Gestione delle chiavi di sicurezza

SANtricity 11.5

NetApp
February 12, 2024

Sommario

Gestione delle chiavi di sicurezza

Concetti

Funzionamento della funzione Drive Security

Drive Security è una funzionalità di storage array che offre un ulteriore livello di sicurezza con dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard). Quando questi dischi vengono utilizzati con la funzione Drive Security, richiedono una chiave di sicurezza per l'accesso ai dati. Quando i dischi vengono fisicamente rimossi dall'array, non possono funzionare fino a quando non vengono installati in un altro array, a questo punto, saranno in uno stato di sicurezza bloccato fino a quando non viene fornita la chiave di sicurezza corretta.

Come implementare Drive Security

Per implementare Drive Security, attenersi alla seguente procedura.

1. Dotare lo storage array di dischi sicuri, sia FDE che FIPS. (Per i volumi che richiedono il supporto FIPS, utilizzare solo dischi FIPS. La combinazione di dischi FIPS e FDE in un gruppo di volumi o in un pool comporterà il trattamento di tutti i dischi come dischi FDE. Inoltre, un disco FDE non può essere aggiunto o utilizzato come spare in un gruppo di volumi o pool all-FIPS.
2. Creare una chiave di sicurezza, ovvero una stringa di caratteri condivisa dal controller e dalle unità per l'accesso in lettura/scrittura. È possibile creare una chiave interna dalla memoria persistente del controller o una chiave esterna da un server di gestione delle chiavi. Per la gestione esterna delle chiavi, è necessario stabilire l'autenticazione con il server di gestione delle chiavi.
3. Abilitare Drive Security per pool e gruppi di volumi:
    - Creare un pool o un gruppo di volumi (cercare **Sì** nella colonna **Secure-capable** della tabella dei candidati).
    - Selezionare un pool o un gruppo di volumi quando si crea un nuovo volume (cercare **Sì** accanto a **Secure-capable** nella tabella dei candidati del pool e del gruppo di volumi).

Funzionamento di Drive Security a livello di unità

Un disco sicuro, FDE o FIPS, crittografa i dati durante la scrittura e decrta i dati durante la lettura. La crittografia e la decrittografia non influiscono sulle prestazioni o sul flusso di lavoro dell'utente. Ogni disco dispone di una propria chiave di crittografia univoca, che non può mai essere trasferita dal disco.

La funzione Drive Security offre un ulteriore livello di protezione con dischi sicuri. Quando si selezionano gruppi di volumi o pool su questi dischi per Drive Security, i dischi cercano una chiave di sicurezza prima di consentire l'accesso ai dati. È possibile attivare Drive Security per pool e gruppi di volumi in qualsiasi momento, senza influire sui dati esistenti sul disco. Tuttavia, non è possibile disattivare Drive Security senza cancellare tutti i dati presenti sul disco.

Funzionamento di Drive Security a livello di storage array

Con la funzione Drive Security, è possibile creare una chiave di sicurezza condivisa tra i dischi e i controller abilitati alla protezione in un array di storage. Ogni volta che si spegne e si riaccende l'alimentazione dei dischi, i dischi abilitati alla protezione cambiano in uno stato di sicurezza bloccato fino a quando il controller

non applica la chiave di sicurezza.

Se un disco abilitato alla protezione viene rimosso dall'array di storage e reinstallato in un array di storage diverso, il disco si trova in uno stato di sicurezza bloccata. L'unità riposizionata cerca la chiave di sicurezza prima di rendere nuovamente accessibili i dati. Per sbloccare i dati, applicare la chiave di sicurezza dall'array di storage di origine. Una volta completato correttamente il processo di sblocco, l'unità riallocata utilizzerà la chiave di sicurezza già memorizzata nell'array di storage di destinazione e il file della chiave di sicurezza importato non sarà più necessario.

Per la gestione interna delle chiavi, la chiave di sicurezza effettiva viene memorizzata nel controller in una posizione non accessibile. Non è in formato leggibile né accessibile all'utente.

Funzionamento di Drive Security a livello di volume

Quando si crea un pool o un gruppo di volumi da dischi con funzionalità di protezione, è anche possibile attivare Drive Security per tali pool o gruppi di volumi. L'opzione Drive Security (protezione disco) rende sicuri i dischi e i gruppi di volumi e i pool associati-*enabled*.

Prima di creare pool e gruppi di volumi abilitati alla protezione, tenere presenti le seguenti linee guida:

- I gruppi di volumi e i pool devono essere costituiti interamente da dischi sicuri. (Per i volumi che richiedono il supporto FIPS, utilizzare solo dischi FIPS. La combinazione di dischi FIPS e FDE in un gruppo di volumi o in un pool comporterà il trattamento di tutti i dischi come dischi FDE. Inoltre, un disco FDE non può essere aggiunto o utilizzato come spare in un gruppo di volumi o pool all-FIPS.
- I gruppi di volumi e i pool devono trovarsi in uno stato ottimale.

Come funziona la gestione delle chiavi di sicurezza

Quando si implementa la funzione Drive Security, i dischi abilitati alla protezione (FIPS o FDE) richiedono una chiave di sicurezza per l'accesso ai dati. Una chiave di sicurezza è una stringa di caratteri condivisa tra questi tipi di dischi e i controller di un array di storage.

Ogni volta che si spegne e si riaccende l'alimentazione dei dischi, i dischi abilitati alla protezione cambiano in uno stato di sicurezza bloccato fino a quando il controller non applica la chiave di sicurezza. Se un disco abilitato alla protezione viene rimosso dall'array di storage, i dati dell'unità vengono bloccati. Quando il disco viene reinstallato in un array di storage diverso, cerca la chiave di sicurezza prima di rendere nuovamente accessibili i dati. Per sbloccare i dati, è necessario applicare la chiave di sicurezza originale.

È possibile creare e gestire le chiavi di sicurezza utilizzando uno dei seguenti metodi:

- Gestione interna delle chiavi nella memoria persistente del controller.
- Gestione esterna delle chiavi su un server di gestione delle chiavi esterno.

Gestione interna delle chiavi

Le chiavi interne vengono conservate nella memoria persistente del controller. Per implementare la gestione interna delle chiavi, attenersi alla seguente procedura:

1. Installare unità sicure nell'array di storage. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
2. Assicurarsi che la funzione Drive Security sia attivata. Se necessario, contattare il fornitore dello storage

per istruzioni sull'attivazione della funzione Drive Security.

3. Creare una chiave di sicurezza interna, che implica la definizione di un identificatore e di una passphrase. L'identificatore è una stringa associata alla chiave di sicurezza e memorizzata sul controller e su tutti i dischi associati alla chiave. La password viene utilizzata per crittografare la chiave di sicurezza a scopo di backup. Per creare una chiave interna, accedere al **Impostazioni › sistema › Gestione chiave di sicurezza › Crea chiave interna**.

La chiave di sicurezza viene memorizzata nel controller in una posizione non accessibile. È quindi possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Gestione esterna delle chiavi

Le chiavi esterne vengono gestite su un server di gestione delle chiavi separato, utilizzando un protocollo KMIP (Key Management Interoperability Protocol). Per implementare la gestione esterna delle chiavi, attenersi alla seguente procedura:

1. Installare unità sicure nell'array di storage. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
2. Assicurarsi che la funzione Drive Security sia attivata. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.
3. Completare e scaricare una CSR (Certificate Signing Request) client per l'autenticazione tra lo storage array e il server di gestione delle chiavi. Accedere al **Impostazioni › certificati › Gestione chiavi › CSR completa**.
4. Creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato.
5. Assicurarsi che il certificato client e una copia del certificato per il server di gestione delle chiavi siano disponibili sull'host locale.
6. Creare una chiave esterna che preveda la definizione dell'indirizzo IP del server di gestione delle chiavi e del numero di porta utilizzato per le comunicazioni KMIP. Durante questo processo, vengono caricati anche i file dei certificati. Per creare una chiave esterna, accedere al **Impostazioni › sistema › Gestione chiave di sicurezza › Crea chiave esterna**.

Il sistema si connette al server di gestione delle chiavi con le credenziali immesse. È quindi possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Promuovere la terminologia in materia di sicurezza

Scopri come si applicano i termini di Drive Security al tuo storage array.

Termine	Descrizione
Funzione di protezione del disco	Drive Security è una funzionalità di storage array che offre un ulteriore livello di sicurezza con dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard). Quando questi dischi vengono utilizzati con la funzione Drive Security, richiedono una chiave di sicurezza per l'accesso ai dati. Quando i dischi vengono fisicamente rimossi dall'array, non possono funzionare fino a quando non vengono installati in un altro array, a questo punto, saranno in uno stato di sicurezza bloccato fino a quando non viene fornita la chiave di sicurezza corretta.
Dischi FDE	I dischi con crittografia completa del disco (FDE) eseguono la crittografia sul disco a livello hardware. Il disco rigido contiene un chip ASIC che crittografa i dati durante le operazioni di scrittura, quindi decrta i dati durante le operazioni di lettura.
Dischi FIPS	I dischi FIPS utilizzano gli standard FIPS (Federal Information Processing Standards) 140-2 livello 2. Si tratta essenzialmente di dischi FDE conformi agli standard governativi degli Stati Uniti per garantire metodi e algoritmi di crittografia efficaci. I dischi FIPS hanno standard di sicurezza più elevati rispetto ai dischi FDE.
Client di gestione	Un sistema locale (computer, tablet, ecc.) che include un browser per l'accesso a System Manager.
Password	La password viene utilizzata per crittografare la chiave di sicurezza a scopo di backup. La stessa passphrase utilizzata per crittografare la chiave di sicurezza deve essere fornita quando la chiave di sicurezza di cui è stato eseguito il backup viene importata come risultato di una migrazione del disco o di uno scambio head. Una password può contenere da 8 a 32 caratteri. La password per Drive Security è indipendente dalla password Administrator dell'array di storage.

Termine	Descrizione
Dischi sicuri	I dischi che supportano la protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard), che crittografano i dati durante la scrittura e decrittare i dati durante la lettura. Questi dischi sono considerati sicuri-*capaci* perché possono essere utilizzati per una maggiore sicurezza utilizzando la funzione Drive Security. Se la funzione Drive Security è attivata per i gruppi di volumi e i pool utilizzati con questi dischi, i dischi diventano sicuri-*abilitati*.
Dischi sicuri	Le unità abilitate alla protezione vengono utilizzate con la funzione Drive Security. Quando si attiva la funzione Drive Security e si applica Drive Security a un pool o a un gruppo di volumi su dischi sicuri-*capaci*, i dischi diventano sicuri-*abilitati*. L'accesso in lettura e scrittura è disponibile solo attraverso un controller configurato con la chiave di sicurezza corretta. Questa sicurezza aggiuntiva impedisce l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dallo storage array.
Chiave di sicurezza	Una chiave di sicurezza è una stringa di caratteri condivisa tra i dischi abilitati alla protezione e i controller di un array di storage. Ogni volta che si spegne e si riaccende l'alimentazione dei dischi, i dischi abilitati alla protezione cambiano in uno stato di sicurezza bloccato fino a quando il controller non applica la chiave di sicurezza. Se un disco abilitato alla protezione viene rimosso dall'array di storage, i dati dell'unità vengono bloccati. Quando il disco viene reinstallato in un array di storage diverso, cerca la chiave di sicurezza prima di rendere nuovamente accessibili i dati. Per sbloccare i dati, è necessario applicare la chiave di sicurezza originale. È possibile creare e gestire le chiavi di sicurezza utilizzando uno dei seguenti metodi: • Gestione interna delle chiavi — Crea e mantieni le chiavi di sicurezza nella memoria persistente del controller. • Gestione esterna delle chiavi — Crea e gestisci le chiavi di sicurezza su un server di gestione delle chiavi esterno.
Identificatore della chiave di sicurezza	L'identificatore della chiave di sicurezza è una stringa associata alla chiave di sicurezza durante la creazione della chiave. L'identificatore viene memorizzato sul controller e su tutti i dischi associati alla chiave di sicurezza.

Come fare

Creare una chiave di sicurezza interna

Per utilizzare la funzione Drive Security, è possibile creare una chiave di sicurezza interna condivisa dai controller e dalle unità sicure nell'array di storage. Le chiavi interne vengono conservate nella memoria persistente del controller.

Prima di iniziare

- Nello storage array devono essere installate unità sicure. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
- La funzione Drive Security deve essere attivata. In caso contrario, viene visualizzata la finestra di dialogo **Impossibile creare la chiave di sicurezza** durante questa attività. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.

> Se nell'array di storage sono installati sia dischi FDE che FIPS, tutti condividono la stessa chiave di sicurezza.

A proposito di questa attività

In questa attività, si definiscono un identificatore e una passphrase da associare alla chiave di sicurezza interna.

> La password per Drive Security è indipendente dalla password Administrator dell'array di storage.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Create Internal Key** (Crea chiave interna).

   Se non è stata ancora generata una chiave di sicurezza, viene visualizzata la finestra di dialogo **Crea chiave di sicurezza**.

3. Inserire le informazioni nei seguenti campi:
   - Definire un identificatore della chiave di sicurezza — è possibile accettare il valore predefinito (nome dello storage array e data/ora, generato dal firmware del controller) o inserire un valore personalizzato. È possibile inserire fino a 189 caratteri alfanumerici senza spazi, punteggiatura o simboli.

     > I caratteri aggiuntivi vengono generati automaticamente, aggiunti a entrambe le estremità della stringa immessa. I caratteri generati garantiscono che l'identificatore sia univoco.

   - Definire una passphrase/immettere nuovamente una passphrase — inserire e confermare una passphrase. Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti elementi:
     - Una lettera maiuscola (una o più lettere). Tenere presente che la password distingue tra maiuscole e minuscole.
     - Un numero (uno o più).

- Un carattere non alfanumerico, ad esempio !, *, @ (uno o più).

Assicurarsi di registrare le voci per un utilizzo successivo. Se è necessario spostare un'unità abilitata per la sicurezza dall'array di storage, è necessario conoscere l'identificatore e la password per sbloccare i dati dell'unità.

4. Fare clic su **Create** (Crea).

   La chiave di sicurezza viene memorizzata nel controller in una posizione non accessibile. Insieme alla chiave effettiva, è disponibile un file di chiavi crittografate che viene scaricato dal browser.

   Il percorso del file scaricato potrebbe dipendere dalla posizione di download predefinita del browser.

5. Registrare l'identificativo della chiave, la password e la posizione del file delle chiavi scaricato, quindi fare clic su **Chiudi**.

Risultato

È ora possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Ogni volta che si spegne e si riaccende l'alimentazione dei dischi, tutti i dischi abilitati per la sicurezza vengono attivati in uno stato di sicurezza bloccata. In questo stato, i dati non sono accessibili finché il controller non applica la chiave di sicurezza corretta durante l'inizializzazione del disco. Se qualcuno rimuove fisicamente un disco bloccato e lo installa in un altro sistema, lo stato Security Locked impedisce l'accesso non autorizzato ai dati.

Al termine

È necessario convalidare la chiave di sicurezza per assicurarsi che il file delle chiavi non sia corrotto.

Creare una chiave di sicurezza esterna

Per utilizzare la funzione Drive Security con un server di gestione delle chiavi, è necessario creare una chiave esterna condivisa dal server di gestione delle chiavi e dalle unità sicure nell'array di storage.

Prima di iniziare

- Nell'array devono essere installate unità sicure. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).

  Se nell'array di storage sono installati sia dischi FDE che FIPS, tutti condividono la stessa chiave di sicurezza.

- La funzione Drive Security deve essere attivata. In caso contrario, viene visualizzata la finestra di dialogo **Impossibile creare la chiave di sicurezza** durante questa attività. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.
- I certificati client e server sono disponibili sull'host locale in modo che l'array di storage e il server di gestione delle chiavi possano autenticarsi l'uno con l'altro. Il certificato del client convalida i controller, mentre il certificato del server convalida il server di gestione delle chiavi.

A proposito di questa attività

In questa attività, definire l'indirizzo IP del server di gestione delle chiavi e il numero di porta utilizzato, quindi caricare i certificati per la gestione delle chiavi esterne.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Create External Key** (Crea chiave esterna).

   Se la gestione interna delle chiavi è attualmente configurata, viene visualizzata una finestra di dialogo che richiede di confermare che si desidera passare alla gestione esterna delle chiavi.

   Viene visualizzata la finestra di dialogo **Crea chiave di sicurezza esterna**.

3. In **Connect to Key Server** (connessione al server chiavi), immettere le informazioni nei seguenti campi:
   - Key management server address (Indirizzo server di gestione delle chiavi) — inserire il nome di dominio completo o l'indirizzo IP (IPv4 o IPv6) del server utilizzato per la gestione delle chiavi.
   - Key management port number (numero porta di gestione delle chiavi) — inserire il numero di porta utilizzato per le comunicazioni KMIP (Key Management Interoperability Protocol). Il numero di porta più comune utilizzato per le comunicazioni del server di gestione delle chiavi è 5696.
   - Select client certificate (Seleziona certificato client) — fare clic sul primo pulsante Browse (Sfoglia) per selezionare il file di certificato per i controller dell'array di storage.
   - Selezionare il certificato del server del server di gestione delle chiavi — fare clic sul secondo pulsante Sfoglia per selezionare il file di certificato per il server di gestione delle chiavi.
4. Fare clic su **Avanti**.
5. In **Create/Backup Key** (chiave di creazione/backup), immettere le informazioni nel campo seguente:
   - Definire una passphrase/immettere nuovamente una passphrase — inserire e confermare una passphrase. Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti elementi:
     - Una lettera maiuscola (una o più lettere). Tenere presente che la password distingue tra maiuscole e minuscole.
     - Un numero (uno o più).
     - Un carattere non alfanumerico, ad esempio !, *, @ (uno o più).

   Assicurarsi di registrare le voci per un utilizzo successivo. Se è necessario spostare un'unità abilitata per la sicurezza dall'array di storage, è necessario conoscere la password per sbloccare i dati dell'unità.

6. Fare clic su **fine**.

   Il sistema si connette al server di gestione delle chiavi con le credenziali immesse. Una copia della chiave di sicurezza viene quindi memorizzata nel sistema locale.

   Il percorso del file scaricato potrebbe dipendere dalla posizione di download predefinita del browser.

7. Registrare la password e la posizione del file delle chiavi scaricato, quindi fare clic su **Chiudi**.

   La pagina visualizza il seguente messaggio con collegamenti aggiuntivi per la gestione esterna delle

chiavi:

```
Current key management method: External
```

8. Verificare la connessione tra lo storage array e il server di gestione delle chiavi selezionando **Test Communication**.

   I risultati del test vengono visualizzati nella finestra di dialogo.

Risultati

Quando è attivata la gestione delle chiavi esterne, è possibile creare gruppi di volumi o pool abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

> Ogni volta che si spegne e si riaccende l'alimentazione dei dischi, tutti i dischi abilitati per la sicurezza vengono attivati in uno stato di sicurezza bloccata. In questo stato, i dati non sono accessibili finché il controller non applica la chiave di sicurezza corretta durante l'inizializzazione del disco. Se qualcuno rimuove fisicamente un disco bloccato e lo installa in un altro sistema, lo stato Security Locked impedisce l'accesso non autorizzato ai dati.

Al termine

- È necessario convalidare la chiave di sicurezza per assicurarsi che il file delle chiavi non sia corrotto.

Modificare la chiave di sicurezza

In qualsiasi momento, è possibile sostituire una chiave di sicurezza con una nuova. Potrebbe essere necessario modificare una chiave di sicurezza nei casi in cui si verifica una potenziale violazione della sicurezza presso l'azienda e si desidera assicurarsi che il personale non autorizzato non possa accedere ai dati dei dischi.

Prima di iniziare

Una chiave di sicurezza esiste già.

A proposito di questa attività

Questa attività descrive come modificare una chiave di sicurezza e sostituirla con una nuova. Dopo questo processo, la vecchia chiave viene invalidata.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Change Key** (Cambia chiave).

   Viene visualizzata la finestra di dialogo **Change Security Key** (Modifica chiave di sicurezza).

3. Immettere le informazioni nei seguenti campi.

   - Definire un identificatore della chiave di sicurezza — (solo per le chiavi di sicurezza interne). Accettare il valore predefinito (nome dell'array di storage e data/ora, generato dal firmware del controller) o inserire un valore personalizzato. È possibile inserire fino a 189 caratteri alfanumerici senza spazi, punteggiatura o simboli.

I caratteri aggiuntivi vengono generati automaticamente e aggiunti a entrambe le estremità della stringa immessa. I caratteri generati garantiscono che l'identificatore sia univoco.

- Definire una passphrase/immettere nuovamente una passphrase — in ciascuno di questi campi, inserire la password. Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti elementi:
  - Una lettera maiuscola (una o più lettere). Tenere presente che la password distingue tra maiuscole e minuscole.
  - Un numero (uno o più).
  - Un carattere non alfanumerico, ad esempio !, *, @ (uno o più).

Assicurarsi di registrare le voci per un utilizzo successivo — se è necessario spostare un disco abilitato alla sicurezza dall'array di storage, è necessario conoscere l'identificatore e la password per sbloccare i dati del disco.

4. Fare clic su **Cambia**.

   La nuova chiave di sicurezza sovrascrive la chiave precedente, che non è più valida.

   Il percorso del file scaricato potrebbe dipendere dalla posizione di download predefinita del browser.

5. Registrare l'identificativo della chiave, la password e la posizione del file delle chiavi scaricato, quindi fare clic su **Chiudi**.

Al termine

È necessario convalidare la chiave di sicurezza per assicurarsi che il file delle chiavi non sia corrotto.

Passare dalla gestione delle chiavi esterna a quella interna

È possibile modificare il metodo di gestione di Drive Security da un server di chiavi esterno al metodo interno utilizzato dall'array di storage. La chiave di sicurezza precedentemente definita per la gestione esterna delle chiavi viene quindi utilizzata per la gestione interna delle chiavi.

Prima di iniziare

È stata creata una chiave esterna.

A proposito di questa attività

In questa attività, si disattiva la gestione delle chiavi esterne e si scarica una nuova copia di backup sull'host locale. La chiave esistente viene ancora utilizzata per Drive Security, ma verrà gestita internamente nell'array di storage.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Disable External Key Management** (Disattiva gestione chiavi esterne).

   Viene visualizzata la finestra di dialogo **Disable External Key Management** (Disattiva gestione chiavi

esterne).

3. In **definire una passphrase/immettere nuovamente la passphrase**, inserire e confermare una passphrase per il backup della chiave. Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti elementi:
   - Una lettera maiuscola (una o più lettere). Tenere presente che la password distingue tra maiuscole e minuscole.
   - Un numero (uno o più).
   - Un carattere non alfanumerico, ad esempio !, *, @ (uno o più).

   > *Assicurarsi di registrare le voci per un utilizzo successivo*. Se è necessario spostare un'unità abilitata per la sicurezza dall'array di storage, è necessario conoscere l'identificatore e la password per sbloccare i dati dell'unità.

4. Fare clic su **Disable** (Disattiva).

   La chiave di backup viene scaricata sull'host locale.

5. Registrare l'identificativo della chiave, la password e la posizione del file delle chiavi scaricato, quindi fare clic su **Chiudi**.

Risultati

Drive Security è ora gestito internamente attraverso lo storage array.

Al termine

- È necessario convalidare la chiave di sicurezza per assicurarsi che il file delle chiavi non sia corrotto.

Modificare le impostazioni del server di gestione delle chiavi

Se è stata configurata la gestione esterna delle chiavi, è possibile visualizzare e modificare le impostazioni del server di gestione delle chiavi in qualsiasi momento.

Prima di iniziare

È necessario configurare la gestione esterna delle chiavi.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **View/Edit Key Management Server Settings** (Visualizza/Modifica impostazioni del server di gestione delle chiavi).
3. Modificare le informazioni nei seguenti campi:
   - Key management server address (Indirizzo server di gestione delle chiavi) — inserire il nome di dominio completo o l'indirizzo IP (IPv4 o IPv6) del server utilizzato per la gestione delle chiavi.
   - KMIP port number (numero porta KMIP) — inserire il numero di porta utilizzato per le comunicazioni KMIP (Key Management Interoperability Protocol).
4. Fare clic su **Save** (Salva).

Eseguire il backup della chiave di sicurezza

Dopo aver creato o modificato una chiave di sicurezza, è possibile creare una copia di backup del file delle chiavi nel caso in cui l'originale venga danneggiato.

Prima di iniziare

- Una chiave di sicurezza esiste già.

A proposito di questa attività

Questa attività descrive come eseguire il backup di una chiave di sicurezza creata in precedenza. Durante questa procedura, viene creata una nuova passphrase per il backup. Questa password non deve corrispondere alla password utilizzata al momento della creazione o dell'ultima modifica della chiave originale. La password viene applicata solo al backup che si sta creando.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Backup key**.

   Viene visualizzata la finestra di dialogo **Backup Security Key** (chiave di sicurezza di backup).

3. Nei campi **Definisci password/Inserisci nuova password**, immettere e confermare una password per il backup.

   Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti elementi:

   - Una lettera maiuscola (una o più lettere)
   - Un numero (uno o più)
   - Un carattere non alfanumerico, ad esempio !, *, @ (uno o più)

   Assicurarsi di registrare i dati immessi per un utilizzo successivo. Per accedere al backup di questa chiave di sicurezza, è necessaria la password.

4. Fare clic su **Backup**.

   Viene scaricato un backup della chiave di sicurezza sull'host locale, quindi viene visualizzata la finestra di dialogo **Conferma/Registra backup chiave di sicurezza**.

   Il percorso del file della chiave di sicurezza scaricato potrebbe dipendere dalla posizione di download predefinita del browser.

5. Registrare la password in una posizione sicura, quindi fare clic su **Chiudi**.

Al termine

È necessario convalidare la chiave di sicurezza per il backup.

Convalidare la chiave di sicurezza

È possibile convalidare la chiave di sicurezza per assicurarsi che non sia stata danneggiata e per verificare di disporre di una password corretta.

Prima di iniziare

È stata creata una chiave di sicurezza.

A proposito di questa attività

Questa attività descrive come convalidare la chiave di sicurezza creata in precedenza. Si tratta di un passaggio importante per assicurarsi che il file delle chiavi non sia corrotto e che la password sia corretta, in modo da poter accedere in seguito ai dati delle unità se si sposta un disco abilitato alla sicurezza da un array di storage a un altro.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Validate Key** (convalida chiave).

   Viene visualizzata la finestra di dialogo **Validate Security Key** (convalida chiave di sicurezza).

3. Fare clic su **Browse**, quindi selezionare il file delle chiavi (ad esempio, `drivesecurity.slk`).
4. Inserire la password associata alla chiave selezionata.

   Quando si seleziona un file di chiavi e una password validi, il pulsante **convalida** diventa disponibile.

5. Fare clic su **Validate** (convalida).

   I risultati della convalida vengono visualizzati nella finestra di dialogo.

6. Se il risultato è "la chiave di sicurezza è stata convalidata correttamente", fare clic su **Chiudi**. Se viene visualizzato un messaggio di errore, seguire le istruzioni suggerite visualizzate nella finestra di dialogo.

Sbloccare i dischi utilizzando una chiave di sicurezza

Se si spostano dischi abilitati alla protezione da un array di storage a un altro, è necessario importare la chiave di sicurezza appropriata nel nuovo array di storage. L'importazione della chiave consente di sbloccare i dati presenti sui dischi.

Prima di iniziare

- L'array di storage di destinazione (in cui si spostano i dischi) deve già disporre di una chiave di sicurezza configurata. I dischi migrati verranno ridimitati nell'array di storage di destinazione.
- È necessario conoscere la chiave di sicurezza associata ai dischi che si desidera sbloccare.
- Il file della chiave di sicurezza è disponibile sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager). Se si spostano i dischi in un array di storage gestito da un sistema diverso, è necessario spostare il file della chiave di sicurezza in quel client di gestione.

A proposito di questa attività

Questa attività descrive come sbloccare i dati in dischi abilitati alla sicurezza che sono stati rimossi da un array di storage e reinstallati in un altro. Una volta che l'array rileva i dischi, viene visualizzata una condizione di "attenzione necessaria" insieme allo stato "chiave di sicurezza necessaria" per questi dischi riposizionati. È possibile sbloccare i dati delle unità importando la chiave di sicurezza nell'array di storage. Durante questo processo, selezionare il file della chiave di sicurezza e immettere la password per la chiave.

La password non corrisponde alla password Administrator dell'array di storage.

Se nel nuovo array di storage sono installate altre unità abilitate alla protezione, potrebbero utilizzare una chiave di sicurezza diversa da quella che si sta importando. Durante il processo di importazione, la vecchia

chiave di sicurezza viene utilizzata solo per sbloccare i dati dei dischi che si stanno installando. Quando il processo di sblocco ha esito positivo, i dischi appena installati vengono reinseriti nella chiave di sicurezza dell'array di storage di destinazione.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Unlock Secure Drives**.

   Viene visualizzata la finestra di dialogo **Unlock Secure Drives**. Tutti i dischi che richiedono una chiave di sicurezza sono mostrati nella tabella.

3. In alternativa, passare il mouse su un numero di disco per visualizzare la posizione dell'unità (numero di shelf e numero di alloggiamento).
4. Fare clic su **Browse**, quindi selezionare il file della chiave di sicurezza corrispondente al disco che si desidera sbloccare.

   Il file delle chiavi selezionato viene visualizzato nella finestra di dialogo.

5. Inserire la password associata al file delle chiavi.

   I caratteri immessi vengono mascherati.

6. Fare clic su **Sblocca**.

   Se l'operazione di sblocco ha esito positivo, viene visualizzata la finestra di dialogo "i dischi protetti associati sono stati sbloccati".

Risultati

Quando tutti i dischi sono bloccati e quindi sbloccati, ogni controller nell'array di storage viene riavviato. Tuttavia, se nell'array di storage di destinazione sono già presenti alcuni dischi sbloccati, i controller non verranno riavviati.

FAQ

Cosa occorre sapere prima di creare una chiave di sicurezza?

Una chiave di sicurezza viene condivisa da controller e dischi abilitati alla sicurezza all'interno di un array di storage. Se un disco abilitato alla protezione viene rimosso dall'array di storage, la chiave di sicurezza protegge i dati da accessi non autorizzati.

È possibile creare e gestire le chiavi di sicurezza utilizzando uno dei seguenti metodi:

- Gestione interna delle chiavi nella memoria persistente del controller.
- Gestione esterna delle chiavi su un server di gestione delle chiavi esterno.

Prima di creare una chiave di sicurezza interna, eseguire le seguenti operazioni:

1. Installare unità sicure nell'array di storage. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
2. Assicurarsi che la funzione Drive Security sia attivata. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.

È quindi possibile creare una chiave di sicurezza interna, che implica la definizione di un identificatore e di una passphrase. L'identificatore è una stringa associata alla chiave di sicurezza e memorizzata sul controller e su tutti i dischi associati alla chiave. La password viene utilizzata per crittografare la chiave di sicurezza a scopo di backup. Al termine, la chiave di sicurezza viene memorizzata nel controller in una posizione non accessibile. È quindi possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Prima di creare una chiave di sicurezza esterna, eseguire le seguenti operazioni:

1. Installare unità sicure nell'array di storage. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
2. Assicurarsi che la funzione Drive Security sia attivata. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.
3. Completare e scaricare una CSR (Certificate Signing Request) client per l'autenticazione tra lo storage array e il server di gestione delle chiavi. Accedere al **Impostazioni › certificati › Gestione chiavi › CSR completa**.
4. Creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato.
5. Assicurarsi che il certificato client e una copia del certificato per il server di gestione delle chiavi siano disponibili sull'host locale.

È quindi possibile creare una chiave esterna che preveda la definizione dell'indirizzo IP del server di gestione delle chiavi e del numero di porta utilizzato per le comunicazioni KMIP. Durante questo processo, vengono caricati anche i file dei certificati. Al termine, il sistema si connette al server di gestione delle chiavi con le credenziali immesse. È quindi possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Perché è necessario definire una passphrase?

La password viene utilizzata per crittografare e decrittare il file della chiave di sicurezza memorizzato nel client di gestione locale. Senza la passphrase, la chiave di sicurezza non può essere decifrata e utilizzata per sbloccare i dati da un disco abilitato alla sicurezza se viene reinstallata in un altro array di storage.

Perché è importante registrare le informazioni sulle chiavi di sicurezza?

Se si perdono le informazioni della chiave di sicurezza e non si dispone di un backup, si potrebbero perdere i dati durante la riassegnazione di dischi abilitati alla protezione o l'aggiornamento di un controller. È necessaria la chiave di sicurezza per sbloccare i dati sui dischi.

Assicurarsi di registrare l'identificatore della chiave di sicurezza, la password associata e la posizione sull'host locale in cui è stato salvato il file della chiave di sicurezza.

Cosa occorre sapere prima di eseguire il backup di una chiave di sicurezza?

Se la chiave di sicurezza originale viene danneggiata e non si dispone di un backup, l'accesso ai dati sui dischi viene perso se vengono migrati da uno storage array a un altro.

Prima di eseguire il backup di una chiave di sicurezza, tenere presenti le seguenti linee guida:

- Assicurarsi di conoscere l'identificatore della chiave di sicurezza e la password del file della chiave originale.

> Solo le chiavi interne utilizzano identificatori. Quando è stato creato l'identificatore, sono stati generati automaticamente caratteri aggiuntivi e aggiunti ad entrambe le estremità della stringa di identificazione. I caratteri generati garantiscono che l'identificatore sia univoco.

- Viene creata una nuova password per il backup. Questa password non deve corrispondere alla password utilizzata al momento della creazione o dell'ultima modifica della chiave originale. La password viene applicata solo al backup che si sta creando.

> La password per Drive Security non deve essere confusa con la password Administrator dell'array di storage. La password per Drive Security protegge i backup di una chiave di sicurezza. La password Administrator protegge l'intero array di storage da accessi non autorizzati.

- Il file della chiave di sicurezza di backup viene scaricato nel client di gestione. Il percorso del file scaricato potrebbe dipendere dalla posizione di download predefinita del browser. Assicurarsi di registrare la posizione in cui sono memorizzate le informazioni della chiave di sicurezza.

Cosa devo sapere prima di sbloccare dischi sicuri?

Per sbloccare i dati da un disco abilitato alla protezione che viene migrato a un nuovo array di storage, è necessario importare la chiave di sicurezza.

Prima di sbloccare dischi sicuri, tenere presenti le seguenti linee guida:

- L'array di storage di destinazione (in cui si spostano i dischi) deve disporre già di una chiave di sicurezza. I dischi migrati verranno ridimitati nell'array di storage di destinazione.
- Per i dischi che si stanno migrando, si conoscono l'identificatore della chiave di sicurezza e la password che corrisponde al file della chiave di sicurezza.
- Il file della chiave di sicurezza è disponibile sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager).

Che cos'è l'accessibilità in lettura/scrittura?

La finestra **Drive Settings** contiene informazioni sugli attributi **Drive Security**. "Read/Write Accessible" (lettura/scrittura accessibile) è uno degli attributi che viene visualizzato se i dati di un disco sono stati bloccati.

Per visualizzare gli attributi **Drive Security**, accedere alla pagina hardware. Selezionare un'unità, fare clic su **Visualizza impostazioni**, quindi fare clic su **Mostra altre impostazioni**. Nella parte inferiore della pagina, il valore dell'attributo Read/Write Accessible (lettura/scrittura accessibile) è **Yes** (Sì) quando il disco è sbloccato. Il valore dell'attributo lettura/scrittura accessibile è **No, chiave di sicurezza non valida** quando l'unità è bloccata. È possibile sbloccare un'unità sicura importando una chiave di sicurezza (accedere a **Impostazioni › sistema › Sblocca unità protette**).

Cosa occorre sapere sulla convalida della chiave di sicurezza?

Dopo aver creato una chiave di sicurezza, è necessario convalidare il file della chiave per assicurarsi che non sia corrotto.

Se la convalida non riesce, procedere come segue:

- Se l'identificatore della chiave di sicurezza non corrisponde all'identificatore sul controller, individuare il file della chiave di sicurezza corretto e riprovare la convalida.
- Se il controller non riesce a decrittare la chiave di sicurezza per la convalida, è possibile che la password sia stata inserita in modo errato. Controllare due volte la password, immetterla di nuovo se necessario, quindi riprovare a eseguire la convalida. Se il messaggio di errore viene visualizzato di nuovo, selezionare un backup del file delle chiavi (se disponibile) e riprovare la convalida.
- Se non si riesce ancora a convalidare la chiave di sicurezza, il file originale potrebbe essere danneggiato. Creare un nuovo backup della chiave e convalidare tale copia.

Qual è la differenza tra la chiave di sicurezza interna e la gestione esterna delle chiavi di sicurezza?

Quando si implementa la funzione **Drive Security**, è possibile utilizzare una chiave di sicurezza interna o una chiave di sicurezza esterna per bloccare i dati quando un disco abilitato alla protezione viene rimosso dall'array di storage.

Una chiave di sicurezza è una stringa di caratteri che viene condivisa tra i dischi abilitati alla protezione e i controller di un array di storage. Le chiavi interne vengono conservate nella memoria persistente del controller. Le chiavi esterne vengono gestite su un server di gestione delle chiavi separato, utilizzando un protocollo KMIP (Key Management Interoperability Protocol).

Informazioni sul copyright

Informazioni sul marchio commerciale