Dell Data Protection

Erste Schritte mit Dell Data Protection

v9.4

2016-07

Inhalt

1

Implementierungsphasen

Der grundlegende Implementierungsvorgang besteht aus den folgenden Phasen:

- Durchführen von Kick-off und Übersicht der Anforderungen
- Abschließen von Checkliste für die Vorbereitung - Erste Implementierung oder Checkliste für die Vorbereitung - Upgrade/Migration
- Führen Sie eine Installation oder eine Aktualisierung/Migration von ***einem*** der folgenden Produkte durch:
  - Dell Enterprise Server
    - Zentralisierte Verwaltung von Geräten
    - Wird auf einem Microsoft Windows-Server ausgeführt
  - DDP Enterprise Server – VE
    - Zentrale Verwaltung von bis zu 3,500 Geräten
    - Wird in einer virtualisierten Umgebung ausgeführt

  Weitere Informationen zu Dell Data Protection-Servern finden Sie im *Enterprise Server-Installations- und Migrationshandbuch* oder im *Virtual Edition-Schnellstart- und Installationshandbuch*. Diese Dokumente erhalten Sie unter Dokumente zum Dell Data Protection-Server.

  Um Informationen zu Client-Anforderungen und zur Installation der Software zu erhalten, wählen Sie die jeweiligen Dokumente für Ihre Bereitstellung aus:

  - *Enterprise Edition - Einfaches Installationshandbuch* oder *Enterprise Edition - Erweitertes Installationshandbuch*
  - *Endpoint Security - Einfaches Installationshandbuch* oder *Endpoint Security Suite - Erweitertes Installationshandbuch*
  - *Endpoint Security Suite Enterprise - Einfaches Installationshandbuch* oder *Endpoint Security Suite Enterprise - Erweitertes Installationshandbuch*
  - *Personal Edition-Installationshandbuch*
  - *Security Tools-Installationshandbuch*
  - *Enterprise Edition für Mac-Administrator-Handbuch*
  - *Mobile Edition-Administrator-Handbuch*

  Diese Dokumente erhalten Sie unter Dokumente zum Dell Data Protection-Client.
- Konfiguration der ersten Richtlinie
  - Dell Enterprise Server - siehe *Enterprise Server-Installations- und Migrationshandbuch*, *Administrative Aufgaben*
  - DDDDP Enterprise Server – VE – siehe *Erste Schritte und Installationsanleitung für Virtual Edition*, *Remote Management Console Administrative Aufgaben*
- Ausführen des Testplans
- Client-Verpackung
- Teilnahme an der grundlegenden Wissensübertragung von Dell Data Protection Administrator
- Implementierung bewährter Verfahren
- Koordinierung des Support für Pilotprojekte oder Bereitstellung mit Dell Client Services

2

Kick-off und Übersicht der Anforderungen

Vor der Installation ist es wichtig, dass Sie Ihre Umgebung und die geschäftlichen und technischen Zielsetzungen Ihres Projekts verstehen, damit Sie Dell Data Protection erfolgreich implementieren können, um genau diese Ziele zu erreichen. Stellen Sie sicher, dass Sie über ein gründliches Verständnis der allgemeinen Datensicherheitsanforderungen Ihrer Organisation verfügen.

Im Folgenden werden einige der häufigsten und wichtigsten Fragen aufgeführt, die dem Dell-Kundendienst helfen, Ihre Umgebung und Anforderungen zu verstehen:

1. Zu welcher Branche gehört Ihre Organisation (Gesundheitswesen, usw)?
2. Welche Anforderungen für die Einhaltung von Regulierungen müssen Sie erfüllen (HIPAA/HITECH, PCI, usw.)?
3. Wie groß ist Ihre Organisation (Anzahl Benutzer, Anzahl physischer Standorte, usw.)?
4. Was ist die angezielte Anzahl von Endpunkten für die Implementierung? Gibt es Pläne für die Zukunft zur Erweiterung über diese Anzahl hinaus?
5. Haben Endbenutzer lokale Admin-Berechtigungen?
6. Welche Daten und Geräte müssen Sie verwalten und verschlüsseln (lokale Festplatten, USB, usw.)?
7. Welche Produkte möchten Sie implementieren?
   - Enterprise Edition
     - Encryption (DE-Berechtigung) – Windows Encryption, Server Encryption, External Media Shield (EMS), SED Management, Advanced Authentication, BitLocker Manager (BLM) und Mac Encryption.
     - External Media Edition (EME-Berechtigung)
     - Cloud Edition (CE-Berechtigung)
   - Endpoint Security Suite
     - Threat Protection (TP-Berechtigung)
     - Encryption (DE-Berechtigung) – Windows Encryption, Server Encryption, External Media Shield (EMS), SED Management, Advanced Authentication, BitLocker Manager (BLM) und Mac Encryption.
     - External Media Edition (EME-Berechtigung)
   - Endpoint Security Suite Enterprise
     - Advanced Threat Protection (ATP-Berechtigung)
     - Encryption (DE-Berechtigung) – Windows Encryption, Server Encryption, External Media Shield (EMS), SED Management, Advanced Authentication, BitLocker Manager (BLM) und Mac Encryption.
     - External Media Edition (EME-Berechtigung)
   - Mobile Edition (ME-Berechtigung) für Android, iOS und Windows Phone
8. Welche Art von Benutzerkonnektivität unterstützt Ihre Organisation? Zu diesen Arten können folgende gehören:
   - Nur lokale LAN-Konnektivität
   - VPN-basierte und/oder drahtlose Enterprise-Benutzer
   - Remote-/nicht angeschlossene Benutzer (Benutzer, die weder direkt noch für längere Zeit über VPN mit dem Netzwerk verbunden sind)
   - Nicht-Domänen-Workstations
9. Welche Daten müssen Sie am Endpunkt schützen? Welche Art von Daten haben typische Benutzer am Endpunkt?
10. Welche Benutzeranwendungen können vertrauliche Daten enthalten? Was sind die Anwendungsdateitypen?
11. Wieviele Domänen haben Sie in Ihrer Umgebung? Wieviele sind im Projektumfang zur Verschlüsselung?

12 Welche Betriebssysteme und BS-Versionen sollen verschlüsselt werden?

13 Haben Sie alternative Startpartitionen auf Ihren Endpunkten konfiguriert?

a Wiederherstellungspartition des Herstellers

b Doppelstart-Workstations

Dokumente zum Dell Data Protection-Client

Informationen zu Installationsanforderungen, unterstützten BS-Versionen und SEDs sowie Benutzeranweisungen für die bereitzustellenden Dell Data Protection-Produkte finden Sie in den entsprechenden unten aufgeführten Dokumenten.

Enterprise Edition (Windows-Clients) - Lesen Sie die folgenden Dokumente, die unter dieser Adresse verfügbar sind: www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

- *Enterprise Edition - Einfaches Installationshandbuch* - Installationshandbuch für Enterprise Edition.
- *Erweitertes Enterprise Edition-Installationshandbuch* - Installationshandbuch für Enterprise Edition mit erweiterten Schaltern und Parametern für benutzerdefinierte Installationen.
- *DDP Console-Benutzerhandbuch* - Anweisungen für Endanwender von Dell Data Protection I Advanced Authentication.
- *Cloud Edition-Benutzerhandbuch* - Anweisungen für Installation, Aktivierung und Betrieb für Endanwender von Dell Data Protection I Cloud Edition.

Enterprise Edition (Mac-Clients) - Lesen Sie das *Enterprise Edition für Mac Administrator-Handbuch* unter www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals.
Das *Administrator-Handbuch* enthält Anweisungen für Installation und Bereitstellung.

Endpoint Security Suite (Windows-Clients) - Lesen Sie die folgenden Dokumente, die unter dieser Adresse verfügbar sind: www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/manuals.

- *Endpoint Security Suite - Einfaches Installationshandbuch* - Installationshandbuch für Endpoint Security Suite.
- *Erweitertes Endpoint Security Suite-Installationshandbuch* - Installationshandbuch für Endpoint Security Suite mit erweiterten Schaltern und Parametern für benutzerdefinierte Installationen.
- *DDP Console-Benutzerhandbuch* - Anweisungen für Endanwender von Dell Data Protection I Endpoint Security Suite.

Endpoint Security Suite Enterprise (Windows-Clients) - Lesen Sie die folgenden Dokumente unter dieser Adresse: www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- *Endpoint Security Suite Enterprise - Einfaches Installationshandbuch* - Installationshandbuch für Endpoint Security Suite Enterprise.
- *Endpoint Security Suite Enterprise - Erweitertes Installationshandbuch* - Installationshandbuch für Endpoint Security Suite Enterprise, mit erweiterten Schaltern und Parametern für benutzerangepasste Installationen.
- *DDP-Konsolenbenutzerhandbuch* - Anweisungen für Dell Data Protection I Endpoint Security Suite Enterprise-Endbenutzer.

Mobile Edition für Android-, iOS- und Windows-Handy

- Lesen Sie das *Mobile Edition Administrator-Handbuch* unter www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals.
  Im *Administrator-Handbuch* wird die Bereitstellung von Dell Data Protection I Mobile Edition erläutert.

Dokumente zum Dell Data Protection-Server

Informationen zu Installationsanforderungen, unterstützten BS-Versionen und Konfigurationen für den bereitzustellenden Dell Data Protection-Server finden Sie in den entsprechenden unten aufgeführten Dokumenten.

Dell Enterprise Server

- Lesen Sie das *Enterprise Server-Installations- und Migrationshandbuch* unter
  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

  oder

  www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/manuals.

  oder

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

DDP Enterprise Server – Virtual Edition

Lesen Sie *Virtual Edition - Schnellstartanleitung und Installationshandbuch* unter
www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

oder

www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/manuals.

oder

www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

3

Checkliste für die Vorbereitung - Erste Implementierung

Verwenden Sie auf der Basis des bei Ihnen eingesetzten Dell Data Protection Servers die zugehörige Checkliste, um sicherzustellen, dass alle Voraussetzungen erfüllt sind, bevor Sie mit der Installation von Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite oder Dell Data Protection | Endpoint Security Suite Enterprise beginnen.

- Checkliste für Dell Enterprise Server
- Checkliste für DDP Enterprise Server - VE

Checkliste für Dell Enterprise Server

Ist die Bereinigung der Proof of Concept-Umgebung vollständig (falls zutreffend)?

- ☐ Die Proof of Concept-Datenbank und -Anwendung wurden vor dem Installations-Engagement mit Dell gesichert und deinstalliert (falls derselbe Server verwendet wird).
- ☐ Alle während dem Proof of Concept-Testen verwendeten Produktionsendpunkte wurden entschlüsselt oder Schlüsselbündel heruntergeladen.
- ☐ Die Proof of Concept-Anwendung wurde aus der Umgebung entfernt.

ANMERKUNG: Alle neuen Implementierungen müssen mit einer neuen Datenbank und Installation der Software Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise beginnen. Die Dell Client Services führen keine neue Implementierung mithilfe einer POC-Umgebung aus. Während einem Proof of Concept verschlüsselte Endpunkte müssen vor dem Installations-Engagement mit Dell entweder entschlüsselt oder neu aufgebaut werden.

Erfüllen Server die erforderlichen Hardware-Spezifikationen?

- ☐ Siehe Architektur für Dell Enterprise Server.

Erfüllen Server die erforderlichen Software-Spezifikationen?

- ☐ Windows Server 2008 SP2 64-Bit (Standard oder Enterprise); 2008 R2 SP0-SP1 64-Bit (Standard oder Enterprise); 2012 R2 (Standard) ist installiert.
- ☐ Windows Installer 4.0 oder höher ist installiert.
- ☐ .NET Framework 4.5 ist installiert.
- ☐ Bei Verwendung von Microsoft SQL Server 2012 ist der Microsoft SQL Native Client 2012 installiert. Falls verfügbar, kann der SQL Native Client 2014 eingesetzt werden.

  ANMERKUNG: SQL Express wird bei Dell Enterprise Server nicht unterstützt.
- ☐ Die Windows Firewall ist deaktiviert oder so konfiguriert, dass sie folgende (eingehende) Ports zulässt: 80, 1099, 1433, 8000, 8050, 8081, 8084, 8443, 8445, 8888, 9000, 9011, 61613, 61616.
- ☐ Die Konnektivität ist zwischen Dell Enterprise Server und Active Directory (AD) über Ports 88, 135, 389, 636, 3268, 3269, 49125+ (RPC) (eingehend zu AD) verfügbar.
- ☐ UAC ist deaktiviert (siehe Windows-Systemsteuerung > Benutzerkonten).
  - Windows Server 2008 SP2 64-Bit/Windows Server 2008 R2 SP0-SP1 64-Bit
  - Windows Server 2012 R2 – das Installationsprogramm deaktiviert UAC.

Wurden Dienstkonten erfolgreich erstellt?

- ☐ Dienstkonto mit schreibgeschütztem Zugriff auf AD (LDAP) - das grundlegende Benutzer-/Domänenbenutzerkonto ist genug.
- ☐ Das Dienstkonto muss über lokale Administratorrechte für die Dell Enterprise Server-Anwendungsserver verfügen.
- ☐ Bei Verwendung der Windows-Authentifizierung für die Datenbank, ein Domänendienstkonto mit Systemadministratorenrechten. Das Benutzerkonto muss im Format DOMAIN\\Username vorliegen und das Default Schema: dbo und Database Role Membership: dbo_owner, public aufweisen.
- ☐ Zur Verwendung von SQL-Authentifizierung muss das verwendete SQL-Konto Systemadministratorenrechte auf dem SQL-Server haben. Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.

Ist die Software heruntergeladen?

Laden Sie die Software von der Dell Support Website herunter.

- ☐ Downloads für die Dell Data Protection-Client-Software und für Dell Enterprise Server befinden sich im Ordner **Treiber & Downloads** unter www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research

  oder

  www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y

  oder

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

  So navigieren Sie von www.dell.com/support zum Zielordner

  1. Wählen Sie unter **Nach Produkt suchen** den Eintrag **Produkte anzeigen** sowie anschließend **Software und Sicherheit** und **Endpoint Security Solutions**.
  2. Wählen Sie **Dell Data Protection I Encryption, Dell Data Protection I Endpoint Security Suite**, oder **Dell Data Protection I Endpoint Security Suite Enterprise** und anschließend **Treiber und Downloads** aus.
  3. Wählen Sie in der Betriebssystem-Pull-Down-Liste das richtige Betriebssystem für das Produkt aus, das Sie herunterladen. Beispiel: Zum Herunterladen von Dell Enterprise Server wählen Sie **eine der Windows Server-Optionen** aus.
  4. Wählen Sie unter der jeweiligen Software-Überschrift **Datei herunterladen** aus.
- ☐ Wenn Sie Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise „On-the-box“ erworben haben, kann die Software von www.dell.com heruntergeladen werden. „On-the-box“-Software ist die Software, die dem von Dell werkseitig mitgelieferten Computerabbild beigegeben ist. Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise können werkseitig auf jedem beliebigen Dell-Computer vorinstalliert werden.

ODER

Laden Sie die Software von der Dell Data Protection-Datenübertragungssite (CFT) herunter.

- ☐ Die Software befindet sich unter https://ddpe.credant.com oder https://cft.credant.com im Ordner **SoftwareDownloads**.
- ☐ Wenn Sie Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise „On-the-box“ erworben haben, kann die Software von www.dell.com heruntergeladen werden. „On-the-box“-Software ist die Software, die dem von Dell werkseitig mitgelieferten Computerabbild beigegeben ist. Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise können werkseitig auf jedem beliebigen Dell-Computer vorinstalliert werden.

Sind Installationsschlüssel und Lizenzdatei verfügbar?

- ☐ Der Lizenzschlüssel ist in der ursprünglichen E-Mail mit den CFT-Anmeldeinformationen enthalten - siehe Beispiel für E-Mail mit Kundenbenachrichtigung.
- ☐ Die Lizenzdatei ist eine XML-Datei auf der CFT-Site im Ordner **Client-Lizenzen**.

ANMERKUNG: Falls Sie Ihre Lizenzen „on-the-box“ gekauft haben, ist keine Lizenzdatei notwendig. Die Berechtigung wird bei der Aktivierung eines neuen Encryption-, Endpoint Security Suite- oder Endpoint Security Suite Enterprise-Clients automatisch von Dell heruntergeladen.

Wurde die Datenbank erstellt?

- ☐ (Optional) Eine neue Datenbank wird auf einem unterstützten Server erstellet – siehe *Anforderungen und Architektur* im *Enterprise Server Installations- und Migrationshandbuch*. Das Installationsprogramm von Enterprise Server erstellt bei der Installation eine Datenbank, falls noch keine angelegt war.
- ☐ Der Zieldatenbankbenutzer hat die Rechte des **db_owner** erhalten.

Wurde das DNS-Alias für Dell Enterprise Server und/oder Policy Proxies mit Split DNS für internen und externen Verkehr erstellt?

Es wird empfohlen, dass Sie DNS-Aliase für die Skalierbarkeit erstellen. Dies ermöglicht Ihnen das spätere Hinzufügen zusätzlicher Server oder separater Komponenten der Anwendung, ohne dass eine Clientaktualisierung nötig ist.

- ☐ DNS-Aliase werden auf Wunsch erstellt. Vorgeschlagene DNS-Aliase:
  - Dell Enterprise Server: ddpe-es.<domain.com>
  - Front-End Server: ddpe-fe.<domain.com>

ANMERKUNG: Split-DNS ermöglicht Ihnen die Verwendung desselben DNS-Namens für interne sowie externe Front-End-Dienste und ist in einigen Fällen notwendig. Split-DNS ermöglicht Ihnen die Verwendung einer einzelnen Adresse für Ihre Clients und bietet Flexibilität bei der Ausführung von Upgrades oder der späteren Skalierung der Lösung. Vorgeschlagener CNAME für Front-End-Server unter Verwendung von Split-DNS: ddpe-fe.<domain.com>.

Haben Sie einen Plan für SSL-Zertifikate?

- ☐ Wir haben eine interne Certificate Authority (CA), die zur Signierung von Zertifikaten verwendet werden kann, und der alle Workstations in der Umgebung vertrauen ***oder*** wir haben vor, ein signiertes Zertifikat mithilfe einer öffentlichen Certificate Authority zu kaufen, wie z. B. VeriSign oder Entrust. Falls Sie eine öffentliche Certificate Authority verwenden, informieren Sie bitte den Kundendienst-Techniker von Dell. Das Zertifikat enthält die gesamte Chain of Trust (Root und Intermediate) mit Public und Private Key Signaturen.
- ☐ Subject Alternate Names (SANs) in der Zertifikatsanforderung erfassen alle DNS-Aliase, die für jeden Server vergeben werden, der zur Installation von Dell Enterprise Server verwendet wird. Gilt nicht für Platzhalter oder selbstsignierte Zertifikatsanforderungen.
- ☐ Zertifikat wird in einem .pfx-Format erzeugt.

Wurden die Anforderungen für Change Control identifiziert und Dell mitgeteilt?

- ☐ Reichen Sie jegliche spezifischen Change Control-Anforderungen für die Installation von Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise vor Installationsbeginn beim Dell Kundendienst ein. Zu diesen Anforderungen gehören u. a. Änderungen am/an den Anwendungsserver/-n, der Datenbank und Client-Workstations.

Wurde die Test-Hardware vorbereitet?

- ☐ Bereiten Sie mindestens drei Computer, die zum Testen verwendet werden sollen, mit dem Computerabbild Ihres Unternehmens vor. Dell empfiehlt, dass Sie zum Testen ***keine*** live Systeme verwenden. Live Systeme sollten während einem Produktionspilotprojekt verwendet werden, nachdem Verschlüsselungsrichtlinien definiert und mit dem von Dell bereitgestellten Testplan getestet wurden.

Checkliste für DDP Enterprise Server - VE

Ist die Bereinigung der Proof of Concept-Umgebung vollständig (falls zutreffend)?

- ☐ Die Proof of Concept-(POC)-Datenbank und -Anwendung wurden vor dem Installations-Engagement mit Dell gesichert und deinstalliert (falls derselbe Server verwendet wird).
- ☐ Alle während dem Proof of Concept-Testen verwendeten Produktionsendpunkte wurden entschlüsselt oder Schlüsselbündel heruntergeladen.
- ☐ Die Proof of Concept-Anwendung wurde aus der Umgebung entfernt.

ANMERKUNG: Alle neuen Implementierungen müssen mit einer neuen Datenbank und Installation der Software Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise beginnen. Die Dell Client Services führen keine neue Implementierung mithilfe einer POC-Umgebung aus. Während einem Proof of Concept verschlüsselte Endpunkte müssen vor dem Installations-Engagement mit Dell entweder entschlüsselt oder neu aufgebaut werden.

Wurden Dienstkonten erfolgreich erstellt?

- ☐ Dienstkonto mit schreibgeschütztem Zugriff auf AD (LDAP) – das grundlegende Benutzer-/Domänenbenutzerkonto ist genug.

Ist die Software heruntergeladen?

- ☐ Downloads für die Dell Data Protection-Client-Software und für Virtual Edition befinden sich im Ordner **Treiber & Downloads** unter www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research

  oder

  www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y

  oder

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

  So navigieren Sie von www.dell.com/support zum Zielordner

  1. Wählen Sie unter **Nach Produkt suchen** den Eintrag **Produkte anzeigen** sowie anschließend **Software und Sicherheit** und **Endpoint Security Solutions**.
  2. Wählen Sie **Dell Data Protection I Encryption, Dell Data Protection I Endpoint Security Suite**, oder **Dell Data Protection I Endpoint Security Suite Enterprise** und anschließend **Treiber und Downloads** aus.
  3. Wählen Sie in der Betriebssystem-Pull-Down-Liste das richtige Betriebssystem für das Produkt aus, das Sie herunterladen. Wählen Sie beispielsweise zum Herunterladen von Virtual Edition **eine der VMware-Versionen** aus.
  4. Wählen Sie unter der jeweiligen Software-Überschrift **Datei herunterladen** aus.
- ☐ Wenn Sie Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise „On-the-box“ erworben haben, kann die Software von www.dell.com heruntergeladen werden. „On-the-box“-Software ist die Software, die dem von Dell werkseitig mitgelieferten Computerabbild beigegeben ist. Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise können werkseitig auf jedem beliebigen Dell-Computer vorinstalliert werden.

Ist (sind) die Lizenzdatei(en) verfügbar?

- ☐ Die Lizenzdatei ist eine XML-Datei auf der CFT-Site im Ordner **Client-Lizenzen**.

ANMERKUNG: Falls Sie Ihre Lizenzen „on-the-box“ gekauft haben, ist keine Lizenzdatei notwendig. Die Berechtigung wird bei der Aktivierung eines neuen Encryption-, Endpoint Security Suite- oder Endpoint Security Suite Enterprise-Clients automatisch von Dell heruntergeladen.

Erfüllen Server die erforderlichen Hardware-Spezifikationen?

- ☐ Siehe DDP Enterprise Server - Virtual Edition.

Haben Sie einen Plan für SSL-Zertifikate?

- ☐ Wir haben eine interne Certificate Authority (CA), die zur Signierung von Zertifikaten verwendet werden kann, und der alle Workstations in der Umgebung vertrauen ***oder*** wir haben vor, ein signiertes Zertifikat mithilfe einer öffentlichen Certificate Authority zu kaufen, wie z. B. VeriSign oder Entrust. Falls Sie eine öffentliche Certificate Authority verwenden, informieren Sie bitte den Kundendienst-Techniker von Dell.

Wurden die Anforderungen für Change Control identifiziert und Dell mitgeteilt?

- ☐ Reichen Sie jegliche spezifischen Change Control-Anforderungen für die Installation von Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise vor Installationsbeginn beim Dell Kundendienst ein. Zu diesen Anforderungen gehören u. a. Änderungen am/an den Anwendungsserver/-n, der Datenbank und Client-Workstations.

Wurde die Test-Hardware vorbereitet?

- ☐ Bereiten Sie mindestens drei Computer, die zum Testen verwendet werden sollen, mit dem Computerabbild Ihres Unternehmens vor. Dell empfiehlt, dass Sie zum Testen ***keine*** live Systeme verwenden. Live Systeme sollten während einem Produktionspilotprojekt verwendet werden, nachdem Verschlüsselungsrichtlinien definiert und mit dem von Dell bereitgestellten Testplan getestet wurden.

4

Checkliste für die Vorbereitung - Upgrade/Migration

Die folgende Checkliste gilt nur für Dell Enterprise Server.

ANMERKUNG: Aktualisieren Sie DDP Enterprise Server - VE über das Menü Grundkonfiguration im VE Terminal. Weitere Informationen finden Sie im Handbuch *Erste Schritte und Installationsanleitung für DDP Enterprise Server – Virtual Edition*.

Verwenden Sie die folgende Checkliste, um sicherzustellen, dass alle Voraussetzungen erfüllt sind, bevor Sie mit der Aktualisierung von Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite oder Dell Data Protection | Endpoint Security Suite Enterprise beginnen.

Erfüllen Server die erforderlichen Software-Spezifikationen?

- ☐ Windows Server 2008 SP2 64-Bit (Standard oder Enterprise); 2008 R2 SP0-SP1 64-Bit (Standard oder Enterprise); 2012 R2 (Standard) ist installiert.
- ☐ Windows Installer 4.0 oder höher ist installiert.
- ☐ .NET Framework 4.5 ist installiert.
- ☐ Bei Verwendung von Microsoft SQL Server 2012 ist der Microsoft SQL Native Client 2012 installiert. Falls verfügbar, kann SQL Native Client 2014 verwendet werden.

  ANMERKUNG: SQL Express wird bei Dell Enterprise Server nicht unterstützt.
- ☐ Die Windows Firewall ist deaktiviert oder so konfiguriert, dass sie folgende (eingehende) Ports zulässt: 80, 1099, 1433, 8000, 8050, 8081, 8084, 8443, 8445, 8888, 9000, 9011, 61613, 61616.
- ☐ Die Konnektivität ist zwischen Dell Enterprise Server und Active Directory (AD) über Ports 88, 135, 389, 636, 3268, 3269, 49125+ (RPC) (eingehend zu AD) verfügbar.
- ☐ UAC ist deaktiviert (siehe Windows Systemsteuerung > Benutzerkonten).
  - Windows Server 2008 SP2 64-Bit/Windows Server 2008 R2 SP0-SP1 64-Bit
  - Windows Server 2012 R2 - das Installationsprogramm deaktiviert UAC.

Wurden Dienstkonten erfolgreich erstellt?

- ☐ Servicekonto mit schreibgeschütztem Zugriff auf AD (LDAP) - das grundlegende Benutzer-/Domänenbenutzerkonto reicht aus.
- ☐ Das Dienstkonto muss über lokale Administratorrechte für die Dell Enterprise Server-Anwendungsserver verfügen.
- ☐ Um die Windows-Authentifizierung für die Datenbank zu verwenden, ein Domönenbenutzerkonto mit Systemadministratorrechten. Das Benutzerkonto muss im Format DOMAIN\\Username vorliegen und das Default Schema: dbo und Database Role Membership: dbo_owner, public aufweisen:
- ☐ Für die Verwendung der SQL Authentifizierung muss das SQL-Konto auf dem SQL-Server über Systemadministratorberechtigungen verfügen. Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.

Sind die Datenbank und alle notwendigen Dateien gesichert?

- ☐ Die gesamte vorhandene Installation wird an einem alternativen Speicherort gesichert. Die Sicherung sollte die SQL Datenbank, secretKeyStore, und Konfigurationsdateien enthalten.
- ☐ Stellen Sie sicher, dass diese wichtigsten Dateien gesichert werden, auf denen für eine Verbindung mit der Datenbank notwendige Informationen gespeichert 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

Sind Installationsschlüssel und Lizenzdatei verfügbar?

- ☐ Der Lizenzschlüssel ist in der ursprünglichen E-Mail mit den CFT-Anmeldeinformationen enthalten - siehe Beispiel für E-Mail mit Kundenbenachrichtigung.
- ☐ Die Lizenzdatei ist eine XML-Datei auf der CFT-Site im Ordner **Client-Lizenzen**.

ANMERKUNG: Falls Sie Ihre Lizenzen „on-the-box" gekauft haben, ist keine Lizenzdatei notwendig. Die Berechtigung wird bei der Aktivierung eines neuen Encryption-, Endpoint Security Suite- oder Endpoint Security Suite Enterprise-Clients automatisch von Dell heruntergeladen.

Wurde neue und vorhandene Dell Data Protection-Software heruntergeladen?

Laden Sie die Software von der Dell Data Protection-Dateiübertragungssite (CFT) herunter.

- ☐ Die Software befindet sich unter https://ddpe.credant.com or https://cft.credant.com im Ordner **SoftwareDownloads**.
- ☐ Wenn Sie Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise „On-the-box" erworben haben, kann die Software von www.dell.com heruntergeladen werden. „On-the-box"-Software ist die Software, die dem von Dell werkseitig mitgelieferten Computerabbild beigegeben ist. Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise können werkseitig auf jedem Dell Computer vorinstalliert werden.

Haben Sie genug Endpunktlizenzen?

Vor dem Upgrade sollten Sie sicherstellen, dass Sie genügend Clientlizenzen zum Abdecken aller Endpunkte in Ihrer Umgebung haben. Falls Sie derzeit mehr Installationen als Lizenzen haben, wenden Sie sich an Ihren Dell-Vertriebsrepräsentanten, bevor Sie ein Upgrade oder eine Migration ausführen. Dell Data Protection führt die Lizenzprüfung durch und die Aktivierungen werden verhindert, wenn keine Lizenzen vorhanden sind.

- ☐ Ich habe genug Lizenzen für meine ganze Umgebung.

Haben Sie einen Plan für SSL-Zertifikate?

- ☐ Wir haben eine interne Certificate Authority (CA), die zur Signierung von Zertifikaten verwendet werden kann, und der alle Workstations in der Umgebung vertrauen ***oder*** wir haben vor, ein signiertes Zertifikat mithilfe einer öffentlichen Certificate Authority zu kaufen, wie z. B. VeriSign oder Entrust. Falls Sie eine öffentliche Certificate Authority verwenden, informieren Sie bitte den Kundendienst-Techniker von Dell. Das Zertifikat enthält die gesamte Vertrauenskette (Root und Intermediate) mit öffentlichen und privaten Schlüsselsignaturen.
- ☐ „Subject Alternate Names"(SANs) auf Certificate Request entsprechen allen DNS-Aliases, die jedem für die Dell Enterprise Server Installation verwendeten Server übergeben werden. Dies trifft nicht für Wildcard- oder selbstsignierte Zertifikatsanfragen zu.
- ☐ Das Zertifikat wird in einem .pfx-Format erstellt.

Wurden die Anforderungen für Change Control identifiziert und Dell mitgeteilt?

- ☐ Reichen Sie spezifische Anforderungen für Change Control für die Installation von Encryption, Endpoint Security Suite oder Endpoint Security Suite Enterprise vor dem Installations-Engagement an den Dell-Kundendienst ein. Zu diesen Anforderungen gehören u. a. Änderungen am/an den Anwendungsserver/-n, der Datenbank und Client-Workstations.

Wurde die Test-Hardware vorbereitet?

- ☐ Bereiten Sie mindestens drei Computer, die zum Testen verwendet werden sollen, mit dem Computerabbild Ihres Unternehmens vor. Dell empfiehlt, dass Sie zum Testen ***keine*** live Systeme verwenden. Live Systeme sollten während einem Produktionspilotprojekt verwendet werden, nachdem Verschlüsselungsrichtlinien definiert und mit dem von Dell bereitgestellten Testplan getestet wurden.

5

Architektur

In diesem Abschnitt werden die Architektur-Design-Empfehlungen für die Dell Data Protection-Implementierung erläutert. Wählen Sie den Dell-Server aus, den Sie bereitstellen möchten:

- Dell Enterprise Server
- DDP Enterprise Server - Virtual Edition

Dell Enterprise Server

Die Lösungen Encryption, Endpoint Security Suite und Endpoint Security Suite Enterprise 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 Kundendienst 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 DDPE-Serverkomponenten können auf einem einzelnen Server installiert werden. Optional kann ein Front-End-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 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 externen Front-End-Server von Dell

Windows Server 2008 R2 SP0-SP1 64-Bit/Windows Server 2008 SP2 64-Bit – Standard oder Enterprise Edition/Windows Server 2012 R2 – Standard Edition

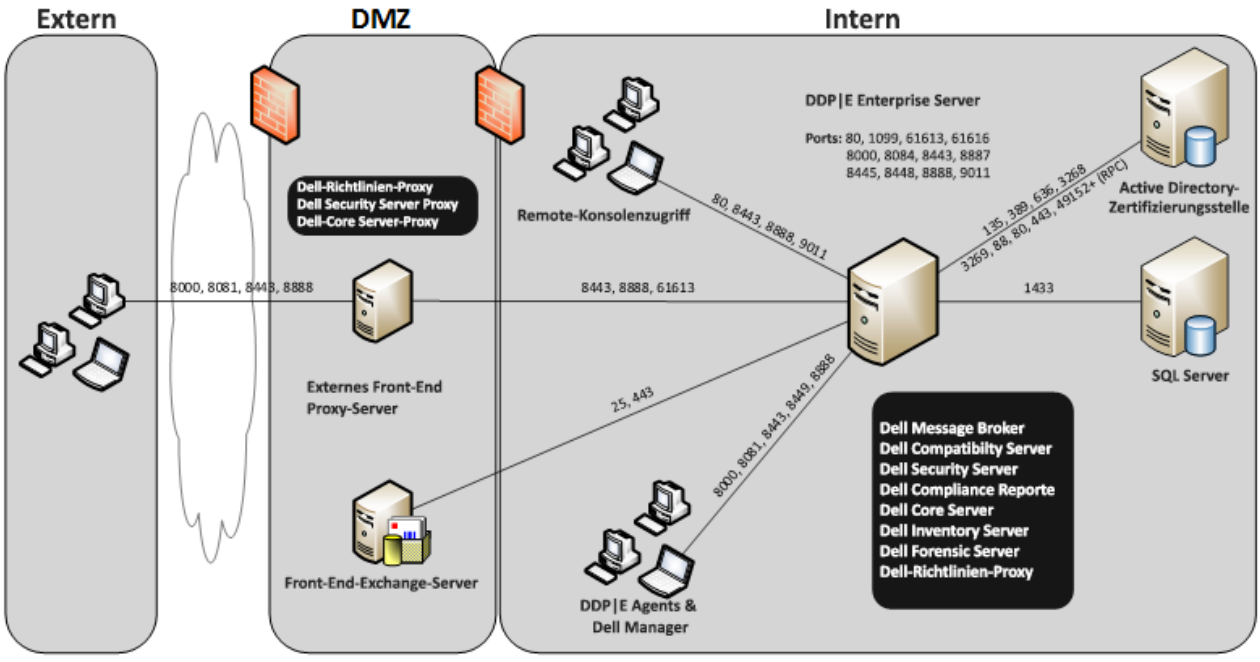
Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

SQL-Server

Microsoft SQL Server 2008 und Microsoft SQL Server 2008 R2 Standard Edition / Enterprise Edition

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

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



5.000 - 20.000 Endpunkte

Diese Architektur ist für Umgebungen mit 5.000 bis 20.000 Endpunkten geeignet. Ein Front-End-Server wird hinzugefügt, um die zusätzliche Last zu verteilen, und soll ungefähr 15.000 bis 20.000 Endpunkte handhaben. Optional kann ein Front-End-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 64-Bit – Standard oder Enterprise Edition/Windows Server 2012 R2 – Standard 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

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 Edition

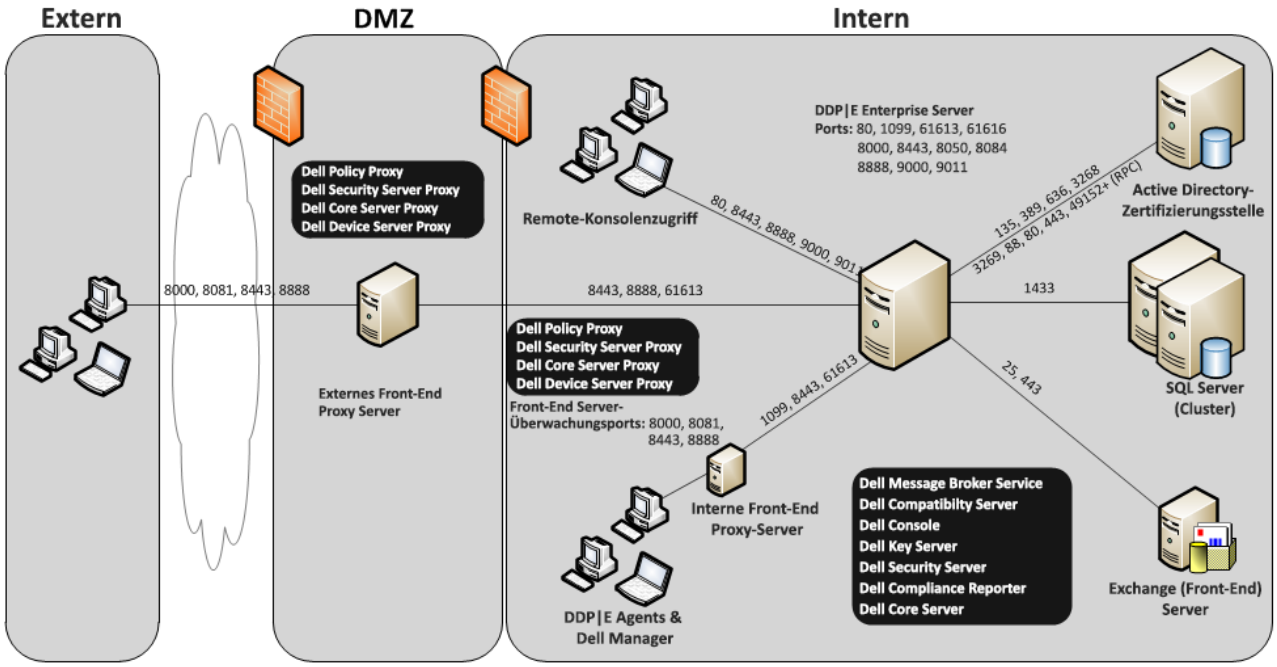
Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

SQL-Server

Microsoft SQL Server 2008 und Microsoft SQL Server 2008 R2 Standard Edition / Enterprise Edition

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

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



20.000 - 40.000 Endpunkte

Diese Architektur ist für Umgebungen mit 20.000 bis 40.000 Endpunkten geeignet. Ein zusätzlicher Front-End-Server wird zur Verteilung der zusätzlichen Last hinzugefügt. Jeder Front-End-Server soll etwa 15.000 bis 20.000 Endpunkte handhaben. Optional kann ein Front-End-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 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 Edition

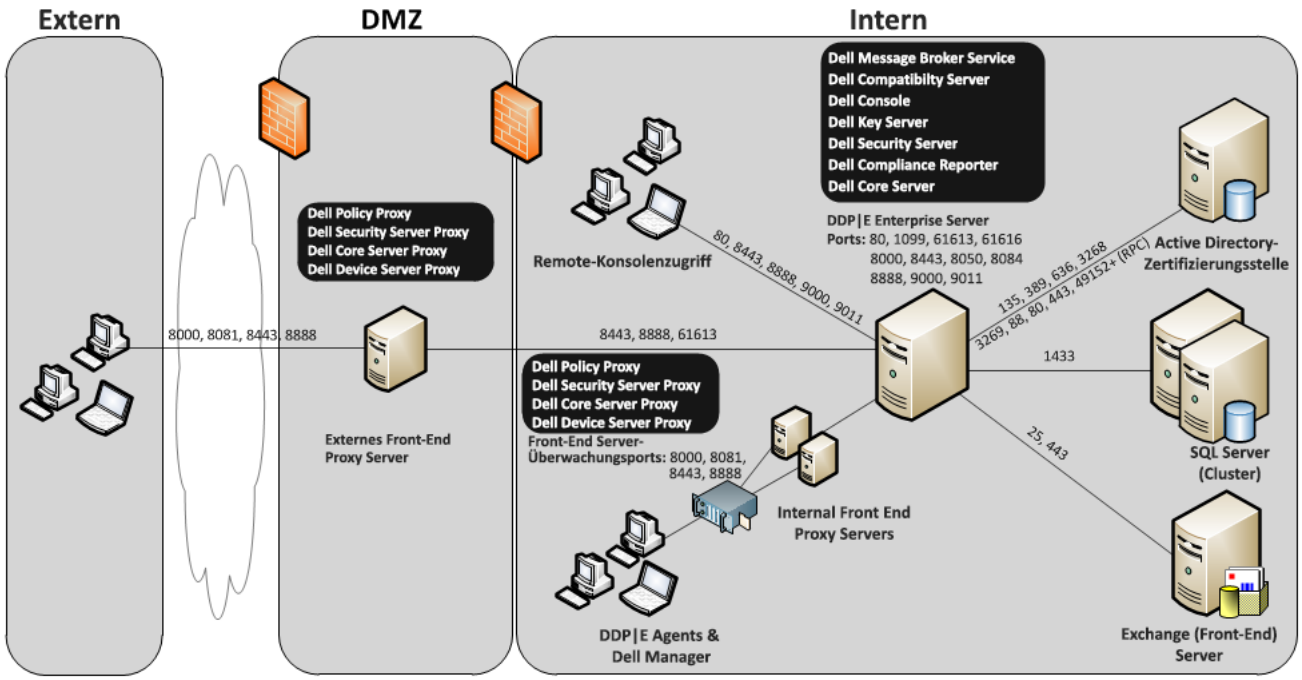
Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

SQL-Server

Microsoft SQL Server 2008 und Microsoft SQL Server 2008 R2 Standard Edition / Enterprise Edition

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

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



40.000 - 60.000 Endpunkte

Diese Architektur ist für Umgebungen mit 40.000 bis 60.000 Endpunkten geeignet. Ein zusätzlicher Front-End-Server wird zur Verteilung der zusätzlichen Last hinzugefügt. Jeder Front-End-Server soll etwa 15.000 bis 20.000 Endpunkte handhaben. Optional kann ein Front-End-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 Kundendienst 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 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 Edition

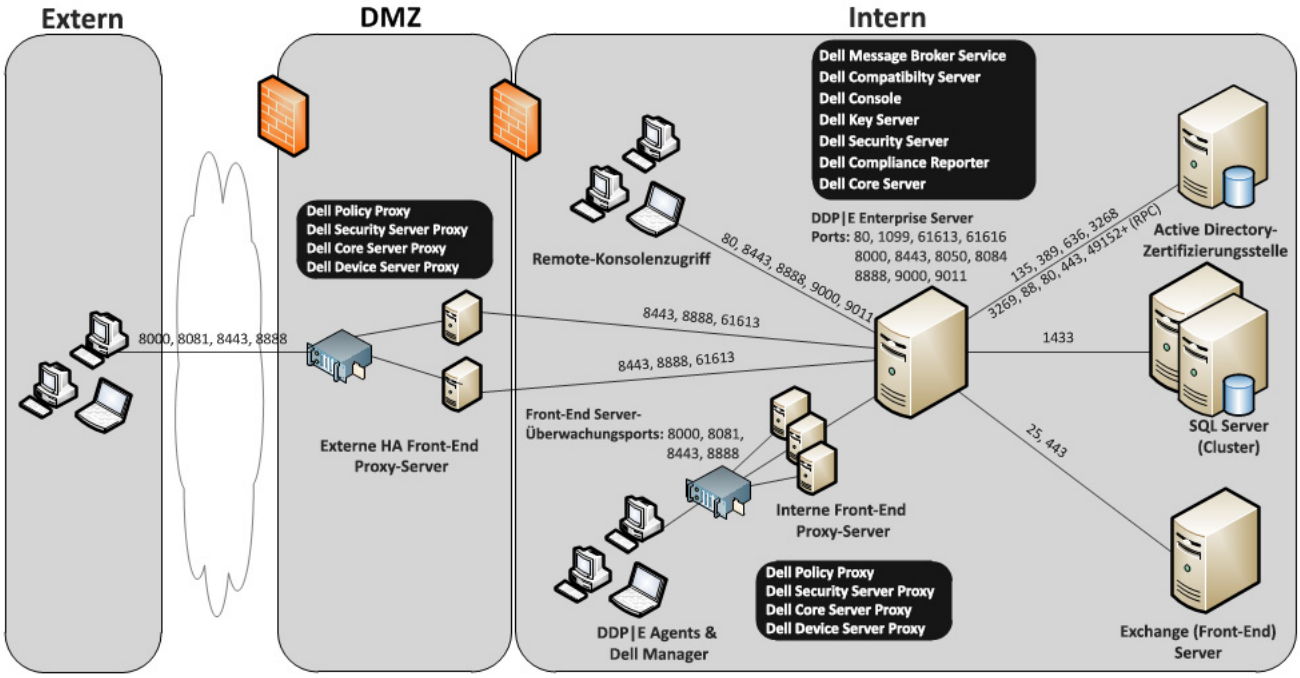
Mindestens 8 GB, je nach Konfiguration; ca. 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher); moderne Dual-Kern-CPU (mit mindestens 2 GHz), einschließlich Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium oder AMD-Entsprechung

SQL-Server

Microsoft SQL Server 2008 und Microsoft SQL Server 2008 R2 Standard Edition / Enterprise Edition

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

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



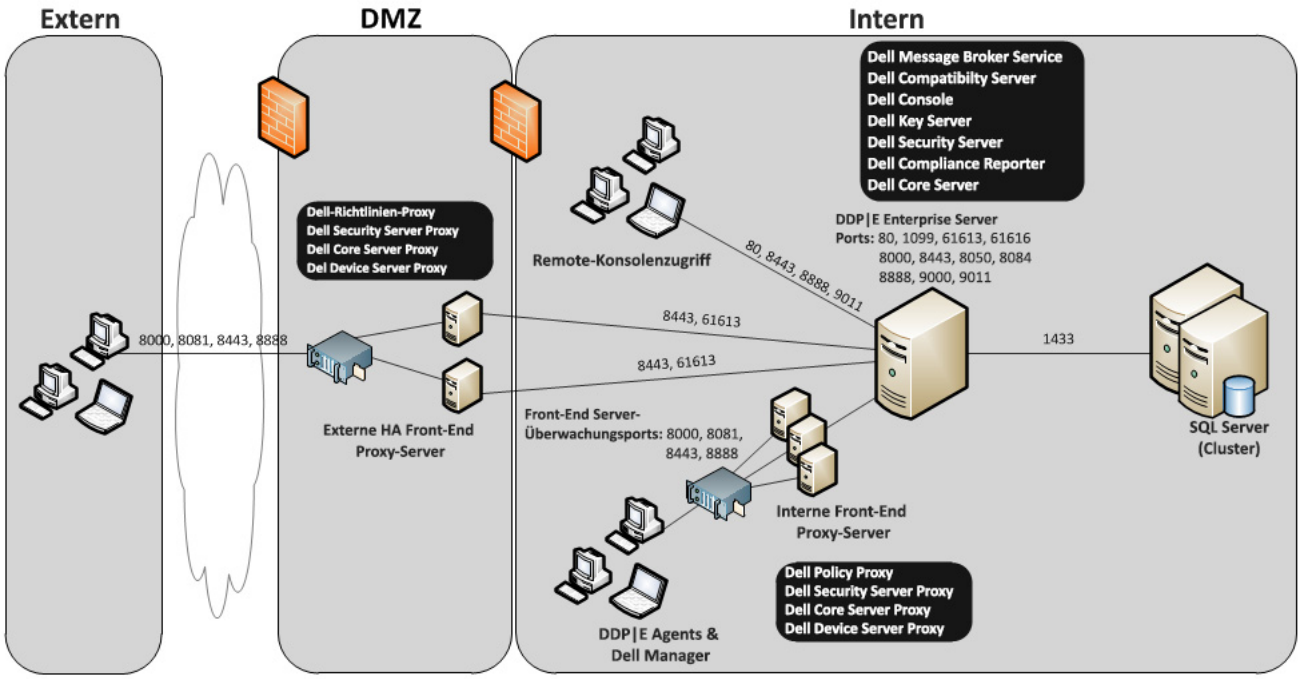
Überlegungen für hohe Verfügbarkeit

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 Front-End-Server verteilt. Optional können Front-End-Server auch zur Aktivierung von Endpunkten und/oder Veröffentlichung von Richtlinien an Endpunkte übers Internet im DMZ platziert werden.



Virtualisierung

Dell Data Protection-Anwendungsserver

Die Festplattengeschwindigkeit auf der Hardware, die den virtuellen Server hostet, die Zuordnung von RAM auf dem Gast und die Speicherkonfiguration können die Leistung bedeutend beeinträchtigen. Am auffälligsten ist der Leistungsabfall während der Aktivierung, der Richtlinien- und Bestandsverarbeitung und der Triage. Dell empfiehlt, soviel RAM wie möglich für den virtuellen Host zu reservieren und dem virtuellen Host die Priorität bei der Ressourcenzuordnung zu geben. Wenn die Leistung eine Rolle spielt, ratet Dell zum Einsatz einer nicht-virtuellen Serverumgebung.

SQL-Server

In größeren Umgebungen wird empfohlen, dass der SQL-Datenbankserver auf physikalischer Hardware und 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.

Weitere Informationen zu bewährten Verfahren für SQL Server finden Sie im *Enterprise Server-Installations- und Migrationshandbuch*.

Dell Enterprise Server-Ports

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

Name	Standardport	Beschreibung	Erforderlich für
Compliance Reporter	HTTP(S)/ 8084	Bietet eine umfassende Übersicht über die Umgebung für die Durchführung von Prüfverfahren und die Erstellung von Berichten über die Regelkonformität. Eine Komponente des Dell Enterprise Server.	Berichterstellung
Remote Management Console	HTTP(S)/ 8443	Verwaltungskonsole und Befehlszentrale für die gesamte Unternehmensimplementierung. Eine Komponente des Dell Enterprise Server.	Alle
Core Server	HTTPS/ 8888 und 9000	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 rollenbasierten Zugriff. Eine Komponente des Dell Enterprise Server.	Alle

Name	Standardport	Beschreibung	Erforderlich für
Device Server	HTTPS/ 8443 HTTPS/ 8081 (mit Back-End-Device Server von Dell	Unterstützt die Aktivierung und Wiederherstellung von Kennwörtern. Eine Komponente des Dell Enterprise Server.	Dell Data Protection I Enterprise Edition für Mac Dell Data Protection I Enterprise Edition für Windows CREDActivate
Security Server	HTTPS/ 8443	Kommuniziert mit Policy Proxy; verwaltet das Abrufen forensischer Schlüssel, Client-Aktivierungen, Cloud Edition-Produkte, SED-PBA-Kommunikation und Active Directory für die Authentifizierung oder Abstimmung, einschließlich der Identitätsvalidierung für die Authentifizierung in der Remote Management-Konsole. Erfordert Zugriff auf die SQL-Datenbank. Eine Komponente des Dell Enterprise Server.	Alle
Compatibility Server	TCP/ 1099	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	TCP/ 61616 und STOMP/ 61613	Handhabt die Kommunikation zwischen Diensten des Dell Enterprise Server. Stellt durch den Compatibility Server für Policy-Proxy-Warteschlangen erzeugte Richtlinieninformationen bereit. Erfordert Zugriff auf die SQL-Datenbank. Eine Komponente des Dell Enterprise Server.	Alle

Name	Standardport	Beschreibung	Erforderlich für
Identity Server	HTTPS/ 8445	Handhabt Domänen-Authentifizierungsanfragen, einschließlich der Authentifizierung des SED Manager. 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
Key Server	TCP/ 8050	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
Dell Policy Proxy	TCP/ 8000	Stellt einen netzwerkbasierten Kommunikationsweg bereit, über den Aktualisierungen der Sicherheitsrichtlinien und der Bestandsdaten übermittelt werden. Eine Komponente von Dell Enterprise Server.	Dell Data Protection | Enterprise Edition für Mac Dell Data Protection | Enterprise Edition für Windows Dell Data Protection | Mobile Edition

Name	Standardport	Beschreibung	Erforderlich für
LDAP	TCP/ 389/636 (lokaler Domänencontroller), 3268/3269 (globaler Katalog) TCP/ 135/ 49125+ (RPC)	Port 389 - Dieser Port wird zur Anforderung von Informationen vom lokalen Domänencontroller verwendet. LDAP-Anfragen, die an Port 389 gesandt wurden, können nur zur Suche nach Objekten innerhalb der Startdomäne des globalen Katalogs verwendet werden. Die anfordernde Anwendung kann jedoch alle Attribute für diese Objekte ermitteln. Eine Anfrage an Port 389 könnte beispielsweise zur Ermittlung des Departements eines Benutzers verwendet werden. Port 3268 - Dieser Port wird für Abfragen verwendet, die spezifisch für den globalen Katalog vorgesehen ist. LDAP-Anfragen, die an Port 3268 gesandt wurden, können zur Suche nach Objekten im ganzen Wald verwendet werden. Es können jedoch nur die Attribute zurückgegeben werden, die zur Replikation im globalen Katalog markiert sind. Das Departement eines Benutzers kann beispielsweise nicht unter Verwendung von Pport 3268 zurückgegeben werden, da dieses Attribut nicht in den globalen Katalog repliziert wurde.	Alle
Microsoft SQL-Datenbank	TCP/ 1433	Der Standardport für SQL Server ist 1433. Client-Ports wird ein zufälliger Wert zwischen 1024 und 5000 zugewiesen.	Alle
Client-Authentifizierung	HTTPS/ 8449	Ermöglicht Client-Servern die Authentifizierung bei Dell Enterprise Server.	Dell Data Protection I Server Encryption (SE)
E-Mail-Kommunikation	25	Ermöglicht die Benachrichtigung bei Ereignissen.	Optional
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.

DDP Enterprise Server - Virtual Edition

Diese Architektur ist für kleine bis mittelgroße Unternehmen mit 1 bis 3500 Endpunkten geeignet. Optional kann ein Front-End-Server zur Veröffentlichung von Richtlinien und/oder zur Aktivierung von Endpunkten übers Internet im DMZ platziert werden.

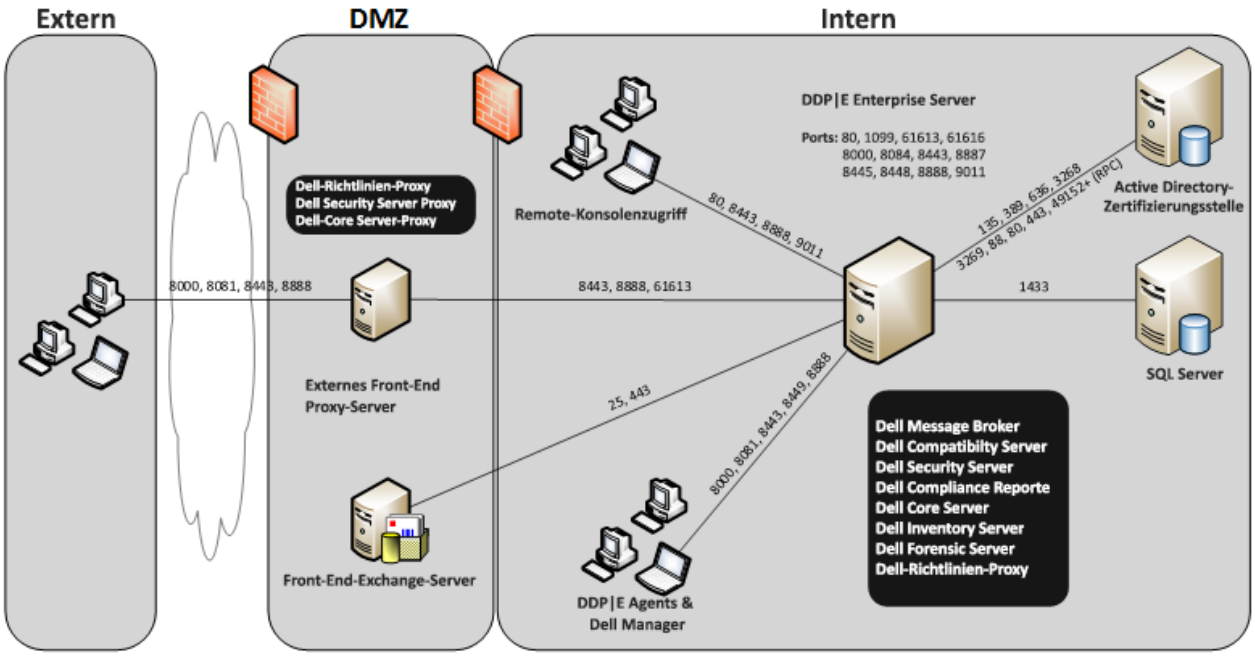
Hardwarespezifikationen

- DDP Enterprise Server - Virtual Edition (VE)
- VMWare Workstation 9, 10 oder 11, VMware ESXi 5.1, ESXi 5.5 oder ESXi 6.0
- 4 GB RAM bei VMWare Workstation 9, 10 oder 11; 8 GB RAM bei ESXi 5.1, 5.5 oder 6.0
- 80 GB freier Speicherplatz
- Mindestens 2-GHz-Prozessor, Dual Core oder größer

Ausführlichere Anforderungen finden Sie im *DDP Enterprise Server - Virtual Edition-Schnellstart- und Installationshandbuch*.

Externer Dell-Front-End-Server

- Windows Server 2008 R2 SP0-SP1 64-Bit/Windows Server 2008 SP2 64-Bit – Standard oder Enterprise Edition/Windows Server 2012 R2 – Standard Edition
- 2 GB dedizierter RAM mindestens/4 GB dedizierter RAM empfohlen
- 1,5 GB freier Speicherplatz (plus virtueller Auslagerungsspeicher)
- 2 GHz Core Duo-Prozessor oder besser



Virtual Edition-Ports

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

Name	Standardport	Beschreibung	Erforderlich für
Compliance Reporter	HTTP(S)/ 8084	Bietet eine umfassende Übersicht über die Umgebung für die Durchführung von Prüfverfahren und die Erstellung von Berichten über die Regelkonformität. Eine Komponente von DDP Enterprise Server - VE.	Berichterstellung
Remote Management Console		Verwaltungskonsole und Befehlszentrale für die gesamte Unternehmensimplementierung. Eine Komponente des DDP Enterprise Server - VE.	Alle
Core Server	HTTPS/ 8888	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 rollenbasierten Zugriff. Eine Komponente des DDP Enterprise Server - VE.	Alle
Core Server HA (High Availability - Hohe Verfügbarkeit)	HTTPS/ 8888	Ein High-Availability-Dienst, der eine höhere Sicherheit und Leistung von HTTPS-Verbindungen mit der Remote-Management-Konsole, Preboot-Authentifizierung, SED-Verwaltung, BitLocker Manager, Threat Protection und Advanced Threat Protection ermöglicht. Eine Komponente des DDP Enterprise Server - VE.	Alle
Dell Security Server	HTTPS/ 8443	Kommuniziert mit dem Policy Proxy; verwaltet Abrufungen von Forensic Keys, Aktivierungen von Clients, Cloud Edition Produkte und die SED-PBA-Kommunikation. Eine Komponente des DDP Enterprise Server - VE.	Alle

Name	Standardport	Beschreibung	Erforderlich für
Compatibility Server	TCP/ 1099 (geschlossen)	Ein Dienst für die Verwaltung der Unternehmensarchitektur. Sammelt und speichert anfängliche Bestandslistendaten während der Aktivierung und Richtliniendaten während Migrationen. Verarbeitet Daten auf Grundlage von Benutzergruppen in diesem Dienst. Eine Komponente des DDP Enterprise Server - VE.	Alle
Message Broker-Service	TCP/ 61616 und STOMP/ 61613 (geschlossen, oder - sofern für DMZ konfiguriert - geöffnet)	Handhabt die Kommunikation zwischen Diensten von DDP Enterprise Server - VE. Stellt durch den Compatibility Server für Policy-Proxy-Warteschlangen erzeugte Richtlinieninformationen bereit. Eine Komponente des DDP Enterprise Server - VE.	Alle
Identity Server	8445	Handhabt Domänen-Authentifizierungsanfragen, einschließlich der Authentifizierung des SED Manager. Erfordert ein Active-Directory-Konto. Eine Komponente des DDP Enterprise Server - VE.	Alle
Forensics Server	HTTPS/ 8448	Ermöglicht es Administratoren mit entsprechenden Berechtigungen, Verschlüsselungsschlüssel von der Remote-Management-Konsole zur Verwendung beim Entsperren von Daten oder Entschlüsselungsaufgaben zu erhalten. Eine Komponente des DDP Enterprise Server - VE.	Forensic API
Inventory Server	8887	Verarbeitet die Bestandswarteschlange. Eine Komponente des DDP Enterprise Server - VE.	Alle
Policy Proxy	TCP/ 8000/8090	Stellt einen netzwerkbasierten Kommunikationsweg bereit, über den Aktualisierungen der Sicherheitsrichtlinien und der Bestandsdaten übermittelt werden. Eine Komponente des DDP Enterprise Server - VE.	Dell Data Protection I Enterprise Edition für Mac Dell Data Protection I Enterprise Edition für Windows Dell Data Protection I Mobile Edition

Name	Standardport	Beschreibung	Erforderlich für
LDAP	389/636, 3268/3269 RPC – 135, 49125+	Port 389 - Dieser Port wird zur Anforderung von Informationen vom lokalen Domänencontroller verwendet. LDAP-Anfragen, die an Port 389 gesandt wurden, können nur zur Suche nach Objekten innerhalb der Startdomäne des globalen Katalogs verwendet werden. Die anfordernde Anwendung kann jedoch alle Attribute für diese Objekte ermitteln. Eine Anfrage an Port 389 könnte beispielsweise zur Ermittlung des Departements eines Benutzers verwendet werden. Port 3268 – Dieser Port wird für Abfragen verwendet, die spezifisch für den globalen Katalog vorgesehen ist. LDAP-Anfragen, die an Port 3268 gesandt wurden, können zur Suche nach Objekten im ganzen Wald verwendet werden. Es können jedoch nur die Attribute zurückgegeben werden, die zur Replikation im globalen Katalog markiert sind. Das Departement eines Benutzers kann beispielsweise nicht unter Verwendung von Pport 3268 zurückgegeben werden, da dieses Attribut nicht in den globalen Katalog repliziert wurde.	Alle
Client-Authentifizierung	HTTPS/ 8449	Ermöglicht Client Servern die Authentifizierung gegenüber DDP Enterprise Server - VE.	Dell Data Protection I Server Encryption.
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.

6

Beispiel für E-Mail mit Kundenbenachrichtigung

Nach dem Kauf von Dell Data Protection erhalten Sie eine E-Mail von der E-Mail-Adresse DellDataProtectionEncryption@Dell.com. Unten finden Sie ein Beispiel für die E-Mail zu Dell Data Protection | Encryption. Diese E-Mail enthält auch Ihre CFT-Anmeldinformationen und den Lizenzschlüssel.

Dell Data Protection | Encryption

Dear [redacted]

Thank you for purchasing Dell Data Protection | Encryption to quickly and easily protect your critical business data.

The following is the information you need to download your software and installation instructions for Dell Order #

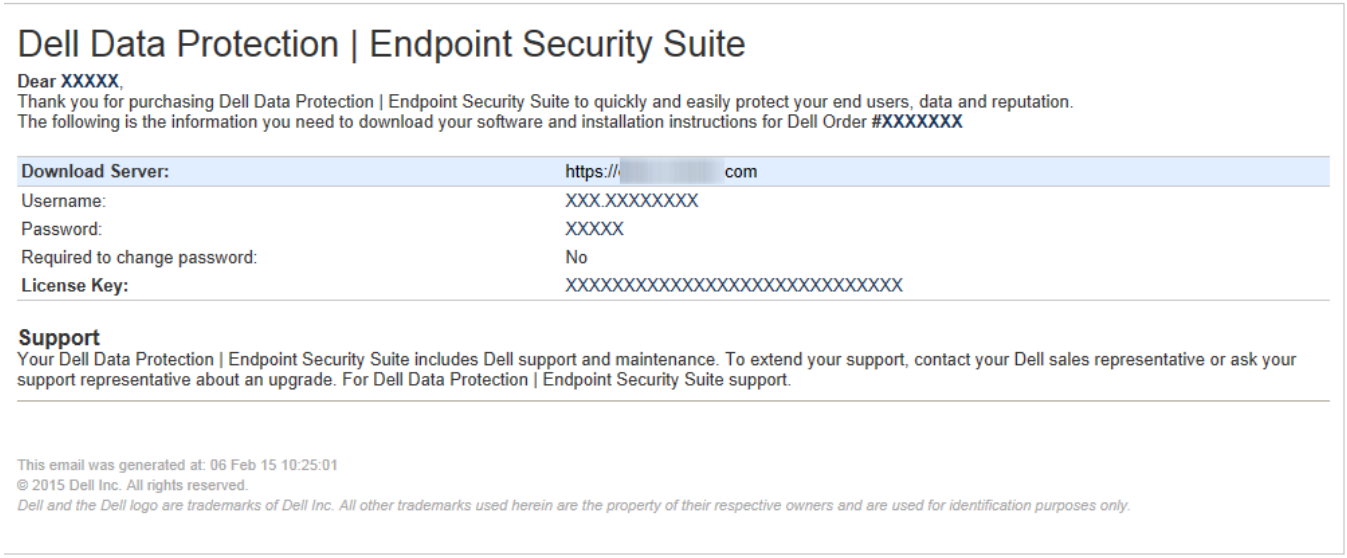
Download Server:	**https://ddpe.credant.com**
Username:	[redacted]
Password:	I1oFqlQe
Required to change password:	No
Account Expiration Date:	Never
License Key:	[redacted]

Support

Your **Dell Data Protection | Encryption Solution** is entitled to Dell service and maintenance. For extending your service, contact your Dell sales representative or ask your support representative about an upgrade. For **Dell Data Protection | Encryption Solution** support, call **1-877-459-7304**.

This email was generated at: 14 Feb 12 07:31:26

Unten finden Sie ein Beispiel für die E-Mail zur Dell Data Protection I Endpoint Security Suite



Dell Data Protection | Endpoint Security Suite

Dear XXXXX,
Thank you for purchasing Dell Data Protection | Endpoint Security Suite to quickly and easily protect your end users, data and reputation.
The following is the information you need to download your software and installation instructions for Dell Order **#XXXXXXX**

Download Server:	https:// com
Username:	XXX.XXXXXXXX
Password:	XXXXX
Required to change password:	No
License Key:	XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Support
Your Dell Data Protection | Endpoint Security Suite includes Dell support and maintenance. To extend your support, contact your Dell sales representative or ask your support representative about an upgrade. For Dell Data Protection | Endpoint Security Suite support.

This email was generated at: 06 Feb 15 10:25:01


0 XXXXXA0 X