Configurare le chiavi di sicurezza

SANtricity 11.7

NetApp
February 12, 2024

Sommario

Configurare le chiavi di sicurezza

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 protezione. 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 protezione, viene visualizzata la finestra di dialogo Crea chiave di protezione.

3. Inserire le informazioni nei seguenti campi:

   - **Definire un identificatore della chiave di sicurezza** — è possibile 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, aggiunti a entrambe le estremità della stringa immessa. I caratteri generati garantiscono che l'identificatore sia univoco.

   - **Definire una passphrase/immettere nuovamente la 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**.

Risultati

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 protezione. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.
- Si dispone di un file di certificato client firmato per i controller dell'array di storage ed è stato copiato nell'host in cui si accede a System Manager. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste del protocollo KMIP

(Key Management Interoperability Protocol).

- È necessario recuperare un file di certificato dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, in modo che lo storage array possa fidarsi del proprio indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

> Per ulteriori informazioni sul certificato del server, consultare la documentazione relativa al 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 protezione esterna.

3. In **Connect to Key Server** (connessione al server chiavi), immettere le informazioni nei seguenti campi.
   - **Indirizzo del 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** — inserire il numero di porta utilizzato per le comunicazioni KMIP. Il numero di porta più comune utilizzato per le comunicazioni del server di gestione delle chiavi è 5696.

     Opzionale: se si desidera configurare un server chiavi di backup, fare clic su **Aggiungi server chiavi**, quindi immettere le informazioni relative al server. Se non è possibile raggiungere il server principale delle chiavi, viene utilizzato il secondo server delle chiavi. Assicurarsi che ciascun server di chiavi abbia accesso allo stesso database di chiavi; in caso contrario, l'array eseguirà il post degli errori e non potrà utilizzare il server di backup.

> Viene utilizzato un solo server di chiavi alla volta. Se lo storage array non riesce a raggiungere il server principale delle chiavi, l'array contatterà il server delle chiavi di backup. Tenere presente che è necessario mantenere la parità su entrambi i server; in caso contrario, potrebbero verificarsi errori.

   - **Select client certificate** — 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. È possibile scegliere un certificato root, intermedio o server per il server di gestione delle chiavi.
4. Fare clic su **Avanti**.
5. In **Create/Backup Key** (Crea/Backup chiave), è possibile creare una chiave di backup per motivi di sicurezza.

- (Consigliato) per creare una chiave di backup, mantenere la casella di controllo selezionata, quindi immettere e confermare una 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'unità abilitata per la sicurezza dall'array di storage, è necessario conoscere la password per sbloccare i dati dell'unità.

+

- Se non si desidera creare una chiave di backup, deselezionare la casella di controllo.

Tenere presente che se si perde l'accesso al server delle chiavi esterno e non si dispone di una chiave di backup, l'accesso ai dati sui dischi viene perso se vengono migrati in un altro array di storage. Questa opzione è l'unico metodo per creare una chiave di backup in System Manager.

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.