Guida introduttiva

Servizi di implementazione di Dell Data Security

Messaggi di N.B., Attenzione e Avvertenza

N.B.: un messaggio N.B. (Nota Bene) indica informazioni importanti che contribuiscono a migliorare l'utilizzo del prodotto.

ATTENZIONE: Un messaggio di ATTENZIONE indica un danno potenziale all'hardware o la perdita di dati, e spiega come evitare il problema.

AVVERTENZA: Un messaggio di AVVERTENZA indica un rischio di danni materiali, lesioni personali o morte.

Guida introduttiva

2019 - 06

Rev. A01

Sommario

1

Fasi di implementazione

Il processo di implementazione di base comprende le seguenti fasi:

- Eseguire Analisi dei requisiti e della preparazione
- Completare Elenco di controllo di preparazione - Implementazione iniziale o Elenco di controllo di preparazione - Aggiornamento/Migrazione
- Installare o eseguire l'aggiornamento/migrazione di ***uno*** dei seguenti:
  - ***Security Management Server***
    - Gestione centralizzata dei dispositivi
    - Un'applicazione basata su Windows eseguita in un ambiente fisico o virtualizzato.
  - ***Security Management Server Virtual***
    - Gestione centralizzata di un massimo di 3500 dispositivi
    - Eseguibile in un ambiente virtualizzato

    Per ulteriori informazioni sull'installazione/migrazione del Dell Server, consultare la *Security Management Server Installation and Migration Guide* (Guida all'installazione e alla migrazione di Security Management Server) o la *Security Management Server Virtual Quick Start and Installation Guide* (Guida introduttiva e all'installazione di Security Management Server Virtual). Per ottenere questi documenti, fare riferimento a Documenti relativi a Dell Data Protection Server.
- Configurazione dei criteri iniziali
  - ***Security Management Server***: consultare la *Security Management Server Installation and Migration Guide, Administrative Tasks* (Guida alla migrazione e all'installazione di Security Management Server, attività amministrative), disponibile all'indirizzo support.dell.com e *AdminHelp* (Guida dell'amministratore), disponibile nella Management Console
  - ***Security Management Server Virtual***: consultare la *Security Management Server Virtual Quick Start and Installation Guide, Management Console Administrative Tasks* (Guida introduttiva rapida e all'installazione di Security Management Server Virtual, attività amministrative della Management Console) disponibile all'indirizzo support.dell.com e *AdminHelp* (Guida dell'amministratore), disponibile nella Management Console
- Imballaggio del client

  Per i documenti sui requisiti dei client e sull'installazione del software, selezionare i documenti appropriati in base alla distribuzione:
  - Guida all'installazione di base di *Encryption Enterprise* o *Guida all'installazione avanzata di Encryption Enterprise*
  - Guida all'installazione di base di Endpoint Security Suite Enterprise o Guida all'installazione avanzata di Endpoint Security Suite Enterprise
  - *Guida dell'amministratore di Advanced Threat Prevention*
  - *Guida all'installazione di Encryption Personal*
  - *Guida dell'amministratore di Encryption Enterprise per Mac*
  - *Guida dell'amministratore di Endpoint Security Suite Enterprise per Mac*
  - *Guida dell'amministratore di Dell Data Guardian*
  - *Guida dell'utente di Dell Data Guardian*

    Per ottenere questi documenti, fare riferimento a Documenti relativi ai client Dell Data Security.
- Partecipazione al trasferimento delle informazioni di base dell'amministratore di Dell Security Administrator
- Implementazione delle procedure consigliate
- Coordinamento del supporto relativo a progetti pilota o distribuzione con Dell Client Services

Analisi dei requisiti e della preparazione

Prima dell'installazione, è importante conoscere il proprio ambiente e gli obiettivi aziendali e tecnici del progetto al fine di completare correttamente l'implementazione di Dell Data Security e raggiungere gli scopi preposti. Accertarsi di conoscere a fondo i requisiti di protezione globale dei dati richiesti dall'azienda.

Di seguito sono riportate alcune delle domande più frequenti che possono aiutare il team Dell Client Services a comprendere l'ambiente e i relativi requisiti:

1. Qual è il tipo di azienda (sanitaria, ecc.)?
2. Quali sono i requisiti di conformità a cui l'azienda deve attenersi (HIPAA/HITECH, PCI, ecc.)?
3. Qual è la dimensione dell'azienda (numero di utenti, numero di sedi fisiche, ecc.)?
4. Qual è il numero di endpoint previsto per la distribuzione? Esistono previsioni di ampliamento di tali numeri nel futuro?
5. Gli utenti dispongono di privilegi di amministratore locale?
6. Quali sono i dati e i dispositivi che l'azienda prevede di gestire e crittografare (dischi fissi locali, USB, ecc.)?
7. Quali prodotti l'utente intende distribuire?
   - Encryption Enterprise
     - Encryption (diritto a DE) - Crittografia Windows, Server Encryption, Encryption External Media, SED Management, FDE, BitLocker Manager e Crittografia Mac.
     - Encryption External Media
   - Endpoint Security Suite Enterprise
     - Advanced Threat Prevention - Con o senza Firewall client e Protezione Web (diritto ad ATP)
     - Encryption (diritto a DE) - Crittografia Windows, Server Encryption, Encryption External Media, SED Management, FDE, BitLocker Manager e Crittografia Mac.
     - Encryption External Media
   - Dell Data Guardian (diritto a CE)
8. Quale tipo di connettività utente è supportata dall'azienda? Le tipologie possono includere quanto segue:
   - Solo connettività LAN locale
   - Utenti wireless aziendali e/o tramite VPN
   - Utenti remoti/disconnessi (gli utenti non connessi alla rete direttamente o tramite VPN per periodi di tempo prolungati)
   - Workstation non di dominio
9. Quali dati è necessario proteggere nell'endpoint? Quali sono i tipi di dati di cui gli utenti tipici dispongono nell'endpoint?
10. Quali applicazioni utente potrebbero contenere informazioni riservate? Quali sono i tipi di file delle applicazioni?
11. Quanti domini sono presenti nell'ambiente? Quanti sono destinati alla crittografia?
12. Quali sistemi operativi o versioni degli stessi sono destinati alla crittografia?
13. Si dispone di partizioni di avvio alternative configurate negli endpoint?
    a. Partizione di ripristino del produttore
    b. Workstation ad avvio doppio

Documenti sui client

Per i requisiti di installazione, le versioni del sistema operativo supportate, le unità autocrittografanti supportate e le istruzioni per i client da implementare, consultare i documenti applicabili, elencati di seguito.

Encryption Enterprise (Windows) - Consultare i documenti all'indirizzo: www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

- *Guida all'installazione avanzata di Encryption Enterprise* - Guida all'installazione con opzioni e parametri avanzati per installazioni personalizzate.
- *Guida per l'utente di* Dell Data Security - Istruzioni per gli utenti.

Encryption Enterprise (Mac) - Consultare la *Encryption Enterprise or Mac Administrator Guide* (Guida dell'amministatore di Encryption Enterprise per Mac) Il'indirizzowww.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. Include le istruzioni sull'installazione e sulla distribuzione.

Endpoint Security Suite Enterprise (Windows) - Consultare i documenti all'indirizzo: www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- *Guida all'installazione avanzata di Endpoint Security Suite Enterprise* - Guida all'installazione con opzioni e parametri avanzati per installazioni personalizzate.
- *Endpoint Security Suite Enterprise Advanced Threat Prevention*: istruzioni per l'amministrazione, incluse raccomandazioni sui criteri, identificazione e gestione delle minacce e risoluzione dei problemi.
- Guida per l'utente di *Dell Data Security Console* - Istruzioni per gli utenti.

Endpoint Security Suite Enterprise (Mac) - Consultare il documento all'indirizzo: www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- Guida dell'amministratore di *Endpoint Security Suite Enterprise per Mac* - Guida all'installazione

Dell Data Guardian - Consultare i documenti all'indirizzo www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/manuals

- Guida dell'amministratore di *Dell Data Guardian* - Istruzioni di installazione, attivazione e uso.
- *Guida dell'utente di Dell Data Guardian* - Istruzioni di installazione, attivazione e uso per gli utenti.

Per informazioni sulle unità autocrittografanti supportate, vedere https://www.dell.com/support/article/us/en/04/sln296720.

Documenti del server

Per i requisiti di installazione, le versioni dei sistemi operativi supportati e le configurazioni del Dell Server che si intende distribuire, fare riferimento al relativo documento elencato qui di seguito.

Security Management Server

- Consultare la *Guida alla migrazione e all'installazione di Security Management Server* all'indirizzo

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

  oppure

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

  Oppure

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

Security Management Server Virtual

- Consultare la Guida introduttiva rapida e all'installazione di *Security Management Server Virtual* all'indirizzo

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

  oppure

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

Oppure

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

3

Elenco di controllo di preparazione - Implementazione iniziale

In base al Dell Server distribuito, utilizzare l'elenco di controllo appropriato per accertarsi di aver soddisfatto tutti i prerequisiti prima di installare Dell Encryption, Data Guardian o Endpoint Security Suite Enterprise.

- Elenco di controllo di Security Management Server
- Elenco di controllo di Security Management Server Virtual

Elenco di controllo di implementazione iniziale per Security Management Server

La pulizia dell'ambiente per il Proof of Concept è stata eseguita (ove applicabile)?

- ☐ L'applicazione e il database Proof of Concept sono stati salvati e disinstallati (se si utilizza lo stesso server) prima dell'intervento di installazione di Dell. Per ulteriori istruzioni su una disinstallazione, vedere 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.
- ☐ Gli endpoint di produzione utilizzati durante il test Proof of Concept sono stati decrittografati oppure sono stati scaricati i pacchetti di chiavi. Per ulteriori informazioni sui client che si intende implementare, vedere Documenti sui client.

N.B.:
Tutte le nuove implementazioni devono essere avviate con un nuovo database e una nuova installazione del software Encryption, Endpoint Security Suite Enterprise o Data Guardian. Dell Client Services non effettuerà una nuova implementazione usando un ambiente PoC. Gli endpoint crittografati durante un POC dovranno essere decrittografati o ricostruiti prima dell'intervento di installazione di Dell.

I server soddisfano le specifiche hardware richieste?

- ☐ Consultare Dell Security Management Server Architecture Design.

I server soddisfano le specifiche software richieste?

- ☐ È installato Windows Server 2012 R2 (Standard o Datacenter), 2016 (Standard o Datacenter) o Windows Server 2019 (Standard o Datacenter). Questi sistemi operativi possono essere installati su hardware fisici o virtuali.
- ☐ È installato Windows Installer 4.0 o versione successiva.
- ☐ .NET Framework 4.5 è installato.
- ☐ È installato Microsoft SQL Native Client 2012 se si utilizza SQL Server 2012 o SQL Server 2016. È possibile utilizzare SQL Native Client 2014, se disponibile.

  N.B.: Un'implementazione di produzione di Security Management Server non supporta SQL Express.

- ☐ Windows Firewall è disabilitato o configurato per consentire il funzionamento delle porte 8000, 8050, 8081, 8084, 8888, 61613 (in ingresso).
- ☐ È disponibile la connettività tra Security Management Server e Active Directory (AD) sulle porte 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (in ingresso verso AD).
- ☐ Il controllo dell'account utente viene disattivato prima dell'installazione su Windows Server 2012 R2, quando l'installazione viene eseguita in C:\Program Files. ed è necessario riavviare il server per rendere effettiva tale modifica. Consultare Pannello di controllo Windows > Account utente.
  - Windows Server 2012 R2 - Il programma di installazione disabilita il controllo dell'account utente.
  - Windows Server 2016 R2 - Il programma di installazione disabilita il controllo dell'account utente.

  N.B.: UAC (Upgrade Authentication Code) non viene più disattivato forzatamente a meno che non venga specificata una directory protetta per l'installazione.

Gli account di servizio sono stati creati?

- ☐ Account di servizio con accesso in sola lettura ad AD (LDAP) - L'account utente base/utente dominio è sufficiente.
- ☐ L'account di servizio deve disporre dei diritti di amministratore locale per i server dell'applicazione Security Management Server.
- ☐ Per usare l'Autenticazione di Windows per il database, impostare un account dei servizi di dominio con diritti di amministratore di sistema. L'account utente deve essere nel formato DOMINIO\Nomeutente ed essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza a ruoli del database per: dbo_owner, public.
- ☐ Per usare l'autenticazione SQL, l'account SQL usato deve avere diritti di amministratore di sistema nell'SQL Server. L'account utente deve essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza al ruolo del database: dbo_owner, public.

Il software è stato scaricato?

Scaricarlo dal sito Web del supporto Dell.

- ☐ I download del software client di Dell Data Security e di Dell Security Management Server si trovano nella cartella **Driver e download** all'indirizzo

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research

  Oppure

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

  Oppure

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

  Dalla pagina del prodotto all'indirizzo http://www.dell.com/support

  1. Selezionare **Driver e download**.
  2. Dall'elenco dei sistemi operativi, selezionare il sistema operativo appropriato per il prodotto che si sta scaricando. Per esempio, per scaricare Dell Enterprise Server, selezionare **una delle opzioni di server Windows.**
  3. Nel riquadro del software applicabile, selezionare **Scarica file**.
- ☐ Se Encryption o Endpoint Security Suite Enterprise sono stati acquistati on-the-box, il software può essere fornito al computer di destinazione tramite Dell Digital Delivery.

OPPURE

Scaricarlo dal sito di trasferimento file (CFT) Dell Data Security

- Il software si trova all'indirizzo https://ddpe.credant.com nella cartella **SoftwareDownloads**.

I file della chiave di installazione e della licenza sono disponibili?

- Il codice di licenza è incluso nel messaggio di posta elettronica originale, insieme alle credenziali FTP. Consultare Esempio di notifica al cliente tramite posta elettronica. Questo codice è incluso anche nel download dell'applicazione dall'indirizzo http://www.dell.com/support e https://ddpe.credant.com.
- Il file della licenza è un file XML situato nel sito FTP, nella cartella **Licenze client**.

N.B.:
Se le licenze acquistate sono on-the-box, non sono necessari file di licenza. I diritti vengono scaricati automaticamente dal sito Dell in seguito all'attivazione dei nuovi client Data Guardian, Encryption, Enterprise o Endpoint Security Suite Enterprise.

Il database è stato creato?

- Viene creato un nuovo database in un server supportato (facoltativo). Consultare Requisiti e architettura nella *Guida alla migrazione e all'installazione di Security Management Server*. Se non ne è già stato creato uno, il programma di installazione di Security Management Server crea un database nel corso dell'installazione.
- All'utente del database di destinazione sono stati assegnati i diritti **db_owner**.

È stato creato l'alias DNS per Security Management Server e/o i Policy Proxy con split DNS per il traffico interno ed esterno?

Ai fini della scalabilità, si consiglia di creare gli alias DNS. Questo consente di aggiungere ulteriori server in un secondo momento o componenti separati dell'applicazione senza dover eseguire l'aggiornamento del client.

- Se lo si desidera, vengono creati gli alias DNS. Alias DNS consigliati:
  - Security Management Server: dds.<domain.com>
  - Server front-end: dds-fe.<domain.com>

N.B.:
Lo split DNS consente all'utente di usare lo stesso nome DNS internamente ed esternamente. Ciò significa che è possibile fornire internamente dds.<domain.com> come nome c interno e indirizzarlo a Dell Security Management Server (back-end), fornire esternamente un record a per dds.<domain.com> e inoltrare le relative porte (vedere Porte per Security Management Server) al server front-end. È possibile utilizzare il round robin DNS o un sistema di bilanciamento del carico per distribuire il carico sui diversi front-end (se ne esiste più di uno).

Si prevede l'utilizzo dei certificati SSL?

- Si dispone di un'autorità di certificazione (CA, Certificate Authority) interna che può essere utilizzata per firmare i certificati ed è attendibile per tutte le workstation dell'ambiente **<2><3>oppure</3></2>** si prevede l'acquisto di un certificato firmato tramite un'autorità di certificazione pubblica, come VeriSign o Entrust. Se si utilizza un'autorità di certificazione pubblica, informare il tecnico di Dell Client Services. Il certificato contiene la catena di attendibilità completa (radice e intermedia) con firme con chiave privata e pubbliche.
- I Nomi soggetto alternativi (SAN, Subject Alternate Name) nella Richiesta certificato corrispondono a tutti gli alias DNS assegnati ad ogni server usato per l'installazione di Dell Server. Non si applica a richieste di certificati Wildcard o autofirmati.
- Il certificato viene generato in un formato .pfx.

I requisiti di controllo delle modifiche sono stati identificati e comunicati a Dell?

- ☐ Inviare tutti i requisiti di controllo delle modifiche specifici per l'installazione di Encryption, Endpoint Security Suite Enterprise o Data Guardian a Dell Client Services prima di richiedere l'intervento per l'installazione. Tali requisiti possono includere modifiche ai server dell'applicazione, al database e alle workstation del client.

È stato preparato l'hardware per la verifica?

- ☐ Preparare almeno tre computer con l'immagine del computer aziendale da utilizzare per la verifica. Dell **sconsiglia** l'uso di computer di produzione per la verifica. I computer di produzione devono essere utilizzati durante un progetto pilota di produzione, dopo la definizione e la verifica dei criteri di crittografia eseguite tramite il piano di verifica fornito da Dell.

Elenco di controllo di implementazione iniziale per Security Management Server Virtual

La pulizia dell'ambiente per il Proof of Concept è stata eseguita (ove applicabile)?

- ☐ L'applicazione e il database Proof of Concept sono stati salvati e disinstallati (se si utilizza lo stesso server) prima dell'intervento di installazione di Dell. Per ulteriori istruzioni su una disinstallazione, vedere 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

- ☐ Gli endpoint di produzione utilizzati durante il test Proof of Concept sono stati decrittografati oppure sono stati scaricati i pacchetti di chiavi. Per ulteriori informazioni sui client che si intende implementare, vedere Documenti sui client.

N.B.:
Tutte le nuove implementazioni devono essere avviate con un nuovo database e una nuova installazione del software Encryption, Endpoint Security Suite Enterprise o Data Guardian. Dell Client Services non effettuerà una nuova implementazione usando un ambiente PoC. Gli endpoint crittografati durante un POC dovranno essere decrittografati o ricostruiti prima dell'intervento di installazione di Dell.

Gli account di servizio sono stati creati?

- ☐ Account di servizio con accesso in sola lettura ad AD (LDAP) - L'account utente base/utente dominio è sufficiente.

Il software è stato scaricato?

- ☐ I download del software client di Dell Data Security e di Dell Security Management Server si trovano nella cartella **Driver e download** all'indirizzo

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research

  Oppure

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

  Oppure

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

  Dalla pagina del prodotto all'indirizzo http://www.dell.com/support

  1. Selezionare **Driver e download**.
  2. Dall'elenco dei sistemi operativi, selezionare il sistema operativo appropriato per il prodotto che si sta scaricando. Per esempio, per scaricare Dell Enterprise Server, selezionare **una delle opzioni di server Windows.**

3 Nel riquadro del software applicabile, selezionare **Scarica file**.

- Se Encryption o Endpoint Security Suite Enterprise sono stati acquistati on-the-box, il software può essere fornito al computer di destinazione tramite Dell Digital Delivery.

I file della licenza sono disponibili?

- Il file della licenza è un file XML situato nel sito ddpe.credant.com nella cartella **Licenze client**.

N.B.:
Se le licenze acquistate sono on-the-box, non sono necessari file di licenza. I diritti vengono scaricati automaticamente dal sito Dell in seguito all'attivazione dei nuovi client Encryption o Endpoint Security Suite Enterprise.

I server soddisfano le specifiche hardware richieste?

- Vedere Progettazione dell'architettura di Security Management Server Virtual.

È stato creato l'alias DNS per Security Management Server Virtual e/o i Policy Proxy con split DNS per il traffico interno ed esterno?

Ai fini della scalabilità, si consiglia di creare gli alias DNS. Questo consente di aggiungere ulteriori server in un secondo momento o componenti separati dell'applicazione senza dover eseguire l'aggiornamento del client.

- Se lo si desidera, vengono creati gli alias DNS. Alias DNS consigliati:
  - Security Management Server: dds.<domain.com>
  - Server front-end: dds-fe.<domain.com>

N.B.:
Lo split DNS consente all'utente di usare lo stesso nome DNS internamente ed esternamente. Ciò significa che è possibile fornire internamente dds.<domain.com> come nome c interno e indirizzarlo a Dell Security Management Server (back-end), fornire esternamente un record a per dds.<domain.com> e inoltrare le relative porte (vedere Porte per Security Management Server Virtual) al server front-end. È possibile utilizzare il round robin DNS o un sistema di bilanciamento del carico per distribuire il carico sui diversi front-end (se ne esiste più di uno).

Si prevede l'utilizzo dei certificati SSL?

- Si dispone di un'autorità di certificazione (CA, Certificate Authority) interna che può essere utilizzata per firmare i certificati ed è attendibile per tutte le workstation dell'ambiente **<2><3>oppure</3></2>** si prevede l'acquisto di un certificato firmato tramite un'autorità di certificazione pubblica, come VeriSign o Entrust. Se si utilizza un'autorità di certificazione pubblica, informare il tecnico di Dell Client Services.

I requisiti di controllo delle modifiche sono stati identificati e comunicati a Dell?

- Inviare tutti i requisiti di controllo delle modifiche specifici per l'installazione di Encryption, Endpoint Security Suite Enterprise o Data Guardian a Dell Client Services prima di richiedere l'intervento per l'installazione. Tali requisiti possono includere modifiche ai server dell'applicazione, al database e alle workstation del client.

È stato preparato l'hardware per la verifica?

- Preparare almeno tre computer con l'immagine del computer aziendale da utilizzare per la verifica. Dell **sconsiglia** l'uso di computer di produzione per la verifica. I computer di produzione devono essere utilizzati durante un progetto pilota di produzione, dopo la definizione e la verifica dei criteri di crittografia eseguite tramite il piano di verifica fornito da Dell.

4

Elenco di controllo di preparazione - Aggiornamento/Migrazione

Questo elenco di controllo è valido solo per Security Management Server.

N.B.:
Aggiornamento di Security Management Server Virtual dal menu di configurazione di base nel terminale del Dell Server. Per maggiori informazioni, consultare la *Guida introduttiva rapida e all'installazione di Security Management Server Virtual.*

Utilizzare il seguente elenco di controllo per verificare di aver soddisfatto tutti i prerequisiti prima di avviare l'aggiornamento di Encryption, Endpoint Security Suite Enterprise o Data Guardian.

I server soddisfano le specifiche software richieste?

- ☐ È installato Windows Server 2012 R2 (Standard o Datacenter), Windows Server 2016 (Standard o Datacenter) o Windows Server 2019 (Standard o Datacenter). In alternativa, può essere installato un ambiente virtualizzato.
- ☐ È installato Windows Installer 4.0 o versione successiva.
- ☐ .NET Framework 4.5 è installato.
- ☐ È installato Microsoft SQL Native Client 2012 se si utilizza SQL Server 2012 o SQL Server 2016. È possibile utilizzare SQL Native Client 2014, se disponibile.

  N.B.: Security Management Server non supporta SQL Express.
- ☐ Windows Firewall è disabilitato o configurato per consentire il funzionamento delle porte 8000, 8050, 8081, 8084, 8443, 8888, 61613 (in ingresso).
- ☐ È disponibile la connettività tra Security Management Server e Active Directory (AD) sulle porte 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (in ingresso verso AD).
- ☐ Il controllo dell'account utente viene disattivato prima dell'installazione su Windows Server 2012 R2, quando l'installazione viene eseguita in C:\Program Files. ed è necessario riavviare il server per rendere effettiva tale modifica. Consultare Pannello di controllo Windows > Account utente.
  - Windows Server 2012 R2 - Il programma di installazione disabilita il controllo dell'account utente.
  - Windows Server 2016 R2 - Il programma di installazione disabilita il controllo dell'account utente.

Gli account di servizio sono stati creati?

- ☐ Account di servizio con accesso in sola lettura ad AD (LDAP) - L'account utente base/utente dominio è sufficiente.
- ☐ L'account di servizio deve disporre dei diritti di amministratore locale per i server dell'applicazione Security Management Server.
- ☐ Per usare l'Autenticazione di Windows per il database, impostare un account dei servizi di dominio con diritti di amministratore di sistema. L'account utente deve essere nel formato DOMINIO\Nomeutente ed essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza a ruoli del database per: dbo_owner, public.

- ☐ Per usare l'autenticazione SQL, l'account SQL usato deve avere diritti di amministratore di sistema nell'SQL Server. L'account utente deve essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza al ruolo del database: dbo_owner, public.

È stato eseguito il backup del database e di tutti i file necessari?

- ☐ È stato eseguito il backup dell'installazione esistente completa in un percorso alternativo. Il backup deve includere database SQL, secretKeyStore e file di configurazione.
- ☐ Verificare che sia stato eseguito il backup dei seguenti file più importanti, che contengono le informazioni necessarie per connettersi al database:

  <cartella di installazione>\Enterprise Edition\Compatibility Server\conf\server_config.xml

  <cartella di installazione>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

  <cartella di installazione>\Enterprise Edition\Compatibility Server\conf\gkresource.xml

I file della chiave di installazione e della licenza sono disponibili?

- ☐ Il codice di licenza è incluso nel messaggio di posta elettronica originale, insieme alle credenziali CFT. Consultare Esempio di notifica al cliente tramite posta elettronica. Questo codice è incluso anche nel download dell'applicazione dall'indirizzo http://www.dell.com/support e https://ddpe.credant.com.
- ☐ Il file della licenza è un file XML situato nel sito CFT, nella cartella **Licenze client**.

N.B.:
Se le licenze acquistate sono on-the-box, non sono necessari file di licenza. I diritti vengono scaricati automaticamente dal sito Dell in seguito all'attivazione dei nuovi client Encryption o Endpoint Security Suite Enterprise.

Il software nuovo ed esistente di Dell Data Security è stato scaricato?

Scaricarlo dal sito di trasferimento file (CFT) Dell Data Security.

- ☐ Il software si trova all'indirizzo https://ddpe.credant.com nella cartella **SoftwareDownloads**.
- ☐ Se Data Guardian, Encryption Enterprise o Endpoint Security Suite Enterprise sono stati acquistati on-the-box (OTB), il software viene facoltativamente fornito tramite Dell Digital Delivery. In alternativa, il software può essere scaricato dal sito all'indirizzo www.dell.com/support o ddpe.credant.com, rispettivamente.

Si dispone di un numero sufficiente di licenze endpoint?

Prima di procedere all'aggiornamento, accertarsi di disporre di un numero sufficiente di licenze client per coprire tutti gli endpoint dell'ambiente. Se le installazioni superano il numero di licenze, contattare il rappresentate locale Dell prima di eseguire l'aggiornamento o la migrazione. Dell Data Security esegue la convalida delle licenze e, se queste non sono disponibili, le attivazioni non vengono eseguite.

- ☐ Dispongo di un numero di licenze sufficiente a coprire l'ambiente.

I record DNS sono documentati?

- ☐ Confermare che i record DNS sono documentati e organizzati per l'aggiornamento se l'hardware è stato modificato.

Si prevede l'utilizzo dei certificati SSL?

- ☐ Si dispone di un'autorità di certificazione (CA, Certificate Authority) interna che può essere utilizzata per firmare i certificati ed è attendibile per tutte le workstation dell'ambiente **<2><3>oppure</3></2>** si prevede l'acquisto di un certificato firmato tramite un'autorità di certificazione pubblica, come VeriSign o Entrust. Se si utilizza un'autorità di certificazione pubblica, informare il tecnico di Dell Client Services. Il certificato contiene la catena di attendibilità completa (radice e intermedia) con firme con chiave privata e pubbliche.

- ☐ I Nomi soggetto alternativi (SAN, Subject Alternate Name) nella Richiesta certificato corrispondono a tutti gli alias DNS assegnati ad ogni server usato per l'installazione di Dell Enterprise Server. Non si applica a richieste di certificati Wildcard o autofirmati.

- ☐ Il certificato viene generato in un formato .pfx.

I requisiti di controllo delle modifiche sono stati identificati e comunicati a Dell?

- ☐ Inviare tutti i requisiti di controllo delle modifiche specifici per l'installazione di Encryption, Endpoint Security Suite Enterprise o Data Guardian a Dell Client Services prima di richiedere l'intervento per l'installazione. Tali requisiti possono includere modifiche ai server dell'applicazione, al database e alle workstation del client.

È stato preparato l'hardware per la verifica?

- ☐ Preparare almeno tre computer con l'immagine del computer aziendale da utilizzare per la verifica. Dell **sconsiglia** l'uso di computer di produzione per la verifica. I computer di produzione devono essere utilizzati durante un progetto pilota di produzione, dopo la definizione e la verifica dei criteri di crittografia eseguite tramite il piano di verifica fornito da Dell.

5

Architettura

Questa sezione descrive in dettaglio i suggerimenti sulla progettazione dell'architettura per l'implementazione di Dell Data Security. Selezionare il Dell Server che verrà distribuito:

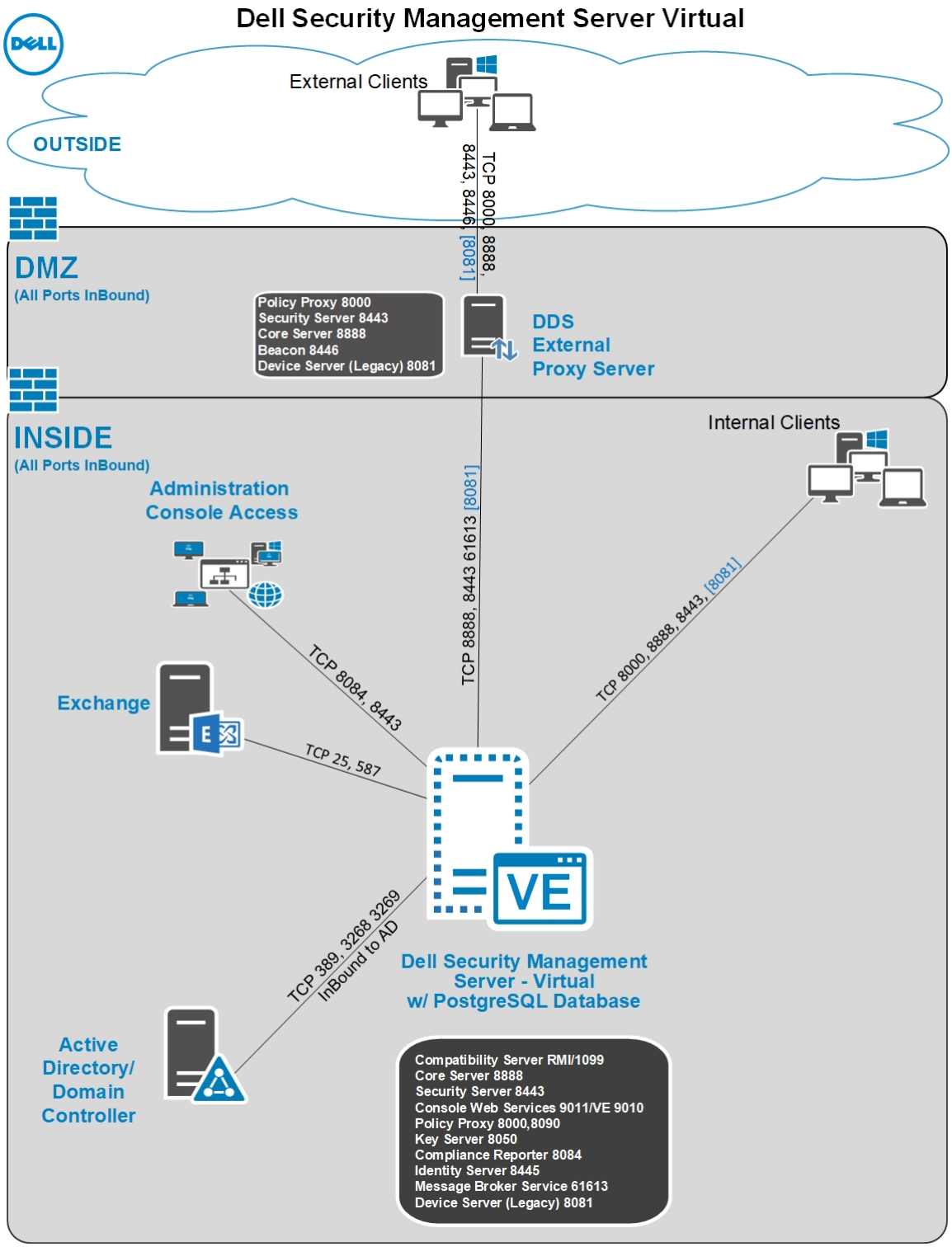
- Progettazione dell'architettura di Security Management Server
- Progettazione dell'architettura di Security Management Server Virtual

Progettazione dell'architettura di Security Management Server Virtual

Il Dell Encryption, Endpoint Security Suite Enterprise, e Data Guardian soluzioni sono altamente scalabili prodotti, in base al numero di terminazioni previsto per la crittografia all'interno dell'organizzazione.

Componenti dell'architettura

Di seguito viene fornito un distribuzione di base per la gestione della sicurezza Dell server virtuali.



Porte

La tabella seguente descrive ciascun componente e la relativa funzione.

Nome	Porta predefinita	Descrizione
Compliance Reporter	HTTP(S)/ 8084	Fornisce una visualizzazione completa dell'ambiente per la creazione di rapporti di controllo e conformità.
Console di gestione	HTTPS/ 8443	Console di amministrazione e centro di controllo per la distribuzione a livello aziendale.
Core Server	HTTPS/ 8887 (chiuso)	Gestisce il flusso dei criteri, le licenze e la registrazione per l'autenticazione di preavvio, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Elabora i dati di inventario utilizzati da Compliance Reporter e dalla Management Console. Raccoglie e archivia i dati di autenticazione. Controlla l'accesso basato sui ruoli.
Core Server HA (elevata disponibilità)	HTTPS/ 8888	Servizio ad elevata disponibilità che consente una maggiore sicurezza e migliori prestazioni delle connessioni HTTPS con la Management Console, l'autenticazione di preavvio, SED Management, FDE, BitLocker Manager, Threat Protection e Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Comunica con Policy Proxy e gestisce i recuperi delle chiavi Forensic, le attivazioni dei client, i prodotti Data Guardian e la comunicazione SED-PBA.
Compatibility Server	TCP/ 1099 (chiusa)	Servizio per la gestione dell'architettura aziendale. Raccoglie e archivia i dati di inventario iniziali durante l'attivazione e i dati dei criteri durante le migrazioni. Elabora i dati basati sui gruppi di utenti.
Message Broker Service	TCP/ 61616 (chiuso) e STOMP/ 61613 (chiusa o, se configurata per DMZ, 61613 è aperta)	Gestisce la comunicazione tra i servizi di Dell Server. Organizza le informazioni sui criteri create dal Compatibility Server per l'accodamento del Policy Proxy.
Identity Server	8445 (chiuso)	Gestisce le richieste di autenticazione del dominio, inclusa l'autenticazione per la gestione SED.
Forensic Server	HTTPS/ 8448	Consente agli amministratori che dispongono dei privilegi appropriati di ottenere dalla Management Console le chiavi di crittografia, da usare per sbloccare i dati o per le attività di decrittografia. Richiesto per le API Forensic.
Inventory Server	8887	Elabora la coda di inventario.
Policy Proxy	TCP/ 8000	Fornisce un percorso di comunicazione di rete per fornire gli aggiornamenti dei criteri di protezione e dell'inventario. Richiesto per Encryption Enterprise (Windows e Mac)
LDAP	389/636, 3268/3269	Porta 389 - Questa porta è usata per richiedere informazioni dal controller di dominio locale. Le richieste LDAP inviate alla porta 389 possono essere usate per cercare gli oggetti solo

Nome	Porta predefinita	Descrizione
	RPC - 135, 49125+	nel dominio principale del catalogo globale. Tuttavia, l'applicazione richiedente può ottenere tutti gli attributi per tali oggetti. Per esempio, una richiesta alla porta 389 potrebbe essere usata per ottenere il reparto di un utente. Porta 3268 - Questa porta è usata per le query destinate specificamente al catalogo globale. Le richieste LDAP inviate alla porta 3268 possono essere usate per cercare gli oggetti nell'intero insieme di strutture. Tuttavia, è possibile restituire solo gli attributi contrassegnati per la replica al catalogo globale. Per esempio, non è possibile restituire il reparto di un utente usando la porta 3268 poiché questo attributo non è replicato al catalogo globale.
Autenticazione client	HTTPS/ 8449	Consente ai server client di eseguire l'autenticazione a Dell Server. Richiesto per Server Encryption
Beacon richiamata	HTTP/TCP 8446	Consente di inserire un beacon richiamata in ciascun file Office protetto, quando si esegue la modalità Office protetto di Data Guardian.

Progettazione dell'architettura di Security Management Server

Le soluzioni Endpoint Security Suite Enterprise e Data Guardian Dell Encryption sono prodotti altamente scalabili, in base al numero di endpoint individuati per la crittografia all'interno dell'organizzazione.

Componenti dell'architettura

Di seguito, si riportano le configurazioni hardware consigliate adattabili alla maggior parte degli ambienti.

Security Management Server

- Sistema operativo: Windows Server 2012 R2 (Standard, Datacenter a 64 bit), Windows Server 2016 (Standard, Datacenter a 64 bit), Windows Server 2019 (Standard, Datacenter)
- Macchina fisica/virtuale
- CPU: 4 core
- RAM: 16 GB
- Unità C: 30 GB di spazio disponibile su disco per i registri e i database delle applicazioni

> **N.B.: È probabile che vengano consumati fino a 10 GB per un database di eventi locale archiviato su PostgreSQL.**

front-end esterno

- Sistema operativo: Windows Server 2012 R2 (Standard, Datacenter a 64 bit), Windows Server 2016 (Standard, Datacenter a 64 bit), Windows Server 2019 (Standard, Datacenter)
- Macchina fisica/virtuale
- CPU: 2 core
- RAM: 8 GB
- Unità C: 20 GB di spazio disponibile su disco per i registri

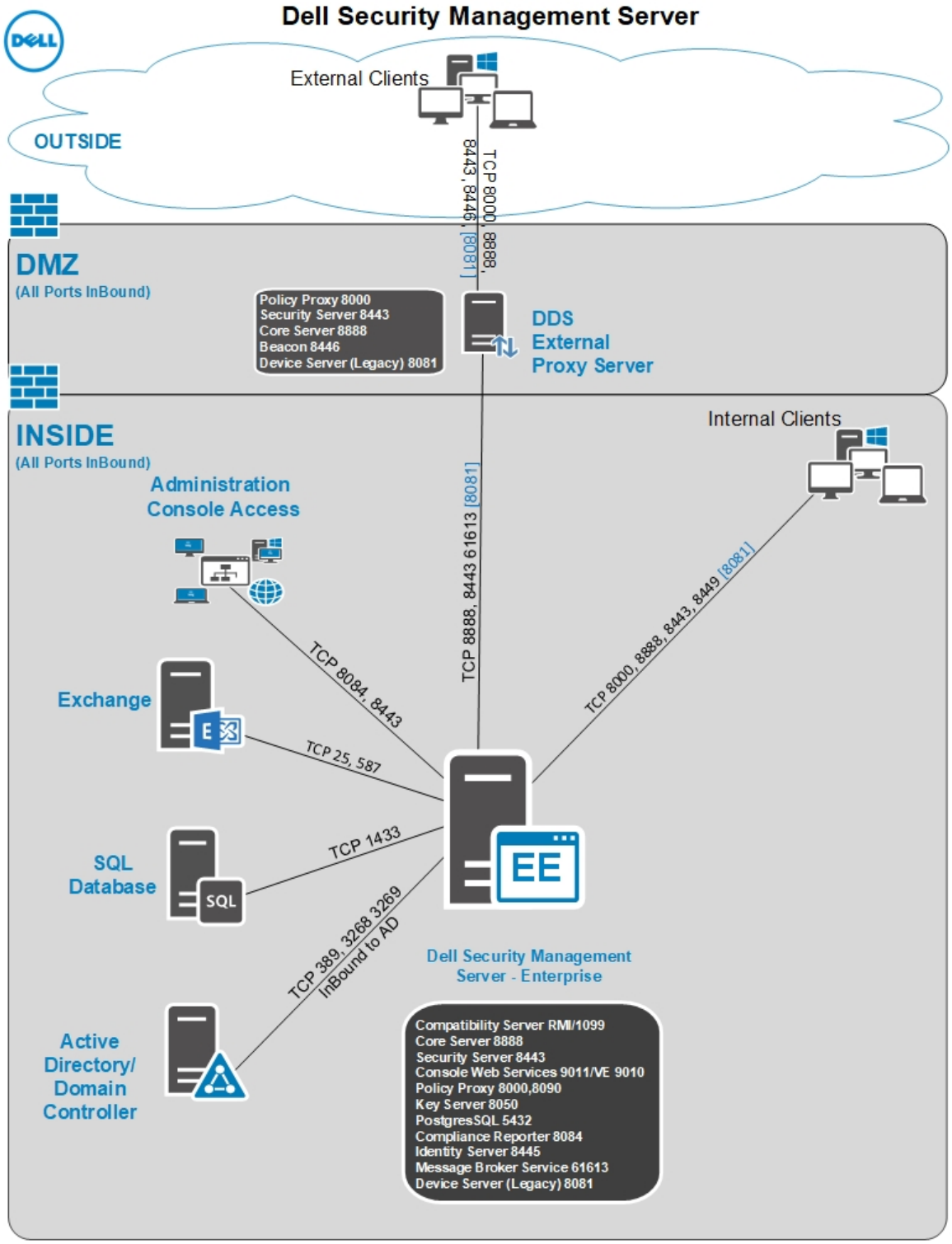
Specifiche hardware di SQL Server

- CPU: 4 core

- RAM: 24 GB
- Unità dati: 100 - 150 GB di spazio disponibile su disco (variabile a seconda dell'ambiente)
- Unità registro: 50 GB di spazio disponibile su disco (variabile a seconda dell'ambiente)

N.B.: Dell consiglia di seguire le procedure consigliate per SQL Server, anche se le informazioni di cui sopra dovrebbero coprire la maggior parte degli ambienti.

Di seguito, si riporta un deployment di base per Dell Security Management Server.



N.B.: Se l'organizzazione dispone di oltre 20.000 endpoint, contattare Dell ProSupport per ricevere assistenza.

Porte

La tabella seguente descrive ciascun componente e la relativa funzione.

Nome	Porta predefinita	Descrizione
Compliance Reporter	HTTP(S)/ 8084	Fornisce una visualizzazione completa dell'ambiente per la creazione di rapporti di controllo e conformità.
Management Console	HTTP(S)/ 8443	Console di amministrazione e centro di controllo per la distribuzione a livello aziendale.
Core Server	HTTPS/ 8888	Gestisce il flusso dei criteri, le licenze e la registrazione per l'autenticazione di preavvio, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Elabora i dati di inventario utilizzati da Compliance Reporter e dalla Management Console. Raccoglie e archivia i dati di autenticazione. Controlla l'accesso basato sui ruoli.
Device Server	HTTPS/ 8081	Supporta le attivazioni e il recupero delle password. Un componente di Security Management Server. Richiesto per Encryption Enterprise (Windows e Mac)
Security Server	HTTPS/ 8443	Comunica con Policy Proxy e gestisce i recuperi delle chiavi Forensic, le attivazioni dei client, Data Guardian, la comunicazione SED-PBA e Active Directory per l'autenticazione o la riconciliazione, inclusa la convalida dell'identità per l'autenticazione nella Management Console. Richiede l'accesso al database SQL.
Compatibility Server	TCP/ 1099	Servizio per la gestione dell'architettura aziendale. Raccoglie e archivia i dati di inventario iniziali durante l'attivazione e i dati dei criteri durante le migrazioni. Elabora i dati basati sui gruppi di utenti.
Message Broker Service	TCP/ 61616 e STOMP/ 61613	Gestisce la comunicazione tra i servizi di Dell Server. Organizza le informazioni sui criteri create dal Compatibility Server per l'accodamento del Policy Proxy. Richiede l'accesso al database SQL.
Key Server	TCP/ 8050	Negozia, autentica e crittografa una connessione client tramite le API Kerberos. Richiede l'accesso al database SQL per estrarre i dati della chiave.
Policy Proxy	TCP/ 8000	Fornisce un percorso di comunicazione di rete per fornire gli aggiornamenti dei criteri di protezione e dell'inventario.
LDAP	TCP/	Porta 389 - Questa porta è usata per richiedere informazioni dal controller di dominio locale. Le richieste LDAP inviate alla

Nome	Porta predefinita	Descrizione
	389/636 (controller di dominio locale), 3268/3269 (catalogo globale)	porta 389 possono essere usate per cercare gli oggetti solo nel dominio principale del catalogo globale. Tuttavia, l'applicazione richiedente può ottenere tutti gli attributi per tali oggetti. Per esempio, una richiesta alla porta 389 potrebbe essere usata per ottenere il reparto di un utente.
	TCP/ 135/ 49125+ (RPC)	Porta 3268 - Questa porta è usata per le query destinate specificamente al catalogo globale. Le richieste LDAP inviate alla porta 3268 possono essere usate per cercare gli oggetti nell'intero insieme di strutture. Tuttavia, è possibile restituire solo gli attributi contrassegnati per la replica al catalogo globale. Per esempio, non è possibile restituire il reparto di un utente usando la porta 3268 poiché questo attributo non è replicato al catalogo globale.
Database di Microsoft SQL Server	TCP/ 1433	La porta SQL Server predefinita è la 1433 e alle porte dei client viene assegnato un valore casuale tra 1024 e 5000.
Autenticazione client	HTTPS/ 8449	Consente ai server client di eseguire l'autenticazione a Dell Server. Richiesto per Server Encryption.
Beacon richiamata	HTTP/TCP 8446	Consente di inserire un beacon richiamata in ciascun file Office protetto, quando si esegue la modalità Office protetto di Data Guardian.

6

Procedure consigliate per SQL Server

L'elenco seguente illustra le procedure consigliate per SQL Server da implementare durante l'installazione di Dell Security, se non ancora implementate.

1 Accertarsi che la dimensione del blocco NTFS in cui si trovano il file di dati e il file di registro sia 64 kB. Gli extent di SQL Server (unità base di SQL Storage) sono di 64 KB.

   Per maggiori informazioni, cercare gli articoli TechNet di Microsoft "Understanding Pages and Extents" (Informazioni su pagine ed extent).

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

2 Come linea guida generale, impostare la quantità massima di memoria di SQL Server all'80% della memoria installata.

   Per maggiori informazioni, cercare gli articoli TechNet di Microsoft *Server Memory Server Configuration Options* (Opzioni di configurazione del server Server Memory).

   - 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 Impostare -t1222 sulle proprietà di avvio dell'istanza per accertarsi che le informazioni di blocco vengano acquisite nel caso in cui dovesse verificarsi un blocco.

   Per maggiori informazioni, cercare gli articoli TechNet di Microsoft sui "Flag di traccia (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 Accertarsi che tutti gli indici siano coperti da un processo di manutenzione settimanale per la ricostruzione degli stessi.

Esempio di notifica al cliente tramite posta elettronica

In seguito all'acquisto di Dell Data Security, si riceverà un messaggio di posta elettronica da DellDataSecurity@Dell.com. Di seguito, è riportato un esempio del messaggio di posta elettronica, che conterrà le credenziali CFT e le informazioni sul codice di licenza.

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