

Dell Data Protection

Guida introduttiva a
Dell Data Protection

v9.4



© 2016 Dell Inc.

Marchi registrati e marchi commerciali usati nella suite di documenti di Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools e Dell Data Protection | Cloud Edition: Dell™ e il logo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ sono marchi commerciali di Dell Inc. Cylance® e il logo Cylance sono marchi registrati di Cylance, Inc. negli Stati Uniti e in altri Paesi. McAfee® e il logo McAfee logo sono marchi commerciali o marchi registrati di McAfee, Inc. negli Stati Uniti e in altri Paesi. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® sono marchi registrati di Intel Corporation negli Stati Uniti e in altri Paesi. Adobe®, Acrobat® e Flash® sono marchi registrati di Adobe Systems Incorporated. Authen Tec® ed Eikon® sono marchi registrati di Authen Tec. AMD® è un marchio registrato di Advanced Micro Devices, Inc. Microsoft®, Windows® e Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server® e Visual C++® sono marchi commerciali o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. VMware® è un marchio registrato o marchio commerciale di VMware, Inc. negli Stati Uniti o in altri Paesi. Box® è un marchio registrato di Box. DropboxSM è un marchio di servizio di Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play sono marchi commerciali o marchi registrati di Google Inc. negli Stati Uniti e in altri Paesi. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloudSM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® e Siri® sono marchi di servizio, marchi commerciali o marchi registrati di Apple, Inc. negli Stati Uniti e/o in altri Paesi. GO ID®, RSA® e SecurID® sono marchi registrati di EMC Corporation. EnCase™ e Guidance Software® sono marchi commerciali o marchi registrati di Guidance Software. Entrust® è un marchio registrato di Entrust®, Inc. negli Stati Uniti e in altri Paesi. InstallShield® è un marchio registrato di Flexera Software negli Stati Uniti, in Cina, nella Comunità Europea, ad Hong Kong, in Giappone, a Taiwan e nel Regno Unito. Micron® e RealSSD® sono marchi registrati di Micron Technology, Inc. negli Stati Uniti e in altri Paesi. Mozilla® Firefox® è un marchio registrato di Mozilla Foundation negli Stati Uniti e/o in altri Paesi. iOS® è un marchio commerciale o marchio registrato di Cisco Systems, Inc. negli Stati Uniti e in alcuni altri Paesi, ed è concesso in licenza. Oracle® e Java® sono marchi registrati di Oracle e/o sue affiliate. Altri nomi possono essere marchi commerciali dei rispettivi proprietari. SAMSUNG™ è un marchio commerciale di SAMSUNG negli Stati Uniti o in altri Paesi. Seagate® è un marchio registrato di Seagate Technology LLC negli Stati Uniti e/o in altri Paesi. Travelstar® è un marchio registrato di HGST, Inc. negli Stati Uniti e in altri Paesi. UNIX® è un marchio registrato di The Open Group. VALIDITY™ è un marchio commerciale di Validity Sensors, Inc. negli Stati Uniti e in altri Paesi. VeriSign® e altri marchi correlati sono marchi commerciali o marchi registrati di VeriSign, Inc. o sue affiliate o filiali negli Stati Uniti e in altri Paesi, e sono concessi in licenza a Symantec Corporation. KVM on IP® è un marchio registrato di Video Products. Yahoo!® è un marchio registrato di Yahoo! Inc.

In questo prodotto vengono utilizzate parti del programma 7-Zip. Il codice sorgente è disponibile all'indirizzo www.7-zip.org. La gestione delle licenze è basata sulla licenza GNU LGPL + restrizioni unRAR (www.7-zip.org/license.txt).

2016-07

Protetto da uno o più brevetti statunitensi, tra cui: numero 7665125; numero 7437752; e numero 7665118.

Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso.

Sommario

- 1 Fasi di implementazione 5
- 2 Analisi dei requisiti e della preparazione 7
 - Documenti relativi ai client Dell Data Protection 8
 - Documenti relativi a Dell Data Protection Server 9
- 3 Elenco di controllo di preparazione - Implementazione iniziale 11
- 4 Elenco di controllo di preparazione - Aggiornamento/Migrazione 17
- 5 Architettura 19
 - Dell Enterprise Server 19
 - Fino a 5.000 endpoint 20
 - Da 5.000 a 20.000 endpoint 21
 - Da 20.000 a 40.000 endpoint 22
 - Da 40.000 a 60.000 endpoint 23
 - Considerazioni sulla disponibilità elevata 24
 - Virtualizzazione. 25
 - Porte di Dell Enterprise Server. 25
 - DDP Enterprise Server - Virtual Edition 28
 - Specifiche hardware 28
 - Server front-end esterno Dell 28
 - Porte di Virtual Edition 29
- 6 Esempio di notifica al cliente tramite posta elettronica 33

Fasi di implementazione

Il processo di implementazione di base comprende le seguenti fasi:

- Esecuzione dell'[Analisi dei requisiti e della preparazione](#)
- Completamento dell'[Elenco di controllo di preparazione - Implementazione iniziale](#) o dell'[Elenco di controllo di preparazione - Aggiornamento/Migrazione](#)
- Installazione o aggiornamento/migrazione di **uno** dei seguenti:
 - **Dell Enterprise Server**
 - Gestione centralizzata dei dispositivi
 - Eseguitibile in un server Microsoft Windows
 - **DDP Enterprise Server - VE**
 - Gestione centralizzata di un massimo di 3500 dispositivi
 - Eseguitibile in un ambiente virtualizzato

Per maggiori informazioni sui server di Dell Data Protection, consultare la *Guida alla migrazione e all'installazione di Enterprise Server* o la *Guida introduttiva e all'installazione di Virtual Edition*. Per ottenere questi documenti, fare riferimento a [Documenti relativi a Dell Data Protection Server](#).

Per istruzioni sui requisiti dei client e sull'installazione del software, selezionare i documenti appropriati in base alla distribuzione:

- *Guida all'installazione di base di Enterprise Edition* o *Guida all'installazione avanzata di Enterprise Edition*
- *Guida all'installazione di base di Endpoint Security Suite* o *Guida all'installazione avanzata di Endpoint Security Suite*
- *Guida all'installazione di base di Endpoint Security Suite Enterprise* o *Guida all'installazione avanzata di Endpoint Security Suite Enterprise*
- *Guida all'installazione di Personal Edition*
- *Guida all'installazione di Security Tools*
- *Guida dell'amministratore di Enterprise Edition per Mac*
- *Guida dell'amministratore di Mobile Edition*

Per ottenere questi documenti, fare riferimento a [Documenti relativi ai client Dell Data Protection](#).

- Configurazione dei criteri iniziali
 - **Dell Enterprise Server** - Consultare la *Guida alla migrazione e all'installazione di Enterprise Server, Attività di amministrazione*
 - **DDP Enterprise Server - VE** - Consultare la *Guida introduttiva e all'installazione di Virtual Edition, Attività di amministrazione della Remote Management Console*
- Esecuzione del piano di verifica
- Imballaggio del client
- Partecipazione al trasferimento delle informazioni di base dell'amministratore di Dell Data Protection
- 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 Protection 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 finali 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?
 - Enterprise Edition
 - Encryption (diritto a DE) - Crittografia Windows, Server Encryption, External Media Shield (EMS), SED Management, Autenticazione avanzata, BitLocker Manager (BLM) e Crittografia Mac.
 - External Media Edition (diritto a EME)
 - Cloud Edition (diritto a CE)
 - Endpoint Security Suite
 - Threat Protection (diritto a TP)
 - Encryption (diritto a DE) - Crittografia Windows, Server Encryption, External Media Shield (EMS), SED Management, Autenticazione avanzata, BitLocker Manager (BLM) e Crittografia Mac.
 - External Media Edition (diritto a EME)
 - Endpoint Security Suite Enterprise
 - Advanced Threat Protection (diritto ad ATP)
 - Encryption (diritto a DE) - Crittografia Windows, Server Encryption, External Media Shield (EMS), SED Management, Autenticazione avanzata, BitLocker Manager (BLM) e Crittografia Mac.
 - External Media Edition (diritto a EME)
 - Mobile Edition (diritto a ME) per Android, iOS e Windows Phone
- 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 relativi ai client Dell Data Protection

Per i requisiti di installazione, le versioni dei SO supportati, le unità autocrittografanti, le istruzioni utente per i prodotti Dell Data Protection che si intende distribuire, fare riferimento ai relativi documenti elencati qui di seguito.

Enterprise Edition (client Windows) - Consultare i seguenti documenti all'indirizzo:

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

- *Guida all'installazione di base di Enterprise Edition* - Guida all'installazione di Enterprise Edition.
- *Guida all'installazione avanzata di Enterprise Edition* - Guida all'installazione di Enterprise Edition con opzioni e parametri avanzati per installazioni personalizzate.
- *Guida dell'utente di DDP Console* - Istruzioni per utenti finali di Dell Data Protection I Advanced Authentication.
- *Guida dell'utente di Cloud Edition* - Istruzioni di installazione, attivazione e funzionamento per gli utenti finali di Dell Data Protection I Cloud Edition.

Enterprise Edition (client Mac) - Consultare la *Guida dell'amministratore di Enterprise Edition per Mac* all'indirizzo

www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. La *Guida dell'amministratore* include le istruzioni di installazione e distribuzione.

Endpoint Security Suite (client Windows) - Consultare i seguenti documenti all'indirizzo:

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

- *Guida all'installazione di base di Endpoint Security Suite* - Guida all'installazione di Endpoint Security Suite.
- *Guida all'installazione avanzata di Endpoint Security Suite* - Guida all'installazione di Endpoint Security Suite, con opzioni e parametri per installazioni personalizzate.
- *Guida dell'utente di DDP Console* - Istruzioni per utenti finali di Dell Data Protection I Endpoint Security Suite.

Endpoint Security Suite Enterprise (client Windows) - Consultare i seguenti documenti all'indirizzo:

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

- *Guida all'installazione di base di Endpoint Security Suite Enterprise* - Guida all'installazione di Endpoint Security Suite Enterprise.
- *Guida all'installazione avanzata di Endpoint Security Suite Enterprise* - Guida all'installazione di Endpoint Security Suite Enterprise, con opzioni e parametri per installazioni personalizzate.
- *Guida dell'utente di DDP Console* - Istruzioni per utenti finali di Dell Data Protection I Endpoint Security Suite Enterprise.

Mobile Edition per Android, iOS e Windows Phone

- Consultare la *Guida dell'amministratore di Mobile Edition* all'indirizzo www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. La *Guida dell'amministratore* spiega come distribuire Dell Data Protection I Mobile Edition.

Documenti relativi a Dell Data Protection Server

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

Dell Enterprise Server

- Consultare la *Guida alla migrazione e all'installazione di Enterprise 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/04/product-support/product/dell-dp-endpt-security-suite/manuals.
oppure
www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

DDP Enterprise Server - Virtual Edition

- Consultare la *Guida introduttiva e all'installazione di Virtual Edition* 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/04/product-support/product/dell-dp-endpt-security-suite/manuals.
oppure
www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

Elenco di controllo di preparazione - Implementazione iniziale

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

- [Elenco di controllo di Dell Enterprise Server](#)
- [Elenco di controllo di DDP Enterprise Server - VE](#)

Elenco di controllo di Dell Enterprise 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.
- Gli endpoint di produzione utilizzati durante il test Proof of Concept sono stati decrittografati oppure sono stati scaricati i pacchetti di chiavi.
- L'applicazione Proof of Concept è stata rimossa dall'ambiente.

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

I server soddisfano le specifiche hardware richieste?

- Consultare l'architettura per [Dell Enterprise Server](#).

I server soddisfano le specifiche software richieste?

- È installato: Windows Server 2008 SP2 a 64 bit (Standard o Enterprise); 2008 R2 SP0-SP1 a 64 bit (Standard o Enterprise); 2012 R2 (Standard).
- È installato Windows Installer 4.0 o versione successiva.
- .NET Framework 4.5 è installato.
- Se si utilizza Microsoft SQL Server 2012, è installato Microsoft SQL Native Client 2012. È possibile utilizzare SQL Native Client 2014, se disponibile.

N.B. Dell Enterprise Server non supporta SQL Express.

- Windows Firewall è disabilitato o configurato per consentire il funzionamento delle porte 80, 1099, 8000, 8050, 8081, 8084, 8443, 8445, 8888, 9000, 9011, 61613, 61616 (in ingresso).
- È disponibile la connettività tra Dell Enterprise Server e Active Directory (AD) sulle porte 88, 135, 389, 636, 3268, 3269, 49125+ (RPC) (in ingresso verso AD).
- Il controllo dell'account utente è disabilitato (consultare Pannello di controllo Windows > Account utente).
 - Windows Server 2008 SP2 a 64 bit/Windows Server 2008 R2 SP0-SP1 a 64 bit
 - Windows Server 2012 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 Dell Enterprise 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 Protection e di Dell Enterprise 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/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y oppure www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals
Per passare alla cartella dall'indirizzo www.dell.com/support
 - 1** In **Cerca un prodotto**, selezionare **Visualizza prodotti** poi **Software e sicurezza** e **Soluzioni per la sicurezza degli endpoint**.
 - 2** Selezionare **Dell Data Protection I Encryption**, **Dell Data Protection I Endpoint Security Suite** o **Dell Data Protection I Endpoint Security Suite Enterprise**, poi **Driver e download**.
 - 3** Dall'elenco a discesa 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**.
 - 4** Nel riquadro del software applicabile, selezionare **Scarica file**.
- Se si è acquistato Encryption, Endpoint Security Suite o Endpoint Security Suite Enterprise on-the-box, è possibile scaricare il software dal sito www.dell.com. On-the-box fa riferimento al software incluso nell'immagine del computer di fabbrica di Dell. Encryption, Endpoint Security Suite o Endpoint Security Suite Enterprise possono essere preinstallati in qualsiasi computer Dell.

OPPURE

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

- Il software si trova all'indirizzo <https://ddpe.credant.com> o <https://cft.credant.com> nella cartella **SoftwareDownloads**.
- Se si è acquistato Encryption, Endpoint Security Suite o Endpoint Security Suite Enterprise on-the-box, è possibile scaricare il software dal sito www.dell.com. On-the-box fa riferimento al software incluso nell'immagine del computer di fabbrica di Dell. Encryption, Endpoint Security Suite o Endpoint Security Suite Enterprise possono essere preinstallati in qualsiasi computer Dell.

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](#).
- 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, Endpoint Security Suite 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 Enterprise Server*. Se non ne è già stato creato uno, il programma di installazione di Enterprise 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 Dell Enterprise 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:
 - Dell Enterprise Server: ddpe-es.<dominio.com>
 - Server front-end: ddpe-fe.<dominio.com>

N.B. Lo split DNS consente di utilizzare lo stesso nome DNS per i servizi front-end interni ed esterni e, in alcuni casi, è necessario. Lo split DNS consente di utilizzare un unico indirizzo per i client e fornisce flessibilità durante gli aggiornamenti o per scalare la soluzione in un secondo momento. Un CNAME consigliato per i server front-end quando si utilizza lo split DNS è: ddpe-fe.<dominio.com>.

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 **oppure** 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 o Endpoint Security Suite Enterprise 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 sistemi attivi per la verifica. I sistemi attivi devono essere utilizzati durante un progetto pilota di produzione, dopo la definizione e la verifica dei criteri di crittografia tramite il piano di verifica fornito da Dell.

Elenco di controllo di DDP Enterprise Server - VE

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

- L'applicazione e il database Proof of Concept (POC) sono stati salvati e disinstallati (se si utilizza lo stesso server) prima dell'intervento di installazione di Dell.
- Gli endpoint di produzione utilizzati durante il test Proof of Concept sono stati decrittografati oppure sono stati scaricati i pacchetti di chiavi.
- L'applicazione Proof of Concept è stata rimossa dall'ambiente.

N.B. Tutte le nuove implementazioni devono essere avviate con un nuovo database e l'installazione del software Encryption, Endpoint Security Suite o Endpoint Security Suite Enterprise. Dell Client Services non effettuerà una nuova implementazione usando un ambiente PoC. Gli endpoint crittografati durante il Proof of Concept 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 Protection e di Virtual Edition 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/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y oppure www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

Per passare alla cartella dall'indirizzo www.dell.com/support

1 In **Cerca un prodotto**, selezionare **Visualizza prodotti** poi **Software e sicurezza** e **Soluzioni per la sicurezza degli endpoint**.

2 Selezionare **Dell Data Protection | Encryption**, **Dell Data Protection | Endpoint Security Suite** o **Dell Data Protection | Endpoint Security Suite Enterprise**, poi **Driver e download**.

3 Dall'elenco a discesa dei sistemi operativi, selezionare il sistema operativo appropriato per il prodotto che si sta scaricando. Per esempio, per scaricare Virtual Edition selezionare **una delle versioni VMWare**.

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

- Se si è acquistato Encryption, Endpoint Security Suite o Endpoint Security Suite Enterprise on-the-box, è possibile scaricare il software dal sito www.dell.com. On-the-box fa riferimento al software incluso nell'immagine del computer di fabbrica di Dell. Encryption, Endpoint Security Suite o Endpoint Security Suite Enterprise possono essere preinstallati in qualsiasi computer Dell.

I file della licenza sono disponibili?

- 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, Endpoint Security Suite o Endpoint Security Suite Enterprise.

I server soddisfano le specifiche hardware richieste?

- Consultare [DDP Enterprise Server - Virtual Edition](#).

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 oppure 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 o Endpoint Security Suite Enterprise 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 sistemi attivi per la verifica. I sistemi attivi devono essere utilizzati durante un progetto pilota di produzione, dopo la definizione e la verifica dei criteri di crittografia tramite il piano di verifica fornito da Dell.

Elenco di controllo di preparazione - Aggiornamento/Migrazione

Questo elenco di controllo è valido solo per Dell Enterprise Server.

N.B. Aggiornare DDP Enterprise Server - VE dal menu Configurazione di base in VE Terminal. Per maggiori informazioni, consultare la *Guida introduttiva e all'installazione di Virtual Edition*.

Utilizzare il seguente elenco di controllo per accertarsi di aver soddisfatto tutti i prerequisiti prima di aggiornare Dell Data Protection I Encryption, Dell Data Protection I Endpoint Security Suite o Dell Data Protection I Endpoint Security Suite Enterprise.

I server soddisfano le specifiche software richieste?

- È installato: Windows Server 2008 SP2 a 64 bit (Standard o Enterprise); 2008 R2 SP0-SP1 a 64 bit (Standard o Enterprise); 2012 R2 (Standard).
- È installato Windows Installer 4.0 o versione successiva.
- .NET Framework 4.5 è installato.
- Se si utilizza Microsoft SQL Server 2012, è installato Microsoft SQL Native Client 2012. È possibile utilizzare SQL Native Client 2014, se disponibile.

N.B. Dell Enterprise Server non supporta SQL Express.

- Windows Firewall è disabilitato o configurato per consentire il funzionamento delle porte 80, 1099, 8000, 8050, 8081, 8084, 8443, 8445, 8888, 9000, 9011, 61613, 61616 (in ingresso).
- È disponibile la connettività tra Dell Enterprise Server e Active Directory (AD) sulle porte 88, 135, 389, 636, 3268, 3269, 49125+ (RPC) (in ingresso verso AD).
- Il controllo dell'account utente è disabilitato (consultare Pannello di controllo Windows > Account utente).
 - Windows Server 2008 SP2 a 64 bit/Windows Server 2008 R2 SP0-SP1 a 64 bit
 - Windows Server 2012 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 Dell Enterprise 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](#).
- 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, Endpoint Security Suite o Endpoint Security Suite Enterprise.

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

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

- Il software si trova all'indirizzo <https://ddpe.credant.com> o <https://cft.credant.com> nella cartella **SoftwareDownloads**.
- Se si è acquistato Encryption, Endpoint Security Suite o Endpoint Security Suite Enterprise on-the-box, è possibile scaricare il software dal sito www.dell.com. On-the-box fa riferimento al software incluso nell'immagine del computer di fabbrica di Dell. Encryption, Endpoint Security Suite o Endpoint Security Suite Enterprise possono essere preinstallati in qualsiasi computer Dell.

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 rappresentante locale Dell prima di eseguire l'aggiornamento o la migrazione. Dell Data Protection eseguirà la convalida delle licenze e, se queste non sono disponibili, le attivazioni non verranno eseguite.

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

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 *oppure* 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 o Endpoint Security Suite Enterprise 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 sistemi attivi per la verifica. I sistemi attivi devono essere utilizzati durante un progetto pilota di produzione, dopo la definizione e la verifica dei criteri di crittografia tramite il piano di verifica fornito da Dell.

Architettura

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

- [Dell Enterprise Server](#)
- [DDP Enterprise Server - Virtual Edition](#)

Dell Enterprise Server

Le soluzioni Encryption, Endpoint Security Suite ed Endpoint Security Suite Enterprise sono prodotti altamente scalabili e vengono scalate in base alle dimensioni della propria organizzazione e al numero di endpoint destinati alla crittografia. La presente sezione offre una serie di linee guida per scalare l'architettura per 5.000-60.000 endpoint.

N.B. Se l'organizzazione dispone di oltre 50.000 endpoint, contattare Dell Client Services per assistenza.

N.B. Tutti i componenti elencati in tutte le sezioni includono le specifiche hardware minime necessarie per garantire prestazioni ottimali nella maggior parte degli ambienti. Non allocando le risorse adeguate ad uno qualsiasi dei componenti elencati, si potrebbe causare la riduzione delle prestazioni o problemi di funzionalità dell'applicazione.

Fino a 5.000 endpoint

Questa architettura è adatta per la maggior parte delle aziende medio-piccole con un numero di endpoint compreso tra 1 e 5.000. Tutti i componenti del DDP Server possono essere installati in un unico server. Facoltativamente, è possibile posizionare un server front-end nella DMZ per la pubblicazione dei criteri e/o per l'attivazione degli endpoint in Internet.

Componenti dell'architettura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 a 64 bit/Windows Server 2008 SP2 a 64 bit - Standard o Enterprise Edition/Windows Server 2012 R2 - Standard Edition

Configurazione con server singolo

16 GB; 20 GB o più di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Quad-Core moderna (2 GHz+)

Configurazione del server quando usata per server front-end Dell esterno

Windows Server 2008 R2 SP0-SP1 a 64 bit/Windows Server 2008 SP2 a 64 bit - Standard o Enterprise Edition/Windows Server 2012 R2 - Standard Edition

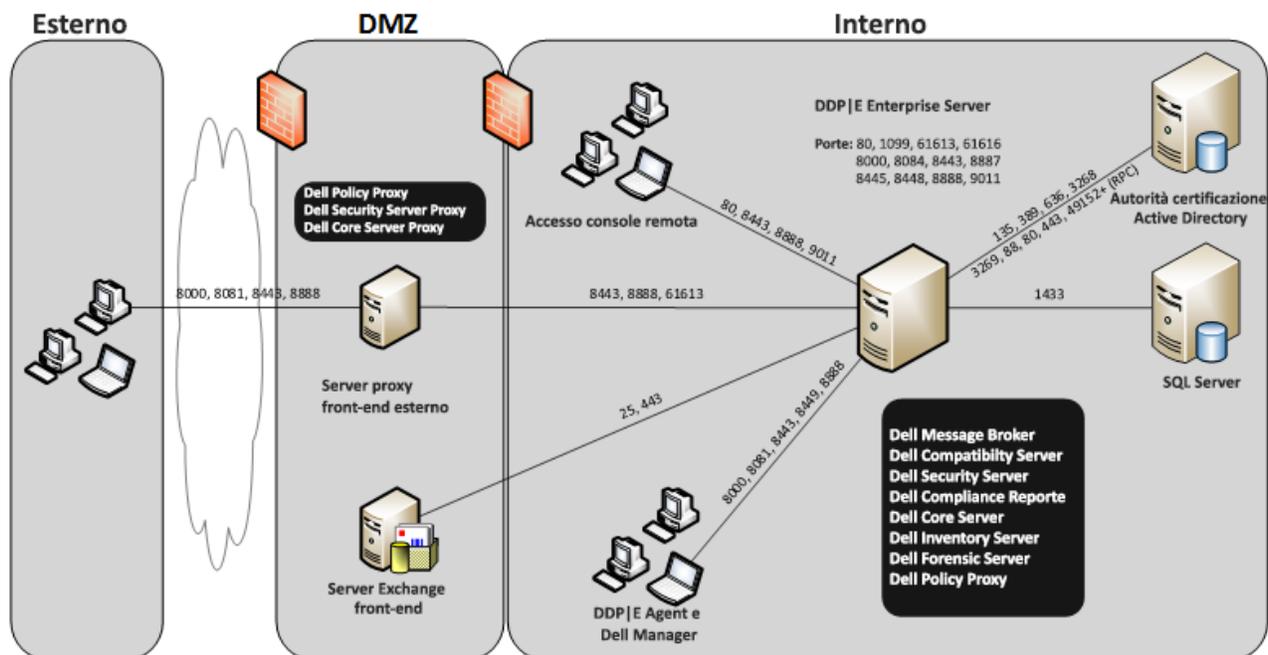
8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

SQL Server

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

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

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



Da 5.000 a 20.000 endpoint

Questa architettura è adatta per ambienti con un numero di endpoint compreso tra 5.000 e 20.000. Per distribuire il carico aggiuntivo, viene aggiunto un server front-end progettato per gestire circa 15.000 - 20.000 endpoint. Facoltativamente, è possibile posizionare un server front-end nella DMZ per la pubblicazione dei criteri e/o per l'attivazione degli endpoint in Internet.

Componenti dell'architettura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 a 64 bit/Windows Server 2008 a 64 bit - Standard o Enterprise Edition/Windows Server 2012 R2 - Standard Edition

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

Server front-end interno Dell (1) e server front-end esterno Dell (1)

Windows Server 2008 R2 SP0-SP1 a 64 bit/Windows Server 2008 SP2 a 64 bit - Standard o Enterprise Edition/Windows Server 2012 R2 - Standard Edition

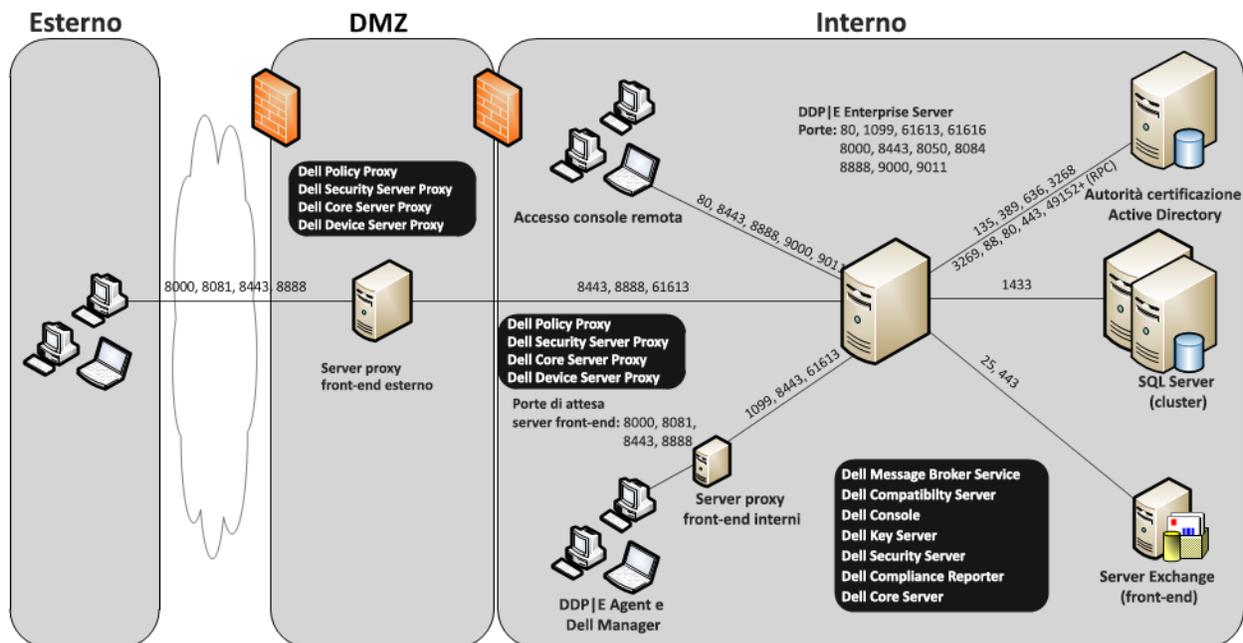
8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

SQL Server

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

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

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



Da 20.000 a 40.000 endpoint

Questa architettura è adatta per ambienti con un numero di endpoint compreso tra 20.000 e 40.000. Viene aggiunto un altro server front-end per distribuire il carico aggiuntivo. Ogni server front-end è progettato per gestire circa 15.000 - 20.000 endpoint. Facoltativamente, è possibile posizionare un server front-end nella DMZ per l'attivazione degli endpoint e/o la pubblicazione dei criteri negli endpoint in Internet.

Componenti dell'architettura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 a 64 bit/Windows Server 2008 SP2 a 64 bit - Standard o Enterprise Edition/Windows Server 2012 R2 - Standard Edition

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

Server front-end interni Dell (2) e server front-end esterno Dell (1)

Windows Server 2008 R2 SP0-SP1 a 64 bit/Windows Server 2008 SP2 a 64 bit - Standard o Enterprise Edition/Windows Server 2012 R2 - Standard Edition

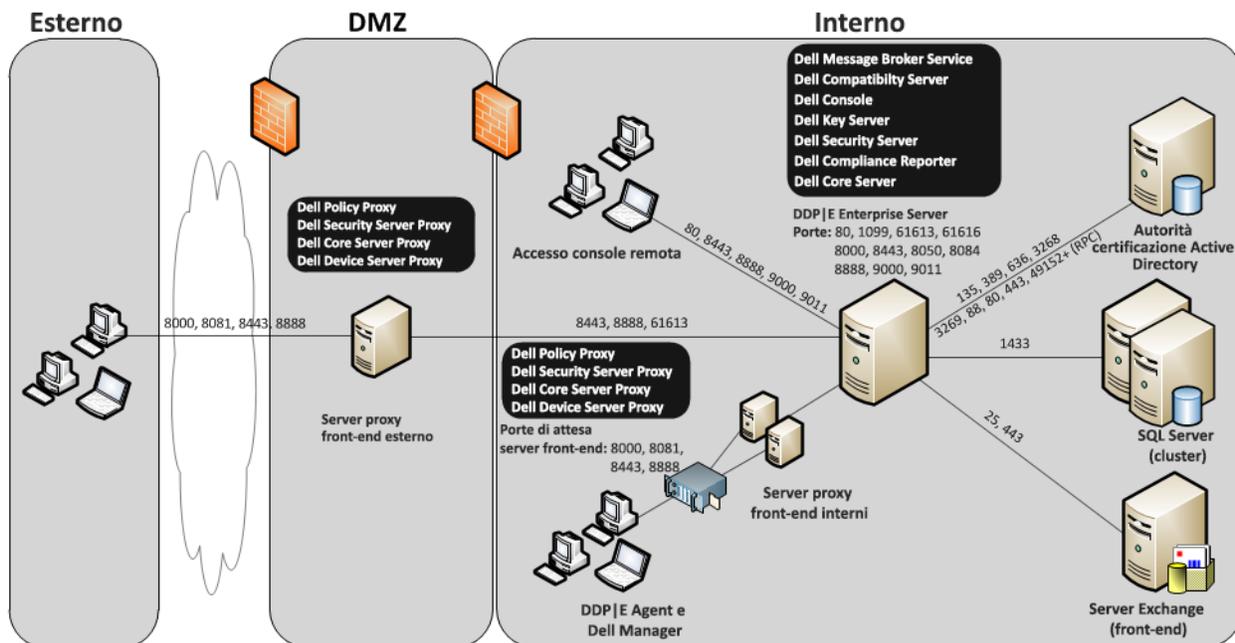
8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

SQL Server

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

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

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



Da 40.000 a 60.000 endpoint

Questa architettura è adatta per ambienti con un numero di endpoint compreso tra 40.000 e 60.000. Viene aggiunto un altro server front-end per distribuire il carico aggiuntivo. Ogni server front-end è progettato per gestire circa 15.000 - 20.000 endpoint. Facoltativamente, è possibile posizionare un server front-end nella DMZ per l'attivazione degli endpoint e/o la pubblicazione dei criteri negli endpoint in Internet.

N.B. Se l'organizzazione dispone di oltre 50.000 endpoint, contattare Dell Client Services per assistenza.

Componenti dell'architettura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 a 64 bit/Windows Server 2008 SP2 a 64 bit - Standard o Enterprise Edition/Windows Server 2012 R2 - Standard Edition

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

Server front-end interni Dell (2) e server front-end esterno Dell (1)

Windows Server 2008 R2 SP0-SP1 a 64 bit/Windows Server 2008 SP2 a 64 bit - Standard o Enterprise Edition/Windows Server 2012 R2 - Standard Edition

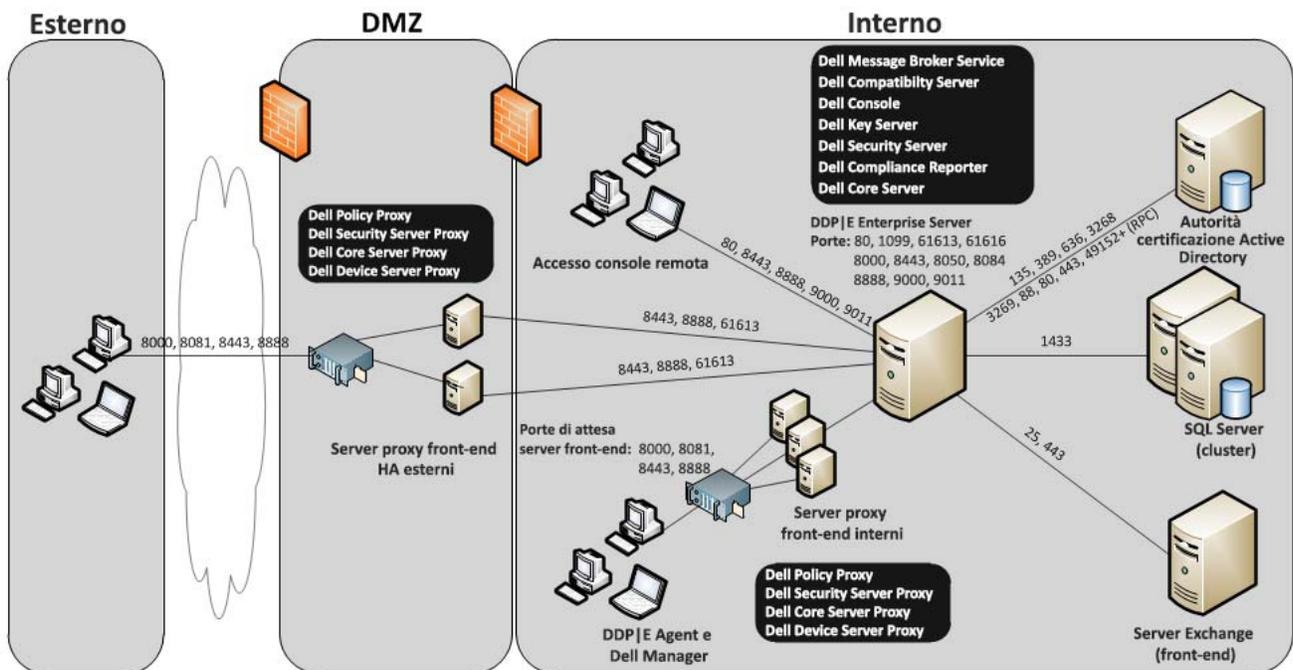
8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

SQL Server

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

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

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



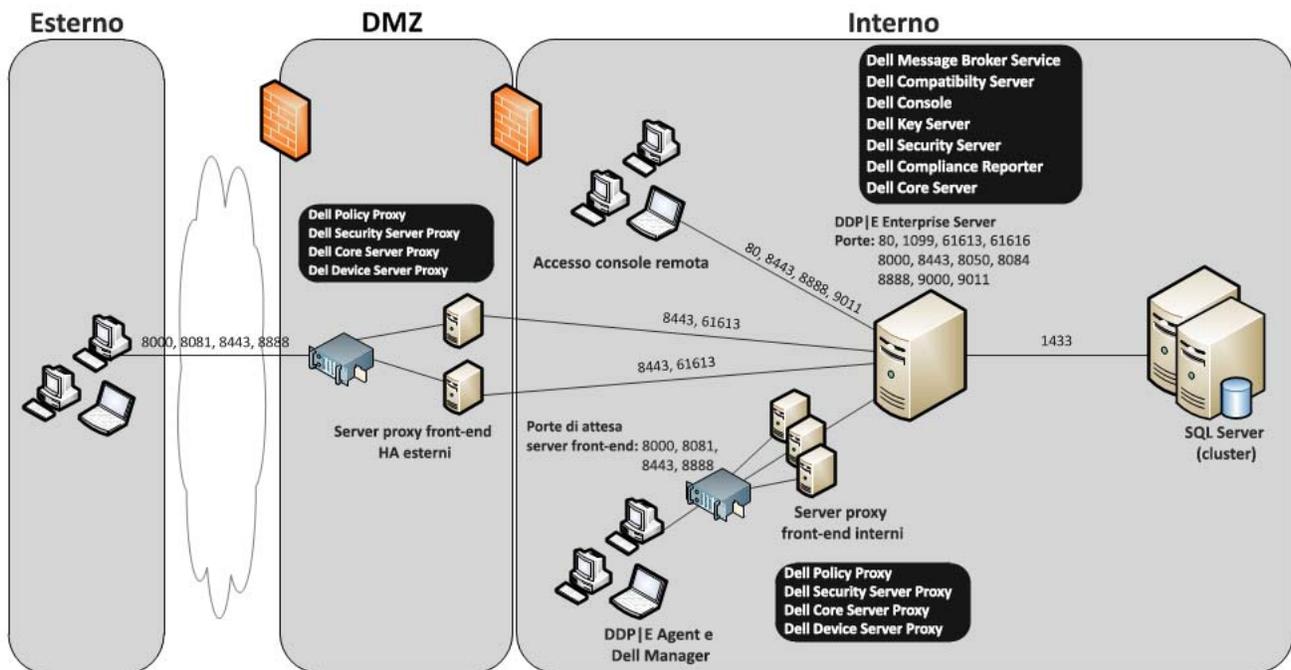
Considerazioni sulla disponibilità elevata

Questa architettura rappresenta un'architettura a disponibilità elevata che supporta fino a 60.000 endpoint. In una configurazione attiva/passiva, sono installati due Dell Enterprise Server. Per eseguire il failover al secondo Dell Enterprise Server, arrestare i servizi sul nodo primario e indirizzare l'alias DNS (CNAME) al secondo nodo. Avviare i servizi sul secondo nodo e la Remote Management Console per accertarsi che l'applicazione funzioni correttamente. I servizi sul secondo nodo (passivo) devono essere configurati come "Manuale" al fine di prevenirne l'avvio accidentale durante le regolari operazioni di manutenzione e applicazione delle patch.

L'organizzazione può inoltre scegliere di avere un server database del cluster SQL. In questa configurazione, il Dell Enterprise Server deve essere configurato in modo da usare l'IP o il nome host del cluster.

N.B. La replica del database non è supportata.

Il traffico dei clienti è distribuito su tre server front-end interni. Facoltativamente, è possibile posizionare più server front-end nella DMZ per l'attivazione degli endpoint e/o per la pubblicazione dei criteri negli endpoint in Internet.



Virtualizzazione

Server dell'applicazione Dell Data Protection

La velocità del disco dell'hardware che ospita il server virtuale, l'allocazione della RAM al guest e la configurazione delle unità di archiviazione potrebbero avere un impatto significativo sulle prestazioni. L'impatto si nota di più durante l'attivazione, l'elaborazione di criteri e inventario e la valutazione. Dell consiglia di riservare quanta più RAM possibile per l'host virtuale, dando priorità all'host virtuale nell'allocazione delle risorse. Se vi è un interesse verso le prestazioni, Dell consiglia di usare la distribuzione in un ambiente server non virtuale.

SQL Server

Negli ambienti più grandi, si consiglia vivamente di eseguire il server del database SQL su hardware fisico e in un sistema ridondante, come un cluster SQL, al fine di garantire disponibilità e continuità dei dati. Si consiglia inoltre di eseguire giornalmente backup completi con la registrazione transazionale attiva, al fine di garantire che le nuove chiavi generate dall'attivazione di un utente/dispositivo siano recuperabili.

Le attività di manutenzione del database devono comprendere la ricostruzione di tutti gli indici dei database e la raccolta dei dati statistici.

Per ulteriori informazioni sulle procedure consigliate per SQL Server, consultare la *Guida alla migrazione e all'installazione di Enterprise Server*.

Porte di Dell Enterprise Server

La tabella seguente descrive ciascun componente e la relativa funzione.

Nome	Porta predefinita	Descrizione	Richiesto per
Compliance Reporter	HTTP(S)/ 8084	Fornisce una visualizzazione completa dell'ambiente per la creazione di rapporti di controllo e conformità. Componente di Dell Enterprise Server.	Creare rapporti
Remote Management Console	HTTP(S)/ 8443	Console di amministrazione e centro di controllo per la distribuzione a livello aziendale. Componente di Dell Enterprise Server.	Tutti
Core Server	HTTPS/ 8888 e 9000	Gestisce il flusso dei criteri, le licenze e la registrazione per l'autenticazione di preavviso, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Protection. Elabora i dati di inventario utilizzati da Compliance Reporter e dalla Remote Management Console. Raccoglie e archivia i dati di autenticazione. Controlla l'accesso basato sui ruoli. Componente di Dell Enterprise Server.	Tutti

Nome	Porta predefinita	Descrizione	Richiesto per
Device Server	HTTPS/ 8443 HTTPS/ 8081 (a Dell Device Server di back-end)	Supporta le attivazioni e il recupero delle password. Componente di Dell Enterprise Server.	Dell Data Protection I Enterprise Edition per Mac Dell Data Protection I Enterprise Edition per Windows CREDActivate
Security Server	HTTPS/ 8443	Comunica con Policy Proxy e gestisce i recuperi delle chiavi Forensic, le attivazioni dei client, i prodotti Cloud Edition, la comunicazione SED-PBA e Active Directory per l'autenticazione o la riconciliazione, inclusa la convalida dell'identità per l'autenticazione nella Remote Management Console. Richiede l'accesso al database SQL. Componente di Dell Enterprise Server.	Tutti
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 in questo servizio. Componente di Dell Enterprise Server.	Tutti
Message Broker Service	TCP/ 61616 e STOMP/ 61613	Gestisce la comunicazione tra i servizi di Dell Enterprise Server. Organizza le informazioni sui criteri create dal Compatibility Server per l'accodamento del Policy Proxy. Richiede l'accesso al database SQL. Componente di Dell Enterprise Server.	Tutti
Identity Server	HTTPS/ 8445	Gestisce le richieste di autenticazione del dominio, inclusa l'autenticazione di SED Manager. Richiede un account di Active Directory. Deve essere l'account usato per accedere a SQL quando viene usata l'Autenticazione di Windows. Componente di Dell Enterprise Server.	Tutti

Nome	Porta predefinita	Descrizione	Richiesto per
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. Componente di Dell Enterprise Server.	Utilità di amministrazione Dell
Policy Proxy	TCP/ 8000	Fornisce un percorso di comunicazione basato su rete per fornire gli aggiornamenti dei criteri di protezione e dell'inventario. Un componente di Dell Enterprise Server.	Dell Data Protection I Enterprise Edition per Mac Dell Data Protection I Enterprise Edition per Windows Dell Data Protection I Mobile Edition
LDAP	TCP/ 389/636 (controller di dominio locale), 3268/3269 (catalogo globale) TCP/ 135/ 49125+ (RPC)	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 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.	Tutti
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.	Tutti
Autenticazione client	HTTPS/ 8449	Consente ai server client di eseguire l'autenticazione a Dell Enterprise Server.	Dell Data Protection I Server Encryption (SE)
Comunicazione tramite posta elettronica	25	Fornisce notifiche di eventi.	Facoltativo
EAS Device Manager		Abilita la funzionalità over-the-air. Installato nel server Accesso client di Exchange.	Gestione di Exchange ActiveSync dei dispositivi mobili.
EAS Mailbox Manager		L'agente della cassetta postale installato nel server Cassette postali di Exchange.	Gestione di Exchange ActiveSync dei dispositivi mobili.

DDP Enterprise Server - Virtual Edition

Questa architettura è adatta per le aziende medio-piccole con un numero di endpoint compreso tra 1 e 3500. Facoltativamente, è possibile posizionare un server front-end nella DMZ per la pubblicazione dei criteri e/o per l'attivazione degli endpoint in Internet.

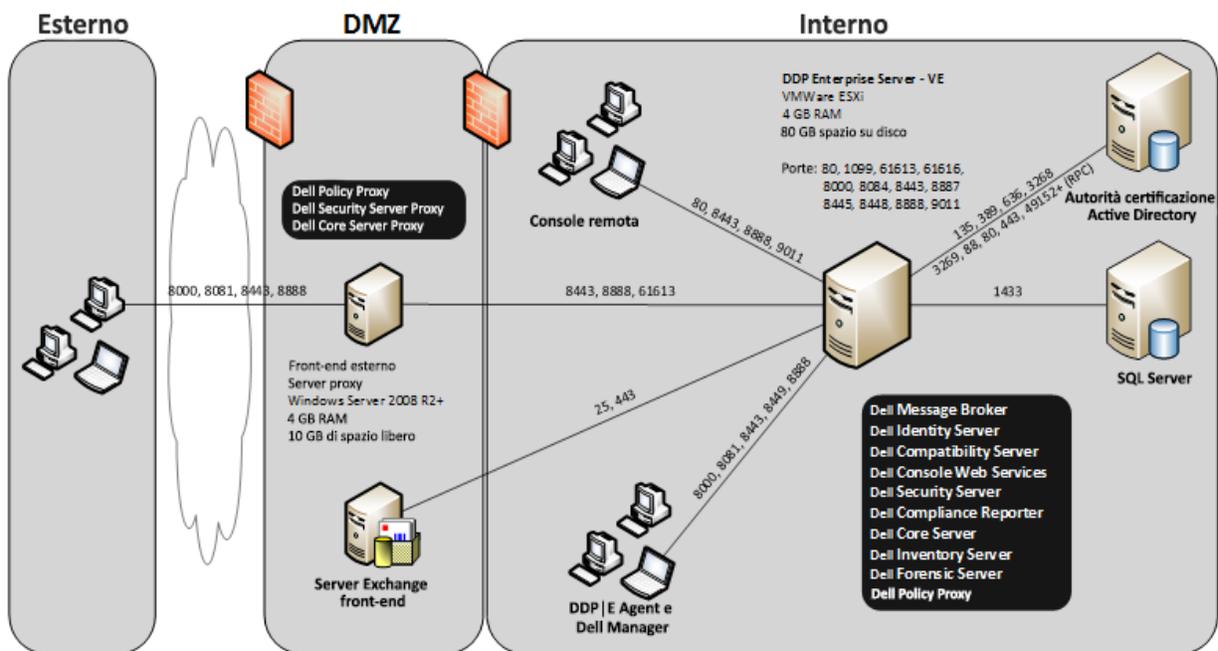
Specifiche hardware

- DDP Enterprise Server - Virtual Edition (VE)
- VMware Workstation 9, 10 o 11; VMware ESXi 5.1, ESXi 5.5 o ESXi 6.0
- 4 GB di RAM con VMWare Workstation 9, 10 o 11; 8 GB di RAM con ESXi 5.1, 5.5 o 6.0
- 80 GB di spazio libero su disco
- Processore 2+ GHz Dual Core o superiore

Per requisiti più dettagliati, consultare la *Guida introduttiva e all'installazione di DDP Enterprise Server - Virtual Edition*.

Server front-end esterno Dell

- Windows Server 2008 R2 SP0-SP1 a 64 bit/Windows Server 2008 SP2 a 64 bit - Standard o Enterprise Edition/Windows Server 2012 R2 - Standard Edition
- 2 GB minimo di RAM dedicata / 4 GB di RAM dedicata consigliati
- 1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale)
- Core Duo da 2 GHz o superiore



Porte di Virtual Edition

La tabella seguente descrive ciascun componente e la relativa funzione.

Nome	Porta predefinita	Descrizione	Richiesto per
Compliance Reporter	HTTP(S)/ 8084	Fornisce una visualizzazione completa dell'ambiente per la creazione di rapporti di controllo e conformità. Componente di DDP Enterprise Server - VE.	Creare rapporti
Remote Management Console		Console di amministrazione e centro di controllo per la distribuzione a livello aziendale. Componente di DDP Enterprise Server - VE.	Tutti
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 Protection. Elabora i dati di inventario utilizzati da Compliance Reporter e dalla Remote Management Console. Raccoglie e archivia i dati di autenticazione. Controlla l'accesso basato sui ruoli. Componente di DDP Enterprise Server - VE.	Tutti
Core Server HA (High Availability, Elevata disponibilità)	HTTPS/ 8888	Servizio ad elevata disponibilità che consente una maggiore sicurezza e migliori prestazioni delle connessioni HTTPS con la Remote Management Console, l'autenticazione di preavvio, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Protection. Componente di DDP Enterprise Server - VE.	Tutti
Security Server	HTTPS/ 8443	Comunica con Policy Proxy e gestisce i recuperi delle chiavi Forensic, le attivazioni dei client, i prodotti Cloud Edition e la comunicazione SED-PBA. Componente di DDP Enterprise Server - VE.	Tutti

Nome	Porta predefinita	Descrizione	Richiesto per
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 in questo servizio. Componente di DDP Enterprise Server - VE.	Tutti
Message Broker Service	TCP/ 61616 e STOMP/ 61613 (chiusa o, se configurata per DMZ, 61613 è aperta)	Gestisce la comunicazione tra i servizi di DDP Enterprise Server - VE. Organizza le informazioni sui criteri create dal Compatibility Server per l'accodamento del Policy Proxy. Componente di DDP Enterprise Server - VE.	Tutti
Identity Server	8445	Gestisce le richieste di autenticazione del dominio, inclusa l'autenticazione di SED Manager. Richiede un account di Active Directory. Componente di DDP Enterprise Server - VE.	Tutti
Forensic Server	HTTPS/ 8448	Consente agli amministratori che dispongono dei privilegi appropriati di ottenere dalla Remote Management Console le chiavi di crittografia, da usare per sbloccare i dati o per le attività di decrittografia. Componente di DDP Enterprise Server - VE.	API Forensic
Inventory Server	8887	Elabora la coda di inventario. Componente di DDP Enterprise Server - VE.	Tutti
Policy Proxy	TCP/ 8000/8090	Fornisce un percorso di comunicazione di rete per fornire gli aggiornamenti dei criteri di protezione e dell'inventario. Componente di DDP Enterprise Server - VE.	Dell Data Protection Enterprise Edition per Mac Dell Data Protection Enterprise Edition per Windows Dell Data Protection Mobile Edition

Nome	Porta predefinita	Descrizione	Richiesto per
LDAP	389/636, 3268/3269 RPC - 135, 49125+	<p>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 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.</p> <p>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.</p>	Tutti
Autenticazione client	HTTPS/ 8449	Consente ai server del client di autenticarsi su DDP Enterprise Server - VE.	Dell Data Protection I Server Encryption
EAS Device Manager		Abilita la funzionalità over-the-air. Installato nel server Accesso client di Exchange.	Gestione di Exchange ActiveSync dei dispositivi mobili.
EAS Mailbox Manager		L'agente della cassetta postale installato nel server Cassetta postali di Exchange.	Gestione di Exchange ActiveSync dei dispositivi mobili.

Esempio di notifica al cliente tramite posta elettronica

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

DELL

Dell Data Protection | Encryption

Dear [Redacted],

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

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

Download Server:	https://ddpe.credant.com
Username:	[Redacted]
Password:	l1oFqQe
Required to change password:	No
Account Expiration Date:	Never
License Key:	[Redacted]

Support

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

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

© 2010 Dell Inc and CREDANT Technologies, Inc. All rights reserved.

Di seguito è riportato un esempio del messaggio di posta elettronica di Dell Data Protection | Endpoint Security Suite.

Dell Data Protection | Endpoint Security Suite

Dear **XXXXX**,

Thank you for purchasing Dell Data Protection | Endpoint Security Suite to quickly and easily protect your end users, data and reputation.

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

Download Server:	https://XXXXXXXXXX.com
Username:	XXXXXXXXXXXX
Password:	XXXXXX
Required to change password:	No
License Key:	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Support

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

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

© 2015 Dell Inc. All rights reserved.

Dell and the Dell logo are trademarks of Dell Inc. All other trademarks used herein are the property of their respective owners and are used for identification purposes only.



0XXXXXA0X

