuing (MSMQ) installieren und konfigurieren.

Während der Implementierung

Wenn Sie Exchange ActiveSync verwenden möchten, um Mobilgeräte über Mobile Edition zu verwalten, muss Ihre Exchange Server-Umgebung konfiguriert werden.

Installation des EAS-Geräte-Managers

1 Navigieren Sie auf dem Dell Installationsmedium zum Ordner „EAS-Management“. Kopieren Sie vom Ordner EAS-Gerätemanager „setup.exe“ in Ihre(n) *Exchange Client-Zugangsserver*.

2 Doppelklicken Sie auf **setup.exe**, um mit der Installation zu beginnen. Wenn Ihre Umgebung mehr als einen *Exchange Client Zugangsserver* enthält, führen Sie dieses Installationsprogramm auf jedem davon aus.

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

4 Klicken Sie im Bildschirm *Willkommen* auf **Weiter**.

5 Lesen Sie die Lizenzvereinbarung, stimmen Sie den Bedingungen zu, und klicken Sie auf **Weiter**.

6 Klicken Sie auf **Weiter**, um den EAS-Geräte-Manager am Standardspeicherort **C:\Inetpub\wwwroot\Dell\EAS Device Manager** zu installieren.

7 Klicken Sie im Bildschirm *Bereit für Installation* auf **Installieren**.

Der Installationsfortschritt wird in einem Statusfenster angezeigt.

8 Markieren Sie nach Wunsch das Kontrollkästchen, um das Windows Installationsprotokoll anzuzeigen und klicken Sie auf **Fertigstellen**.

Installation des EAS-Postfach-Managers

1 Navigieren Sie auf dem Dell Installationsmedium zum Ordner „EAS-Management“. Kopieren Sie setup.exe aus dem Ordner „EAS-Postfachmanagement“ in Ihre(n) *Exchange Mailbox-Server*.

2 Doppelklicken Sie auf **setup.exe**, um mit der Installation zu beginnen. Sollte Ihre Umgebung mehr als einen *Exchange Mailbox Server* enthalten, führen Sie dieses Installationsprogramm auf jedem davon aus.

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

4 Klicken Sie im *Startbildschirm* auf **Weiter**.

5 Lesen Sie die Lizenzvereinbarung, stimmen Sie den Bedingungen zu, und klicken Sie auf **Weiter**.

6 Klicken Sie auf **Weiter**, um den EAS-Postfachmanager am Standardspeicherort **C:\Programme\Dell\EAS Mailbox Manager** zu installieren.

7 Geben Sie auf dem Anmeldebildschirm die Anmeldeinformationen für das Benutzerkonto ein, über das auf diesen Dienst zugegriffen werden soll.

Benutzername: DOMÄNE\Benutzername

Passwort: das mit diesem Benutzernamen verknüpfte Passwort

Klicken Sie auf **Weiter**.

8 Klicken Sie im Bildschirm *Bereit für Installation* auf **Installieren**.

Der Installationsfortschritt wird in einem Statusfenster angezeigt.

9 Markieren Sie nach Wunsch das Kontrollkästchen, um das Windows Installationsprotokoll anzuzeigen und klicken Sie auf **Fertigstellen**.

Verwendung des EAS-Konfigurationsprogramms

1 Wechseln Sie auf demselben Computer zu **Start** > **Dell** > **EAS-Konfigurationsprogramm** > **EAS-Konfiguration**, und führen Sie das EAS-Konfigurationsprogramm aus.

2 Klicken Sie auf **Setup**, um die EAS-Management-Einstellungen zu konfigurieren.

3 Geben Sie die folgenden Informationen ein:

FQDN des Dell Policy Proxy

Dell Policy Proxy-Port (der Standard-Port ist 8090)

Intervall für Dell Policy Proxy-Abfragen (die Standardeinstellung ist 1 Minute)

Aktivieren Sie das Kontrollkästchen für die Ausführung des EAS-Geräte-Managers im Berichtsmodus (während der Implementierung empfohlen).

> **ANMERKUNG:**
> Im Berichtsmodus erhalten unbekannte Geräte/Benutzer Zugriff auf Exchange ActiveSync, aber Sie empfangen die Berichte zum Datenverkehr. Sobald Ihre Implementierung abgeschlossen ist, können Sie diese Einstellung ändern, um die Sicherheit zu erhöhen.

Klicken Sie auf **OK**.

4 Eine Erfolgsmeldung wird angezeigt. Klicken Sie auf **Ja**, um IIS- und EAS-Postfach-Manager-Dienste neu zu starten.

5 Klicken Sie nach Abschluss auf **Beenden**.

Einstellungen für EAS-Management konfigurieren

Führen Sie nach Abschluss der Implementierung die folgenden Schritte aus, um die Sicherheit zu erhöhen.

1 Wechseln Sie zu **Start** > **Dell** > **EAS-Konfigurationsprogramm** > **EAS-Konfiguration**, um das EAS-Konfigurationsprogramm auszuführen.
2 Klicken Sie auf **Setup**, um die EAS-Management-Einstellungen zu konfigurieren.
3 Geben Sie die folgenden Informationen ein:

   FQDN des Dell Policy Proxy

   Dell Policy Proxy-Port (der Standard-Port ist 8090)

   Intervall für Dell Policy Proxy-Abfragen (die Standardeinstellung ist 1 Minute)

   Heben Sie die Aktivierung des Kontrollkästchens auf, um den EAS-Geräte-Manager im Berichtsmodus auszuführen.

   Klicken Sie auf **OK**.
4 Eine Erfolgsmeldung wird angezeigt. Klicken Sie auf **Ja**, um IIS- und EAS-Postfach-Manager-Dienste neu zu starten.
5 Klicken Sie nach Abschluss auf **Beenden**.

Dell Security Server im DMZ-Modus konfigurieren

Wenn der Dell Security Server in einem DMZ und einem privaten Netzwerk bereitgestellt wird und nur der DMZ-Server über ein Domänenzertifikat einer vertrauenswürdigen Zertifikatsstelle (CA) verfügt, müssen einige manuelle Schritte ausgeführt werden, um das vertrauenswürdige Zertifikat zu einem Java-Schlüsselspeicher auf dem Dell Security Server des privaten Netzwerks hinzuzufügen.

Falls ein vertrauenswürdiges Zertifikat verwendet wird, überspringen Sie diesen Abschnitt, und fahren Sie fort mit APNs-Eintragung.

ANMERKUNG: Wir empfehlen dringend, Domänenzertifikate einer vertrauenswürdigen Zertifikatsstelle für DMZ- und private Netzwerkserver zu verwenden.

Verwenden von Keytool für den Import des DMZ-Domänenzertifikats

WICHTIG:
Sichern Sie die vorhandenen **Dell** Security Server-Cacerts, bevor Sie die Keytool-Anweisungen umsetzen. Falls ein Konfigurationsfehler auftritt, können Sie zur gespeicherten Datei zurückkehren.

Annahmen

- Dell Security Server wurde mit einem nicht vertrauenswürdigen Zertifikat installiert.
- Dell Security Server im DMZ-Modus wurde über ein signiertes Zertifikat (Entrust, Verisign usw.) installiert.
- Eine PFX-Zertifikatsdatei ist verfügbar. Falls Sie Ihr Zertifikat in das Format PFX konvertieren möchten, lesen Sie den Abschnitt „Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren“.

Verfahren

1 Fügen Sie Keytool in den Systempfad ein.

```
set path=%path%;<Dell Java Install Dir>\bin
```

2 Verwenden Sie Keytool, um die Inhalte des vertrauenswürdigen Domänenzertifikats aufzulisten, das Sie importieren möchten. Machen Sie eine Notiz des angezeigten Aliasnamens.

```
keytool -list -v -keystore "
```

3 Verwenden Sie Keytool, um den Inhalt des signierten Zertifikats in eine Cacert-Datei für den Dell Security Server zu importieren:

```
keytool -importkeystore -v -srckeystore "
```

Bei „-srcalias“ müssen Sie diese Informationen aus den exportierten Inhalten des signierten Zertifikats abrufen.

Bei „-destalias“ kann dies ein von Ihnen gewählter Speicherort sein.

4 Sichern Sie die vorhandene Cacerts-Datei im Verzeichnis <Security Server install dir>\conf\, und ersetzen Sie sie auf dem Dell Security Server durch die neu erstellte Cacerts-Datei.

Ändern der Datei „application.properties“

Ändern Sie die Datei „application.properties“, um den Aliasnamen für das signierte Zertifikat anzugeben.

1 Gehen Sie zu <Security Server install dir>\conf\application.properties
2 Ändern Sie die folgenden Informationen:
keystore.alias.signing=<Ändern Sie diesen Wert in den Wert von Schritt 3 oben für `-destalias` ab>
3 Führen Sie einen Neustart des Dell Security Server-Services durch.

APNs-Eintragung

Wenn Sie vorhaben, Mobile Edition für mobile Gerätesicherheit mit iOS-Geräten zu verwenden, muss der Assistent für die APNs-Eintragung für folgende Aufgaben verwendet werden:

- CSR erstellen
- Apple Push-Zertifikat erstellen
- Push-Zertifikat hochladen

Wenn Sie nicht vorhaben, Mobile Edition für mobile Gerätesicherheit mit iOS-Geräten zu verwenden, überspringen Sie diesen Abschnitt, und fahren Sie fort mit Serverkonfigurationstool.

Mit dem Apple Push Notification-Dienst (APNs) können Sie die sichere Kommunikation mit iOS-Geräten nach dem over-the-air-Prinzip aktivieren. Der APN-Dienst wird verwendet, um eine Benachrichtigung an ein iOS-Gerät zu senden und es am Dell Enterprise Server anzumelden. Der APN-Dienst kann nur Benachrichtigungen an ein Gerät senden; es werden keine Daten versendet.

Verfahren

1 Öffnen Sie einen Browser und rufen Sie die Website „https://<FQDN-of-security-server>:8443/csrweb“ auf.
2 Geben Sie im Dialogfeld „Anmeldung“ des APNs-Eintragungsassistenten Ihre Dell Administrator-Anmeldeinformationen ein, und klicken Sie auf **Anmelden**.
3 Daraufhin wird ein Dialogfeld angezeigt, das die anstehenden Schritte beschreibt. Klicken Sie auf **Weiter**.

Schritt I: CSR erstellen

4 Geben Sie die folgenden Informationen ein:

E-Mail: Die E-Mail-Adresse kann ein beliebiger UPN sein, wird empfehlen jedoch die Verwendung eines Kontos für den Administrator, der das APNs-Zertifikat verwaltet.

Allgemeiner Name: Geben Sie den allgemeinen Namen ein, der mit dieser E-Mail-Adresse verknüpft ist.

Klicken Sie auf **CSR generieren**.

5 Speichern Sie nach der CSR-Generierung die Datei auf einen einfach zu erreichenden Speicherort.

6 Klicken Sie auf **Weiter**.

Schritt II: Apple Push-Zertifikat erstellen

7 Klicken Sie auf den Link für das **Apple Push-Zertifikatsportal**. Melden Sie sich mit Ihrer Apple ID und dem Passwort an.

8 Lesen Sie die Nutzungsbedingungen, und klicken Sie zum Akzeptieren dieser Bedingungen auf **Ich stimme zu**.

9 Klicken Sie auf **Durchsuchen**, und führen Sie einen **Upload** der soeben erstellten CSR durch.

10 Klicken Sie auf der Seite *Zertifikate für Drittanbieter-Server* auf **Herunterladen**. Speichern Sie die Datei auf einen leicht erreichbaren Speicherort.

11 Kehren Sie zum Eintragungsassistent für APN-Dienste zurück, und klicken Sie dann auf **Weiter**.

Schritt III: Push-Zertifikat hochladen

12 Geben Sie die folgenden Informationen ein (verwenden Sie die gleichen Anmeldeinformationen wie unter Schritt I: CSR erstellen.

E-Mail:

Allgemeiner Name:

Push-Zertifikatsdatei: Klicken Sie auf **Durchsuchen**, um die Datei zu finden, die Sie inSchritt 7 gespeichert haben. Klicken Sie auf **Hochladen**.

13 Eine Erfolgsmeldung wird angezeigt. Klicken Sie auf **Fertigstellen**.

Die Eintragung des APNs-Zertifikats auf dem Dell Enterprise Server ist abgeschlossen.

Serverkonfigurationstool

Wenn nach Abschluss Ihrer Installation Konfigurationen in Ihrer Umgebung erforderlich sind, nehmen Sie die Änderungen mit dem Dell Serverkonfigurationstool vor.

Mit dem Dell Serverkonfigurationstool lassen sich folgende Aufgaben durchführen:

- Neue oder aktualisierte Zertifikate hinzufügen
- Dell Manager-Zertifikat importieren
- Identitätszertifikat importieren
- Einstellungen für Server SSL-Zertifikat oder Mobile Edition konfigurieren
- SMTP-Einstellungen für Data Guardian oder E- Mail-Dienste konfigurieren
- Datenbankname, Speicherort oder Anmeldeinformationen ändern
- Datenbank migrieren

Dell Core Server und Dell Compatibility Server dürfen nicht zusammen mit dem Serverkonfigurationstool ausgeführt werden. Halten Sie den Dell Core Server-Service und den Dell Compatibility Server-Service unter *Services* (**Start > Ausführen**) an. Geben Sie ***services.msc*** ein, bevor Sie das Dell Serverkonfigurationstool starten.

Das Dell Serverkonfigurationstool starten Sie über **Start > Programme > Dell > Enterprise Edition > Serverkonfigurationstool > Serverkonfigurationstool ausführen**.

Die vom Dell Serverkonfigurationstool erstellten Protokolle werden im Ordner **C:\Programme\Dell\Enterprise Edition\Konfigurationstool \Protokolle** gespeichert.

Neue oder aktualisierte Zertifikate hinzufügen

Sie können auswählen, welchen Zertifikatstyp Sie nutzen möchten: selbstsigniert oder signiert.

- **Selbstsignierte** Zertifikate werden durch den Ersteller signiert. Selbstsignierte Zertifikate eignen sich für Piloten, Machbarkeitsnachweise usw. Für Produktionsumgebungen empfiehlt Dell die Verwendung von öffentlichen, durch eine Zertifizierungsstelle signierte Zertifikate oder domänensignierte Zertifikate.
- **Signierte** (öffentlich und von einer Zertifizierungsstelle oder Domäne signierte) Zertifikate werden von einer öffentlichen Zertifizierungsstelle oder einer Domäne signiert. Für Zertifikate, die von einer öffentlichen Zertifizierungsstelle signiert wurden, ist normalerweise ein Zertifikat der Zertifizierungsstelle im Microsoft-Zertifikatsspeicher vorhanden, und es wird automatisch eine Vertrauenskette erstellt. Für Zertifikate, die von einer Domäne und Zertifizierungsstelle signiert wurden, gilt Folgendes: Wurde die Workstation zur Domäne hinzugefügt, dann wurden das von der Domäne und Zertifizierungsstelle signierte Zertifikat zum Microsoft-Zertifikatsspeicher hinzugefügt und eine Vertrauenskette angelegt.

Komponenten, die durch Zertifikatskonfiguration beeinflusst werden:

- Java Services (zum Beispiel Dell Device Server usw.)
- .NET-Anwendungen (Dell Core Server)
- Die Validierung von Smart Cards wird für die Preboot-Authentifizierung verwendet (Dell Security Server)
- Import privater Verschlüsselungscodes, die zum Signieren von Richtlinienpaketen genutzt werden, die ihrerseits an Dell Manager gesendet werden Dell Manager führt die SSL-Validierung für remote verwaltete Enterprise Edition-Clients mit selbstverschlüsselnden Laufwerken oder BitLocker Manager aus.
- Client-Workstations:
    - Workstations, auf denen BitLocker Manager ausgeführt wird
    - Workstations, auf denen Enterprise Edition (Windows-Clients) ausgeführt wird
    - Workstations, auf denen Endpoint Security Suite ausgeführt wird
    - Workstations, auf denen Endpoint Security Suite Enterprise ausgeführt wird

Informationen zur Nutzung verschiedener Zertifikatstypen:

Die Preboot-Authentifizierung, die Smartcards verwendet, erfordert die SSL-Validierung mit dem Dell Security Server. Dell Manager führt beim Herstellen der Verbindung mit dem Dell Core Server eine SSL-Validierung durch. Für diese Verbindungen muss sich die signierende Zertifikatsstelle im Keystore befinden (entweder im Java-Keystore oder im Microsoft-Keystore, je nach Dell Server-Komponente). Falls selbstsignierte Zertifikate ausgewählt werden, stehen die folgenden Optionen zur Verfügung:

- Validierung von Smartcards, die für die Preboot-Authentifizierung verwendet werden:
    - Importieren Sie das Signierungszertifikat „Root Agency“ und die vollständige Vertrauenskette in den Java-Keystore des Dell Security Servers. Weitere Informationen finden Sie unter „Selbstsigniertes Zertifikat erstellen“ und „Zertifikatsignierungsanforderung generieren“. Die vollständige Vertrauenskette muss importiert werden.

Dell Manager:

- Fügen Sie das Signierungszertifikat „Root Agency“(vom selbstsignierten Zertifikat generiert) bei „Vertrauenswürdige Stammzertifizierungsstellen” (für „lokaler Computer“) der Workstation im Microsoft-Keystore ein.
- Ändern Sie das Verhalten der serverseitigen SSL-Validierung. Aktivieren Sie zum Deaktivieren der serverseitigen SSL-Vertrauensvalidierung das Kontrollkästchen **Prüfung der Vertrauenskette deaktivieren** auf der Registerkarte „Einstellungen“.

Es gibt zwei Methoden für die Erstellung eines Zertifikats – *Express* und *Erweitert*.

Wählen Sie **eine** Methode aus:

- Express – Wählen Sie diese Methode aus, um ein selbstsigniertes Zertifikat für alle Komponenten zu generieren. Dies ist die einfachere Methode. Beachten Sie jedoch, dass selbstsignierte Zertifikate nur für Piloten, Machbarkeitsnachweise usw. angemessen sind. Für

Produktionsumgebungen empfiehlt Dell den Gebrauch von öffentlichen und von einer Zertifizierungsstelle oder Domäne signierten Zertifikaten.

- Erweitert – Wählen Sie diese Methode aus, um jede Komponente separat zu konfigurieren.

Express

1 Wählen Sie aus dem Hauptmenü **Aktionen** > **Zertifikate konfigurieren** aus.

2 Nachdem der Konfigurationsassistent gestartet wurde, wählen Sie **Express** aus, und klicken Sie auf **Weiter**. Falls verfügbar, werden die Informationen aus dem selbstsignierten Zertifikat verwendet, das im Rahmen der Installation von Enterprise Server erstellt wurde.

3 Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

Die Einrichtung des Zertifikats ist abgeschlossen. Im verbleibenden Teil dieses Abschnitts wird die erweiterte Methode für die Erstellung eines Zertifikats erläutert.

Erweitert

Es gibt zwei Pfade zur Erstellung eines Zertifikats – *Selbstsigniertes Zertifikat generieren* und *Aktuelle Einstellungen verwenden*. Wählen Sie **einen** dieser Pfade aus:

- Pfad 1 – Selbstsigniertes Zertifikat erstellen
- Pfad 2 – Aktuelle Einstellungen verwenden

Pfad 1 – Selbstsigniertes Zertifikat erstellen

1 Wählen Sie aus dem Hauptmenü **Aktionen** > **Zertifikate konfigurieren** aus.

2 Nachdem der Konfigurationsassistent gestartet wurde, wählen Sie **Erweitert** aus, und klicken auf **Weiter**.

3 Wählen Sie **Selbstsigniertes Zertifikat generieren** aus, und klicken Sie auf **Weiter**. Falls verfügbar, werden die Informationen aus dem selbstsignierten Zertifikat verwendet, das im Rahmen der Installation von Enterprise Server erstellt wurde.

4 Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

Die Einrichtung des Zertifikats ist abgeschlossen. Im verbleibenden Teil dieses Abschnitts wird die andere Methode für die Erstellung eines Zertifikats erläutert.

Pfad 2 – Aktuelle Einstellungen verwenden

1 Wählen Sie aus dem Hauptmenü **Aktionen** > **Zertifikate konfigurieren** aus.

2 Nachdem der Konfigurationsassistent gestartet wurde, wählen Sie **Erweitert** aus, und klicken auf **Weiter**.

3 Wählen Sie **Aktuelle Einstellungen verwenden** aus, und klicken Sie auf **Weiter**.

4 Wählen Sie im Fenster *SSL-Zertifikat für Compatibility Server* die Option **Selbstsigniertes Zertifikat generieren** aus, und klicken Sie auf **Weiter.** Falls verfügbar, werden die Informationen aus dem selbstsignierten Zertifikat verwendet, das im Rahmen der Installation von Enterprise Server erstellt wurde.

   Klicken Sie auf **Weiter**.

5 Wählen Sie im Fenster „*SSL-Zertifikat für den Core Server*“ eine der folgenden Optionen aus:

   - *Zertifikat auswählen* – Wählen Sie diese Option aus, um ein vorhandenes Zertifikat zu verwenden. Klicken Sie auf **Weiter**.

     Navigieren Sie zum Speicherort des vorhandenen Zertifikats, geben Sie das zugehörige Passwort ein, und klicken Sie auf **Weiter**.

     Klicken Sie anschließend auf **Fertig stellen**.
   - *Selbstsigniertes Zertifikat generieren* – Falls verfügbar, werden die Informationen aus dem selbstsignierten Zertifikat verwendet, das im Rahmen der Installation von Enterprise Server erstellt wurde. Wenn Sie diese Option auswählen, erscheint kein Fenster

vom Typ „Zertifikat für die Nachrichtensicherheit“ (das Fenster wird jedoch angezeigt, wenn Sie die Option *Aktuelle Einstellungen verwenden* auswählen), und es wird das für den Dell Compatibility Server erstellte Zertifikat verwendet.

Stellen Sie sicher, dass der vollständige Computername korrekt ist. Klicken Sie auf **Weiter**.

Sie erhalten eine Warnmeldung, weil es bereits ein Zertifikat mit demselben Namen gibt. Wenn Sie gefragt werden, ob Sie es benutzen möchten, klicken Sie auf **Ja**.

Klicken Sie anschließend auf **Fertig stellen**.

- *Aktuelle Einstellungen verwenden* – Wählen Sie diese Option aus, um eine Einstellung für ein Zertifikat zu einem beliebigen Zeitpunkt nach der erstmaligen Konfiguration von Dell Enterprise Server zu ändern. Das bereits konfigurierte Zertifikat bleibt dabei erhalten. Wenn Sie diese Option auswählen, gelangen Sie zum Fenster „Zertifikat für die Nachrichtensicherheit“.

  Wählen Sie im Fenster Zertifikat für die Nachrichtensicherheit **eine** der folgenden Optionen aus:

  - *Zertifikat auswählen* – Wählen Sie diese Option, um ein vorhandenes Zertifikat zu verwenden. Klicken Sie auf **Weiter**.

    Navigieren Sie zum Speicherort des vorhandenen Zertifikats, geben Sie das zugehörige Passwort ein, und klicken Sie auf **Weiter**.

    Klicken Sie anschließend auf **Fertig stellen**.
  - *Selbstsigniertes Zertifikat generieren* – Falls verfügbar, werden die Informationen aus dem selbstsignierten Zertifikat verwendet, das im Rahmen der Installation von Enterprise Server erstellt wurde.

    Klicken Sie auf **Weiter**.

    Klicken Sie anschließend auf **Fertig stellen**.

Die Einrichtung des Zertifikats ist abgeschlossen.

Wenn die Änderungen abgeschlossen wurden:

1 Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

2 Schließen Sie das Dell Serverkonfigurationstool.

3 Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn *Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

Dell Manager-Zertifikat importieren

Falls Ihre Bereitstellung remote verwaltete Clients der Enterprise Edition mit selbstverschlüsselnden Laufwerken oder BitLocker Manager einschließt, müssen Sie Ihr neu erstelltes (oder vorhandenes) Zertifikat importieren. Das Dell Manager-Zertifikat wird dazu verwendet, den privaten Schlüssel zu schützen, der zum Signieren der Richtlinienpakete genutzt wird, die an remote verwaltete Enterprise Edition-Clients und BitLocker Manager gesendet werden. Dieses Zertifikat kann unabhängig von allen weiteren Zertifikaten genutzt werden. Außerdem kann dieser Schlüssel, wenn er beschädigt ist, durch einen neuen Schlüssel ersetzt werden. Dell Manager wird daraufhin einen neuen öffentlichen Schlüssel anfordern, wenn die Richtlinienpakete nicht entschlüsselt werden können.

1 Öffnen Sie die Microsoft Management Console.

2 Klicken Sie auf **Datei > Snapin hinzufügen/entfernen**.

3 Klicken Sie auf **Hinzufügen**.

4 Wählen Sie im Fenster *Standalone-Snapin hinzufügen* **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.

5 Wählen Sie **Computerkonto** aus und klicken Sie auf **Weiter**.

6 Wählen Sie im Fenster *Computer auswählen* **Lokaler Computer (der Computer, auf dem diese Konsole läuft)** und klicken Sie auf **Fertigstellen**.

7 Klicken Sie auf **Schließen**.

8 Klicken Sie auf **OK**.

9 Erweitern Sie im Ordner *Konsolenstamm* die *Zertifikate (Lokaler Computer)*.

10 Gehen Sie zum Ordner *Privat*, und suchen Sie das gewünschte Zertifikat.

11 Markieren Sie das gewünschte Zertifikat, und klicken Sie mit der rechten Maustaste auf **Alle Aufgaben > Exportieren**.

12 Sobald der Assistent „Zertifikat exportieren“ angezeigt wird, klicken Sie auf **Weiter**.

13 Wählen Sie **Ja, privaten Schlüssel exportieren** aus, und klicken Sie auf **Weiter**.

14 Wählen Sie **Privater Informationsaustausch - PKCS #12 (.PFX)** aus, und wählen Sie anschließend die Unteroptionen **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen** und **Alle erweiterten Eigenschaften exportieren** aus. Klicken Sie auf **Weiter**.

15 Geben Sie das Passwort ein und bestätigen Sie es. Sie können das Passwort frei wählen. Wählen Sie ein Passwort, das nur Sie selbst sich leicht merken können, nicht aber andere. Klicken Sie auf **Weiter**.

16 Klicken Sie auf **Durchsuchen**, um zu dem Speicherort zu navigieren, auf dem Sie die Datei speichern möchten.

17 Geben Sie im Feld `Dateiname` einen Namen für die zu speichernde Datei ein. Klicken Sie auf **Speichern**.

18 Klicken Sie auf **Weiter**.

19 Klicken Sie auf **Fertigstellen**.

20 Sie erhalten die Meldung, dass der Export erfolgreich abgeschlossen wurde. Schließen Sie die MMC.

21 Kehren Sie zurück zum Dell Serverkonfigurationstool.

22 Wählen Sie aus dem Hauptmenü **Aktionen** > **Manager-Zertifikat importieren** aus.

23 Navigieren Sie zu der Stelle, an der die exportierte Datei gespeichert wurde. Wählen Sie die Datei aus, und klicken Sie auf **Öffnen**.

24 Geben Sie das mit dieser Datei verknüpfte Passwort ein, und klicken Sie auf **OK**.

Der Import des Dell Manager-Zertifikats ist nun abgeschlossen.

Wenn die Änderungen abgeschlossen wurden:

1 Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

2 Schließen Sie das Dell Serverkonfigurationstool.

3 Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn*Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

Identitätszertifikat importieren

Wenn Ihre Implementierung die Serververschlüsselung umfasst, müssen Sie das neu erstellte (oder bestehende) Zertifikat importieren. Das Identitätszertifikat wird dazu verwendet, den privaten Schlüssel zu schützen, der zum Signieren der Richtlinienpakete genutzt wird, die an Client-Server gesendet werden. Dieses Zertifikat kann unabhängig von allen weiteren Zertifikaten genutzt werden.

1 Wählen Sie aus dem Hauptmenü **Aktionen** > **Identitätszertifikat importieren**.

2 Navigieren Sie zum Zertifikat, das Sie auswählen möchten, und klicken Sie auf **Weiter**.

3 Geben Sie bei der Aufforderung zur Eingabe des Passworts das Passwort ein, das zum vorhandenen Zertifikat gehört.

4 Wählen Sie im Windows-Kontodialogfeld eine Option aus:

   a Um die Anmeldeinformationen für das Identitätszertifikat zu ändern, wählen Sie **Andere Windows-Konto-Anmeldeinformationen mit dem Identitätszertifikat verwenden**.

   b Um weiterhin die Anmeldeinformationen des angemeldeten Kontos zu verwenden, klicken Sie auf **Weiter**.

5 Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

Einstellungen für Server SSL-Zertifikat oder Mobile Edition konfigurieren

Klicken Sie im Server Configuration Tool auf die Registerkarte **Einstellungen**.

Dell Manager:

Aktivieren Sie zum Deaktivieren der serverseitigen SSL-Vertrauensbestätigung für Dell Manager das Kontrollkästchen **Vertrauenskettenprüfung deaktivieren**.

SCEP:

Geben Sie bei Verwendung von Mobile Edition die URL des SCEP-Hostservers ein.

Wenn die Änderungen abgeschlossen wurden:

1 Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

2 Schließen Sie das Dell Serverkonfigurationstool.

3 Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn *Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

SMTP-Einstellungen für Data Guardian oder E-Mail-Services konfigurieren

Klicken Sie im Server Configuration Tool auf die Registerkarte **SMTP**.

Diese Registerkarte konfiguriert die SMTP-Einstellungen für Data Guardian. Informationen zum Konfigurieren der SMTP-Einstellungen für andere Zwecke als Data Guardian finden Sie in der Administrator-Hilfe unter „SMTP-Server für Lizenz-E-Mail-Benachrichtigungen aktivieren“.

Geben Sie die folgenden Informationen ein:

1 Geben Sie in das Feld „Hostname“ den FQDN Ihres SMTP-Serves ein, z. B. „smtpservername.domain.com“.

2 Geben Sie in das Feld „Benutzername“ den Benutzernamen ein, der sich am Mailserver anmelden wird. Das Format kann „DOMAIN \hschmid“, „hschmid“ oder ein anderes, organisationsspezifisches Format sein.

3 Geben Sie in das Feld „Passwort“ das mit diesem Benutzernamen verknüpfte Passwort ein.

4 Geben Sie im Feld „Absenderadresse“ die E-Mail-Adresse ein, von der die E-Mail versandt wird. Sie können das mit dem Benutzernamen verknüpfte E-Mail-Konto (hschmidt@domäne.com) oder ein anderes Konto angeben, auf das der Benutzer Zugriff hat (CloudRegistration@domäne.com).

5 Geben Sie in das Feld „Port“ die Port-Nummer ein (in der Regel 25).

6 Wählen Sie im Menü „Authentifizierung“ entweder „Wahr“ oder „Falsch“ aus.

Wenn die Änderungen abgeschlossen wurden:

1 Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

2 Schließen Sie das Dell Serverkonfigurationstool.

3 Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn *Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

Datenbankname, Speicherort oder Anmeldeinformationen ändern

Klicken Sie im Serverkonfigurationstool auf die Registerkarte **Datenbank**.

1 Geben Sie im Feld *Servername:* den vollständigen Domänennamen des Servers ein, auf dem die Datenbank gehostet wird (falls es einen Instanznamen gibt, nehmen Sie diesen mit auf). Beispiel: SQLTest.domain.com\DellDB.

   Dell empfiehlt die Verwendung eines vollständigen Domänennames, wenngleich eine IP-Adresse verwendet werden kann.

2 Geben Sie im Feld `Serverport:` die Portnummer ein.

   Bei Verwendung einer nicht standardmäßigen SQL Server-Instanz müssen Sie im Feld *Port*: den dynamischen Port der Instanz angeben. Alternativ dazu aktivieren Sie den SQL Server Browser-Service und stellen Sie sicher, dass UDP-Port 1434 geöffnet ist. Weitere Informationen finden Sie unter https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

3 Geben Sie im Feld `Datenbank:` den Namen der Datenbank ein.

4 Wählen Sie im Feld *Authentifizierung:* entweder **Windows-Authentifizierung** oder **SQL Server-Authentifizierung**. Bei Auswahl der Option „Windows-Authentifizierung“ werden zur Authentifizierung dieselben Anmeldeinformationen verwendet wie bei der Anmeldung bei Windows (die Felder „Benutzername“ und „Kennwort“ sind nicht bearbeitbar).

5 Geben Sie im Feld `Benutzername:` den Benutzernamen ein, der mit dieser Datenbank verknüpft ist.

6 Geben Sie im Feld `Passwort:` das Passwort für den Benutzernamen ein, der im Feld „Benutzername“ angezeigt wird.

7 Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

8 Wählen Sie zum Testen der Datenbankkonfiguration **Aktionen** > **Datenbankkonfiguration testen** aus dem Hauptmenü. Daraufhin wird der Konfigurationsassistent gestartet.

9 Lesen Sie im Fenster *Konfigurationstest* die Testinformationen, und klicken Sie dann auf **Weiter**.

10 Wenn Sie auf der Registerkarte *Datenbank* die Option „Windows-Authentifizierung“ ausgewählt haben, können Sie alternative Anmeldeinformationen eingeben, damit die gleichen Anmeldeinformationen verwendet werden können wie für die Ausführung von Dell Enterprise Server. Klicken Sie auf **Weiter**.

11 Im Fenster *Konfiguration testen* werden die Ergebnisse für die Tests der Verbindungseinstellungen, der Kompatibilität und der Datenbankmigration angezeigt.

12 Klicken Sie auf **Fertigstellen**.

ANMERKUNG:

Falls entweder die SQL-Datenbank oder SQL-Instanz mit einer nicht standardmäßigen Sortierreihenfolge konfiguriert wird, muss bei der nicht-standardmäßigen Sortierung die Groß- und Kleinschreibung nicht beachtet werden. Eine Liste der Sortierreihenfolgen und Groß- und Kleinschreibung finden Sie unter https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx.

Wenn die Änderungen abgeschlossen wurden:

1 Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

2 Schließen Sie das Dell Serverkonfigurationstool.

3 Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn *Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

Datenbank migrieren

Sie können eine v8.x-Datenbank mit der neuesten Version des Serverkonfigurationstools auf das neueste Schema migrieren. Um die neueste Version des Serverkonfigurationstools zu erhalten oder eine Datenbank vor Version 8.0 zu migrieren, wenden Sie sich bitte an Dell ProSupport.

Klicken Sie im Serverkonfigurationstool auf die Registerkarte **Datenbank**.

1 Wenn Sie noch keine Sicherungsdatei Ihrer bestehenden Dell Datenbank angelegt haben, sollten Sie dies **jetzt** tun.

2 Wählen Sie aus dem Hauptmenü **Aktionen** > **Datenbank migrieren**. Daraufhin wird der Konfigurationsassistent gestartet.

3 Im Fenster *Enterprise-Datenbank migrieren* wird eine Warnung angezeigt. Bestätigen Sie, dass Sie die gesamte Datenbank gesichert haben bzw. dass eine Sicherung der vorhandenen Datenbank nicht erforderlich ist. Klicken Sie auf **Weiter**.

   Im Fenster *Datenbank wird migriert* zeigen informative Meldungen den Status der Migration an.

   Führen Sie nach der Initialisierung eine Fehlersuche durch.

   ANMERKUNG: Eine Fehlermeldung, die durch gekennzeichnet ist, weist darauf hin, dass eine Datenbankaufgabe fehlgeschlagen ist und dass Korrekturmaßnahmen erforderlich sind, damit die Datenbank ordnungsgemäß migriert werden kann. Klicken Sie auf Fertigstellen, beheben Sie die Datenbankfehler und führen Sie die Anweisungen in diesem Abschnitt erneut durch.

4 Klicken Sie auf **Fertigstellen**.

Wennd die Migration abgeschlossen ist:

1 Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

2 Schließen Sie das Dell Serverkonfigurationstool.

3 Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn *Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

Administrative Aufgaben

Dell Administratorrolle zuweisen

1 Melden Sie sich als Dell Administrator an der Remote Management Console an. Verwenden Sie dazu die folgende Adresse: https://server.domain.com:8443/webui/. Die Standardanmeldeinformationen lauten **superadmin/changeit**.

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

3 Klicken Sie auf eine Domäne, der Sie einen Benutzer hinzufügen möchten.

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 aufgeführt 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 Remote Management Console/bei Enterprise Server ab.

2 Melden Sie sich mit den Anmeldeinformationen eines Domänenbenutzers bei der Remote Management Console/beim Enterprise Server an.

Hochladen der Client-Zugriffslizenz

Sie haben separat von den Installationsdateien Client-Zugriffslizenzen erhalten, entweder beim anfänglichen Kauf oder später, wenn Sie zusätzliche Client-Zugriffslizenzen hinzugefügt haben.

1 Klicken Sie im linken Fensterbereich auf **Verwaltung**.

2 Klicken Sie auf **Lizenzverwaltung**.

3 Klicken Sie auf **Datei auswählen**, um die Client-Lizenzdatei zu suchen und auszuwählen.

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 das Kommentarfeld eine Beschreibung der Änderung ein.
3 Klicken Sie auf **Richtlinien bestätigen**.

Dell Compliance Reporter konfigurieren

1 Klicken Sie im linken Fensterbereich auf **Compliance Reporter**.
2 Wenn Dell Compliance Reporter gestartet wird, melden Sie sich mit den Standard-Anmeldeinformationen *superadmin/changeit* an.
3 Es werden zwei Authentifizierungsverfahren unterstützt. Wählen Sie für die Konfiguration eines der folgenden Verfahren aus:

- SQL-Authentifizierung mit Compliance Reporter konfigurieren
- Windows-Authentifizierung mit Compliance Reporter konfigurieren

SQL-Authentifizierung mit Compliance Reporter konfigurieren

Ab Version 8.1 ist die Datenquelle softwareseitig vorkonfiguriert. Es ist keine Konfiguration erforderlich. Führen Sie die folgenden Schritte aus, um die Datenquelle ggf. zu ändern.

1 Klicken Sie zum Festlegen der Datenquelle im Hauptmenü auf **Einstellungen**. Klicken Sie im Menü auf der linken Seite auf **Datenquelle**.
2 Geben Sie zur Anmeldung bei der Dell-Datenbank den Benutzernamen ein.
3 Geben Sie zur Anmeldung bei der Dell-Datenbank das Passwort ein.
4 Geben Sie zur Anmeldung bei der Dell-Datenbank den Hostnamen ein.
5 Geben Sie zur Anmeldung bei der Dell-Datenbank den Namen der Datenbank ein.
6 Geben Sie die maximal zulässige Anzahl untätiger Verbindungen ein. Der Standardwert ist 2.
7 Geben Sie die maximal zulässige Anzahl (aktiver) Verbindungen ein. Der Standardwert ist 10.
8 Geben Sie die Wartezeit ein (die maximale Anzahl von Millisekunden, die auf eine Verbindung gewartet wird). -1 steht für unendlich.
9 Zur Bestätigung der Datenbank-URL und Überprüfung der Verbindung zwischen Dell Compliance Reporter und der Dell Datenbank klicken Sie auf **Testverbindung**.
10 Klicken Sie auf **Aktualisieren**. Zum Verwerfen der Informationen klicken Sie auf Abbrechen.

Die administrativen Aufgaben sind abgeschlossen. In den verbleibenden Abschnitten dieses Kapitels wird die Windows-Authentifizierung erläutert; Sie können diese Abschnitte ignorieren, wenn Sie die SQL-Authentifizierung für Dell Compliance Reporter verwenden.

Fahren Sie **bei Bedarf** fort mit Selbstsigniertes Zertifikat erstellen und Zertifikatsignierungsanforderung generieren oder Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

Windows-Authentifizierung mit Compliance Reporter konfigurieren

Ab Version 8.1 ist die Datenquelle softwareseitig vorkonfiguriert. Es ist keine Konfiguration erforderlich. Führen Sie die folgenden Schritte aus, um die Datenquelle ggf. zu ändern.

1 Geben Sie zur Anmeldung bei der Dell-Datenbank den Benutzernamen ein.
2 Lassen Sie das Passwort leer. Wenn der Domänenbenutzer sich anmeldet, wird sein Passwort auf die Datenbank übertragen.
3 Geben Sie zur Anmeldung bei der Dell-Datenbank den Hostnamen ein.
4 Geben Sie zur Anmeldung bei der Dell-Datenbank den Namen der Datenbank ein.
5 Geben Sie die maximal zulässige Anzahl untätiger Verbindungen ein. Der Standardwert ist 2.

6 Geben Sie die maximal zulässige Anzahl (aktiver) Verbindungen ein. Der Standardwert ist 10.

7 Geben Sie die Wartezeit ein (die maximale Anzahl von Millisekunden, die auf eine Verbindung gewartet wird). -1 steht für unendlich.

8 Zur Bestätigung der Datenbank-URL und Prüfung der Verbindung zwischen Dell Compliance Reporter und der Dell Datenbank klicken Sie auf **Testverbindung**.

9 Klicken Sie auf **Aktualisieren**. Zum Verwerfen der Informationen klicken Sie auf Abbrechen.

Die administrativen Aufgaben sind abgeschlossen. Fahren Sie **bei Bedarf** fort mit Selbstsigniertes Zertifikat erstellen und Zertifikatsignierungsanforderung generieren oder Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

Ausführen von Sicherungen

Zum Zwecke der Notfallwiederherstellung stellen Sie sicher, dass die folgenden Speicherorte wöchentlich mit nächtlichen Differenzialen gesichert werden:

Enterprise Server-Sicherungen

Sichern Sie regelmäßig die Dateien an den Speicherorten, die Sie bei der Installation für die Sicherung von Konfigurationsdateien ausgewählt haben (Schritt 10 auf Seite 27) oder Aktualisierung/Migration (Schritt 6 auf Seite 68). Wöchentliche Sicherungen dieser Daten sind akzeptabel, da sie sich selten ändern und falls nötig manuell neu konfiguriert werden können. Die wichtigsten Dateien speichern Informationen, die zur Verbindungsaufnahme mit der Datenbank nötig sind:

<Installationsverzeichnis>\Enterprise Edition\Compatibility Server\conf\server_config.xml

<Installationsverzeichnis>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

<Installationsverzeichnis>\Enterprise Edition\Compatibility Server\conf\gkresource.xml

SQL Server-Sicherungen

Führen Sie vollständige nächtliche Sicherungen mit aktivierter Transaktionsprotokollierung durch, und führen Sie differenzielle Datenbanksicherungen alle 3-4 Stunden durch. Falls eine Sicherungsdatenbank vorhanden ist, sollten Transaktionsprotokolle und/oder Protokollversandaufgaben alle 15 Minuten (oder in kürzeren Intervallen) ausgeführt werden. Wie immer empfehlen wir Ihnen, für die Dell Datenbank die bewährten Verfahren für Datenbanken zu verwenden und Dell Software in den Notfall-Wiederherstellungsplan Ihres Unternehmens einzubeziehen.

Weitere Informationen zu bewährten Verfahren für SQL Server finden Sie hier Die folgende Liste erläutert bewährte Verfahren für SQL Server, die dann implementiert werden sollten, wenn Dell Data Protection installiert ist, aber die Verfahren noch nicht implementiert sind..

PostgreSQL Server-Sicherungen

Audit-Ereignisse werden in PostgreSQL-Server gespeichert, der routinemäßig gesichert werden sollte. Eine Anleitung zur Sicherung erhalten Sie unter https://www.postgresql.org/docs/9.5/static/backup.html.

Dell empfiehlt, für die PostgreSQL-Datenbank die bewährten Verfahren für Datenbanken zu verwenden und Dell Software in den Notfallwiederherstellungsplan Ihres Unternehmens einzubeziehen.

Beschreibung der Dell Komponenten

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

Name	Beschreibung	Erforderlich für
Compliance Reporter	Bietet eine umfassende Übersicht der Umgebung über die Durchführung von Prüfverfahren und die Erstellung von Berichten über die Regelkonformität. Eine Komponente des Dell Enterprise Server.	Berichterstellung
Key Server	Verhandlung, Authentifizierung und Verschlüsselung einer Client-Verbindung unter Verwendung von Kerberos APIs. Erfordert Zugriff auf die SQL-Datenbank, um die Schlüsseldaten abzurufen. Eine Komponente des Dell Enterprise Server.	Dell-Administrator-Dienstprogramme
Serverkonfigurationstool	Konfiguriert die Kommunikation der Datenbank mit dem Core Server und dem Compatibility Server/Security Server. Dient der Datenbankinitialisierung bei der Installation oder der Umstellung der Datenbank auf ein neueres Schema. Wird zur Steuerung der Dell Dienste verwendet. Eine Komponente des Dell Enterprise Server.	Alle
Remote Management Console/Enterprise Server-Konsole	Verwaltungskonsole und Befehlszentrale für die gesamte Unternehmensimplementierung. Eine Komponente des Dell Enterprise Server.	Alle
Core Server	Verwaltet den Richtlinienablauf, Lizenzen und die Registrierung für die Preboot-Authentifizierung, SED-Verwaltung, BitLocker Manager, Threat Protection und Advanced Threat Protection Verarbeitet Bestandslistendaten zur Verwendung durch den Compliance Reporter und die Remote-Management-Konsole. Sammelt und speichert Authentifizierungsdaten Steuert den rollenbasierten Zugriff. Eine Komponente des Dell Enterprise Server.	Alle
Security Server	Kommuniziert mit Policy Proxy; verwaltet das Abrufen forensischer Schlüssel, Client-Aktivierungen, Data Guardian-Produkte, die SED-PBA- und Active Directory-Kommunikation für die Authentifizierung oder Abstimmung, einschließlich Identitätsvalidierung für die Authentifizierung	Alle

Name	Beschreibung	Erforderlich für
	an der Remote Management Console. Erfordert Zugriff auf die SQL-Datenbank. Eine Komponente des Dell Enterprise Server.	
Compatibility Server	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 in diesem Dienst. Eine Komponente des Dell Enterprise Server.	Alle
Message Broker-Service	Handhabt die Kommunikation zwischen Diensten von Enterprise Server. Stellt Richtlinieninformationen bereit, die vom Compatibility Server für Policy Proxy-Warteschlangen erzeugt wurden. Erfordert Zugriff auf die SQL-Datenbank. Eine Komponente des Dell Enterprise Server.	Alle
Device Server	Unterstützt die Aktivierung und Wiederherstellung von Kennwörtern. Eine Komponente des Dell Enterprise Server.	Enterprise Edition für Mac Enterprise Edition für Windows Handheld Shields CREDActivate
Device Server-Plugins	Bietet Unterstützung für verschiedene Komponenten. Eine Komponente des Dell Enterprise Server.	Alle
Identity Server	Verarbeitet Authentifizierungsanforderungen für die Domäne. Erfordert ein Active-Directory-Konto. Muss das Konto sein, das für den Zugriff auf den SQL-Server bei Nutzung der Windows-Authentifizierung verwendet wird. Eine Komponente des Dell Enterprise Server.	Alle
Policy Proxy	Stellt einen netzwerkbasierten Kommunikationsweg bereit, über den Aktualisierungen der Sicherheitsrichtlinien und der Bestandsdaten übermittelt werden. Eine Komponente des Dell Enterprise Server.	Enterprise Edition für Mac Enterprise Edition für Windows Mobile Edition für mobiles Gerätesicherheit
Security Token Services (STS)	Diese Funktion wird verwendet, um einen sicheren Authentifizierungskanal zwischen der Dell Enterprise Server-Benutzeroberfläche und den Dell Back-End-Diensten zu erstellen.	Alle

Name	Beschreibung	Erforderlich für
EAS-Geräte-Manager	Aktiviert die over-the-air-Funktionalität. Ist auf dem Exchange-Client-Zugriffsserver installiert.	Exchange ActiveSync-Verwaltung von Mobilgeräten.
EAS Mailbox Manager	Der Postfach-Agent, der auf dem Exchange-Postfachserver installiert ist.	Exchange ActiveSync-Verwaltung von Mobilgeräten.

8

Bewährte Verfahren für SQL Server

Die folgende Liste erklärt die bewährten Verfahren für SQL Server, die implementiert werden sollten, wenn Dell Data Protection installiert wird, falls sie noch nicht implementiert wurden.

1 Stellen Sie sicher, dass die Größe des NTFS-Blocks, der die Datendatei und Protokolldatei enthält, 64 KB beträgt. SQL Server umfasst (Grundeinheit von SQL-Speicher) 64 KB.

   Weitere Informationen finden Sie in den TechNet-Artikeln von Microsoft für „Erläuterungen zu Seiten und Umfang".

   - Microsoft SQL Server 2008 – http://technet.microsoft.com/en-us/library/ms190969%28v=sql.100%29
   - Microsoft SQL Server 2008 R2 – http://technet.microsoft.com/en-us/library/ms190969(v=sql.105).aspx

2 Generell soll die maximale Größe des SQL-Server-Speichers 80% des installierten Speichers betragen.

   Weitere Informationen finden Sie in den TechNet-Artikeln von Microsoft für „Serverspeicher, Serverkonfigurationsoptionen".

   - Microsoft SQL Server 2008 – http://technet.microsoft.com/en-us/library/ms178067%28v=sql.100%29
   - Microsoft SQL Server 2008 R2 – http://technet.microsoft.com/en-us/library/ms178067%28v=sql.105%29
   - Microsoft SQL Server 2012 – https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014 – https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016 – https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)

3 Stellen Sie -t1222 in den Instanz-Starteigenschaften ein, um sicherzustellen, dass Deadlock-Informationen erfasst werden, falls sie eintreten.

   Weitere Informationen finden Sie in den TechNet-Artikeln von Microsoft für „Ablaufverfolgungsflags (Transact-SQL)".

   - Microsoft SQL Server 2008 – http://technet.microsoft.com/en-us/library/ms188396%28v=sql.100%29
   - Microsoft SQL Server 2008 R2 – http://technet.microsoft.com/en-us/library/ms188396%28v=sql.105%29
   - Microsoft SQL Server 2012 – https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014 – https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016 – https://msdn.microsoft.com/en-us/library/ms188396.aspx

4 Stellen Sie sicher, dass alle Indizes wöchentlich gewartet werden, um sie neu aufzubauen.

Erstellen eines selbstsignierten Zertifikats und Generieren einer Zertifikatssignieranforderung

In diesem Abschnitt werden die Schritte zum Erstellen eines selbstsignierten Zertifikats für die Java-basierten Komponenten beschrieben. Mit diesem Verfahren können **keine** selbstsignierten Zertifikate für .NET-basierte Komponenten erstellt werden.

Für Produktionsumgebungen sind selbstsignierte Zertifikate nicht zu empfehlen.

Falls Ihre Organisation ein SSL-Serverzertifikat benötigt oder Sie aus anderen Gründen ein Zertifikat erstellen müssen, wird in diesem Abschnitt das Verfahren zum Erstellen eines Java-Keystore mit Keytool beschrieben.

Wenn Ihre Organisation die Verwendung von Smart Cards für die Authentifizierung plant, müssen Sie Keytool verwenden, um die vollständige Zertifikatsvertrauenskette zu importieren, die im Zertifikat des Smart Card-Benutzers verwendet wird.

Keytool erstellt private Schlüssel, die im CSR-Format (Certificate Signing Request) an eine Zertifizierungsstelle wie VeriSign® oder Entrust® übertragen werden. Anhand dieser CSR erstellt die Zertifizierungsstelle dann ein Serverzertifikat und signiert es. Danach wird das Serverzertifikat zusammen mit dem Zertifikat der Zertifizierungsstelle in eine Datei heruntergeladen. Anschließend werden die Zertifikate in die cacerts-Datei importiert.

Neue Key-Paare und selbstsignierte Zertifikate erstellen

1 Navigieren Sie zum Verzeichnis **conf** von Dell Compliance Reporter, Dell Security Server oder Dell Device Server.

2 Erstellen Sie eine Sicherungskopie der Standard-Zertifikatsdatenbank:

Klicken Sie auf **Start** > **Ausführen** und geben Sie **move cacerts cacerts.old** ein.

3 Fügen Sie Keytool in den Systempfad ein. Geben Sie den folgenden Befehl in eine Eingabeaufforderung ein:

```
set path=%path%;<Dell Java Install Dir>\bin
```

4 Führen Sie zum Erstellen eines Zertifikats Keytool wie folgt aus:

```
keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias Dell -keystore .\cacerts
```

5 Geben Sie nach der entsprechenden Aufforderung in Keytool die folgenden Informationen ein.

> **ANMERKUNG:**
> Erstellen Sie vor der Bearbeitung von Konfigurationsdateien eine Sicherungskopie. Ändern Sie nur die angegebenen Parameter. Wenn Sie andere Daten in diesen Dateien ändern, beispielsweise Tags, kann dies zu einem Systemschaden und -ausfall führen. **Dell** kann nicht gewährleisten, dass sich Probleme infolge nicht autorisierter Änderungen an diesen Dateien ohne Neuinstallation von **Dell** Enterprise Server beheben lassen.

- *Keystore-Passwort*: Geben Sie ein Passwort ein (die Zeichen <>;&" ' sind nicht zulässig), und setzen Sie die Variable in der Datei **conf** der Komponente auf denselben Wert, wie hier gezeigt:

  <Compliance Reporter install dir>\conf\eserver.properties. Bestimmen Sie den Wert eserver.keystore.password =

<Device Server install dir>\conf\eserver.properties. Bestimmen Sie den Wert eserver.keystore.password =

<Security Server install dir>\conf\eserver.properties. Bestimmen Sie den Wert eserver.keystore.password =

- *Vollständiger Servername*: Geben Sie den vollständigen Namen des Servers ein, auf dem die Komponente, mit der Sie arbeiten, installiert ist. Zum vollständigen Namen gehören der Hostname und der Domänenname (Beispiel: server.domain.com).
- *Organisationseinheit*: Geben Sie den entsprechenden Wert ein (Beispiel: Sicherheit).
- *Organisation*: Geben Sie den entsprechenden Wert ein (Beispiel: Dell).
- *Ort*: Geben Sie den entsprechenden Wert ein (Beispiel: München).
- *Bundesstaat bzw. Bundesland*: Geben Sie den Namen des Bundesstaats oder -landes ohne Abkürzungen ein (Beispiel: Bayern).
- Landescode mit zwei Buchstaben.
- Sie müssen im Dienstprogramm bestätigen, dass die Angaben stimmen. Ist dies der Fall, geben Sie `Ja` ein.

  Falls nicht, geben Sie `Nein` ein. Keytool zeigt jeden zuvor eingegebenen Wert an. Drücken Sie die Eingabetaste, um den Wert zu akzeptieren, oder ändern Sie den Wert und drücken Sie anschließend die **Eingabetaste**.
- *Schlüsselpasswort für Alias*: Wenn Sie hier kein anderes Passwort eingeben, wird automatisch das Keystore-Passwort verwendet.

Signierte Zertifikate von einer Zertifizierungsstelle anfordern

Verwenden Sie dieses Verfahren, um eine Anfrage zum Signieren von Zertifikaten (CSR) für das bei Neues Key-Paar und selbstsigniertes Zertifikat erstellen erstellte, selbstsignierte Zertifikat zu generieren.

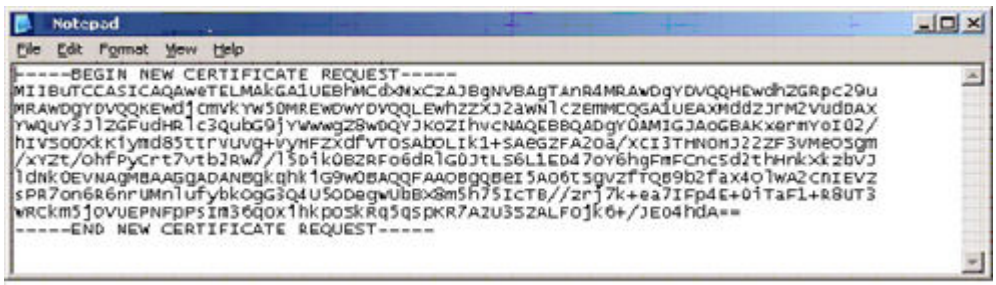
1 Verwenden Sie die denselben Wert wie zuvor für <**certificatealias**>:

```
keytool -certreq -sigalg SHA1withRSA -alias <certificate-alias> -keystore .\cacerts -file
<csr-filename>
```

Beispiel: `keytool -certreq -sigalg SHA1withRSA -alias sslkey -keystore .\cacerts -file Dell.csr`

Die .csr-Datei enthält ein BEGIN/END-Paar, das während der Erstellung des Zertifikats bei der Zertifizierungsstelle verwendet wird.

Beispiel .CSR-Datei



2 Befolgen Sie Ihr Organisationsverfahren zum Erwerb eines SSL-Serverzertifikats bei einer Zertifizierungsstelle. Senden Sie den Inhalt von <CSR-Dateiname> zum Signieren.

> **ANMERKUNG:**
> Es gibt verschiedene Methoden zur Anforderung eines gültigen Zertifikats. Ein Beispiel finden Sie unter **Beispielmethode zur Anforderung eines Zertifikats**.

3 Speichern Sie das signierte Zertifikat nach Erhalt in einer Datei.

4 Wir empfehlen, immer eine Sicherungskopie dieses Zertifikats anzufertigen, falls beim Import ein Fehler auftritt. Die Sicherungskopie verhindert, dass der Vorgang noch einmal von vorn begonnen werden muss.

Stammzertifikate importieren

Wenn die Zertifizierungsstelle für das Stammzertifikat Verisign (aber nicht Verisign Test) ist, gehen Sie zum nächsten Verfahren weiter und importieren Sie das signierte Zertifikat.

Mit dem Stammzertifikat der Zertifizierungsstelle werden signierte Zertifikate validiert.

1 Führen Sie **eine** der folgenden Maßnahmen durch:

- Laden Sie das Stammzertifikat der Zertifizierungsstelle herunter und speichern Sie es in einer Datei.
- Rufen Sie das Stammzertifikat vom Unternehmensverzeichnisserver ab.

2 Führen Sie **eine** der folgenden Maßnahmen durch:

- Wenn Sie SSL für Dell Compliance Reporter, Dell Security Server oder Dell Device Server aktivieren möchten, wechseln Sie in das Komponentenverzeichnis **conf**.
- Wenn Sie SSL zwischen dem Dell Enterprise Server und dem Unternehmensverzeichnisserver aktivieren möchten, wechseln Sie in das Verzeichnis <**Dell install dir>\Java Runtimes\jre1.x.x_xx\lib\security** (das Standardpasswort für JRE-Cacerts lautet **changeit**).

3 Führen Sie Keytool wie folgt aus, um das Stammzertifikat zu installieren:

```
keytool -import -trustcacerts -alias <ca-cert-alias> -keystore .\cacerts -file <ca-cert-filename>
```

Beispiel: `keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer`

Beispielmethode zur Anforderung eines Zertifikats

Eine Methode zur Anforderung eines Zertifikats besteht darin, über einen Webbrowser auf den Microsoft-Zertifizierungsstellenserver zuzugreifen, der intern von Ihrer Organisation eingerichtet wird.

1 Navigieren Sie zum Microsoft-Zertifizierungsstellenserver. Die IP-Adresse wird von Ihrer Organisation bereitgestellt.

2 Wählen Sie **Zertifikat anfordern** aus, und klicken Sie auf **Weiter.**

Microsoft-Zertifikatdienste

3 Wählen Sie **Erweiterte Anforderung** aus, und klicken Sie auf **Weiter**.

Art der Anforderung auswählen

4 Wählen Sie die Option **Einreichen einer Zertifikatanforderung, die eine Base64-codierte PKCS #10-Datei verwendet**, und klicken Sie auf **Weiter**.

Erweiterte Zertifikatanforderung

5 Kopieren Sie den Inhalt der CSR-Anforderung in das Textfeld. Wählen Sie die Zertifikatvorlage **Web Server** aus, und klicken Sie auf **Einreichen.**

Gespeicherte Anforderung senden

6 Speichern Sie das Zertifikat. Wählen Sie **DER-codiert** und klicken Sie auf **Download des Zertifizierungsstellenzertifikats**.

Download des Zertifizierungsstellenzertifikats

7 Speichern Sie das Zertifikat. Wählen Sie **DER-codiert** und klicken Sie auf **Download des Zertifizierungsstellenzertifikats**.

Download des Zertifizierungsstellen-Zertifizierungspfads

8 Importieren Sie das konvertierte Zertifikat der Zertifizierungsstelle. Kehren Sie zum DOS-Fenster zurück. Geben Sie Folgendes ein:

```
keytool -import -trustcacerts -file <csr-filename> -keystore cacerts
```

9 Nach dem Import des Zertifikats der Zertifizierungsstelle kann nun das Serverzertifikat importiert werden (die Zertifikatkette kann eingerichtet werden). Geben Sie Folgendes ein:

```
keytool -import -alias sslkey -file <csr-filename> -keystore cacerts
```

Verwenden Sie das Alias des selbstsignierten Zertifikats, um die CSR-Anforderung mit dem Serverzertifikat zu verknüpfen.

10 Eine Auflistung der Cacerts-Datei zeigt, dass das Serverzertifikat eine **Zertifikatkettenlänge** von 2 hat. Dies ist ein Hinweis darauf, dass das Zertifikat nicht selbstsigniert ist. Geben Sie Folgendes ein:

```
keytool -list -v -keystore cacerts
```

Der Zertifikat-Fingerabdruck des zweiten Zertifikats in der Kette ist das importierte Zertifikat der signierenden Zertifizierungsstelle (außerdem unter dem Serverzertifikat in der Auflistung aufgeführt).

Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren

Sobald Ihnen ein Zertifikat in Form einer CRT-Datei im MMC vorliegt, muss diese für die Kompatibilität mit Keytool in eine PFX-Datei konvertiert werden, wenn Sie Dell Security Server im DMZ-Modus verwenden *und* ein Dell Manager-Zertifikat in das Dell Serverkonfigurationstool importieren möchten.

1 Öffnen Sie die Microsoft Management Console.
2 Klicken Sie auf **Datei > Snapin hinzufügen/entfernen**.
3 Klicken Sie auf **Hinzufügen**.
4 Wählen Sie im Fenster *Standalone-Snapin hinzufügen* **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
5 Wählen Sie **Computerkonto** aus und klicken Sie auf **Weiter**.
6 Wählen Sie im Fenster *Computer auswählen* **Lokaler Computer (der Computer, auf dem diese Konsole läuft)** und klicken Sie auf **Fertigstellen**.
7 Klicken Sie auf **Schließen**.
8 Klicken Sie auf **OK**.
9 Erweitern Sie im Ordner *Konsolenstamm* die *Zertifikate (Lokaler Computer)*.
10 Gehen Sie zum Ordner *Privat*, und suchen Sie das gewünschte Zertifikat.
11 Markieren Sie das gewünschte Zertifikat, und klicken Sie mit der rechten Maustaste auf **Alle Aufgaben > Exportieren**.
12 Sobald der Assistent „Zertifikat exportieren“ angezeigt wird, klicken Sie auf **Weiter**.
13 Wählen Sie **Ja, privaten Schlüssel exportieren** aus, und klicken Sie auf **Weiter**.
14 Wählen Sie **Privater Informationsaustausch - PKCS #12 (.PFX)** aus, und wählen Sie anschließend die Unteroptionen **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen** und **Alle erweiterten Eigenschaften exportieren** aus. Klicken Sie auf **Weiter**.
15 Geben Sie das Passwort ein und bestätigen Sie es. Sie können das Passwort frei wählen. Wählen Sie ein Passwort, das nur Sie selbst sich leicht merken können, nicht aber andere. Klicken Sie auf **Weiter**.
16 Klicken Sie auf **Durchsuchen**, um zu dem Speicherort zu navigieren, auf dem Sie die Datei speichern möchten.
17 Geben Sie im Feld `Dateiname` einen Namen für die zu speichernde Datei ein. Klicken Sie auf **Speichern**.
18 Klicken Sie auf **Weiter**.
19 Klicken Sie auf **Fertigstellen**.

Sie erhalten die Meldung, dass der Export erfolgreich abgeschlossen wurde. Schließen Sie die MMC.

Vertrauenswürdiges, signiertes Zertifikat zum Security Server hinzufügen, wenn ein nicht vertrauenswürdiges Zertifikat für SSL verwendet wurde

1 Wenn der Security Server-Service ausgeführt wird, halten Sie ihn an.

2 Sichern Sie die Cacerts-Datei unter <Security Server install dir>\conf\.

Verwenden Sie Keytool, um die folgenden Schritte auszuführen:

3 Vertrauenswürdige PFX-Datei in eine Textdatei exportieren und den Aliasnamen dokumentieren:

```
keytool -list -v -keystore "
```

4 PFX-Datei in die Cacerts-Datei nach <Security Server install dir>\conf\. importieren

```
keytool -importkeystore -v -srckeystore "
```

5 Ändern Sie den Wert für „keystore.alias.signing“ unter <Security Server install dir>\conf\application.properties.

```
keystore.alias.signing=AliasNamePreviouslyDocumented
```

Starten Sie den Security Server-Service.