Gestire le chiavi di sicurezza

SANtricity 11.8

NetApp
December 16, 2024

Sommario

Gestire le chiavi di sicurezza

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.

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 protezione).

3. Immettere le informazioni nei seguenti campi.
   - **Definire un identificatore della chiave di protezione** — (solo per le chiavi di protezione interne). Accettare il valore predefinito (nome dell'array di archiviazione e indicatore data e ora, generato dal firmware del controller) oppure immettere 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 la passphrase** — in ciascuno di questi campi, inserire la 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).
4. Per le chiavi di sicurezza esterne, se si desidera eliminare la vecchia chiave di sicurezza quando viene creata la nuova, selezionare "Delete current Security key…" (Elimina chiave di sicurezza corrente…). casella di controllo nella parte inferiore della finestra di dialogo.

   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.

5. 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.

6. 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.

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 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.

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:
   - **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 (Key Management Interoperability Protocol).

     Opzionale: è possibile includere un altro server chiavi facendo clic su **Aggiungi server chiavi**.
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.

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 Back Up Security Key (Esegui backup chiave di protezione).
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.

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 protezione).

3. Fare clic su **Sfoglia**, 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 quando si utilizza la gestione interna delle chiavi

Se è stata configurata la gestione interna delle chiavi e successivamente sono state spostate le unità abilitate alla protezione da un array di storage a un altro, è necessario riassegnare la chiave di sicurezza al nuovo array di storage per accedere ai dati crittografati sui dischi.

Prima di iniziare

- Nell'array di origine (l'array in cui si rimuovono i dischi), sono stati esportati gruppi di volumi e rimossi i dischi. Nell'array di destinazione, i dischi sono stati reinstallati.

> La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia della riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

  Le istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite nella "Knowledge base di NetApp" . Seguire le istruzioni appropriate per gli array più recenti gestiti da System Manager o per i sistemi legacy.

- 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.
- 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

Quando si utilizza la gestione interna delle chiavi, la chiave di sicurezza viene memorizzata localmente nell'array di storage. Una chiave di sicurezza è una stringa di caratteri condivisa dal controller e dai dischi per l'accesso in lettura/scrittura. Quando i dischi vengono fisicamente rimossi dall'array e installati in un altro, non possono funzionare fino a quando non si fornisce la chiave di sicurezza corretta.

> È possibile creare una chiave interna dalla memoria persistente del controller o una chiave esterna da un server di gestione delle chiavi. Questo argomento descrive lo sblocco dei dati quando viene utilizzata la gestione delle chiavi *interne*. Se è stata utilizzata la gestione delle chiavi *external*, vedere "Sbloccare i dischi quando si utilizza la gestione esterna delle chiavi". Se si sta eseguendo un aggiornamento dei controller e si sta scambiando tutti i controller con la versione hardware più recente, è necessario seguire i diversi passaggi descritti nel centro di documentazione di e-Series e SANtricity, nella "Sbloccare i dischi".

Una volta reinstallate le unità protette in un altro array, tale array rileva le unità e visualizza una condizione di "intervento richiesto" insieme allo stato "chiave di sicurezza necessaria". Per sbloccare i dati dell'unità, selezionare il file della chiave di sicurezza e immettere la password della chiave. (Questa 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. **Opzionale:** posizionare 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.

Al termine

Nell'array di destinazione (l'array con i dischi appena installati), è ora possibile importare gruppi di volumi.

> La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia della riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

Le istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite nella "Knowledge base di NetApp" .

Sbloccare i dischi quando si utilizza la gestione esterna delle chiavi

Se è stata configurata la gestione delle chiavi esterne e successivamente sono state spostate le unità abilitate alla protezione da un array di storage a un altro, è necessario riassegnare la chiave di sicurezza al nuovo array di storage per accedere ai dati crittografati sui dischi.

Prima di iniziare

- Nell'array di origine (l'array in cui si rimuovono i dischi), sono stati esportati gruppi di volumi e rimossi i dischi. Nell'array di destinazione, i dischi sono stati reinstallati.

  > La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia della riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

  Le istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite nella "Knowledge base di NetApp" . Seguire le istruzioni appropriate per gli array più recenti gestiti da System Manager o per i sistemi legacy.

- 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.
- È necessario conoscere l'indirizzo IP e il numero di porta del server di gestione delle chiavi.
- 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

Quando si utilizza la gestione esterna delle chiavi, la chiave di sicurezza viene memorizzata esternamente su un server progettato per proteggere le chiavi di sicurezza. Una chiave di sicurezza è una stringa di caratteri condivisa dal controller e dai dischi per l'accesso in lettura/scrittura. Quando i dischi vengono fisicamente rimossi dall'array e installati in un altro, non possono funzionare fino a quando non si fornisce la chiave di sicurezza corretta.

È possibile creare una chiave interna dalla memoria persistente del controller o una chiave esterna da un server di gestione delle chiavi. Questo argomento descrive lo sblocco dei dati quando viene utilizzata la gestione delle chiavi *esterne*. Se è stata utilizzata la gestione delle chiavi *internal*, vedere "Sbloccare i dischi quando si utilizza la gestione interna delle chiavi". Se si sta eseguendo un aggiornamento dei controller e si sta scambiando tutti i controller con la versione hardware più recente, è necessario seguire i diversi passaggi descritti nel centro di documentazione di e-Series e SANtricity, nella "Sbloccare i dischi".

Una volta reinstallate le unità protette in un altro array, tale array rileva le unità e visualizza una condizione di "intervento richiesto" insieme allo stato "chiave di sicurezza necessaria". Per sbloccare i dati dell'unità, si importa il file della chiave di sicurezza e si immette la password della chiave. (Questa password non corrisponde alla password Administrator dell'array di storage). Durante questa procedura, lo storage array viene configurato in modo da utilizzare un server di gestione chiavi esterno e la chiave protetta risulterà accessibile. È necessario fornire le informazioni di contatto del server per consentire all'array di storage di connettersi e recuperare la chiave di sicurezza.

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 **Create External Key** (Crea chiave esterna).
3. Completare la procedura guidata con le informazioni di connessione e i certificati richiesti.
4. Fare clic su **Test Communication** (verifica comunicazione) per garantire l'accesso al server di gestione

delle chiavi esterno.

5. 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.

6. **Opzionale:** posizionare il mouse su un numero di disco per visualizzare la posizione dell'unità (numero di shelf e numero di alloggiamento).
7. 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.

8. Inserire la password associata al file delle chiavi.

   I caratteri immessi vengono mascherati.

9. 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.

Al termine

Nell'array di destinazione (l'array con i dischi appena installati), è ora possibile importare gruppi di volumi.

> La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia della riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

Le istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite nella "Knowledge base di NetApp" .