Erste Schritte

Dell Data Security Implementation Services

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.

Erste Schritte

2019 - 06

Rev. A01

Inhaltsverzeichnis

1

Implementierungsphasen

Der grundlegende Implementierungsvorgang besteht aus den folgenden Phasen:

- Führen Sie Kick-off und Übersicht der Anforderungen aus
- Schließen Sie die Checkliste zur Vorbereitung - Erste Implementierung oder Checkliste zur Vorbereitung - Upgrade/Migration ab
- Führen Sie eine Installation oder Aktualisierung/Migration von ***einem*** der folgenden Produkte durch:
  - ***Security Management Server***
    - Zentralisierte Verwaltung von Geräten
    - Eine Windows-basierte Anwendung, die in einer physischen oder virtualisierten Umgebung ausgeführt wird.
  - ***Security Management Server Virtual***
    - Zentrale Verwaltung von bis zu 3,500 Geräten
    - Wird in einer virtualisierten Umgebung ausgeführt

    Anweisungen zur Dell Server-Installation/Migration finden Sie im *Installations- und Migrationshandbuch für Security Management Server* oder im *Schnellstart- und Installationshandbuch für Security Management Server Virtual.* Zum Abrufen dieser Dokumente sehen Sie die Dell Data Security Server-Dokumente.
- Konfiguration der ersten Richtlinie
  - ***Security Management Server*** – siehe *Installations- und Migrationshandbuch für Security Management Server*, *Verwaltungsaufgaben*, verfügbar über support.dell.com sowie *AdminHelp*, verfügbar über die Verwaltungskonsole
  - ***Security Management Server Virtual*** – siehe *Schnellstart- und Installationshandbuch für Security Management Server Virtual*, *Verwaltungsaufgaben für die Verwaltungskonsole*, verfügbar unter support.dell.com sowie *AdminHelp*, verfügbar über die Verwaltungskonsole
- Client-Verpackung

  Um Dokumente zu Client-Anforderungen und zur Installation der Software zu erhalten, wählen Sie die jeweiligen Dokumente für Ihre Bereitstellung aus:
  - *Einfaches Installationshandbuch für Encryption Enterprise* oder *Erweitertes Installationshandbuch für Encryption Enterprise*
  - *Einfaches Installationshandbuch für Endpoint Security Suite Enterprise* oder *Erweitertes Installationshandbuch für Endpoint Security Suite Enterprise*
  - *Administratorhandbuch für Advanced Threat Prevention*
  - *Installationshandbuch für Encryption Personal*
  - *Administratorhandbuch für Encryption Enterprise for Mac*
  - *Administratorhandbuch für Endpoint Security Suite Enterprise for Mac*
  - *Dell Data Guardian Administratorhandbuch*
  - *Dell Data Guardian Benutzerhandbuch*

    Zum Abrufen dieser Dokumente sehen Sie die Dell Data Security Client-Dokumente.
- Teilnahme an der grundlegenden Wissensübertragung von Dell Security Administrator
- Implementierung bewährter Verfahren
- Koordinierung des Support für Pilotprojekte oder Bereitstellung mit Dell Clientservices

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 Security 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 Benutzer lokale Administratorrechte?
6. Welche Daten und Geräte müssen Sie verwalten und verschlüsseln (lokale Festplatten, USB, usw.)?
7. Welche Produkte möchten Sie implementieren?
   - Encryption Enterprise
     - Encryption (DE-Berechtigung) – Windows Encryption, Server Encryption, Encryption External Media, SED Management, FDE, BitLocker Manager und Mac Encryption.
     - Encryption External Media
   - Endpoint Security Suite Enterprise
     - Advanced Threat Prevention – mit oder ohne optionale Client-Firewall und Web-Schutz (ATP-Berechtigung)
     - Encryption (DE-Berechtigung) – Windows Encryption, Server Encryption, Encryption External Media, SED Management, FDE, BitLocker Manager und Mac Encryption.
     - Encryption External Media
   - Dell Data Guardian (CE-Berechtigung)
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 Betriebssystemversionen sollen verschlüsselt werden?
13. Haben Sie alternative Startpartitionen auf Ihren Endpunkten konfiguriert?
    a. Wiederherstellungspartition des Herstellers
    b. Doppelstart-Workstations

Clientdokumente

Installationsanforderungen, unterstützte Betriebssystemversionen, unterstützte selbstverschlüsselnde Festplatten und Anweisungen für die Clients, die Sie bereitstellen möchten, finden Sie in den unten aufgeführten Dokumenten.

Encryption Enterprise (Windows) – Lesen Sie die folgenden Dokumente unter: www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

- *Erweitertes Installationshandbuch* Encryption Enterprise – Installationshandbuch mit erweiterten Schaltern und Parametern für benutzerdefinierte Installationen.
- *Konsolen-Benutzerhandbuch für Dell Data Security* – Anweisungen für Benutzer.

Encryption Enterprise (Mac) – Lesen Sie das *Administratorhandbuch für Encryption Enterprise for Mac* unter www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. Enthält Installations- und Bereitstellungsanweisungen.

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

- *Erweitertes Installationshandbuch Endpoint Security Suite Enterprise* – Installationshandbuch mit erweiterten Schaltern und Parametern für benutzerdefinierte Installationen.
- *Endpoint Security Suite Enterprise Advanced Threat Prevention Quick Start Guide* (Schnellstarthandbuch) – Anleitung für die Verwaltung, einschließlich Richtlinienempfehlungen, Identifizierung und Management von Bedrohungen und Fehlerbehebung.
- *Konsolen-Benutzerhandbuch für Dell Data Security* – Anweisungen für Benutzer.

Endpoint Security Suite Enterprise (Mac) – Lesen Sie das Dokument unter: www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- *Endpoint Security Suite Enterprise for Mac – Administratorhandbuch* – Installationshandbuch

Dell Data Guardian – Lesen Sie die Dokumente unter: www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/manuals

- *Administratorhandbuch für Dell Data Guardian* – Installation, Aktivierung und Betriebshinweise.
- *Dell Data Guardian Benutzerhandbuch* – Installation, Aktivierung und Betriebshinweise für Benutzer.

Informationen zu unterstützten selbstverschlüsselnden Festplatten finden Sie unter https://www.dell.com/support/article/us/en/04/sln296720.

Server-Dokumente

Informationen zu Installationsanforderungen, unterstützten Betriebssystemversionen und Konfigurationen für den bereitzustellenden Dell Server finden Sie in den entsprechenden unten aufgeführten Dokumenten.

Security Management Server

- Lesen Sie das *Installations- und Migrationshandbuch für Security Management Server*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/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

  oder

  www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/manuals

Security Management Server Virtual

- Siehe *Schnellstart- und Installationshandbuch für Security Management Server Virtual 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/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

  oder

  www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/manuals

3

Checkliste für die Vorbereitung - Erste Implementierung

Je nach dem von Ihnen installierten Dell Server verwenden Sie eine der folgenden Checklisten, um sicherzustellen, dass alle Voraussetzungen erfüllt werden, bevor Sie mit der Installation von Dell Encryption, Endpoint Security Suite Enterprise oder Data Guardian beginnen.

- Checkliste für Security Management Server
- Checkliste für Security Management Server Virtual

Checkliste für Security Management Server, erste Implementierung

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). Weitere Anweisungen zur Deinstallation finden Sie unter https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us.
- ☐ Alle während dem Proof of Concept-Testen verwendeten Produktionsendpunkte wurden entschlüsselt oder Schlüsselbündel heruntergeladen. Weitere Informationen zu den Clients, die Sie bereitstellen möchten, finden Sie unter Clientdokumente.

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

Erfüllen Server die erforderlichen Hardware-Spezifikationen?

- ☐ Siehe Dell Security Management Server Architektur-Design.

Erfüllen Server die erforderlichen Software-Spezifikationen?

- ☐ Windows Server 2012 R2 (Standard oder Datacenter), 2016 (Standard oder Datacenter) oder Windows Server 2019 (Standard oder Datacenter) ist installiert. Diese Betriebssysteme können auf physischer oder virtueller Hardware installiert werden.
- ☐ Windows Installer 4.0 oder höher ist installiert.
- ☐ .NET Framework 4.5 ist installiert.
- ☐ Bei der Verwendung von QL Server 2012 bzw. SQL Server 2016 ist Microsoft SQL Native Client 2012 installiert Falls verfügbar, kann der SQL Native Client 2014 eingesetzt werden.

  ANMERKUNG: SQL Express wird bei einer Produktionsbereitstellung von Security Management Server nicht unterstützt.

- ☐ Die Windows-Firewall ist deaktiviert oder so konfiguriert, dass sie folgende (eingehende) Ports zulässt: 8000, 8050, 8081, 8084, 8888, 61613.
- ☐ Die Konnektivität ist zwischen Security Management Server und Active Directory (AD) über die Ports 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (eingehend zu AD) verfügbar.
- ☐ Die Benutzerkontensteuerung wird deaktiviert, bevor Windows Server 2012 R2 unter C:\Programme installiert wird. Der Server muss neu gestartet werden, damit diese Änderung in Kraft tritt. (siehe Windows-Systemsteuerung > Benutzerkonten).
  - Windows Server 2012 R2 – das Installationsprogramm deaktiviert UAC.
  - Windows Server 2016 R2 – das Installationsprogramm deaktiviert UAC.

  ANMERKUNG: Die Deaktivierung von UAC wird nicht mehr erzwungen, außer es wird ein geschütztes Verzeichnis als Installationsverzeichnis angegeben.

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 Security Management 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 Security-Client-Software und für Security Management Server befinden sich im Ordner **Treiber und 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/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research

  oder

  www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research

  Auf der Produktseite http://www.dell.com/support

  1. Wählen Sie **Treiber und Downloads** aus.
  2. Wählen Sie in der Betriebssystem-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.
  3. Wählen Sie unter der jeweiligen Software-Überschrift **Datei herunterladen** aus.
- ☐ Wenn Sie Encryption oder Endpoint Security Suite Enterprise „on-the-box“ erworben haben, kann die Software über Dell Digital Delivery an den Zielrechner verteilt werden.

ODER

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

- ☐ Die Software befindet sich unter https://ddpe.credant.com im Ordner **SoftwareDownloads**.

Sind Installationsschlüssel und Lizenzdatei verfügbar?

- ☐ Der Lizenzschlüssel ist in der ursprünglichen E-Mail mit den FTP-Anmeldeinformationen enthalten – siehe Beispiel einer E-Mail zur Benachrichtigung von Kunden. Dieser Schlüssel ist ebenfalls im Download der Anwendung von http://www.dell.com/support und https://ddpe.credant.com enthalten.
- ☐ Die Lizenzdatei ist eine XML-Datei auf der FTP-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 Data Guardian-, Encryption-, Enterprise- oder Endpoint Security Suite Enterprise-Clients automatisch von Dell heruntergeladen.

Wurde die Datenbank erstellt?

- ☐ (Optional) Eine neue Datenbank wird auf einem unterstützten Server erstellt – siehe Anforderungen und Architektur im *Installations- und Migrationshandbuch für Security Management Server*. Das Installationsprogramm von Security Management 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 Security Management 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:
  - Security Management Server: dds.<domain.com>
  - Front-End-Server: dds-fe.<domain.com>

ANMERKUNG:
Split-DNS-ermöglicht die Verwendung des gleichen DNS-Namen intern und extern. Das bedeutet, dass wir intern dds.<domain.com> als internen c-Namen bereitstellen und diesen an den Dell Security Management Server (Back-end) verweisen können, während wir extern einen a-Record für dds.<domain.com> bereitstellen und die entsprechenden Ports (siehe Ports für Security Management Server) an den Front-End-Server weiterleiten. Wir könnten DNS Round-Robin oder einen Lastenausgleich verwenden, um die Last auf die verschiedenen Front-ends zu verteilen (falls mehrere vorhanden sind).

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 Zertifizierungsstelle verwenden, informieren Sie den Techniker für Clientservices 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 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 Enterprise oder Data Guardian 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** Produktionsrechner verwenden. Produktionsrechner sollten während eines Produktionspilotprojekts verwendet werden, nachdem Verschlüsselungsrichtlinien definiert und mit dem von Dell bereitgestellten Testplan getestet wurden.

Checkliste für Security Management Server Virtual, erste Implementierung

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). Weitere Anweisungen zur Deinstallation finden Sie unter https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us

- ☐ Alle während dem Proof of Concept-Testen verwendeten Produktionsendpunkte wurden entschlüsselt oder Schlüsselbündel heruntergeladen. Weitere Informationen zu den Clients, die Sie bereitstellen möchten, finden Sie unter Clientdokumente.

ANMERKUNG:
Alle neuen Implementierungen müssen mit einer neuen Datenbank und Neuinstallation der Encryption, Endpoint Security Suite Enterprise oder Data Guardian Software beginnen. Die Dell Client Services führen keine neue Implementierung mithilfe einer POC-Umgebung aus. Während eines POC 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 Security-Client-Software und für Security Management Server befinden sich im Ordner **Treiber und 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/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research

  oder

  www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research

  Auf der Produktseite http://www.dell.com/support

  1. Wählen Sie **Treiber und Downloads** aus.
  2. Wählen Sie in der Betriebssystem-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.

3 Wählen Sie unter der jeweiligen Software-Überschrift **Datei herunterladen** aus.

- ☐ Wenn Sie Encryption oder Endpoint Security Suite Enterprise „on-the-box“ erworben haben, kann die Software über Dell Digital Delivery an den Zielrechner verteilt werden.

Ist (sind) die Lizenzdatei(en) verfügbar?

- ☐ Die Lizenzdatei ist eine XML-Datei auf der Website ddpe.credant.com 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- oder Endpoint Security Suite Enterprise-Clients automatisch von Dell heruntergeladen.

Erfüllen Server die erforderlichen Hardware-Spezifikationen?

- ☐ Siehe Security Management Server Virtual Architektur-Design.

Wurde das DNS-Alias für Security Management Server Virtual 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:
  - Security Management Server: dds.<domain.com>
  - Front-End-Server: dds-fe.<domain.com>

ANMERKUNG:
Split-DNS-ermöglicht die Verwendung des gleichen DNS-Namen intern und extern. Das bedeutet, dass wir intern dds.<domain.com> als internen c-Namen bereitstellen und diesen an den Dell Security Management Server (Back-end) verweisen können, während wir extern einen a-Record für dds.<domain.com> bereitstellen und die entsprechenden Ports (siehe Ports für Security Management Server Virtual) an den Front-End-Server weiterleiten. Wir könnten DNS Round-Robin oder einen Lastenausgleich verwenden, um die Last auf die verschiedenen Front-ends zu verteilen (falls mehrere vorhanden sind).

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 Enterprise oder Data Guardian 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** Produktionsrechner verwenden. Produktionsrechner sollten während eines

Produktionspilotprojekts verwendet werden, nachdem Verschlüsselungsrichtlinien definiert und mit dem von Dell bereitgestellten Testplan getestet wurden.

Checkliste zur Vorbereitung - Upgrade/Migration

Die folgende Checkliste gilt nur für Security Management Server.

ANMERKUNG:
Aktualisierung von Security Management Server Virtual über das Menü Grundkonfiguration in Ihrem Dell Server Terminal. Weitere Informationen finden Sie im Schnellstart- und Installationshandbuch für *Security Management Server Virtual*.

Verwenden Sie die folgende Checkliste um sicherzustellen, dass alle Voraussetzungen erfüllt werden, bevor Sie mit der Aktualisierung für Encryption, Endpoint Security Suite Enterpriseoder Data Guardian beginnen.

Erfüllen Server die erforderlichen Software-Spezifikationen?

- ☐ Windows Server 2012 R2 (Standard oder Datacenter), Windows Server 2016 (Standard oder Datacenter) oder Windows Server 2019 (Standard oder Datacenter) ist installiert. Alternativ kann eine virtualisierte Umgebung installiert werden.
- ☐ Windows Installer 4.0 oder höher ist installiert.
- ☐ .NET Framework 4.5 ist installiert.
- ☐ Bei der Verwendung von QL Server 2012 bzw. SQL Server 2016 ist Microsoft SQL Native Client 2012 installiert Falls verfügbar, kann der SQL Native Client 2014 eingesetzt werden.

  ANMERKUNG: SQL Express wird bei Security Management Server nicht unterstützt.
- ☐ Die Windows-Firewall ist deaktiviert oder so konfiguriert, dass sie folgende (eingehende) Ports zulässt: 8000, 8050, 8081, 8084, 8443, 8888, 61613.
- ☐ Die Konnektivität ist zwischen Security Management Server und Active Directory (AD) über die Ports 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (eingehend zu AD) verfügbar.
- ☐ Die Benutzerkontensteuerung wird deaktiviert, bevor Windows Server 2012 R2 unter C:\Programme installiert wird. Der Server muss neu gestartet werden, damit diese Änderung in Kraft tritt. (siehe Windows-Systemsteuerung > Benutzerkonten).
  - Windows Server 2012 R2 – das Installationsprogramm deaktiviert UAC.
  - Windows Server 2016 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 Security Management 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.

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 einer E-Mail zur Benachrichtigung von Kunden. Dieser Schlüssel ist ebenfalls im Download der Anwendung von http://www.dell.com/support und https://ddpe.credant.com enthalten.
- ☐ 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- oder Endpoint Security Suite Enterprise-Clients automatisch von Dell heruntergeladen.

Wurde neue und vorhandene Dell Data Security-Software heruntergeladen?

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

- ☐ Die Software befindet sich unter https://ddpe.credant.com im Ordner **SoftwareDownloads**.
- ☐ Wenn Sie Data Guardian, Encryption Enterprise oder Endpoint Security Suite Enterprise „on-the-box“ (OTB) erworben haben, wird die Software optional über Dell Digital Delivery bereitgestellt. Alternativ kann die Software unter www.dell.com/support bzw. ddpe.credant.com heruntergeladen 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 zuständigen Dell Vertriebsmitarbeiter, bevor Sie ein Upgrade oder eine Migration ausführen. Dell Data Security führt die Lizenzprüfung durch und die Aktivierungen werden verhindert, wenn keine Lizenzen vorhanden sind.

- ☐ Ich habe genug Lizenzen für meine ganze Umgebung.

Sind DNS-Datensätze dokumentiert?

- ☐ Überprüfen Sie, ob DNS-Datensätze dokumentiert und zur Aktualisierung bereitgestellt sind, wenn die Hardware geändert wurde.

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 Zertifizierungsstelle verwenden, informieren Sie den

Techniker für Clientservices 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 Enterprise oder Data Guardian 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** Produktionsrechner verwenden. Produktionsrechner sollten während eines Produktionspilotprojekts 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 Security-Implementierung erläutert. Wählen Sie den Dell Server aus, den Sie bereitstellen möchten:

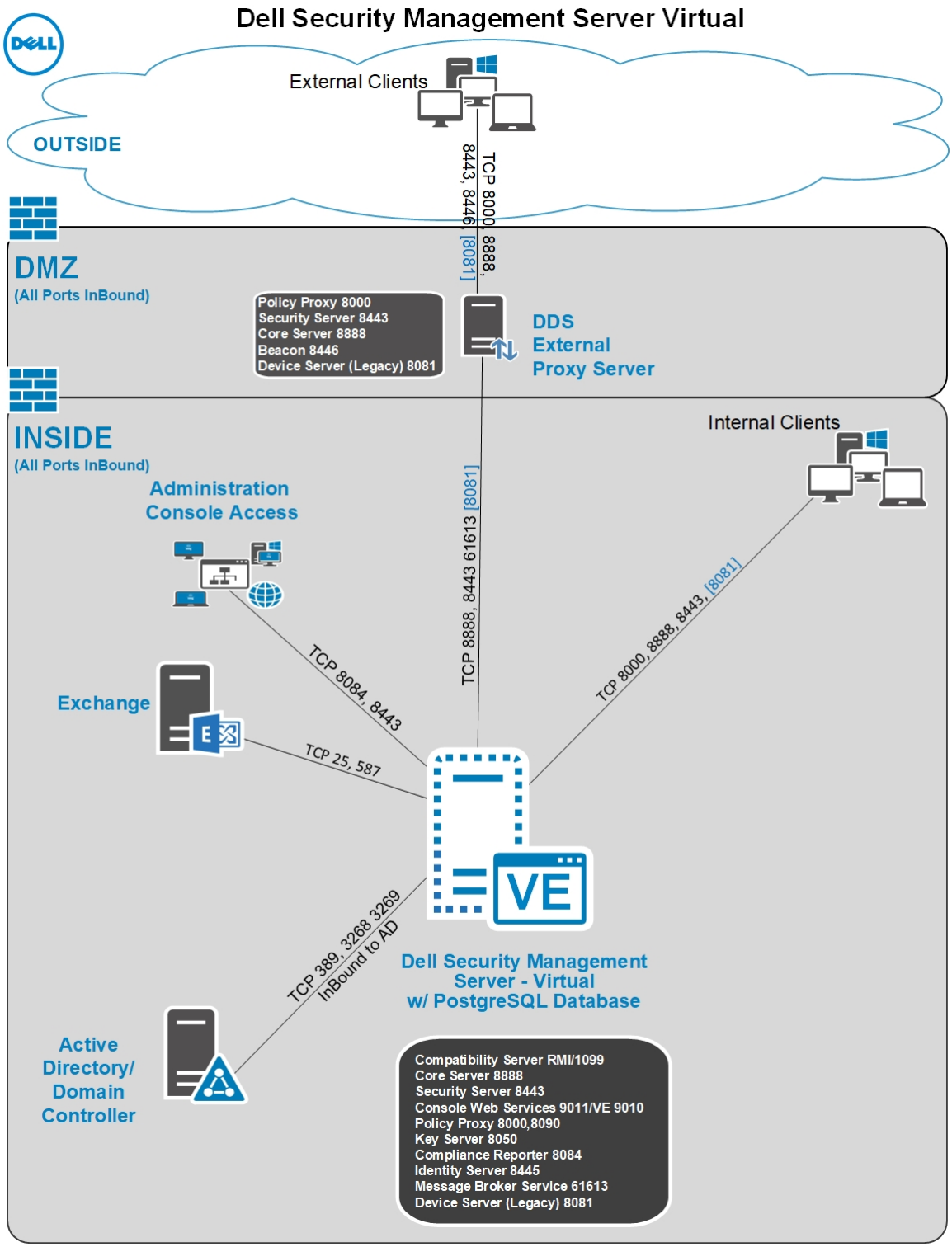
- Architektur-Design von Security Management Server
- Architektur-Design von Security Management Server Virtual

Architektur-Design von Security Management Server Virtual

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

Architekturkomponenten

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



Ports

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

Name	Standardport	Beschreibung
Compliance Reporter	HTTP(S)/ 8084	Bietet eine umfassende Übersicht über die Umgebung für die Durchführung von Prüfverfahren und die Erstellung von Berichten über die Regelkonformität.
Management Console	HTTPS/ 8443	Verwaltungskonsole und Befehlszentrale für die gesamte Unternehmensimplementierung.
Core Server	HTTPS/ 8887 (geschlossen)	Verwaltet den Richtlinienablauf, Lizenzen und die Registrierung für die Preboot-Authentifizierung, SED-Verwaltung, BitLocker Manager, Threat Protection und Advanced Threat Prevention. Verarbeitet Bestandslistendaten zur Verwendung durch den Compliance Reporter und die Verwaltungskonsole. Sammelt und speichert Authentifizierungsdaten Steuert den rollenbasierten Zugriff.
Core Server HA (Hohe Verfügbarkeit)	HTTPS/ 8888	Ein High-Availability-Dienst, der eine höhere Sicherheit und Leistung von HTTPS-Verbindungen mit der Verwaltungskonsole, Preboot-Authentifizierung, SED-Verwaltung, FDE, BitLocker Manager, Threat Protection und Advanced Threat Prevention ermöglicht.
Security Server	HTTPS/ 8443	Kommuniziert mit dem Policy Proxy; verwaltet Abrufungen von Forensic Keys, Aktivierungen von Clients, Data Guardian Produkte und die SED-PBA-Kommunikation.
Compatibility Server	TCP/ 1099 (geschlossen)	Ein Dienst für die Verwaltung der Unternehmensarchitektur. Sammelt und speichert anfängliche Bestandslistendaten während der Aktivierung und Richtliniendaten während Migrationen. Verarbeitet Daten auf Grundlage von Benutzergruppen.
Message Broker-Service	TCP/ 61616 (geschlossen) und STOMP/ 61613 (geschlossen, oder - sofern für DMZ konfiguriert - geöffnet)	Handhabt die Kommunikation zwischen Diensten von Dell Server. Stellt durch den Compatibility Server für Policy-Proxy-Warteschlangen erzeugte Richtlinieninformationen bereit.
Identity Server	8445 (geschlossen)	Handhabt Domänen-Authentifizierungsanfragen, einschließlich der Authentifizierung für SED Management.
Forensics Server	HTTPS/ 8448	Ermöglicht es Administratoren mit entsprechenden Berechtigungen, Verschlüsselungsschlüssel von der Verwaltungskonsole zur Verwendung beim Entsperren von Daten oder Entschlüsselungsaufgaben zu erhalten. Erforderlich für forensische API.
Inventory Server	8887	Verarbeitet die Bestandswarteschlange.
Policy Proxy	TCP/ 8000	Stellt einen netzwerkbasierten Kommunikationsweg bereit, über den Aktualisierungen der Sicherheitsrichtlinien und der Bestandsdaten übermittelt werden.

Name	Standardport	Beschreibung
		Erforderlich für Encryption Enterprise (Windows und Mac)
LDAP	389/636, 3268/3269 RPC – 135, 49125+	Port 389 - Dieser Port wird für die Anforderung von Informationen aus dem lokalen Domänencontroller verwendet. LDAP-Anfragen, die an Port 389 gesandt wurden, können nur zur Suche nach Objekten innerhalb der Startdomäne des globalen Katalogs verwendet werden. Die anfordernde Anwendung kann jedoch alle Attribute für diese Objekte ermitteln. Eine Anfrage an Port 389 könnte beispielsweise zur Ermittlung des Departements eines Benutzers verwendet werden. Port 3268 – Dieser Port wird für Abfragen verwendet, die spezifisch für den globalen Katalog vorgesehen ist. LDAP-Anfragen, die an Port 3268 gesandt wurden, können zur Suche nach Objekten im ganzen Wald verwendet werden. Es können jedoch nur die Attribute zurückgegeben werden, die zur Replikation im globalen Katalog markiert sind. Das Departement eines Benutzers kann beispielsweise nicht unter Verwendung von Pport 3268 zurückgegeben werden, da dieses Attribut nicht in den globalen Katalog repliziert wurde.
Client-Authentifizierung	HTTPS/ 8449	Ermöglicht Client-Servern die Authentifizierung bei Dell Server. Erforderlich für Server Encryption
Callback-Signal	HTTP/TCP 8446	Bei einem Front-End-Server kann in jede geschützte Office-Datei ein Rückrufsignal eingefügt werden, wenn Data Guardian im geschützten Office-Modus ausgeführt wird.

Architektur-Design von Security Management Server

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

Architekturkomponenten

Nachstehend finden Sie empfohlene Hardware-Konfigurationen, die sich für die meisten Umgebungen eignen.

Security Management Server

- Betriebssystem: Microsoft Windows Server 2012 R2 (Standard, Datacenter 64-Bit), Windows Server 2016 (Standard, Datacenter 64-Bit), Windows Server 2019 (Standard und Datacenter)
- Virtuelle/physische Maschine
- CPU: 4 Kern(e)
- RAM: 16,00 GB
- Laufwerk C: 30 GB freier Festplattenspeicher für Protokolle und Anwendungsdatenbanken

ANMERKUNG: Bis zu 10 GB können für eine lokale Ereignisdatenbank mit PostgreSQL verbraucht werden.

Proxy-Server

- Betriebssystem: Microsoft Windows Server 2012 R2 (Standard, Datacenter 64-Bit), Windows Server 2016 (Standard, Datacenter 64-Bit), Windows Server 2019 (Standard und Datacenter)
- Virtuelle/physische Maschine
- CPU: 2 Kern(e)
- RAM: 8,00 GB

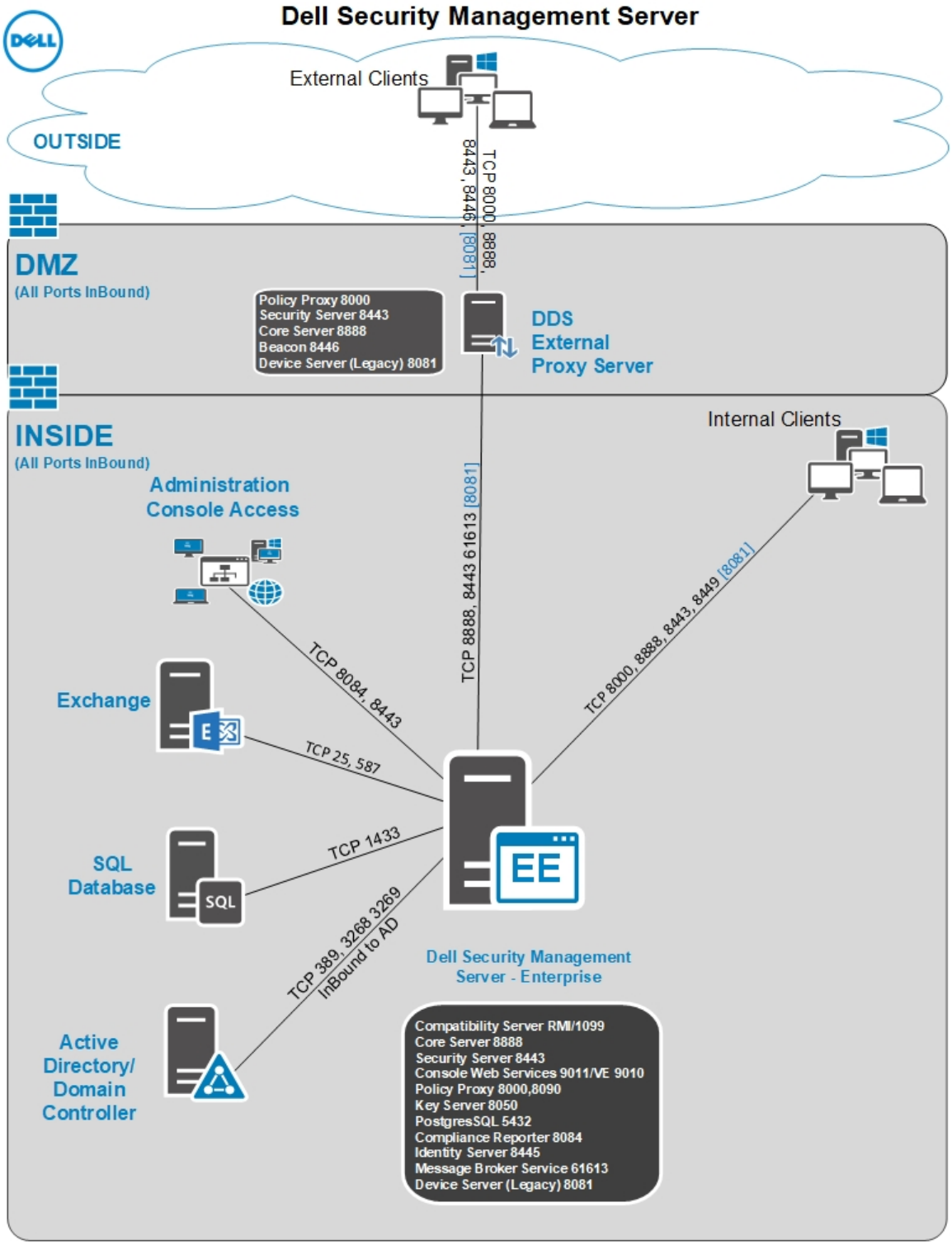
- Laufwerk C: 20 GB freier Festplattenspeicher für Protokolle

SQL Server - Hardwarespezifikationen

- CPU: 4 Kern(e)
- RAM: 24,00 GB
- Datenlaufwerk: 100 bis 150 GB verfügbaren Speicherplatz (dies kann variieren je nach Umgebung)
- Protokolllaufwerk: 50 GB freier Speicherplatz (dies kann variieren je nach Umgebung)

> **ANMERKUNG: Dell empfiehlt, dass Sie die SQL Server Best Practices befolgen, obwohl die oben genannten Informationen den Großteil von Umgebungen abdecken sollten.**

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



ANMERKUNG: Falls die Organisation mehr als 20.000 Endpunkte hat, bitten Sie den ProSupport von Dell um Hilfe.

Ports

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

Name	Standardport	Beschreibung
Compliance Reporter	HTTP(S)/ 8084	Bietet eine umfassende Übersicht über die Umgebung für die Durchführung von Prüfverfahren und die Erstellung von Berichten über die Regelkonformität.
Management Console	HTTP(S)/ 8443	Verwaltungskonsole und Befehlszentrale für die gesamte Unternehmensimplementierung.
Core Server	HTTPS/ 8888	Verwaltet den Richtlinienablauf, Lizenzen und die Registrierung für die Preboot-Authentifizierung, SED-Verwaltung, BitLocker Manager, Threat Protection und Advanced Threat Prevention. Verarbeitet Bestandslistendaten zur Verwendung durch den Compliance Reporter und die Verwaltungskonsole. Sammelt und speichert Authentifizierungsdaten Steuert den rollenbasierten Zugriff.
Device Server	HTTPS/ 8081	Unterstützt die Aktivierung und Wiederherstellung von Kennwörtern. Eine Komponente von Security Management Server. Erforderlich für Encryption Enterprise (Windows und Mac)
Security Server	HTTPS/ 8443	Kommuniziert mit Policy Proxy; verwaltet das Abrufen forensischer Schlüssel, Client-Aktivierungen, Data Guardian, 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.
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.
Message Broker-Service	TCP/ 61616 und STOMP/ 61613	Handhabt die Kommunikation zwischen Diensten von Dell Server. Stellt durch den Compatibility Server für Policy-Proxy-Warteschlangen erzeugte Richtlinieninformationen bereit. Erfordert Zugriff auf die SQL-Datenbank.
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.
Policy Proxy	TCP/ 8000	Stellt einen netzwerkbasierten Kommunikationsweg bereit, über den Aktualisierungen der Sicherheitsrichtlinien und der Bestandsdaten übermittelt werden.
LDAP	TCP/ 389/636 (lokaler Domänencontroller), 3268/3269 (globaler Katalog)	Port 389 - Dieser Port wird für die Anforderung von Informationen aus dem lokalen Domänencontroller verwendet. LDAP-Anfragen, die an Port 389 gesandt wurden, können nur zur Suche nach Objekten innerhalb der Startdomäne des globalen Katalogs verwendet werden. Die anfordernde Anwendung kann jedoch alle Attribute für diese

Name	Standardport	Beschreibung
	TCP/ 135/ 49125+ (RPC)	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.
Microsoft SQL-Datenbank	TCP/ 1433	Der Standardport für SQL Server ist 1433. Client-Ports wird ein zufälliger Wert zwischen 1024 und 5000 zugewiesen.
Client-Authentifizierung	HTTPS/ 8449	Ermöglicht Client-Servern die Authentifizierung bei Dell Server. Erforderlich für Server Encryption.
Callback-Signal	HTTP/TCP 8446	In jede geschützte Office-Datei kann ein Rückrufsignal eingefügt werden, wenn Data Guardian Office im gesicherten Modus ausgeführt wird.

Bewährte Verfahren für SQL Server

Die folgende Liste erklärt die bewährten Verfahren für SQL Server, die implementiert werden sollten, wenn Dell Security 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 Extents (Grundeinheit von SQL-Speicher) entspricht 64 KB.

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

   - 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 *Server Memory Server Configuration Options* (Serverspeicher, Serverkonfigurationsoptionen).

   - 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)
   - Microsoft SQL Server 2017 – 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 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
   - Microsoft SQL Server 2017 – https://msdn.microsoft.com/en-us/library/ms188396.aspx

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

Beispiel für E-Mail mit Kundenbenachrichtigung

Nach dem Kauf von Dell Data Security erhalten Sie eine E-Mail von der E-Mail-Adresse DellDataSecurity@Dell.com. Unten finden Sie ein Beispiel für die E-Mail. Diese E-Mail enthält auch Ihre CFT-Anmeldeinformationen und den Lizenzschlüssel.

Dell Data Security

Thank you for purchasing Dell Encryption Enterprise - Order %USER.CUSTOM2%

Dell Encryption offers a comprehensive data-centric encryption solution that secures data wherever it goes while enabling IT end-users to do more. Listed below are helpful links and information about the support services that are available to you.

Get your Software

Download your software and its accompanying documentation.

Download Now

Username:	%USER.LOGIN%
Password:	%USER.PASSWORD%
Required to change password:	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
License Key:	xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx

Explore our top knowledge base solutions for Dell Encryption Enterprise.

ProSupport for Software

- Online Support: www.dell.com/datasecuritysupport
- 1.877.459.7304, Option 1, X4310039 - U.S. & Canada Only
- Outside the U.S., click here for a list of numbers

Need Support? CHAT NOW! Click Here

You will need your software service tag to open a Support ticket. This is a seven digit alphanumeric code located above or also can be found on your asset.

Other Products and Services

- Explore our Products
- Subscribe to our Newsletter
- Search our Knowledge Base
- Deployment and Training Services - please contact your sales representative for options