Dell Data Guardian

Guida dell'amministratore Windows, Mac, Mobile e Web v2.0

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 dell'amministratore Windows, Mac, Mobile e Web

2018 - 08

Rev. A01

Sommario

1

Introduzione

Tutte le informazioni sui criteri e le relative descrizioni sono reperibili nella Guida dell'amministratore.

Prima di iniziare

1 Installare il Dell Server prima di procedere con la distribuzione dei client. Individuare la guida corretta come mostrato di seguito, seguire le istruzioni, quindi tornare a questa guida.

- *Guida alla migrazione e all'installazione di Security Management Server*
- *Guida introduttiva e all'installazione di Security Management Server Virtual*
- Verificare che i criteri siano impostati come desiderato. Sfogliare la Guida dell'amministratore, disponibile da **?** nella parte in alto destra della schermata. La Guida dell'amministratore è una guida a livello di pagina progettata per aiutare l'utente a impostare e modificare i criteri e comprendere le opzioni a disposizione con il Dell Server.

2 Leggere attentamente il capitolo Requisiti del presente documento.

3 Distribuire i client agli utenti.

Contattare Dell ProSupport

Per assistenza telefonica sui prodotti Dell, chiamare il numero 877-459-7304, interno 4310039, 24h su 24, 7 giorni su 7.

Inoltre, il supporto online per i prodotti Dell è disponibile all'indirizzo dell.com/support. L'assistenza online comprende driver, manuali, consulenze tecniche, FAQ e problemi emergenti.

Assicurarsi di avere a portata di mano il codice di matricola o il codice di servizio rapido per essere messi rapidamente in contatto con l'esperto tecnico più adatto.

Per i numeri di telefono al di fuori degli Stati Uniti, vedere Numeri di telefono internazionali di Dell ProSupport.

2

Requisiti

Dell Server

Data Guardian per Windows, Mac e dispositivi mobili richiede Security Management Server o Security Management Server Virtual v9.6 o successiva. Il client Web Data Guardian richiede Security Management Server o Security Management Server Virtual v9.8 o successiva. Ai fini del presente documento, entrambi i server sono indicati come Dell Server, a meno che non sia necessario indicare una versione specifica (ad esempio, se una procedura è diversa quando si utilizza Security Management Server Virtual).

Data Guardian per Windows

- Durante la distribuzione è opportuno seguire le procedure consigliate. In queste procedure sono compresi, a titolo esemplificativo, ambienti di testing controllati per i test iniziali e distribuzioni scaglionate agli utenti.
- L'account utente che esegue l'installazione/l'aggiornamento/la disinstallazione deve essere un utente amministratore del dominio o locale, che può essere assegnato temporaneamente tramite uno strumento di distribuzione, ad esempio Microsoft SMS o Dell KACE. Non sono supportati gli utenti non amministratori con privilegi elevati.
- Prima di iniziare l'installazione/la disinstallazione, eseguire il backup di tutti i dati importanti.
- Durante l'installazione non apportare modifiche al computer, quali l'inserimento o la rimozione di unità esterne (USB).
- Data Guardian è supportato con alcune versioni specifiche di Microsoft Office 2016 e di Microsoft Office 365 Business e Business Premium. Non è supportato nel caso di Office 365 Business Essentials.
- Per la crittografia cloud, il computer deve disporre di un'unità disco assegnabile (valore letterale).
- Verificare che i dispositivi di destinazione siano in grado di connettersi a https://yoursecurityservername.domain.com:8443/cloudweb/register e https://yoursecurityservername.domain.com:8443/cloudweb.
- Prima di distribuire Data Guardian, è consigliabile non configurare account di archiviazione cloud nei dispositivi di destinazione.

  Se gli utenti finali decidono di mantenere gli account esistenti, devono assicurarsi che i file che devono rimanere *decrittati* vengano rimossi dal client di sincronizzazione prima dell'installazione di Data Guardian.
- Gli utenti dovranno riavviare il computer al termine dell'installazione del client.
- Data Guardian non interferisce con il comportamento dei client di sincronizzazione. Prima di distribuire Data Guardian, gli amministratori e gli utenti dovranno pertanto familiarizzare con le modalità di funzionamento di queste applicazioni. Per maggiori informazioni, consultare il supporto di Box all'indirizzo https://support.box.com/home, il supporto di Dropbox all'indirizzo https://www.dropbox.com/help o il supporto di OneDrive all'indirizzo http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- I documenti di Office protetti sono supportati da Mozy, una soluzione complementare di Data Guardian e da altri prodotti di archiviazione NFS, e-mail e cloud.
- Se si utilizza Office 2010: se sono stati configurati criteri per proteggere i documenti Office e i documenti con attivazione macro, gli utenti devono disporre di Office 2010 Service Pack 1 o versioni successive (v14.0.6029 o versioni successive). Vedere https://support.microsoft.com/en-us/kb/2121559 per determinare se è stato applicato un Service Pack alla suite Microsoft Office 2010. Senza questo aggiornamento, i documenti protetti non sono accessibili. I nuovi documenti Office non sono protetti, a prescindere dal criterio attivo, a meno che non sia abilitata la funzionalità di scansione. La scansione successiva converte i documenti Office in file protetti, ma gli utenti non potranno accedervi senza una versione supportata di Office.
- Sebbene Dell Encryption non sia necessario, se utilizzato, il client di crittografia deve essere nella versione v8.12 o successiva.
- Data Guardian non supporta lo strumento di ripristino del sistema di Windows, né il programma Windows Insider Preview.
- La funzione Reindirizzamento cartelle di Microsoft non è supportata con Data Guardian.
- IPv6 non è supportato con la cifratura su cloud.
- Visitare periodicamente dell.com/support per la documentazione più recente e i suggerimenti tecnici.

Prerequisiti

Se non è già stato installato, il programma di installazione installa Microsoft Visual C++ 2015 Redistributable Package (x86 e x64).

N.B.:

Per Windows 7 e Windows 8.1, i computer devono essere aggiornati con Windows Updates. Per ulteriori informazioni, vedere https://support.microsoft.com/en-us/help/2919355 e https://support.microsoft.com/en-us/help/2999226.

Microsoft .Net 4.5.2 (o versioni successive) è necessario per Data Guardian. Tutti i computer spediti dalla fabbrica Dell sono dotati di .Net 4.5.2 preinstallato. Tuttavia, se non si installa Data Guardian sull'hardware Dell oppure se lo si aggiorna su un hardware Dell precedente, è necessario verificare quale versione di .Net è installata e aggiornarla, se necessario, prima di installare Data Guardian per evitare errori di installazione o di aggiornamento. Per verificare la versione di Microsoft .Net installata, seguire queste istruzioni nel computer destinato all'installazione: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Per installare Microsoft .Net Framework 4.5.2 , accedere a https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Hardware

I requisiti hardware minimi devono soddisfare le specifiche minime del sistema operativo. La tabella seguente descrive in dettaglio l'hardware supportato per il client Windows.

Hardware per Windows

- 200 MB di spazio libero su disco, a seconda del sistema operativo
- Scheda di interfaccia di rete 10/100/1000 o Wi-Fi
- TCP/IP installato e attivato

Se la vostra azienda crittografa i dati per l'archiviazione in ambienti cloud, il computer deve avere una lettera dell'alfabeto disponibile da assegnare a un'unità disco.

Sistemi operativi

La tabella seguente descrive in dettaglio i sistemi operativi supportati.

Sistemi operativi Windows (a 32 e 64 bit)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro dalla versione 1607 (Anniversary Update/Redstone 1) alla versione 1803 (Spring Creators Update/Redstone 4)

N.B.:

Il client deve trovarsi su uno di questi sistemi operativi altrimenti verrà bloccato. Se necessario, un'impostazione in una chiave di registro consente all'amministratore di ignorare il blocco.

Per il supporto Redstone 4, è necessario aggiornare l'agente prima del sistema operativo.

N.B.:
Data Guardian non è compatibile con Windows Defender Exploit Guard (WDEG) di Microsoft in Redstone 3 e versioni successive o con Enhanced Mitigation Experience Toolkit (EMET) di Microsoft in Redstone 2 e versioni precedenti.

Windows 7 non è supportato con il criterio di georilevazione per gli eventi di controllo di Data Guardian.

Data Guardian non supporta più versioni di Office su un unico computer.

Provider di archiviazione cloud

La tabella seguente descrive in dettaglio i provider di archiviazione cloud che funzionano con Data Guardian per Windows. Gli aggiornamenti dei provider di archiviazione cloud sono rilasciati frequentemente. Dell consiglia di eseguire un test sulle nuove versioni con Data Guardian prima di introdurle nell'ambiente di produzione.

Provider di archiviazione cloud
• Dropbox • Dropbox for Business (solo Windows) **N.B.:** A seconda della versione del Dell Server usato dall'azienda, tutti i file e le cartelle presenti negli account Dropbox personali che sono collegati agli account aziendali potrebbero essere crittografati. • Box **N.B.:** Data Guardian non supporta gli strumenti di Box e la funzione di modifica di Box. L'uso degli strumenti di Box può causare la comparsa di una schermata blu. • Google Drive **N.B.:** La funzione Backup e sincronizzazione di Google non è supportata. • OneDrive • OneDrive for Business • Unified OneDrive **N.B.:** Unified OneDrive è un client di sincronizzazione unificato per OneDrive e OneDrive for Business.

Microsoft Office

Data Guardian supporta le seguenti versioni di Office. È necessario, tuttavia, installare solo una versione di Office.

Microsoft Office
• Office 2010 SP2 • Office 2013 SP1

Microsoft Office

- Office 2016
- Office 365 ProPlus: Deferred 1705, Semi-Annual 1708, e Monthly 1803

Data Guardian per Mac

Nella tabella seguente, è elencato l'hardware supportato per il client Mac.

Hardware Mac

- Processore Intel Core 2 Duo, Core i3, Core i5, Core i7 o Xeon
- 2 GB RAM
- 10 GB di spazio libero su disco

Sistemi operativi

Nella tabella seguente, sono elencati i sistemi operativi supportati.

Sistemi operativi Mac

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6

Provider di archiviazione cloud

In base alle impostazioni dei criteri, è possibile che nell'interfaccia di Data Guardian per Mac vengano visualizzati i seguenti provider. Non è necessario che l'utente scarichi o installi il client di sincronizzazione cloud.

Provider di archiviazione cloud

- Dropbox
- Box
- Google Drive
- OneDrive
- OneDrive for Business

Applicazione Data Guardian per dispositivi mobili

Di seguito sono elencati i sistemi operativi supportati con l'applicazione Data Guardian per dispositivi mobili.

Sistemi operativi Android

- 4.4-4.4.4 KitKat
- 5.0-5.1.1 Lollipop
- 6.0-6.0.1 Marshmallow
- 7.0-7.1.2 Nougat
- 8.0-8.1 Oreo

Sistemi operativi iOS

- iOS 9.x
- iOS 10.x-10.3
- iOS 11-11.3

Data Guardian per il Web

Per abilitare il client Web Data Guardian, l'amministratore imposta una macchina virtuale che ospita il client Web e comunica con Dell Server v9.8 o versione successiva.

Per distribuire il client Web Data Guardian è possibile utilizzare i seguenti ambienti virtualizzati.

Ambienti virtualizzati

- VMware ESXi 6.0
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - Non sono richiesti sistemi operativi
  - Visitare http://www.vmware.com/resources/compatibility/search.php per un elenco completo di sistemi operativi host supportati
  - L'hardware deve essere conforme ai requisiti minimi VMware
  - Almeno 4 GB di RAM per la risorsa immagine dedicata
  - Per maggiori informazioni, visitare il sito http://pubs.vmware.com/vsphere-60/index.jsp
- VMware ESXi 5.5
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - Non sono richiesti sistemi operativi
  - Visitare http://www.vmware.com/resources/compatibility/search.php per un elenco completo di sistemi operativi host supportati

Ambienti virtualizzati

- L'hardware deve essere conforme ai requisiti minimi VMware
- Almeno 4 GB di RAM per la risorsa immagine dedicata
- Per maggiori informazioni, visitare il sito http://pubs.vmware.com/vsphere-55/index.jsp

Browser Web

È possibile utilizzare Data Guardian con Internet Explorer, Mozilla Firefox, Google Chrome e Microsoft Edge.

Per Mac, è supportato anche Safari.

Supporto lingue

Questi client sono compatibili con l'interfaccia utente multilingue (MUI) e supportano le seguenti lingue.

Supporto lingue

- EN - Inglese
- ES - Spagnolo
- FR - Francese
- IT - Italiano
- DE - Tedesco
- JA - Giapponese
- KO - Coreano
- PT-BR - Portoghese (Brasile)
- PT-PT - Portoghese (Portogallo)

3

Configurare e installare Data Guardian su Windows

Impostazioni di registro del client Data Guardian

Questa sezione descrive in dettaglio tutte le impostazioni di registro approvate da Dell ProSupport per i computer client locali, indipendentemente dal motivo di tale impostazione. Se un'impostazione di registro è sovrapposta in due prodotti, viene elencata in ciascuna categoria.

Queste modifiche di registro devono essere effettuate solo da parte degli amministratori e potrebbero non essere appropriate o non funzionare in tutti gli scenari.

- Per favorire la risoluzione dei problemi, è possibile aumentare i livelli di registrazione. Creare o modificare la seguente impostazione di registro:

  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  "LogVerbosity"=dword:0x1f (31)

  Per impostazione predefinita, il livello di registrazione è 0xf (15).

  Valori disponibili:

  Disattivato = 0x0 (0)

  Critico = 0x1 (1)

  Errore = 0x3 (3)

  Avviso = 0x7 (7)

  Informazioni = 0xf (15)

  Debug = 0x1f (31)

- Dopo l'installazione di Data Guardian, gli utenti interni sono attivati automaticamente. Se necessario, è possibile modificare un'impostazione di registro per escludere l'attivazione automatica.
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  Valore DWORD: DisableAutomaticActivation=1

  N.B.:
  Inoltre, è possibile confermare gli alias per il dominio sul Dell Server. Vedere Risoluzione dei problemi di attivazione automatica.

Configurare il server per Data Guardian

In base ai criteri impostati dall'amministratore, Data Guardian consente di proteggere i dati nei seguenti modi:

- Documenti Office memorizzati localmente, condivisi con altri utenti in vari modi, o archiviati su supporti rimovibili. Questi documenti Office possono essere protetti: .docx, .pptx, .xlsx .docm, .pptm, .xlsm, .pdf.
- Sistemi di condivisione di file basati su cloud - I computer o i dispositivi mobili Windows acquisiscono dati destinati all'archiviazione cloud, crittografano i dati, quindi caricano i dati crittografati nel cloud.

Informare gli utenti se la propria azienda utilizza Data Guardian solo con l'archiviazione cloud, solo con i documenti Office, o con entrambi.

Configurare Dell Security Management Server Virtual per Data Guardian

Per configurare Dell Security Management Server Virtual in modo che supporti Data Guardian, nella Management Console, impostare uno o entrambi i criteri Data Guardian su **Attivato**:

- *Documenti Office protetti* - Solo a livello aziendale
- *Crittografia cloud* - Livello azienda, gruppi di endpoint o endpoint

Configurare Dell Security Management Server per Data Guardian

Per configurare Dell Security Management Server in modo che supporti Data Guardian, nella Management Console, impostare uno o entrambi i criteri Data Guardian su **Attivato**:

- *Documenti Office protetti* - Solo a livello aziendale
- *Crittografia cloud* - Livello azienda, gruppi di endpoint o endpoint

Quindi Configurare il Security Server per consentire i download dei client per il cloud.

Configurare il Security Management Server per consentire i download di Data Guardian

Questa sezione descrive in dettaglio la procedura necessaria per consentire agli utenti di scaricare Data Guardian per il client Windows da Security Management Server.

1 In Security Management Server, accedere a *<directory di installazione di Security Server>\webapps\root\cloudweb\brand\dell \resources* e aprire il *file messages.properties* con un editor di testo.

2 Verificare che le voci siano impostate come segue:

download.deviceWin.mode=remote

download.deviceWin.local.filename.32=DataGuardian_32bit_setup.exe

download.deviceWin.local.filename.64=DataGuardian_64bit_setup.exe

3 Modificare le voci nel modo seguente

download.deviceWin.remote.link.32=https://<URL DELL'HOST IN USO>:<PORTA>/cloudweb/download/DataGuardian_32bit_setup.exe

download.deviceWin.remote.link.64=https://<URL DELL'HOST IN USO>:<PORTA>/cloudweb/download/DataGuardian_64bit_setup.exe

4 Salvare e chiudere i file.

5 Accedere alla <directory di installazione di Security Server> e al suo interno creare una nuova cartella di nome Download (Security Server\Download).

6 Nella cartella Download, creare un'altra nuova cartella e denominarla cloudweb (Security Server\Download\cloudweb).

7 Aggiungere nella cartella cloudweb i file di installazione a 64 e a 32 bit per Data Guardian e, opzionalmente, rinominarli rispettivamente, ad esempio, come DataGuardian64.exe e DataGuardian32.exe.

Questi sono definiti dall'utente, ma devono corrispondere ai nomi file nel file versions.xml.

8 Riavviare Security Server per rendere effettive le modifiche.

Configurare Security Management Server per i download automatici del client Windows Data Guardian (facoltativo)

Per i download automatici, il file versions.xml e i file binari devono trovarsi nello stesso percorso. Il percorso deve essere accessibile dal client, perciò potrebbe essere IIS oppure è possibile utilizzare la cartella **Security Server\Download\cloudweb** creata. Se si utilizza la cartella cloudweb, seguire questa configurazione di esempio.

1 Accedere alla cartella **Security Server\Download\cloudweb** (vedere il passaggio 6 in Configurare Security Server per consentire i download del client di Data Guardian).

2 Creare una cartella sotto denominata DataGuardianUpdate.

N.B.:

In questo esempio viene utilizzato DataGuardianUpdate, ma è possibile scegliere qualsiasi nome.

3 Copiare nella cartella DataGuardianUpdate i file eseguibili aggiornati.

4 Creare un file *versions.xml* nella cartella DataGuardianUpdate.

5 Aprire il file *versions.xml* in un editor di testo e verificare che il percorso del file sia corretto per il proprio ambiente.

Esempio:

```
<?xml version="1.0"?>
<VERSIONS>
<VERSION arch="x86" product="sl" version="0.x.x.xxxx" filename="/setup32.exe"/>
<VERSION arch="x64" product="sl" version="0.x.x.xxxx" filename="/setup64.exe"/>
</VERSIONS>
```

Version: versione dei file eseguibili aggiornati

Nome file setup.exe: il nome di configurazione dei file eseguibili è definito dall'utente, ma deve corrispondere al nome di configurazione nel file messages.properties (vedere il passaggio 3 in Configurare Security Server per consentire i download del client di Data Guardian).

6 Salvare e chiudere i file.

7 Aggiungere i file binari a questa cartella.

8 Se si utilizza IIS, riavviarlo.

9 Eseguire l'accesso alla Management Console come amministratore Dell.

10 Nel riquadro di sinistra, fare clic su **Popolamenti** > **Azienda**: viene visualizzata la scheda Criteri di protezione.

11 Nel gruppo di tecnologie Data Guardian, fare clic su **Crittografia cloud** > **Mostra impostazioni avanzate**.

12 Scorrere fino al criterio *URL server di aggiornamento software* e immettere **https://<YOUR HOST URL> /DataGuardianUpdate**.

N.B.:

DataGuardianUpdate viene utilizzato solo per coerenza con l'esempio precedente.

13 Fare clic su **Salva** per archiviare le modifiche ai criteri nella coda per il commit.

14 Fare clic su **Gestione** > **Esegui commit**.

15 Immettere un commento e fare clic su **Commit criteri**.

Ricreare l'immagine del computer con Data Guardian

Se è necessario ricreare l'immagine del computer che dispone di Data Guardian, chiedere se l'utente ha lavorato offline e ha creato eventuali documenti Office protetti in modalità offline. In tal caso, le chiavi offline sono state generate per quei documenti e quelle chiavi non sono state depositate nel database del Dell Server.

1 Per informazioni sul ripristino delle chiavi di Data Guardian generate offline e non depositate nel database del Dell Server, consultare la *Guida al ripristino*.

2 Verificare la presenza di una cartella con chiavi offline prima di ricreare l'immagine del computer.

Quando vengono create le prime chiavi depositate, viene aggiunta una cartella Data Guardian a C:\Programmi\Dell. Accedere alla cartella Data Guardian > Chiavi offline. Se la cartella Chiavi offline non esiste,a controllare la cartella Documenti dell'utente.

Disattivazione di Exploit Guard o EMET di Microsoft per le applicazioni gestite

In Windows 10, le seguenti funzionalità possono essere attivate o integrate nel sistema operativo:

- Redstone 3 e versioni successive: Windows Defender Exploit Guard (WDEG)
- Redstone 2 e versioni precedenti: Enhanced Mitigation Experience Toolkit (EMET)

Se queste funzionalità sono attive o integrate, è necessario configurare le relative impostazioni in modo da disattivare le applicazioni gestite per Data Guardian:

- winword.exe
- powerpnt.exe
- excel.exe
- acrord32.exe

Windows Defender Exploit Guard (WDEG)

Per disattivare le applicazioni gestite:

1 Andare a **Windows Defender Security Center**.

2 Fare clic su **Controllo delle app e del browser**.

3 Scorrere fino alla fine della schermata e fare clic su **Impostazioni di protezione dagli exploit**.

4 Selezionare **Impostazioni programmi**.

5 Fare clic su **+** per aggiungere ogni applicazione gestita elencata qui sopra.

6 In Proprietà per ogni applicazione gestita, selezionare la casella di controllo *Sostituisci* per qualsiasi opzione impostata su *Attivo*, quindi disattivare l'opzione selezionando **Disattivato**.

N.B.:
Se un'applicazione gestita è aperta e una finestra di dialogo indica che è necessario riavviare il file .exe, riavviarlo dopo aver completato questi passaggi.

7 Fare clic su **Applica**.

8 Fare clic su **Sì**.

In Impostazioni programmi, l'applicazione gestita elenca le sostituzioni delle opzioni modificate.

Enhanced Mitigation Experience Toolkit (EMET)

Per disattivare le applicazioni gestite:

1 Andare a **Configurazione applicazioni**.

2 Nelle opzioni **ROP Caller Check (Controllo chiamante ROP)** e **Export Address Table Address Filter (EAF) (Esporta filtro indirizzi di tabella indirizzi)**, deselezionare le caselle di controllo per le applicazioni gestite elencate qui sopra.

Gestire i profili dei provider di protezione dell'archiviazione cloud

Data Guardian crittografa i file degli utenti e invia gli eventi di controllo a Dell Server. Per modificare il comportamento per ciascun provider di archiviazione cloud supportato, impostare ciascuno sui valori seguenti:

Valore	Descrizione
Proteggi	consente il provider/la connessione, crittografa i file, invia eventi di controllo relativi all'attività di file/cartelle.
Blocca	Per bloccare completamente l'accesso al provider/alla connessione.
Consenti	consente di utilizzare il provider/la connessione senza crittografia, ma controlla l'attività di file/cartelle.
Ignora	ignora la protezione del provider/della connessione senza crittografia né controllo. Quando è impostato questo valore, la cartella del provider di archiviazione cloud non viene visualizzata nell'unità virtuale di Data Guardian nel computer client.

Per maggiori informazioni, consultare la *Guida dell'amministratore* disponibile nella Remote Management Console del Dell Server.

Consentire/Negare gli utenti presenti nelle liste nere/bianche

È possibile determinare quali utenti esterni possono eseguire la registrazione con Dell Server per utilizzare Data Guardian. Per ragioni di sicurezza, accertarsi di configurare e gestire con attenzione questi elenchi.

- Un utente interno è all'interno del dominio.
- Un utente esterno è un utente non del dominio, una persona di un'altra organizzazione con cui un utente interno vuole condividere documenti aziendali sensibili o un utente interno che desidera accedere al computer da un dispositivo non di dominio.

Per consentire a un utente che non è presente nel dominio dell'organizzazione di registrarsi per l'utilizzo di Data Guardian:

1 Nel riquadro sinistro della console di gestione remota, fare clic su **Gestione > Gestione utenti esterni**.

2 Fare clic su **Aggiungi**.

3 Selezionare Tipo di accesso per la registrazione:

Lista nera: blocca la registrazione per un utente o un dominio. L'utente non è in grado di aprire un documento Office protetto o un file .xen.

Elenco accesso completo: consente la registrazione e l'accesso ai file per un utente o un dominio. Se l'utente o il dominio è presente anche nella lista nera, l'accesso non viene autorizzato.

4 Nel campo Immetti dominio/indirizzo e-mail, immettere il dominio dell'utente per impostare l'accesso per l'intero dominio o l'indirizzo e-mail per impostare l'accesso solo per tale utente.

N.B.: Per gli utenti mobili esterni in un ambiente ospitato, l'indirizzo e-mail deve essere in lettere minuscole.

5 Fare clic su **Aggiungi**.

Per ulteriori informazioni sull'uso della lista ad accesso completo/lista nera, consultare la *Guida dell'amministratore* accessibile dalla Management Console.

Installare Data Guardian

Vi sono due metodi per eseguire l'installazione di Data Guardian:

- Installazione di Data Guardian in modo interattivo
- Installazione di Data Guardian con riga di comando

Gli utenti di Data Guardian devono seguire le seguenti procedure al fine di proteggere file e cartelle inseriti nei propri client di sincronizzazione cloud. Dopo l'installazione di Data Guardian, gli utenti devono scaricare un provider di archiviazione cloud:

- L'amministratore deve specificare quale provider di sincronizzazione del cloud usare.

  Oppure
- Fornire agli utenti un collegamento per scaricare e installare Dropbox for Business o OneDrive for Business/Unified OneDrive qualora l'azienda utilizzi uno di questi due provider. Ricordare che gli utenti Dropbox for Business devono connettersi a Dropbox for Business attraverso Data Guardian.

Cartelle preesistenti con file non crittografati

Al momento di distribuire Data Guardian, è consigliabile non configurare account di archiviazione cloud nei dispositivi di destinazione.

Se un provider di archiviazione cloud è configurato con cartelle che sono sincronizzate con il computer locale prima dell'installazione di Data Guardian:

- File e cartelle preesistenti che vengono sincronizzati con il cloud rimangono in chiaro
- I file aggiunti a quelle cartelle preesistenti rimangono in chiaro
- Il file sincronizzati dal cloud sono crittografati

  Se si desidera che i file pre-esistenti siano crittografati, accedere all'Disco virtuale DDG VDisk (creata al momento dell'installazione di Data Guardian), creare una nuova sottocartella all'interno del client di sincronizzazione cloud, e spostare la pre-i file esistenti in quella cartella.

  Oppure

  Per contenuti di grandi dimensioni, un manager o l'amministratore può richiedere temporaneamente il menu Gestione cartelle.

Menu Gestione cartelle

Alcuni manager o amministratori potrebbero dover eseguire una risoluzione temporanea dei problemi delle cartelle condivise da più utenti. È possibile richiedere all'amministratore l'autorizzazione per l'opzione Gestione cartelle. In genere, si tratta di un'opzione temporanea.

Installare Data Guardian in modo interattivo su Windows

Per installare Data Guardian, è necessario essere amministratore locale. Se gli utenti non potranno installare il prodotto, informarli della posizione dei supporti di installazione.

Prima di iniziare

A seconda del server e del prodotto Data Guardian, effettuare le operazioni riportate di seguito:

Dell Security Center ospitato	Locale (per Dell Management Server)	Crittografia cloud
Per future release.	Accertarsi di conoscere il nome di Dell Security Management Server.	Il computer deve avere una lettera dell'alfabeto disponibile da assegnare a un'unità disco.

Installare Data Guardian

Il computer dovrà essere riavviato dopo l'installazione di Data Guardian.

1 Per scaricare il programma di installazione di Data Guardian, accedere alla posizione specificata dall'amministratore.

2 In base al sistema operativo in uso, selezionare il programma di installazione a 32 bit o a 64 bit, in genere **setup32.exe** o **setup64.exe**, e copiarlo sul computer locale.

3 Fare doppio clic sul file per avviare il programma di installazione.

4 Se viene visualizzato un avviso di protezione, fare clic su **Esegui**.

5 Selezionare una lingua e fare clic su **OK**.

6 Se viene richiesto di installare Microsoft Visual C++ 2015 Redistributable Package o Microsoft .NET Framework 4.5.2 Client Profile, fare clic su **OK**.

7 Nella schermata iniziale, fare clic su **Avanti**.

8 Leggere il contratto di licenza, accettare i termini, e fare clic su **Avanti**.

9 Nella schermata Cartella di destinazione, fare clic su **Avanti** per eseguire l'installazione nel percorso predefinito: **C:\Program Files\Dell \Data Guardian\.**

In **C:**, non installare Data Guardian nelle cartelle Users o Windows o nella radice di qualsiasi unità. Verrà visualizzato un messaggio di errore.

10 Selezionare **Dell Management Server locale**:

Dell Security Center ospitato	Dell Management Server locale
Per future release.	Nel campo `Nome Dell Management Server`, immettere il nome del server con cui comunicherà questo computer, ad esempio server.domain.com. Non è necessario includere www o http(s). Queste informazioni sono fornite dall'amministratore. Non deselezionare la casella di controllo *Abilita verifica trust SSL*, a meno che l'amministratore non lo richieda.

11 Fare clic su **Avanti**.

12 Nella schermata Informazioni di Conferma Dell Management Server, confermare che l'indirizzo URL del server è corretto. Il programma di installazione aggiunge www o http(s), e la porta. Fare clic su **Avanti**.

13 Nella finestra Tipo di gestione, selezionare questa opzione:

- Utente interno - Un utente con un indirizzo e-mail nel dominio dell'azienda.

14 Fare clic su **Installa** per avviare l'installazione.

Viene visualizzata una finestra di stato che mostra l'avanzamento dell'installazione.

15 Fare clic su **Fine** quando viene visualizzata la schermata Installazione completata.

16 Fare clic su **Sì** per riavviare il sistema.

L'installazione di Data Guardian è completata.

17 Chiedere agli utenti finali di verificare l'attivazione. L'icona della barra delle applicazioni di Data Guardian dovrebbe presentare un segno di spunta verde  . A seconda del modo in cui Data Guardian viene distribuito all'interno dell'azienda, l'attivazione può non essere immediata. In caso negativo, l'utente finale deve eseguire manualmente l'attivazione. In un ambiente ospitato, un utente che esegue manualmente l'attivazione deve effettuare questa operazione ad ogni riavvio del computer o del servizio Data Guardian. Consultare la *Data Guardian User Guide* (Guida dell'utente di Data Guardian).

Installare Data Guardian con la riga di comando

- Le opzioni e i parametri della riga di comando fanno distinzione tra maiuscole e minuscole.
- È importante ricordare che tutti i valori contenenti uno o più caratteri speciali, ad esempio uno spazio nella riga di comando, devono essere racchiusi tra virgolette con escape.
- La tabella seguente descrive in dettaglio le opzioni disponibili per l'installazione.

Opzione	Significato
/V	Consente di passare variabili al file .msi all'interno di setup.exe. Il contenuto deve sempre essere racchiuso tra virgolette con testo normale.
/S	Modalità non interattiva

Opzione	Significato
/QB	Viene visualizzata una finestra di dialogo con il pulsante **Annulla** e viene richiesto di riavviare il sistema
/QB!	Viene visualizzata una finestra di dialogo senza il pulsante **Annulla** e viene richiesto di riavviare il sistema
/QN	L'interfaccia utente non viene visualizzata

- La tabella seguente descrive in dettaglio i parametri disponibili per l'installazione.

Parametri
SERVER=<ServerName> (FQDN del server Dell per l'attivazione)
ENTERPRISE=1 (utente interno)
ENABLESSLTRUST=0 (Disabilita la convalida dell'attendibilità SSL)
REBOOT=SUPPRESS (Null consente i riavvii automatici, SUPPRESS li disabilita)

Esempio di riga di comando

- Il seguente esempio consente di installare Data Guardian in modo invisibile all'utente, per un utente interno, senza convalida dell'attendibilità SSL, con i registri archiviati in C:\Library\Logs\Install.log.

```
setup.exe /S /V"/QB! REBOOT=SUPPRESS ENTERPRISE=1 SERVER=server.domain.com /L*V "c:\Library
\Logs\install.log" ENABLESSLTRUST=0"
```

Impostare l'oggetto criterio di gruppo nel controller di dominio per abilitare i diritti

- Se i client ricevono i diritti da Dell Digital Delivery, seguire queste istruzioni per impostare l'oggetto criterio di gruppo nel controller di dominio per abilitare i diritti (potrebbe non trattarsi dello stesso server in cui è in esecuzione il Dell Server).
- La workstation deve appartenere all'unità organizzativa in cui è applicato l'oggetto criterio di gruppo.
- Verificare che la porta in uscita 443 sia disponibile per comunicare con il Dell Server. Se la porta 443 è bloccata (per qualsiasi motivo), la funzione per i diritti non sarà utilizzabile.

1 Nel controller di dominio per gestire i client, fare clic su **Start** > **Strumenti di amministrazione** > **Gestione Criteri di gruppo**.

2 Fare clic con il pulsante destro del mouse sull'unità organizzativa in cui dovrebbe essere applicato il criterio e selezionare **Crea un oggetto Criteri di gruppo in questo dominio** e **crea qui un collegamento**.

3 Immettere un nome per il nuovo oggetto criterio di gruppo, selezionare (nessuno) per l'Oggetto Criteri di gruppo Starter di origine e fare clic su **OK**.

4 Fare clic con il pulsante destro del mouse sull'oggetto criterio di gruppo creato e selezionare **Modifica**.

5 Viene caricato l'editor di gestione dei criteri di gruppo. Accedere a **Configurazione computer** > **Preferenze** > **Impostazioni di Windows** > **Registro**.

6 Fare clic con il pulsante destro del mouse sul Registro e selezionare **Nuovo** > **Elemento del registro**. Completare i campi seguenti:

Azione: Create

Hive: HKEY_LOCAL_MACHINE

Percorso chiave: SOFTWARE\Dell\Dell Data Protection

Nome valore: Server

Tipo valore: REG_SZ

Dati valore: <indirizzo IP del Dell Server>

7 Fare clic su **OK**.

8 Effettuare la disconnessione e quindi accedere nuovamente alla workstation, oppure eseguire **gpupdate /force** per applicare il criterio di gruppo.

Disinstallare Data Guardian

- Se dispone di un account amministratore locale, l'**utente finale** può eseguire la disinstallazione di Data Guardian. Per informazioni, consultare la *Guida dell'utente di* Data Guardian. In questa sezione, viene illustrata la procedura amministrativa per la disinstallazione di Data Guardian.

> **IMPORTANTE: File non Office sull'Disco virtuale DDG VDisk**
> Prima di disinstallare Data Guardian, spostare eventuali file importanti in un percorso esterno all'Disco virtuale DDG VDisk. Quando Data Guardian viene disinstallato dal computer di un utente finale, i relativi file e cartelle nel cloud sono crittografati e illeggibili. Nel caso in cui un utente finale lasci l'azienda e nessun altro utente condivide tali file o cartelle, i dati sono illeggibili ma protetti (per visualizzare tali file è necessario reinstallare Data Guardian).
>
> I documenti Office protetti rimangono crittografati se si disinstalla Data Guardian. Per decrittografarli, consultare la *Guida al ripristino > Ripristino di Data Guardian.*

Disinstallazione dalla riga di comando

- Una volta estratto dal programma di installazione principale, il programma di installazione del client Data Guardian è disponibile al percorso **C:\Dell\DataGuardian_XXbit_setup.exe**.
- Nell'esempio seguente viene eseguita la disinstallazione automatica del client Data Guardian.

```
setup.exe /x /s /v" /qn"
```

Quando richiesto, riavviare il sistema.

Usare Data Guardian con Dropbox for Business

Data Guardian con Dropbox for Business offre funzionalità aggiuntive rispetto alla versione Dropbox di base.

È possibile impostare criteri per controllare le modalità di protezione di cartelle Dropbox personali e aziendali. Se la propria azienda consente l'utilizzo di account sia personali che aziendali, gli utenti finali devono conoscere la crittografia di ciascun tipo di account. Consultare Criteri per gli account aziendali e personali.

Criteri per gli account aziendali e personali

L'azienda potrebbe aver stabilito delle linee guida sull'utilizzo, da parte dei membri del team, degli account aziendali e personali, pertanto potrebbe consentire solo ad alcuni utenti di possedere entrambi gli account.

N.B.:
Se l'azienda consente l'utilizzo di account sia personali che aziendali e un utente finale sceglie di usarli entrambi, egli deve conoscere la gestione delle cartelle di entrambi i tipi di account.

La seguente tabella descrive la crittografia basata sull'impostazione del criterio *Crittografia cartelle personali Dropbox*.

Crittografia	Impostazione di criteri	Considerazioni sulla distribuzione
Crittografia di tutti i file e le cartelle personali e aziendali.	Criterio > Crittografia cartelle personali Dropbox > impostato su **Selezionato** (impostazione predefinita)	Prima della distribuzione di Data Guardian, gli utenti devono effettuare un backup dei file aziendali già esistenti presenti nelle cartelle di sincronizzazione dell'archiviazione cloud, spostandoli in percorsi esterni a tali cartelle. Gli utenti con file personali da conservare crittografati devono spostare tali file fuori dalle cartelle di sincronizzazione aziendali o rimuovere il collegamento degli account personali dai client di sincronizzazione aziendale. Una volta distribuito Data Guardian, i file e le cartelle cloud possono essere visualizzati solamente su computer o dispositivi che eseguono Data Guardian. Se una cartella personale viene crittografata involontariamente, consultare "Decrittografare le cartelle in un account personale" nella Guida dell'utente di Dell Data Guardian.
Crittografia di tutti i file e cartelle dell'account aziendale. I file e le cartelle dell'account personale non vengono crittografati.	Criterio > Crittografia cartelle personali Dropbox > impostato su **Non selezionato**	È possibile usare il criterio opzionale Messaggio crittografia cartelle personali Dropbox per visualizzare un messaggio personalizzato che ricorda agli utenti di **non** archiviare i file aziendali in account personali in quanto tali file non verranno protetti. Il messaggio viene visualizzato in queste situazioni: • Ogni volta che l'utente effettua l'accesso • Quando l'utente crea o aggiunge un nuovo file o una nuova cartella ad un account Dropbox personale Se si imposta il criterio Crittografia cartelle personali Dropbox su **Falso** per un endpoint o gruppo di endpoint, gli account personali di tutti gli utenti in tali endpoint non verranno crittografati.

Cartelle aziendali e personali

Se l'azienda dispone di Dropbox for Business e si consente agli utenti finali di avere sia cartelle aziendali che personali, è possibile eseguire rapporti per assicurarsi che tutti i file di tipo aziendale posseggano l'estensione file .xen, in caso un utente copi un file sensibile non protetto in una cartella aziendale. Vedere Risoluzione dei problemi di Data Guardian.

Visualizzazione dei report

Le informazioni relative all'ambiente Data Guardian sono disponibili nella Management Console. Selezionare **Creazione di report > Eventi di controllo** per gli eventi di controllo relativi alle cartelle client di sincronizzazione cloud e ai documenti Office protetti.

Per la conformità e il monitoraggio dei dettagli del dispositivo, dettagli Shield o eventi di controllo, vedere **Creazione di report > Gestione dei report**.

Per maggiori informazioni, consultare la *Guida dell'amministratore* disponibile nella Management Console.

Risoluzione dei problemi di Data Guardian

Usare la schermata Dettagli

La schermata *Dettagli* può essere utilizzata per la risoluzione di problemi oppure per ottenere assistenza. Per esempio:

- Se un utente crea una cartella, ma non esegue la crittografia, selezionare **Dettagli** > **File** > **Stato cartella** per verificare lo stato.
- Se un utente finale richiede assistenza, è possibile istruirlo sulla configurazione della schermata Dettagli avanzati e selezionare la scheda **Dettagli** > **Criterio**. In questa scheda è riportato un elenco dei criteri in vigore.
- Visualizzare i registri per la risoluzione dei problemi.

Usare la schermata Dettagli avanzati

- Mentre si preme **<Ctrl><Shift>**, fare clic sull'icona nell'area di notifica Data Guardian, quindi selezionare **Dettagli**.
- Oltre a File e Cartelle viene visualizzato quanto segue:

  Sicurezza: elenca la chiave, il tipo di chiave e lo stato. Questo riquadro elenca temporaneamente alcuni file Office protetti finché non vengono inviati al Dell Server. Il periodo di tempo dipende dall'intervallo di polling.

  Controllo: elenca moduli, ID utente e tipo di evento. In questo registro di controllo, le informazioni vengono messe in coda e inviate al Dell Server secondo intervalli specificati. L'amministratore può visualizzare gli **Eventi di controllo** nel riquadro a sinistra della Management Console per il controllo.

  Criterio: elenca i valori e i nomi dei criteri.

Visualizzare i file di registro

- Fare clic su **Visualizza registro** nell'angolo inferiore sinistro della schermata Dettagli.

  I file di registro sono disponibili anche nel percorso **C:\ProgramData\Dell\Data Guardian**.

  I file di registro dei documenti Office protetti si trovano nella cartella Custom.xml.

Risoluzione dei problemi di attivazione automatica

Se Data Guardian non si attiva automaticamente per diversi utenti, è possibile modificare le impostazioni di registro del client Data Guardian. È necessario inoltre verificare gli alias sul Dell Server:

1 Nella Management Console, accedere a **Popolamenti > Domini** e selezionare un dominio ed eventuali sottodomini.
2 Nella pagina Dettagli dominio, fare clic sulla scheda **Impostazioni**.
3 Nel campo *Alias*, confermare che tutti gli alias siano corretti.

Fornire diritti di Gestione cartelle temporanei

È possibile concedere a un amministratore o un utente i diritti temporanei per gestire le cartelle. Ad esempio, se gli utenti hanno caricato i file sul cloud prima dell'installazione di Data Guardian, è possibile fornire i diritti di gestione cartelle temporanei ad alcuni utenti per gestire la crittografia cartella per cartella all'interno delle cartelle client di sincronizzazione.

Per concedere i diritti di gestione delle cartelle:

1 Nella Management Console, fare clic su **Popolamenti** > **Endpoint**.
2 Cercare o fare clic su un endpoint, quindi fare clic sulla scheda **Criteri di protezione**.
3 Selezionare **Crittografia cloud**, quindi fare clic su **Mostra impostazioni avanzate**.
4 Fare clic sulla casella di controllo accanto a *Gestione cartelle attivata* per selezionare il criterio.
5 Fare clic su **Salva**.
6 Nel riquadro sinistro, fare clic su **Gestione** > **Esegui commit**.
7 Immettere un commento e fare clic su **Commit criteri**.

N.B.:
Dopo aver crittografato le cartelle, o dopo aver completato la risoluzione dei problemi, Dell consiglia di deselezionare la casella di controllo relativa al criterio *Gestione cartelle attivata*, per disabilitare il criterio per quell'endpoint.

Per gestire le cartelle sull'endpoint:

1 Creare una cartella all'interno della cartella client di sincronizzazione e aggiungere i file, in modo che i file siano crittografati nel cloud.
2 Fare clic sull'icona della barra delle applicazioni Data Guardian e selezionare **Gestione cartelle**.

   Per ogni client di sincronizzazione viene visualizzata una struttura ad albero delle cartelle sincronizzate con il cloud. Tutte le cartelle sono selezionate per impostazione predefinita. Deselezionare le cartelle che non si desidera crittografare. Se l'utente deseleziona una cartella in Gestione cartelle, una ricerca della decrittografia decrittografa i file esistenti in quella cartella. I nuovi file in quella cartella non sono crittografati nell'unità locale né nel cloud.

   N.B.:
   Se si trascina un file crittografato in una cartella deselezionata in Gestione cartelle nel cloud o nell'unità virtuale di Data Guardian, il file rimane crittografato e non è possibile visualizzarne il contenuto. Se l'utente condivide la cartella con un altro utente Data Guardian che non ha abilitato il criterio Gestione cartelle, i file rimarranno crittografati e il collega non potrà visualizzarli.

3 Per crittografare una cartella pre-esistente, attivare manualmente la crittografia per quella cartella. I file vengono crittografati una volta eseguita la loro sincronizzazione nel cloud.

FAQ - Domande frequenti

FAQ sulla gestione delle cartelle

Domanda

Ho una cartella contenente file che ho condiviso con un altro utente. Nella barra di sistema, ho usato l'utilità **Data Guardian > Gestione cartelle** per decrittografare il contenuto di quella cartella. Di recente, i miei file sono stati crittografati nuovamente nel cloud. Tale cartella non è più visualizzata nell'utilità Gestione cartelle, quindi non posso più decrittografare quei file nel cloud.

Risposta

Un ID della chiave di crittografia è associato ad una cartella basata sul primo utente che aggiunge un file in tale cartella. Se un utente crea una cartella e non aggiunge file, la chiave non è associata a tale cartella. L'utente il cui ID della chiave di crittografia è stato impostato nella cartella è l'unico che può visualizzare la cartella nell'utilità Gestisci cartelle. Se l'utente il cui ID della chiave di crittografia è stato impostato nella cartella deseleziona la cartella nell'utilità Gestione cartelle e la condivide con un altro utente Data Guardian, il Data Guardian del secondo utente ne crittograferà nuovamente il contenuto.

Soluzione

1 Creare una nuova cartella.

2 Spostare tutti i file da crittografare nella nuova cartella.

3 Nella barra di sistema, utilizzare nuovamente l'utilità **Dell Data Guardian** > **Gestione cartelle** per decrittografare questi file.

N.B.:
Se l'utente ha decrittografato il contenuto di una cartella condivisa con altri utenti di Data Guardian, il client Data Guardian dell'altro utente applicherà il criterio di crittografia. La procedura consigliata consiste nell'usare l'utilità Gestione cartelle per decrittografare solo i file non condivisi con altri utenti Data Guardian.

Domanda

Sto sincronizzando una cartella decrittografata che avevo deselezionato usando l'utilità Gestione cartelle. Tuttavia, quando provo a caricarla tramite il browser Web, riesco a caricare solo i file crittografati.

Risposta

Data Guardian non è progettato per cercare attivamente le cartelle nel cloud. Con le cartelle non crittografate, Data Guardian può effettuare la sincronizzazione tramite il client perché controlla tale ambiente. I file che accedono al browser Web devono essere crittografati.

Soluzione

Aggiungere i file alla cartella di sincronizzazione.

Domanda

Di recente ho disinstallato dal computer il sistema di condivisione dei file basato su cloud, ma quando ho aperto l'utilità Gestisci cartelle, uno dei client di sincronizzazione era ancora elencato come opzione.

Risposta

Data Guardian non controlla l'installazione o la disinstallazione di software di terze parti. Tali opzioni sono ancora elencate perché, per impostazione predefinita, al momento della disinstallazione di questi client, non vengono rimossi i file esistenti. Questi file sono ancora protetti da Data Guardian anche se il client di sincronizzazione non è più installato.

Soluzione

Per rimuovere l'opzione del client di sincronizzazione disinstallata dall'utilità Gestione cartelle, spostare eventuali cartelle/file che si desidera tenere fuori dalla cartella di sincronizzazione, quindi eliminare la cartella. Dopo la rimozione, a cartella non sarà più elencata nell'utilità Gestione cartelle.

Domande frequenti varie

Domanda

Un utente ha Data Guardian con documenti Office protetti e non può effettuare attività di copia e incolla.

Risposta

Per Data Guardian, alcune funzionalità vengono gestite tramite il systray. Controllare se l'utente ha modificato il systray.

Soluzione

È necessario utilizzare le impostazioni predefinite di systray. L'utente deve mantenere le impostazioni predefinite di systray.

Domanda

Ho modificato il criterio **Offuscamento nomi di file** da GUID a Solo estensione. Tuttavia, nelle cartelle in cui stavo eseguendo precedentemente la sincronizzazione, è ancora in esecuzione la crittografia dei file nell'altro formato con nomi di file GUID. Perché?

Risposta

Quando viene modificato un criterio nel Security Management Server/Security Management Server Virtual, Data Guardian mantiene il criterio precedente per tale cartella. Alle nuove cartelle create verrà applicato il nuovo criterio e la crittografia verrà eseguita nel formato **Solo estensione**.

Soluzione

Per riapplicare il formato **Solo estensione** ai file precedenti, tagliarli e incollarli in una nuova cartella alla quale è applicato il nuovo criterio.

Configurare e installare Data Guardian su Mac

Data Guardian per Mac è progettato per la condivisione di file nei provider di crittografia cloud. Tuttavia, se vengono attivati i criteri dei documenti Office protetti per Mac, si perderanno tutti i dati di controllo e tracciabilità se il file viene salvato dall'utente nel computer Mac locale. Se l'organizzazione richiede severi criteri di controllo e tracciabilità, deselezionare il criterio *Consenti attivazione di Data Guardian su Mac* per evitare l'attivazione di Data Guardian sui computer Mac.

Attività del server

Prerequisiti

Prima di eseguire queste attività, confermare quanto segue:

- Installare il Dell Server e i suoi componenti. Consultare una delle sezioni seguenti:
  - *Guida alla migrazione e all'installazione di Security Management Server*
  - *Guida introduttiva e all'installazione di Security Management Server Virtual*
- Nella Management Console, assegnare un appropriato ruolo di amministratore Dell.

Criteri

Per impostazione predefinita, Data Guardian crittografa i file degli utenti e invia gli eventi di controllo al Security Management Server Virtual. Ai fini del presente documento, entrambi i server sono indicati come Dell Server, a meno che non sia necessario indicare una versione specifica (ad esempio, se una procedura è diversa quando si utilizza Security Management Server Virtual).

Se si desidera che gli eventi di controllo includano i dati di georilevazione, è necessario abilitare il Wi-Fi. Per ulteriori informazioni sulla georilevazione e sugli eventi di controllo, consultare la *Guida dell'amministratore*.

Per modificare il comportamento predefinito per ciascun provider di archiviazione cloud supportato, impostare il criterio *Provider di protezione di archiviazione cloud*. Se l'azienda preferisce un provider di archiviazione cloud specifico, impostare questo criterio su **Blocca** per altri provider. Per informazioni sui criteri, consultare la *Guida dell'amministratore*, disponibile nella Console di gestione.

N.B.:
L'opzione Ignora di questo criterio è per Windows. Se viene selezionato Ignora per Mac, viene visualizzato come Consenti all'utente finale.

Configurazione di Security Server per consentire i download dei client cloud

Prima di eseguire queste attività, confermare quanto segue:

- Installare il Dell Server e i suoi componenti. Consultare una delle sezioni seguenti:
  - *Guida alla migrazione e all'installazione di Security Management Server*
  - *Guida introduttiva e all'installazione di Security Management Server Virtual*
- Nella Management Console, assegnare un appropriato ruolo di amministratore Dell.

Security Management Server

1 In Security Management Server, accedere a <directory di installazione del Security Server>\webapps\cloudweb\brand\dell\resources\

2 Aprire il file **messages.properties** con un editor di testo.

3 Verificare che le voci siano impostate come segue.
Per l'installazione **locale**:

download.deviceWin.mode=local

download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg

Per l'installazione **remota**:

```
download.deviceWin.mode=remote
```

```
download.deviceMac.remote.link=https://[NomeMacchina:IndirizzoIP]:[porta]/percorso/nomefile.dmg
```

4 Salvare e chiudere i file.

5 Accedere alla <directory di installazione di Security Server> e creare una cartella di nome Download (Security Server\Download).

6 All'interno della cartella Download, creare una cartella CloudWeb (Security Server\Download\CloudWeb).

7 Aggiungere i programmi di installazione di Dell Data Guardian a questa cartella.

Virtual Edition: installazione manuale di una versione differente del client cloud

Non è necessaria alcuna azione per consentire agli utenti di scaricare il programma di installazione più recente di Dell Data Guardian. Il programma di installazione più recente è preinstallato sul Security Management Server Virtual Security Server.

Per installare manualmente una versione differente del programma di installazione di Data Guardian sul Security Management Server Virtual Security Server, aggiornare il file message.properties.

1 Andare a:
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/

2 Aprire il file **messages.properties** con un editor di testo.
Per l'installazione **locale**:

```
download.deviceWin.mode=local
```

```
download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg
```

Per l'installazione **remota**:

download.deviceWin.mode=remote

```
download.deviceMac.remote.link=https://[NomeMacchina:IndirizzoIP]:[porta]/percorso/
nomefile.dmg
```

3 Salvare e chiudere i file.

4 Copiare i file in /opt/dell/server/security-server/download/cloudweb.

5 Aggiungere i programmi di installazione di Data Guardian a questa cartella.

Consentire/Negare gli utenti presenti negli elenchi di accesso completo/degli utenti non consentiti

Le voci degli elenchi di accesso completo e degli utenti non consentiti stabiliscono quali utenti sono autorizzati a registrarsi nel Dell Server per l'utilizzo di Data Guardian.

Elenco accesso completo

L'elenco di accesso completo permette a utenti o gruppi di utenti specifici di registrarsi nel Dell Server e utilizzare Data Guardian.

Gli utenti esterni devono essere inseriti nell'elenco di accesso completo per poter effettuare la registrazione. Seguono alcuni esempi per consentire agli utenti di registrarsi:

Tipo di utente	Immettere
Tutti gli indirizzi di posta elettronica del dominio organizzazione.com	`organization.com`
Un utente specifico	`jdoe@organization.com`
Tutti gli utenti Gmail	`gmail.com`

Elenco degli utenti non consentiti

L'elenco degli utenti non consentiti impedisce a utenti o gruppi di utenti specifici di registrarsi nel Dell Server e utilizzare Data Guardian. Gli utenti corrispondenti agli indirizzi e-mail inclusi nell'elenco degli utenti non consentiti ricevono un messaggio in cui vengono informati che non possono registrarsi a Data Guardian.

N.B.:
Se un utente è già registrato, questo elenco **non** gli impedisce di usare Data Guardian.

È possibile usare l'elenco degli utenti non consentiti per escludere determinati utenti che appartengono ai gruppi approvati nell'elenco di accesso completo. Inoltre, è possibile includere interi domini nell'elenco degli utenti non consentiti per impedire la registrazione a chiunque utilizzi un indirizzo e-mail appartenente a tale dominio. Seguono alcuni esempi per impedire a un utente o a un gruppo di utenti di registrarsi nel Dell Server:

Tipo di utente	Immettere
Tutti gli indirizzi di posta elettronica del dominio organizzazione.com	`organization.com`
Un utente specifico e quell'indirizzo di posta elettronica	`jdoe@organization.com`
Tutti gli utenti Gmail	`gmail.com`

Per modificare gli elenchi di accesso completo/degli utenti non consentiti, attenersi a queste istruzioni:

1 Nel riquadro sinistro della Remote Management Console, fare clic su **Gestione > Gestione utenti esterni**.

2 Fare clic su **Aggiungi**.

3 Selezionare Tipo di accesso per la registrazione:

Lista nera: blocca la registrazione per un utente o un dominio. L'utente non è in grado di aprire un documento Office protetto o un file .xen.

Elenco accesso completo: consente la registrazione e l'accesso ai file per un utente o un dominio. Se l'utente o il dominio è presente anche nella lista nera, l'accesso non viene autorizzato.

4 Nel campo Immetti dominio/indirizzo e-mail, immettere il dominio dell'utente per impostare l'accesso per l'intero dominio o l'indirizzo e-mail per impostare l'accesso solo per tale utente.

5 Fare clic su **Aggiungi**.

Per ulteriori informazioni sull'uso di lista ad accesso completo/lista nera, consultare la *Guida dell'amministratore*, accessibile dalla Remote Management Console del Dell Server.

Un utente esterno può richiedere l'accesso da parte di un utente interno per la chiave di un file protetto. Se l'utente interno non è disponibile, è possibile utilizzare la Remote Management Console per approvare o negare l'accesso.

1 Selezionare **Gestione > Gestione richieste chiavi**.

2 Per ulteriori informazioni, selezionare **?** (Guida).

Attività del client

Prerequisiti

- Verificare che i dispositivi di destinazione siano in grado di connettersi a:
  - https://nomesecurityserver.dominio.com:8443/cloudweb/register
  - https://nomesecurityserver.dominio.com:8443/cloudweb
- Verificare che l'utente che esegue l'installazione abbia un account amministratore locale per installare.
- Se si installa usando la riga di comando, verificare di essere in possesso del nome di dominio completo del Security Server con cui gli utenti eseguiranno l'attivazione.

Procedure consigliate

Durante la distribuzione, assicurarsi di seguire le procedure consigliate. Questo include, ma non è limitato a:

- Ambienti di testing controllati per i test iniziali
- Distribuzioni scaglionate agli utenti

Client di installazione

Ora, gli utenti che erano stati aggiunti all'elenco degli utenti consentiti possono effettuare la registrazione alla pagina: https://nomesecurityserver.dominio.com:8443/cloudweb/register.

Dopo essersi registrato, l'utente riceve un'e-mail che lo indirizza alla pagina https://nomesecurityserver.dominio.com:8443/cloudweb per effettuare l'accesso e scaricare il client appropriato.

L'installazione del client Mac è opzionale per gli amministratori, poiché gli utenti finali in genere installano il client Mac autonomamente (dopo la registrazione) dalla pagina https://yoursecurityservername.domain.com:8443/cloudweb.

Tuttavia, è possibile installare il client Mac se l'organizzazione lo richiede. Installare il client di Data Guardian tramite l'interfaccia utente o la riga di comando, utilizzando qualsiasi tecnologia push a disposizione della propria organizzazione. Sono ancora richieste la registrazione e l'attivazione da parte dell'utente finale.

Aggiornamento da versioni precedenti di Cloud Edition

Se un'azienda dispone di una versione precedente di Cloud Edition ed effettua l'aggiornamento a Data Guardian, la versione precedente di Cloud Edition viene rimossa.

N.B.:
Se l'azienda effettua l'aggiornamento da Cloud Edition per Data Guardian, gli utenti devono autenticare e ricollegare Data Guardian con il proprio provider di archiviazione cloud. Per maggiori informazioni sull'autenticazione, consultare la Guida di Dell Data Guardian online.

Opzioni di installazione

Per installare/aggiornare il client, selezionare uno dei metodi seguenti:

- Installazione interattiva - Questo è il metodo più semplice per installare Data Guardian per Mac. Tuttavia, utilizzare questo metodo solo se si intende installare il client in un computer alla volta.

  Oppure

- Installazione dalla riga di comando - Per questo metodo di installazione avanzato, gli amministratori devono aver esperienza con la sintassi della riga di comando. Questo metodo può essere utilizzato per un'installazione tramite script, utilizzando file batch o qualsiasi altra tecnologia push a disposizione della propria organizzazione.

Installazione interattiva

1. Per il client di Data Guardian, individuare il programma di installazione in **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Utilizzare il file **.pkg** in DDPSL-Explorer-0.x.x.xxxx.dmg per l'installazione o l'aggiornamento. È possibile utilizzare un'installazione tramite script, file batch o qualsiasi altra tecnologia push a disposizione della propria organizzazione.
3. Fare doppio clic sul pacchetto **Dell-Data-Guardian-x.x.x**.
4. Fare clic su **Continua**.
5. Nella finestra Introduzione, fare clic su **Continua**.
6. Nella finestra Contratto di licenza software, fare clic su **Continua**.
7. Fare clic su **Accetto**per continuare.
8. Nella finestra Tipo di configurazione, selezionare **Dell Management Server locale**.

   N.B.:
   Dell Security Center ospitato è previsto in una futura release.

9. Nella finestra Tipo di installazione, effettuare una delle seguenti operazioni:
   - Fare clic su **Installa**, quindi andare al passaggio 9.
   - Fare clic su **Modifica posizione di installazione**.
     1. Nella finestra Selezione della destinazione, selezionare tutti gli utenti o un singolo utente.
     2. Fare clic su **Continua.**
     3. Fare clic su **Installa**, quindi andare al passaggio 9
10. Nella finestra di dialogo, immettere nome e password e fare clic su **Installa software**.
11. Nella finestra Riepilogo, fare clic su **Chiudi**.
12. Vedere Attivazione dell'utente finale.

    N.B.:
    Se l'azienda effettua l'aggiornamento da Cloud Edition per Data Guardian, gli utenti devono autenticare e ricollegare Data Guardian con il proprio provider di archiviazione cloud. Per maggiori informazioni sull'autenticazione, consultare la Guida di Dell Data Guardian online.

13 Chiudere la finestra .dmg per aprire Finder.

Installazione dalla riga di comando

1 Montare il file .dmg.
2 Eseguire un'installazione del pacchetto dalla riga di comando utilizzando il comando del programma di installazione:
```
sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
```
3 Indicare agli utenti di attivare Data Guardian. Vedere Attivazione dell'utente finale.

Attivazione dell'utente finale

Dopo aver aperto Dell Data Guardian sul computer Mac per la prima volta, seguire questi passaggi:

1 Nel Finder, selezionare **Applicazioni**, e fare doppio clic su **Dell Data Guardian**.
2 Quando viene visualizzata la finestra Dell Server, immettere l'indirizzo del Dell Server e fare clic su **Salva**.

   Si apre la finestra Credenziali.
3 Immettere l'indirizzo e-mail di dominio e la password di dominio.
4 Fare clic su **Accesso** per attivare Dell Data Guardian.

   Una volta aperta l'applicazione Dell Data Guardian e completata l'attivazione, il nome del provider di archiviazione su cloud in dissolvenza viene visualizzato nel riquadro sinistro.

   Se un'azienda desidera che tutti gli utenti collaborino utilizzando lo stesso provider di servizi cloud, l'amministratore può impostare un criterio per abilitare solo quel provider e bloccare la visualizzazione degli altri.

   Se l'autenticazione dell'applicazione Dell Data Guardian è stata revocata o è scaduta, anche il nome del provider di archiviazione cloud è disattivato.

5 Nel riquadro sinistro, selezionare il provider di archiviazione cloud.

   Si apre una finestra che richiede le credenziali dell'utente. Una volta eseguita l'autenticazione, il nome del provider di archiviazione cloud risulterà attivo.

6 Per maggiori informazioni sull'autenticazione, consultare la Guida di Dell Data Guardian online.

Disinstallazione di Data Guardian

In questa sezione, viene illustrata la procedura amministrativa per la disinstallazione di Data Guardian. Per eseguire la disinstallazione, è necessario disporre di un account amministratore locale. Se dispone di un account amministratore locale, l'utente finale può eseguire la disinstallazione di Data Guardian per Mac autonomamente.

Per rimuovere Data Guardian, effettuare una delle operazioni seguenti:

Finder

1 Mentre si preme il tasto <opzione>, selezionare **Vai** dalla barra dei menu.
2 Aprire la cartella **~/Library/Application Support/Dell**.
3 Fare clic con il pulsante destro del mouse sulla cartella **DellDataGuardian** e selezionare **Sposta nel cestino**.
4 Da **Vai** nella barra dei menu, aprire la cartella Applicazioni e spostare l'applicazione **Dell Data Guardian** nel cestino.
5 Fare clic su **OK**.
6 Se richiesto, immettere la password di amministratore.

Terminale

È possibile avere Data Guardian in una o entrambe le posizioni seguenti.

1 Utilizzare i comandi indicati qui di seguito:
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Rimuovere la cartella **DellDataGuardian**.

Configurare e installare Data Guardian per il client Web

Questo client Web consente agli utenti di visualizzare un documento Office protetto o un file .xen senza dover installare il client Data Guardian. Come regola generale, Dell consiglia di installare prima Security Management Server o Security Management Server Virtual.

Scaricare il file OVA

In occasione dell'installazione iniziale, Data-Guardian-Web viene fornito come file OVA, una Open Virtual Application (Applicazione virtuale aperta) usata per fornire un software in esecuzione in una macchina virtuale.

Per scaricare il file OVA:

1 Accedere alla pagina del supporto prodotto Data Guardian.
2 Fare clic su **Driver e download**.
3 Accanto a "Visualizza tutti gli aggiornamenti disponibili per <versione sistema operativo>", fare clic su **Cambia sistema operativo** e selezionare una delle seguenti opzioni: **VMware ESXi 6.0** o **VMware ESXi 5.5**.
4 In "Visualizza per:" selezionare **Mostra tutti**.
5 In Dell Data Security, selezionare **Scarica**.

Installare Data Guardian per il Web

Installare e configurare Data-Guardian-Web

Prima di iniziare, verificare che siano soddisfatti tutti i Requisiti del sistema e dell'ambiente virtuale.

1 Individuare i file Data Guardian nel supporto di installazione e fare doppio clic su **Data-Guardian-Web-1.x.x.ova** per eseguirne l'importazione in VMware.
2 Attivare Data-Guardian-Web.
3 Selezionare la lingua per il contratto di licenza, quindi selezionare **Visualizza EULA**.
4 Leggere il contratto, quindi selezionare **Accetta EULA**.
5 Se è disponibile un aggiornamento, selezionare **Accetta**.
6 Alla richiesta di modifica della password predefinita, selezionare **Sì**.
7 Nella schermata *Imposta password ddguser* immettere la password corrente (predefinita), ossia **ddguser**, quindi immettere una password univoca, reinserire la password univoca e selezionare **OK**.

   Le password devono includere i seguenti elementi:

   - Almeno 8 caratteri
   - Almeno 1 lettera maiuscola
   - Almeno 1 cifra
   - Almeno 1 carattere speciale

8 Ripetere il passaggio precedente per gli account *ddgconsole* e *ddgsupport*.

N.B.:
Per conservare la password predefinita, che è identica al nome, fare clic su **Annulla**. Per modificare la password, immettere **ddgconsole** o **ddgsupport** nel campo Password corrente.

9 Nella finestra di dialogo *Configura nome host* utilizzare il tasto BACKSPACE per rimuovere il nome host predefinito. Inserire un nome host FQDN e selezionare **OK**.

10 Se si dispone di più nodi e di un bilanciatore del carico, immettere un nome per il bilanciatore del carico.

11 Nella finestra di dialogo *Configura impostazioni di rete*, scegliere una delle opzioni seguenti, quindi selezionare **OK**.

- (Impostazione predefinita) Usa DHCP
- (Impostazione consigliata) Nel campo usa DHCP, premere la barra spaziatrice per rimuovere la X e inserire manualmente questi indirizzi, se applicabili: IP statico Network mask Gateway predefinito Server DNS 1 Server DNS 2 Server DNS 3

N.B.:
Quando si usa un IP statico, è necessario creare anche una voce host nel server DNS.

12 Quando viene visualizzata la schermata scp, non fare clic su OK. Aggiungere prima i file .cer e .key all'applicazione o estrarla dal file .pfx o .p7b di CA. Consultare la sezione Utilizzo dello strumento WinSCP.

N.B.:
Se si fa clic su OK nella schermata SCP prima di estrarre i file, è necessario riavviare Data-Guardian-Web e navigare nella finestra di dialogo *Configura impostazioni di rete*.

Utilizzo dello strumento WinSCP

In Windows, utilizzare l'account ddgconsole per copiare tramite scp il file del certificato SSL e il file della chiave SSL.

1 In Windows, aprire lo strumento WinSCP.

2 Nella pagina WinSCP, immettere il nome host.

3 Immettere il nome utente ddgconsole predefinito e la password predefinita (oppure nome utente e password modificati).

4 Fare clic su **Accedi**.

5 Trascinare il certificato e la chiave, il file .pfx o il file .p7b, dall'unità locale alla directory **opt/dell/files**.

6 Se è stato aggiunto un file .pfx o un file .p7b, immettere una password quando richiesto. Il certificato e la chiave vengono estratti da CA e aggiunti in **apache2/ssl/folder**.

In alternativa, invece di trascinare il file .pfx o .p7b, è possibile estrarre manualmente il certificato. Ecco un codice di esempio:

```
openssl pkcs12 -in domain.pfx -clcerts -nokeys -out domain.cer
```

Qui di seguito è riportato un codice di esempio per l'estrazione della chiave privata dal file .pfx:

```
openssl pkcs12 -in domain.pfx -nocerts -nodes -out domain.key
```

7 Tornare alla schermata scp della Console di amministrazione.

Console di amministrazione

Nella schermata scp della Console di amministrazione:

1 Fare clic su **OK**. Si apre la schermata *Installazione certificato Apache2 Reverse Proxy*, in cui è elencato il certificato.

2 Selezionare un certificato e premere **Invio**.

3 Eseguire una delle azioni seguenti:

- Se è stata aggiunta una chiave nello strumento WinSCP, selezionare la chiave nella schermata successiva e premere **Invio**.
- Se è stata immessa una password nello strumento WinSCP per un file .pfx o .p7b, immettere la password quando richiesto e fare clic su **OK**.

4 Nella schermata Imposta Dell Server, immettere il nome host del server e fare clic su **OK**. Viene visualizzata una finestra di dialogo contenente un URL da utilizzare per il provisioning. Il formato dell'URL è il seguente: **https://node.domain.com/edap-admin-ui/provision_node**.

N.B.:
node.domain.com è il nome immesso in *Configura nome host*. L'URL punta a tale nodo.

5 Aprire un browser e digitare l'URL indicato.

6 Quando viene visualizzata la pagina di provisioning del nodo Dell Data Guardian, fare clic su **Avvio provisioning del nodo**.

7 Nella pagina di accesso, immettere l'indirizzo e-mail di dominio e la password, quindi fare clic su **Accedi**. La finestra di dialogo di Dell Data Guardian conferma che il provisioning è stato completato correttamente.

8 Tornare alla schermata Console di amministrazione in cui è elencato il proprio URL e fare clic su **OK**. Il server delle applicazioni viene riavviato e viene visualizzato il menu principale della console di amministrazione.

Attività aggiuntive:

- Fornire l'URL agli utenti interni per consentire loro di accedere al client Web Data Guardian.
  - Per un nodo singolo, il formato dell'URL è il seguente: **https://nomenodo/** dove il nome del nodo corrisponde al nome host immesso nella schermata Configura nome host.
  - Per più nodi, il formato dell'URL è il seguente: **https://nomebilanciatorecarico/** dove il nome del nodo corrisponde al nome host del bilanciatore del carico immesso nella schermata Configura nome host.
- Per accedere al server in futuro per eseguire gli aggiornamenti di questa macchina virtuale o per controllare i registri, è necessario abilitare SSH per la macchina virtuale. Selezionare **Configurazione base > Impostazioni SSH** per abilitare SSH per un utente ddgsupport.
- Nella Management Console, se si modifica un qualsiasi criterio del portale Web basato sul nodo, è necessario riavviare l'applicazione. Vedere Riavviare l'applicazione. Dopo il riavvio, è necessario eseguire l'accesso con le credenziali ddguser.

Aprire la Management Console

Aprire la Management Console all'indirizzo: https://server.domain.com:8443/webui/

Le credenziali predefinite sono **superadmin/changeit.**

Per l'accesso alla Management Console, sono supportati i seguenti browser Web:

- Internet Explorer 11.x o versione successiva
- Mozilla Firefox 41.x o versione successiva
- Google Chrome 46.x o versione successiva
- Safari

Attività di configurazione del terminale di base di Data Guardian

Le operazioni di configurazione di base sono accessibili dal menu principale.

Modificare il nome host

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare a utilizzare .

1 Dal menu *Configurazione di base*, selezionare **Nome host**.

2 Utilizzare il tasto BACKSPACE di rimuovere il nome host Data-Guardian -Web esistente, quindi sostituirlo con un nuovo nome host e selezionare **OK**.

Modificare le impostazioni di rete

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare a utilizzare .

1 Dal menu *Configurazione di base*, selezionare **Rete**.
2 Nella schermata *Configura impostazioni di rete*, scegliere una delle opzioni seguenti, quindi selezionare **OK**.
   - (Impostazione predefinita) Usa DHCP (IPv4).
   - (Impostazione consigliata) Nel campo Usa DHCP, premere la barra spaziatrice per rimuovere la X e inserire manualmente questi indirizzi, se applicabili:

     IP statico

     Network mask

     Gateway predefinito

     Server DNS 1

     Server DNS 2

     Server DNS 3

     È possibile selezionare IPv6 o IPv4 per una configurazione statica.

   N.B.:
   Quando si utilizza un IP statico, è necessario creare una voce host nel server DNS.

Modificare le password utente

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare a utilizzare .

È possibile modificare le password dei seguenti utenti:

- ddguser (amministratore del terminale) - Questo utente ha accesso al terminale di Data Guardian e ai relativi menu.
- ddgconsole (accesso alla shell) - Questo utente ha accesso alla shell di Data Guardian. Un amministratore di rete ha a disposizione l'accesso alla shell per controllare e risolvere i problemi della connettività di rete.
- ddgsupport (amministratore di Dell ProSupport) - Questo utente esiste esclusivamente per l'utilizzo con Dell ProSupport. Ai fini della sicurezza, l'utente controlla la password per questo account.

1 Dal menu *Configurazione di base*, selezionare **Modifica password utente**.
2 Nella schermata *Modifica password utente*, selezionare la password utente da modificare e selezionare **Invio**.
3 Nella schermata *Imposta password*, immettere la password corrente, immettere la nuova password, immettere nuovamente la nuova password, quindi selezionare **OK**.

   Le password devono includere i seguenti elementi:

   - Almeno 8 caratteri
   - Almeno 1 lettera maiuscola
   - Almeno 1 cifra
   - Almeno 1 carattere speciale

   N.B.: Per selezionare diversi account utente, utilizzare il tasto "barra spaziatrice" sulla tastiera per visualizzare l'elenco di selezione.

Abilitare SSH

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare a utilizzare .

È possibile abilitare SSH per l'accesso come amministratore del supporto, l'accesso alla shell e l'interfaccia della riga di comando del terminale.

1 Dal menu *Configurazione di base*, selezionare **SSH**.
2 Evidenziare l'utente per il quale si desidera abilitare l'SSH, premere la barra spaziatrice per inserire una **X** e selezionare **OK**.

Avviare o arrestare i servizi

Eseguire questa operazione solo se necessario.

1 Per avviare o arrestare contemporaneamente tutti i servizi, dal menu *Configurazione di base*, selezionare **Avvia applicazione** o **Interrompi applicazione**.
2 Al prompt di conferma, selezionare **Sì**.

N.B.: Il completamento delle modifiche allo stato del server potrebbe richiedere fino a due minuti.

Riavviare l'applicazione

Eseguire questa operazione solo se necessario.

1 Dal menu *Configurazione di base*, selezionare **Riavvia applicazione**.
2 Al prompt di conferma, selezionare **Sì**.
3 Dopo il riavvio, eseguire l'accesso a Data Guardian.

Arrestare l'applicazione

Eseguire questa operazione solo se necessario.

1 Dal menu *Configurazione di base*, scorrere verso il basso e selezionare **Arresta applicazione**.
2 Al prompt di conferma, selezionare **Sì**.
3 Dopo il riavvio, eseguire l'accesso a Data Guardian.

Attività dell'amministratore

Impostare o cambiare la lingua del Terminal

La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

1 Nel menu principale, selezionare **Imposta lingua.**
2 Utilizzare i tasti freccia per selezionare la lingua preferita.

Generare un registro snapshot del sistema

Per generare un registro snapshot del sistema per Dell ProSupport, nel menu principale selezionare **Strumenti supporto.**

1 Dal menu *Strumenti supporto*, selezionare **Genera registro snapshot sistema.**
2 All'indicazione della creazione del file, selezionare **OK**.