Impostazioni

SANtricity 11.6

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/it-it/e-series-santricity-116/sm-settings/how-alerts-work.html on February 12, 2024. Always check docs.netapp.com for the latest.

Sommario

Impostazioni

Avvisi

Concetti

Come funzionano gli avvisi

Gli avvisi informano gli amministratori degli eventi importanti che si verificano sullo storage array. Gli avvisi possono essere inviati tramite e-mail, trap SNMP e syslog.

Il processo di notifica funziona come segue:

1. Un amministratore configura uno o più dei seguenti metodi di avviso in System Manager:
   - **Email** — i messaggi vengono inviati agli indirizzi email.
   - **SNMP** — i trap SNMP vengono inviati a un server SNMP.
   - **Syslog** — i messaggi vengono inviati a un server syslog.
2. Quando il monitor degli eventi dello storage array rileva un problema, scrive le informazioni relative a tale problema nel registro eventi (disponibile dal menu **Support[Event Log]**). Ad esempio, i problemi possono includere eventi come un guasto alla batteria, un componente che passa da ottimale a offline o errori di ridondanza nel controller.
3. Se il monitor degli eventi determina che l'evento è "allertabile", invia una notifica utilizzando i metodi di avviso configurati (e-mail, SNMP e/o syslog). Tutti gli eventi critici sono considerati "allertabili", insieme ad alcuni eventi di avviso e informativi.

Configurazione degli avvisi

È possibile configurare gli avvisi dalla configurazione guidata iniziale (solo per gli avvisi e-mail) o dalla pagina Avvisi. Per verificare la configurazione corrente, andare al **Impostazioni › Avvisi**.

Il riquadro Avvisi visualizza la configurazione degli avvisi, che può essere una delle seguenti:

- Non configurato.
- Configurato; è impostato almeno un metodo di avviso. Per determinare quali metodi di avviso sono configurati, puntare il cursore sul riquadro.

Informazioni sugli avvisi

Gli avvisi possono includere i seguenti tipi di informazioni:

- Nome dell'array di storage.
- Tipo di errore di evento correlato a una voce del registro eventi.
- Data e ora in cui si è verificato l'evento.
- Breve descrizione dell'evento.

> Gli avvisi syslog seguono lo standard di messaggistica RFC 3164.

Terminologia degli avvisi

Scopri in che modo i termini degli avvisi si applicano al tuo array di storage.

Componente	Descrizione
Monitoraggio degli eventi	Il monitor degli eventi risiede nell'array di storage e viene eseguito come attività in background. Quando il monitor degli eventi rileva anomalie sull'array di storage, scrive informazioni sui problemi nel registro eventi. I problemi possono includere eventi come guasti alla batteria, spostamento di un componente da ottimale a offline o errori di ridondanza nel controller. Se il monitor degli eventi determina che l'evento è "allertabile", invia una notifica utilizzando i metodi di avviso configurati (e-mail, SNMP e/o syslog). Tutti gli eventi critici sono considerati "allertabili", insieme ad alcuni eventi di avviso e informativi.
Server di posta	Il server di posta viene utilizzato per inviare e ricevere avvisi e-mail. Il server utilizza il protocollo SMTP (Simple Mail Transfer Protocol).
SNMP	SNMP (Simple Network Management Protocol) è un protocollo standard Internet utilizzato per la gestione e la condivisione delle informazioni tra dispositivi su reti IP.
Trap SNMP	Un trap SNMP è una notifica inviata a un server SNMP. La trap contiene informazioni su problemi significativi con l'array di storage.
Destinazione trap SNMP	Una destinazione trap SNMP è un indirizzo IPv4 o IPv6 del server che esegue un servizio SNMP.
Nome di comunità	Un nome di comunità è una stringa che agisce come una password per i server di rete in un ambiente SNMP.
File MIB	Il file MIB (Management Information base) definisce i dati monitorati e gestiti nell'array di storage. Deve essere copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB è disponibile con il software System Manager sul sito del supporto.
Variabili MIB	Le variabili MIB (Management Information base) possono restituire valori come il nome dell'array di storage, la posizione dell'array e una persona di contatto in risposta a SNMP GetRequests.
Syslog	Syslog è un protocollo utilizzato dalle periferiche di rete per inviare messaggi di evento a un server di registrazione.
UDP	User Datagram Protocol (UDP) è un protocollo di livello di trasporto che specifica un numero di porta di origine e di destinazione nelle intestazioni dei pacchetti.

Come fare

Gestire gli avvisi e-mail

Configurare il server di posta e i destinatari per gli avvisi

Per configurare gli avvisi e-mail, è necessario specificare un indirizzo del server di posta e gli indirizzi e-mail dei destinatari degli avvisi. Sono consentiti fino a 20 indirizzi e-mail.

Prima di iniziare

- L'indirizzo del server di posta deve essere disponibile. L'indirizzo può essere un indirizzo IPv4 o IPv6 o un nome di dominio completo.

  > Per utilizzare un nome di dominio completo, è necessario configurare un server DNS su entrambi i controller. È possibile configurare un server DNS dalla pagina hardware.

- L'indirizzo e-mail da utilizzare come mittente dell'avviso deve essere disponibile. Indirizzo visualizzato nel campo "da" del messaggio di avviso. Nel protocollo SMTP è richiesto un indirizzo mittente; senza di esso, si verifica un errore.
- Gli indirizzi e-mail dei destinatari degli avvisi devono essere disponibili. Il destinatario è in genere un indirizzo per un amministratore di rete o di storage. È possibile inserire fino a 20 indirizzi e-mail.

A proposito di questa attività

Questa attività descrive come configurare il server di posta, inserire gli indirizzi e-mail per il mittente e i destinatari e verificare tutti gli indirizzi e-mail immessi nella pagina Avvisi.

> Gli avvisi e-mail possono essere configurati anche dalla procedura di installazione guidata iniziale.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Email**.

   Se un server di posta elettronica non è ancora configurato, nella scheda e-mail viene visualizzato il messaggio "Configura server di posta".

3. Selezionare **Configura server di posta**.

   Viene visualizzata la finestra di dialogo **Configura server di posta**.

4. Immettere le informazioni sul server di posta, quindi fare clic su **Salva**.
   - **Indirizzo server di posta** — immettere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6 del server di posta.

     > Per utilizzare un nome di dominio completo, è necessario configurare un server DNS su entrambi i controller. È possibile configurare un server DNS dalla pagina **hardware**.

   - **Indirizzo email mittente** — Inserisci un indirizzo email valido da utilizzare come mittente del messaggio. Questo indirizzo viene visualizzato nel campo "da" del messaggio di posta elettronica.
   - **Include contact information in email** — per includere le informazioni di contatto del mittente nel messaggio di avviso, selezionare questa opzione, quindi inserire un nome e un numero di telefono. Dopo aver fatto clic su **Salva**, gli indirizzi e-mail vengono visualizzati nella scheda **e-mail** della pagina

Avvisi.

5. Selezionare **Aggiungi email**.

   Viene visualizzata la finestra di dialogo Aggiungi e-mail.

6. Inserire uno o più indirizzi e-mail per i destinatari degli avvisi, quindi fare clic su **Aggiungi**.

   Gli indirizzi e-mail vengono visualizzati nella pagina Avvisi.

7. Se si desidera assicurarsi che gli indirizzi e-mail siano validi, fare clic su **Test all emails** (verifica tutte le e-mail) per inviare i messaggi di prova ai destinatari.

Risultati

Dopo aver configurato gli avvisi e-mail, il monitor degli eventi invia messaggi e-mail ai destinatari specificati ogni volta che si verifica un evento verificabile.

Modificare gli indirizzi e-mail per gli avvisi

È possibile modificare gli indirizzi e-mail dei destinatari che ricevono gli avvisi e-mail.

Prima di iniziare

L'indirizzo di posta elettronica che si desidera modificare deve essere definito nella scheda Email della pagina Alerts.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Email**.
3. Nella tabella **Indirizzo email**, selezionare l'indirizzo che si desidera modificare, quindi fare clic sull'icona **Modifica** (matita) all'estrema destra.

   La riga diventa un campo modificabile.

4. Inserire un nuovo indirizzo, quindi fare clic sull'icona **Salva** (segno di spunta).

   Per annullare le modifiche, selezionare l'icona **Annulla** (X).

Risultati

La scheda Email della pagina Alerts (Avvisi) visualizza gli indirizzi e-mail aggiornati.

Aggiungere indirizzi e-mail per gli avvisi

È possibile aggiungere fino a 20 destinatari per gli avvisi e-mail.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Email**.
3. Selezionare **Aggiungi email**.

   Viene visualizzata la finestra di dialogo **Aggiungi email**.

4. Nel campo vuoto, immettere un nuovo indirizzo e-mail. Se si desidera aggiungere più indirizzi, selezionare **Aggiungi un'altra e-mail** per aprire un altro campo.
5. Fare clic su **Aggiungi**.

Risultati

Nella scheda **Email** della pagina **Alerts** vengono visualizzati i nuovi indirizzi e-mail.

Eliminare gli indirizzi e-mail o i server di posta per gli avvisi

È possibile rimuovere il server di posta precedentemente definito in modo che gli avvisi non vengano più inviati agli indirizzi di posta elettronica oppure rimuovere singoli indirizzi di posta elettronica.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Email**.
3. Dalla tabella, eseguire una delle seguenti operazioni:
   - Per rimuovere un server di posta in modo che gli avvisi non vengano più inviati agli indirizzi di posta elettronica, selezionare la riga del server di posta.
   - Per rimuovere un indirizzo e-mail in modo che gli avvisi non vengano più inviati a questo indirizzo, selezionare la riga dell'indirizzo e-mail che si desidera eliminare. Il pulsante **Delete** (Elimina) in alto a destra della tabella diventa disponibile per la selezione.
4. Fare clic su **Delete** (Elimina) e confermare l'operazione.

Modificare il server di posta per gli avvisi

È possibile modificare l'indirizzo del server e-mail e l'indirizzo del mittente utilizzati per gli avvisi e-mail.

Prima di iniziare

L'indirizzo del server di posta che si sta modificando deve essere disponibile. L'indirizzo può essere un indirizzo IPv4 o IPv6 o un nome di dominio completo.

> Per utilizzare un nome di dominio completo, è necessario configurare un server DNS su entrambi i controller. È possibile configurare un server DNS dalla pagina hardware.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Email**.
3. Selezionare **Configura server di posta**.

   Viene visualizzata la finestra di dialogo Configura server di posta.

4. Modificare l'indirizzo del server di posta, le informazioni sul mittente e le informazioni di contatto.
   - **Indirizzo del server di posta** — consente di modificare il nome di dominio completo, l'indirizzo IPv4 o l'indirizzo IPv6 del server di posta.

> Per utilizzare un nome di dominio completo, è necessario configurare un server DNS su entrambi i controller. È possibile configurare un server DNS dalla pagina hardware.

- **Email sender address** — Modifica l'indirizzo email da utilizzare come mittente del messaggio. Questo indirizzo viene visualizzato nel campo "da" del messaggio di posta elettronica.
- **Include contact information in email** — per modificare le informazioni di contatto del mittente, selezionare questa opzione, quindi modificare il nome e il numero di telefono.

5. Fare clic su **Save** (Salva).

Gestire gli avvisi SNMP

Configurare comunità e destinazioni per gli avvisi SNMP

Per configurare gli avvisi SNMP (Simple Network Management Protocol), è necessario identificare almeno un server in cui il monitor degli eventi dell'array di storage può inviare trap SNMP. La configurazione richiede un nome di comunità e un indirizzo IP per il server.

Prima di iniziare

- Un server di rete deve essere configurato con un'applicazione di servizio SNMP. È necessario l'indirizzo di rete di questo server (un indirizzo IPv4 o IPv6), in modo che il monitor eventi possa inviare messaggi trap a tale indirizzo. È possibile utilizzare più di un server (sono consentiti fino a 10 server).
- È necessario creare un nome di comunità composto solo da caratteri ASCII stampabili. Il nome di comunità, che è una stringa che agisce come una password per i server di rete, viene in genere creato da un amministratore di rete. È possibile creare fino a 256 community.
- Il file MIB (Management Information base) è stato copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB definisce i dati monitorati e gestiti.

  Se non si dispone del file MIB, è possibile ottenerlo dal sito NetApp Support:

  - Passare a. "Supporto NetApp".
  - Fare clic su **Downloads**.
  - Fare clic su **Software**.
  - Individuare il software di gestione (ad esempio, Gestore di sistema di SANtricity), quindi fare clic su **Go!** (Vai) a destra.
  - Fare clic su**View & Download** (Visualizza e scarica) sulla versione più recente.
  - Fare clic su **continua** nella parte inferiore della pagina.
  - Accettare l'EULA.
  - Scorrere verso il basso fino a visualizzare **MIB file for SNMP trap**, quindi fare clic sul collegamento per scaricare il file.

A proposito di questa attività

Questa attività descrive come identificare il server SNMP per le destinazioni trap, quindi verificare la configurazione.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

Se una community non è ancora configurata, nella scheda SNMP viene visualizzato "Configure Communities" (Configura community).

3. Selezionare **Configura community**.

   Viene visualizzata la finestra di dialogo **Configura comunità**.

4. Nel campo **Nome comunità**, immettere una o più stringhe di comunità per i server di rete, quindi fare clic su **Salva**.

   Nella pagina Avvisi viene visualizzato "Add Trap Destinations" (Aggiungi destinazioni trap).

5. Selezionare **Add Trap Destinations** (Aggiungi destinazioni trap).

   Viene visualizzata la finestra di dialogo **Add Trap Destinations** (Aggiungi destinazioni trap).

6. Inserire una o più destinazioni trap, selezionare i nomi di comunità associati, quindi fare clic su **Aggiungi**.
   - **Destinazione trap** — immettere un indirizzo IPv4 o IPv6 del server che esegue un servizio SNMP.
   - **Nome di comunità** — dal menu a discesa, selezionare il nome di comunità per questa destinazione trap. (Se è stato definito un solo nome di comunità, il nome viene già visualizzato in questo campo).
   - **Send Authentication Failure Trap** — selezionare questa opzione (la casella di controllo) se si desidera avvisare la destinazione della trap ogni volta che una richiesta SNMP viene rifiutata a causa di un nome di comunità non riconosciuto. Dopo aver fatto clic su **Aggiungi**, le destinazioni trap e i nomi di comunità associati vengono visualizzati nella scheda **SNMP** della pagina **Avvisi**.
7. Per assicurarsi che un trap sia valido, selezionare una destinazione trap dalla tabella, quindi fare clic su **Test Trap Destination** (destinazione trap test) per inviare un trap di test all'indirizzo configurato.

Risultati

Il monitor degli eventi invia trap SNMP ai server ogni volta che si verifica un evento verificabile.

Modificare i nomi di comunità per i trap SNMP

È possibile modificare i nomi di comunità per i trap SNMP e associare un nome di comunità diverso a una destinazione dei trap SNMP.

Prima di iniziare

È necessario creare un nome di comunità composto solo da caratteri ASCII stampabili. Il nome di comunità, che è una stringa che agisce come una password per i server di rete, viene creato da un amministratore di rete.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi di comunità vengono visualizzati nella tabella.

3. Modificare i nomi delle community come segue:
   - Per modificare un nome di comunità, selezionare **Configura community**. Immettere il nuovo nome di comunità, quindi fare clic su **Salva**. I nomi di comunità possono essere costituiti solo da caratteri ASCII stampabili.

- Per associare un nome di comunità a una nuova destinazione trap, selezionare il nome della community dalla tabella, quindi fare clic sull'icona **Edit** (matita) all'estrema destra. Dall'elenco a discesa Community Name (Nome comunità), selezionare un nuovo nome di comunità per una destinazione trap SNMP, quindi fare clic sull'icona **Save** (Salva) (segno di spunta).

  Per annullare le modifiche, selezionare l'icona **Annulla** (X).

Risultati

La scheda **SNMP** della pagina **Alerts** visualizza le community aggiornate.

Aggiungere nomi di comunità per i trap SNMP

È possibile aggiungere fino a 256 nomi di comunità per i trap SNMP.

Prima di iniziare

È necessario creare i nomi di comunità. Il nome di comunità, che è una stringa che agisce come una password per i server di rete, viene in genere creato da un amministratore di rete. È costituito solo da caratteri ASCII stampabili.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi di comunità vengono visualizzati nella tabella.

3. Selezionare **Configura community**.

   Viene visualizzata la finestra di dialogo Configura comunità.

4. Selezionare **Aggiungi un'altra community**.
5. Immettere il nuovo nome di comunità, quindi fare clic su **Salva**.

Risultati

Il nuovo nome di comunità viene visualizzato nella scheda **SNMP** della pagina **Alerts**.

Rimuovere il nome di comunità per i trap SNMP

È possibile rimuovere un nome di comunità per i trap SNMP.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi di comunità vengono visualizzati nella pagina Avvisi.

3. Selezionare **Configura community**.

   Viene visualizzata la finestra di dialogo **Configura comunità**.

4. Selezionare il nome della community che si desidera eliminare, quindi fare clic sull'icona **Rimuovi** (X) all'estrema destra.

Se le destinazioni trap sono associate a questo nome di comunità, la finestra di dialogo **Conferma rimozione comunità** mostra gli indirizzi di destinazione trap interessati.

5. Confermare l'operazione, quindi fare clic su **Rimuovi**.

Risultati

Il nome di comunità e la destinazione trap associata vengono rimossi dalla pagina **Alerts**.

Configurare le variabili SNMP MIB

Per gli avvisi SNMP, è possibile configurare facoltativamente le variabili MIB (Management Information base) che vengono visualizzate nei trap SNMP. Queste variabili possono restituire il nome dell'array di storage, la posizione dell'array e una persona di contatto.

Prima di iniziare

Il file MIB deve essere copiato e compilato sul server con l'applicazione di servizio SNMP.

Se non si dispone di un file MIB, è possibile ottenerlo come segue:

- Passare a. "Supporto NetApp".
- Fare clic su **Downloads**.
- Fare clic su **Software**.
- Individuare il software di gestione (ad esempio, Gestore di sistema di SANtricity), quindi fare clic su **Go!** (Vai) a destra.
- Fare clic su **View & Download** (Visualizza e scarica) nella versione più recente.
- Fare clic su **continua** nella parte inferiore della pagina.
- Accettare l'EULA.
- Scorrere verso il basso fino a visualizzare **MIB file for SNMP trap**, quindi fare clic sul collegamento per scaricare il file.

A proposito di questa attività

Questa attività descrive come definire le variabili MIB per i trap SNMP. Queste variabili possono restituire i seguenti valori in risposta a SNMP GetRequests:

- `sysName` (nome dell'array di storage)
- `sysLocation` (posizione dello storage array)
- `sysContact` (nome di un amministratore)

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.
3. Selezionare **Configure SNMP MIB variables** (Configura variabili SNMP MIB).

   Viene visualizzata la finestra di dialogo Configura variabili MIB SNMP.

4. Immettere uno o più dei seguenti valori, quindi fare clic su **Save** (Salva).

- **Name** — il valore per la variabile MIB `sysName`. Ad esempio, inserire un nome per l'array di storage.
- **Location** — il valore della variabile MIB `sysLocation`. Ad esempio, inserire una posizione dell'array di storage.
- **Contatto** — il valore della variabile MIB `sysContact`. Ad esempio, inserire un amministratore responsabile dello storage array.

Risultati

Questi valori vengono visualizzati nei messaggi trap SNMP per gli avvisi degli array di storage.

Aggiungere destinazioni trap per gli avvisi SNMP

È possibile aggiungere fino a 10 server per l'invio di trap SNMP.

Prima di iniziare

- Il server di rete che si desidera aggiungere deve essere configurato con un'applicazione di servizio SNMP. È necessario l'indirizzo di rete di questo server (un indirizzo IPv4 o IPv6), in modo che il monitor eventi possa inviare messaggi trap a tale indirizzo. È possibile utilizzare più di un server (sono consentiti fino a 10 server).
- È necessario creare un nome di comunità composto solo da caratteri ASCII stampabili. Il nome di comunità, che è una stringa che agisce come una password per i server di rete, viene in genere creato da un amministratore di rete. È possibile creare fino a 256 community.
- Il file MIB (Management Information base) è stato copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB definisce i dati monitorati e gestiti.

  Se non si dispone del file MIB, è possibile ottenerlo dal sito NetApp Support:

  - Passare a. "Supporto NetApp".
  - Fare clic su **Downloads**.
  - Fare clic su **Software**.
  - Individuare il software di gestione (ad esempio, Gestore di sistema di SANtricity), quindi fare clic su **Go!** (Vai) a destra.
  - Fare clic su **View & Download** (Visualizza e scarica) nella versione più recente.
  - Fare clic su **continua** nella parte inferiore della pagina.
  - Accettare l'EULA.
  - Scorrere verso il basso fino a visualizzare **MIB file for SNMP trap**, quindi fare clic sul collegamento per scaricare il file.

Fasi

1. Selezionare **Impostazioni** > **Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap attualmente definite vengono visualizzate nella tabella.

3. Selezionare **Add Trap Desinations** (Aggiungi Desination trap).

   Viene visualizzata la finestra di dialogo Add Trap Destinations (Aggiungi destinazioni trap).

4. Inserire una o più destinazioni trap, selezionare i nomi di comunità associati, quindi fare clic su **Aggiungi**.

- **Destinazione trap** — immettere un indirizzo IPv4 o IPv6 del server che esegue un servizio SNMP.
- **Nome di comunità** — dal menu a discesa, selezionare il nome di comunità per questa destinazione trap. (Se è stato definito un solo nome di comunità, il nome viene già visualizzato in questo campo).
- **Send Authentication Failure Trap** — selezionare questa opzione (la casella di controllo) se si desidera avvisare la destinazione della trap ogni volta che una richiesta SNMP viene rifiutata a causa di un nome di comunità non riconosciuto. Dopo aver fatto clic su **Aggiungi**, nella tabella vengono visualizzate le destinazioni trap e i nomi di comunità associati.

5. Per assicurarsi che un trap sia valido, selezionare una destinazione trap dalla tabella, quindi fare clic su **Test Trap Destination** (destinazione trap test) per inviare un trap di test all'indirizzo configurato.

Risultati

Il monitor degli eventi invia trap SNMP ai server ogni volta che si verifica un evento verificabile.

Eliminare le destinazioni trap

È possibile eliminare un indirizzo di destinazione trap in modo che il monitor eventi dell'array di storage non invii più trap SNMP a tale indirizzo.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Gli indirizzi di destinazione trap vengono visualizzati nella tabella.

3. Selezionare una destinazione trap, quindi fare clic su **Delete** (Elimina) in alto a destra nella pagina.
4. Confermare l'operazione, quindi fare clic su **Delete** (Elimina).

   L'indirizzo di destinazione non viene più visualizzato nella pagina **Alerts**.

Risultati

La destinazione dei trap cancellati non riceve più trap SNMP dal monitor degli eventi dell'array di storage.

Gestire gli avvisi syslog

Configurare il server syslog per gli avvisi

Per configurare gli avvisi syslog, è necessario immettere un indirizzo del server syslog e una porta UDP. Sono consentiti fino a cinque server syslog.

Prima di iniziare

- L'indirizzo del server syslog deve essere disponibile. Questo indirizzo può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Il numero della porta UDP del server syslog deve essere disponibile. Questa porta è generalmente 514.

A proposito di questa attività

Questa attività descrive come inserire l'indirizzo e la porta per il server syslog, quindi verificare l'indirizzo immesso.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Syslog**.

   Se un server syslog non è ancora definito, nella pagina **Alerts** viene visualizzato "Add Syslog Servers" (Aggiungi server Syslog).

3. Fare clic su **Aggiungi server Syslog**.

   Viene visualizzata la finestra di dialogo **Add Syslog Server** (Aggiungi server Syslog).

4. Inserire le informazioni relative a uno o più server syslog (massimo cinque), quindi fare clic su **Aggiungi**.
   - **Server Address** — inserire un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
   - **UDP Port** — in genere, la porta UDP per syslog è 514. Nella tabella vengono visualizzati i server syslog configurati.
5. Per inviare un avviso di test agli indirizzi del server, selezionare **Test All Syslog Servers** (verifica tutti i server Syslog).

Risultati

Il monitor degli eventi invia avvisi al server syslog ogni volta che si verifica un evento verificabile.

Modificare i server syslog per gli avvisi

È possibile modificare l'indirizzo del server utilizzato per ricevere gli avvisi syslog.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Syslog**.
3. Dalla tabella, selezionare un indirizzo server syslog, quindi fare clic sull'icona **Edit** (matita) a destra.

   La riga diventa un campo modificabile.

4. Modificare l'indirizzo del server e il numero della porta UDP, quindi fare clic sull'icona **Salva** (segno di spunta).

Risultati

L'indirizzo del server aggiornato viene visualizzato nella tabella.

Aggiungere server syslog per gli avvisi

È possibile aggiungere un massimo di cinque server per gli avvisi syslog.

Prima di iniziare

- L'indirizzo del server syslog deve essere disponibile. Questo indirizzo può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Il numero della porta UDP del server syslog deve essere disponibile. Questa porta è generalmente 514.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Syslog**.

3. Selezionare **Aggiungi server Syslog**.

   Viene visualizzata la finestra di dialogo Add Syslog Server (Aggiungi server Syslog).

4. Selezionare **Aggiungi un altro server syslog**.
5. Inserire le informazioni relative al server syslog, quindi fare clic su **Aggiungi**.
   - **Syslog Server Address** — inserire un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
   - **UDP Port** — in genere, la porta UDP per syslog è 514.

   È possibile configurare fino a cinque server syslog.

Risultati

Gli indirizzi del server syslog vengono visualizzati nella tabella.

Eliminare i server syslog per gli avvisi

È possibile eliminare un server syslog in modo che non riceva più avvisi.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Syslog**.
3. Selezionare un indirizzo del server syslog, quindi fare clic su **Remove** (Rimuovi) dall'alto a destra.

   Viene visualizzata la finestra di dialogo Conferma eliminazione server Syslog.

4. Confermare l'operazione, quindi fare clic su **Delete** (Elimina).

Risultati

Il server rimosso non riceve più avvisi dal monitor eventi.

FAQ

Cosa fare se gli avvisi sono disattivati?

Se si desidera che gli amministratori ricevano notifiche su eventi importanti che si verificano nell'array di storage, è necessario configurare un metodo di avviso.

Per gli array di storage gestiti con Gestore di sistema di SANtricity, è possibile configurare gli avvisi dalla pagina Avvisi. Le notifiche di avviso possono essere inviate tramite e-mail, trap SNMP o messaggi syslog. Inoltre, gli avvisi e-mail possono essere configurati dall'installazione guidata iniziale.

Come si configurano gli avvisi SNMP o syslog?

Oltre agli avvisi via email, è possibile configurare gli avvisi in modo che vengano inviati tramite trap SNMP (Simple Network Management Protocol) o messaggi syslog.

Per configurare gli avvisi SNMP o syslog, accedere al **Impostazioni › Avvisi**.

Perché i timestamp non sono coerenti tra l'array e gli avvisi?

Quando lo storage array invia avvisi, non corregge il fuso orario del server o dell'host di destinazione che riceve gli avvisi. Invece, l'array di storage utilizza l'ora locale (GMT) per creare l'indicazione dell'ora utilizzata per il record di avviso. Di conseguenza, potrebbero verificarsi delle incoerenze tra i timestamp per lo storage array e il server o l'host che riceve un avviso.

Poiché l'array di storage non corregge il fuso orario durante l'invio degli avvisi, l'indicazione dell'ora sugli avvisi è relativa al GMT, con un offset del fuso orario pari a zero. Per calcolare un indicatore data e ora appropriato al fuso orario locale, è necessario determinare l'offset dell'ora dal GMT, quindi aggiungere o sottrarre tale valore dai contrassegni data e ora.

> Per evitare questo problema, configurare il protocollo NTP (Network Time Protocol) sui controller degli array di storage. NTP garantisce che i controller siano sempre sincronizzati con l'ora corretta.

System (sistema): Impostazioni dello storage array

Concetti

Performance e impostazioni della cache

La memoria cache è un'area di storage volatile temporaneo sul controller che ha un tempo di accesso più rapido rispetto ai supporti del disco.

Con il caching, le performance di i/o complessive possono essere aumentate come segue:

- I dati richiesti dall'host per una lettura potrebbero essere già nella cache da un'operazione precedente, eliminando così la necessità di accesso al disco.
- I dati di scrittura vengono scritti inizialmente nella cache, consentendo all'applicazione di continuare invece di attendere la scrittura dei dati sul disco.

Le impostazioni predefinite della cache soddisfano i requisiti della maggior parte degli ambienti, ma è possibile modificarle se necessario.

Impostazioni della cache dell'array di storage

Per tutti i volumi nell'array di storage, è possibile specificare i seguenti valori dalla pagina System (sistema):

- **Valore iniziale per il flushing** — la percentuale di dati non scritti nella cache che attiva un flush della cache (scrittura su disco). Quando la cache contiene la percentuale iniziale specificata di dati non scritti, viene attivato un flusso. Per impostazione predefinita, il controller avvia lo svuotamento della cache quando la cache raggiunge il 80% di memoria piena.
- **Cache block size** — dimensione massima di ciascun blocco di cache, un'unità organizzativa per la gestione della cache. La dimensione predefinita del blocco della cache è 8 KiB, ma può essere impostata su 4, 8, 16 o 32 KiB. Idealmente, la dimensione del blocco della cache dovrebbe essere impostata sulla dimensione i/o predominante delle applicazioni. I file system o le applicazioni di database utilizzano generalmente dimensioni inferiori, mentre le dimensioni maggiori sono adatte per le applicazioni che richiedono un trasferimento di dati di grandi dimensioni o l'i/o sequenziale

Impostazioni della cache del volume

Per i singoli volumi in un array di storage, è possibile specificare i seguenti valori dalla pagina Volumes (**Storage › Volumes**):

- **Read caching** — la cache di lettura è un buffer che memorizza i dati letti dai dischi. I dati di un'operazione di lettura potrebbero essere già presenti nella cache di un'operazione precedente, eliminando così la necessità di accedere ai dischi. I dati rimangono nella cache di lettura fino a quando non vengono scaricati.
  - **Dynamic Read cache prefetch** — Dynamic cache Read prefetch consente al controller di copiare ulteriori blocchi di dati sequenziali nella cache durante la lettura dei blocchi di dati da un disco alla cache. Questo caching aumenta la possibilità che le future richieste di dati possano essere compilate dalla cache. Il prefetch dinamico della lettura della cache è importante per le applicazioni multimediali che utilizzano l'i/o sequenziale La velocità e la quantità di dati precaricati nella cache vengono regolate automaticamente in base alla velocità e alle dimensioni della richiesta dell'host. L'accesso casuale non fa sì che i dati vengano precaricati nella cache. Questa funzione non si applica quando il caching in lettura è disattivato.
- **Write caching** — la cache di scrittura è un buffer che memorizza i dati dell'host che non sono ancora stati scritti sui dischi. I dati rimangono nella cache di scrittura fino a quando non vengono scritti sui dischi. Il caching in scrittura può aumentare le performance di i/O.

> **Possibile perdita di dati** — se si attiva l'opzione Write caching without batteries e non si dispone di un alimentatore universale per la protezione, si potrebbero perdere i dati. Inoltre, è possibile perdere i dati se non si dispone di batterie del controller e si attiva l'opzione Write caching without batteries (cache di scrittura senza batterie).

  - **Write caching senza batterie** — l'impostazione write caching senza batterie consente di continuare il caching in scrittura anche quando le batterie sono mancanti, guaste, completamente scariche o non completamente cariche. La scelta del caching in scrittura senza batterie non è generalmente consigliata, in quanto i dati potrebbero andare persi in caso di interruzione dell'alimentazione. In genere, il caching in scrittura viene disattivato temporaneamente dal controller fino a quando le batterie non vengono caricate o non viene sostituita una batteria guasta.
  - **Cache in scrittura con mirroring** — il caching in scrittura con mirroring si verifica quando i dati scritti nella memoria cache di un controller vengono scritti anche nella memoria cache dell'altro controller. Pertanto, se un controller si guasta, l'altro può completare tutte le operazioni di scrittura in sospeso. Il mirroring della cache di scrittura è disponibile solo se il caching di scrittura è attivato e sono presenti due controller. Il caching in scrittura con mirroring è l'impostazione predefinita alla creazione del volume.

Panoramica del bilanciamento automatico del carico

Il bilanciamento automatico del carico offre una migliore gestione delle risorse di i/o reagendo in modo dinamico alle variazioni di carico nel tempo e regolando automaticamente la proprietà del controller del volume per correggere eventuali problemi di sbilanciamento del carico quando i carichi di lavoro si spostano tra i controller.

Il carico di lavoro di ciascun controller viene costantemente monitorato e, grazie alla collaborazione dei driver multipath installati sugli host, può essere automaticamente bilanciato quando necessario. Quando il carico di lavoro viene riregolato automaticamente tra i controller, l'amministratore dello storage viene alleggerito dall'onere di regolare manualmente la proprietà del controller di volume per adattarsi alle modifiche di carico sull'array di storage.

Quando il bilanciamento automatico del carico è attivato, esegue le seguenti funzioni:

- Monitora e bilancia automaticamente l'utilizzo delle risorse dei controller.
- Regola automaticamente la proprietà del controller del volume quando necessario, ottimizzando in tal modo la larghezza di banda i/o tra gli host e lo storage array.

Attivazione e disattivazione del bilanciamento automatico del carico

Il bilanciamento automatico del carico è attivato per impostazione predefinita su tutti gli array di storage.

È possibile disattivare il bilanciamento automatico del carico sull'array di storage per i seguenti motivi:

- Non si desidera modificare automaticamente la proprietà del controller di un determinato volume per bilanciare il carico di lavoro.
- Si opera in un ambiente altamente ottimizzato in cui la distribuzione del carico è appositamente configurata per ottenere una distribuzione specifica tra i controller.

Tipi di host che supportano la funzione di bilanciamento automatico del carico

Anche se il bilanciamento automatico del carico è attivato a livello di array di storage, il tipo di host selezionato per un cluster di host o host ha un'influenza diretta sul funzionamento della funzione.

Durante il bilanciamento del carico di lavoro dell'array di storage tra controller, la funzione di bilanciamento automatico del carico tenta di spostare volumi accessibili da entrambi i controller e mappati solo a un host o a un cluster host in grado di supportare la funzione di bilanciamento automatico del carico.

Questo comportamento impedisce a un host di perdere l'accesso a un volume a causa del processo di bilanciamento del carico; tuttavia, la presenza di volumi mappati agli host che non supportano il bilanciamento automatico del carico influisce sulla capacità dell'array di storage di bilanciare il carico di lavoro. Per bilanciare il carico di lavoro, il driver multipath deve supportare TPGS e il tipo di host deve essere incluso nella tabella seguente.

> Affinché un cluster host possa essere considerato in grado di eseguire il bilanciamento automatico del carico, tutti gli host del gruppo devono essere in grado di supportare il bilanciamento automatico del carico.

Tipo di host che supporta il bilanciamento automatico del carico	Con questo driver multipath
Windows o Windows Clustered	MPIO con NetApp e-Series DSM
Linux DM-MP (kernel 3.10 o successivo)	DM-MP con `scsi_dh_alua` gestore di dispositivi
VMware	Plug-in multipathing nativo (NMP) con `VMW_SATP_ALUA Storage Array Type` plug-in

> Con eccezioni minori, i tipi di host che non supportano il bilanciamento automatico del carico continuano a funzionare normalmente, indipendentemente dal fatto che la funzione sia attivata o meno. Un'eccezione è rappresentata dal fatto che se un sistema presenta un failover, gli array di storage spostano di nuovo i volumi non mappati o non assegnati al controller proprietario quando il percorso dei dati ritorna. Tutti i volumi mappati o assegnati a host con bilanciamento del carico non automatico non vengono spostati.

Vedere "Tool di matrice di interoperabilità" Per informazioni sulla compatibilità di driver multipath specifici, livello di sistema operativo e supporto del vassoio del disco del controller.

Verifica della compatibilità del sistema operativo con la funzione di bilanciamento automatico del carico

Verificare la compatibilità del sistema operativo con la funzione di bilanciamento automatico del carico prima di configurare un nuovo sistema (o di migrare un sistema esistente).

1. Accedere alla "Tool di matrice di interoperabilità" per trovare la soluzione e verificare il supporto.

   Se il sistema esegue Red Hat Enterprise Linux 6 o SUSE Linux Enterprise Server 11, contattare il supporto tecnico.

2. Aggiornare e configurare `/etc/multipath.conf file`.
3. Assicurarsi che entrambi `retain_attached_device_handler` e. `detect_prio` sono impostati su `yes` per il vendor e il prodotto applicabili, oppure utilizzare le impostazioni predefinite.

Tipo di sistema operativo host predefinito

Il tipo di host predefinito viene utilizzato dall'array di storage quando gli host sono inizialmente connessi. Definisce il modo in cui i controller dell'array di storage funzionano con il sistema operativo dell'host quando si accede ai volumi. È possibile modificare il tipo di host in caso di necessità di modificare il funzionamento dello storage array rispetto agli host ad esso collegati.

In genere, è necessario modificare il tipo di host predefinito prima di connettere gli host all'array di storage o quando si collegano altri host.

Tenere presenti le seguenti linee guida:

- Se tutti gli host che si desidera connettere all'array di storage hanno lo stesso sistema operativo (ambiente host omogeneo), modificare il tipo di host in modo che corrisponda al sistema operativo.
- Se si prevede di collegare host con sistemi operativi diversi allo storage array (ambiente host eterogeneo), modificare il tipo di host in modo che corrisponda alla maggior parte dei sistemi operativi degli host.

  Ad esempio, se si connettono otto host diversi all'array di storage e sei di questi host eseguono un sistema operativo Windows, è necessario selezionare Windows come tipo di sistema operativo host predefinito.

- Se la maggior parte degli host connessi dispone di diversi sistemi operativi, impostare il tipo di host su Factory Default (impostazione predefinita).

  Ad esempio, se si collegano otto host diversi all'array di storage e due di questi host eseguono un sistema operativo Windows, tre eseguono un sistema operativo VMware, Altri tre sistemi operativi Linux sono in esecuzione, è necessario selezionare Factory Default (predefinito) come tipo di sistema operativo host predefinito.

Come fare

Modificare il nome dell'array di storage

È possibile modificare il nome dell'array di storage visualizzato nella barra del titolo di Gestore di sistema di SANtricity.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Generale**, cercare il campo **Nome:**.

   Se non è stato definito un nome di array di storage, in questo campo viene visualizzato "Sconosciuto".

3. Fare clic sull'icona **Edit** (matita) accanto al nome dell'array di storage.

   Il campo diventa modificabile.

4. Immettere un nuovo nome.

   Un nome può contenere lettere, numeri e caratteri speciali sottolineatura (_), trattino (-) e cancelletto (n.). Un nome non può contenere spazi. Un nome può avere una lunghezza massima di 30 caratteri. Il nome deve essere univoco.

5. Fare clic sull'icona **Salva** (segno di spunta).

   Se si desidera chiudere il campo modificabile senza apportare modifiche, fare clic sull'icona **Annulla** (X).

Risultati

Il nuovo nome viene visualizzato nella barra del titolo di Gestore di sistema di SANtricity.

Accendere le spie di localizzazione degli array di storage

Per individuare la posizione fisica di un array di storage in un cabinet, è possibile accendere i relativi indicatori LED.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **General**, fare clic su **Turn on Storage Array Locator Lights**.

   Viene visualizzata la finestra di dialogo **Turn on Storage Array Locator Lights** (attiva indicatori array di storage) e si accendono le spie di localizzazione degli array di storage corrispondenti.

3. Una volta individuato fisicamente lo storage array, tornare alla finestra di dialogo e selezionare **Spegni**.

Risultati

Le luci di individuazione si spengono e la finestra di dialogo si chiude.

Sincronizzare gli orologi degli array di storage

Se il protocollo NTP (Network Time Protocol) non è attivato, è possibile impostare manualmente gli orologi sui controller in modo che siano sincronizzati con il client di gestione (il sistema utilizzato per eseguire il browser che accede a Gestore di sistema di SANtricity).

A proposito di questa attività

La sincronizzazione garantisce che i timbri dell'ora dell'evento nel registro eventi corrispondano ai timestamp

scritti nei file di registro dell'host. Durante il processo di sincronizzazione, i controller rimangono disponibili e operativi.

> Se NTP è attivato in System Manager, non utilizzare questa opzione per sincronizzare gli orologi. Al contrario, NTP sincronizza automaticamente i clock con un host esterno utilizzando SNTP (Simple Network Time Protocol).

> Dopo la sincronizzazione, si potrebbe notare che le statistiche delle performance vengono perse o inclinate, che le pianificazioni vengono influenzate (ASUP, snapshot, ecc.) e che i timestamp nei dati del registro risultano inclinati. L'utilizzo di NTP evita questo problema.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **General**, fare clic su **Synchronize Storage Array Clocks** (Sincronizza blocchi array di storage).

   Viene visualizzata la finestra di dialogo Synchronize Storage Array Blocks (Sincronizza blocchi array di storage) Mostra la data e l'ora correnti dei controller e del computer utilizzato come client di gestione.

   > Per gli array di storage simplex, viene visualizzato un solo controller.

3. Se gli orari visualizzati nella finestra di dialogo non corrispondono, fare clic su **Synchronize** (Sincronizza).

Risultati

Una volta completata la sincronizzazione, i timestamp degli eventi sono gli stessi per il registro eventi e per i registri host.

Salvare la configurazione dello storage array

È possibile salvare le informazioni di configurazione di uno storage array in un file di script per risparmiare tempo durante la configurazione di storage array aggiuntivi con la stessa configurazione.

Prima di iniziare

Lo storage array non deve essere sottoposto a operazioni che modificano le impostazioni di configurazione logica. Esempi di queste operazioni includono la creazione o l'eliminazione di volumi, il download del firmware del controller, l'assegnazione o la modifica di dischi hot spare o l'aggiunta di capacità (dischi) a un gruppo di volumi.

A proposito di questa attività

Il salvataggio della configurazione dello storage array genera uno script CLI (Command Line Interface) che contiene le impostazioni dello storage array, la configurazione del volume, la configurazione dell'host o le assegnazioni host-to-volume per uno storage array. È possibile utilizzare questo script CLI generato per replicare una configurazione in un altro array di storage con la stessa configurazione hardware.

Tuttavia, non si consiglia di utilizzare questo script CLI generato per il disaster recovery. Invece, per eseguire un ripristino del sistema, utilizzare il file di backup del database di configurazione creato manualmente o contattare il supporto tecnico per ottenere questi dati dai dati di supporto automatico più recenti.

Questa operazione *non* salva queste impostazioni:

- La durata della batteria

- L'ora del giorno del controller
- Le impostazioni della memoria ad accesso casuale statica non volatile (NVSRAM)
- Qualsiasi funzionalità premium
- La password dello storage array
- Lo stato operativo e gli stati dei componenti hardware
- Lo stato operativo (eccetto ottimale) e gli stati dei gruppi di volumi
- Servizi di copia, come il mirroring e la copia del volume

> **Rischio di errori dell'applicazione** — non utilizzare questa opzione se lo storage array sta eseguendo un'operazione che modificherà qualsiasi impostazione di configurazione logica. Esempi di queste operazioni includono la creazione o l'eliminazione di volumi, il download del firmware del controller, l'assegnazione o la modifica di dischi hot spare o l'aggiunta di capacità (dischi) a un gruppo di volumi.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Selezionare **Save Storage Array Configuration** (Salva configurazione array di storage).
3. Selezionare gli elementi della configurazione che si desidera salvare:
   - **Impostazioni array di storage**
   - **Configurazione del volume**
   - **Configurazione host**
   - **Assegnazioni host-to-volume**

   > Se si seleziona la voce **host-to-volume assignments**, per impostazione predefinita vengono selezionate anche la voce **Volume Configuration** (Configurazione volume) e la voce **host Configuration** (Configurazione host). Non è possibile salvare **assegnazioni host-to-volume** senza salvare anche **Configurazione volume** e **Configurazione host**.

4. Fare clic su **Save** (Salva).

   Il file viene salvato nella cartella Download del browser con il nome `storage-array-configuration.cfg`.

Al termine

Per caricare la configurazione dell'array di storage salvata in un altro array di storage, utilizzare l'interfaccia della riga di comando (SMcli) di SANtricity con `-f` per applicare `.cfg` file.

> È inoltre possibile caricare una configurazione di array di storage in altri array di storage utilizzando l'interfaccia di Unified Manager (selezionare **Gestisci › Import Settings**).

Configurazione chiara degli array di storage

Utilizzare l'operazione Clear Configuration (Cancella configurazione) per eliminare tutti i pool, i gruppi di volumi, i volumi, le definizioni degli host e le assegnazioni degli host dall'array di storage.

Prima di iniziare

- Prima di cancellare la configurazione dello storage array, eseguire il backup dei dati.

A proposito di questa attività

Sono disponibili due opzioni di configurazione Clear Storage Array:

- **Volume** — in genere, è possibile utilizzare l'opzione Volume per riconfigurare un array di storage di test come array di storage di produzione. Ad esempio, è possibile configurare un array di storage per il test e, al termine del test, rimuovere la configurazione di test e configurare l'array di storage per un ambiente di produzione.
- **Storage Array** - in genere, è possibile utilizzare l'opzione Storage Array per spostare uno storage array in un altro reparto o gruppo. Ad esempio, è possibile utilizzare uno storage array in Engineering e ora Engineering sta ottenendo un nuovo storage array, quindi si desidera spostare lo storage array corrente in Administration, dove verrà riconfigurato.

  L'opzione Storage Array elimina alcune impostazioni aggiuntive.

	Volume	Array di storage
Elimina pool e gruppi di volumi	X	X
Elimina i volumi	X	X
Elimina host e cluster di host	X	X
Elimina le assegnazioni degli host	X	X
Elimina il nome dell'array di storage		X
Ripristina le impostazioni predefinite della cache dell'array di storage		X

Rischio di perdita di dati — questa operazione elimina tutti i dati dall'array di storage. (Non esegue una cancellazione sicura). Non è possibile annullare questa operazione dopo l'avvio. Eseguire questa operazione solo se richiesto dal supporto tecnico.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Selezionare **Clear Storage Array Configuration** (Cancella configurazione array di storage).
3. Nell'elenco a discesa, selezionare **Volume** o **Storage Array**.
4. **Opzionale:** se si desidera salvare la configurazione (non i dati), utilizzare i collegamenti nella finestra di dialogo.
5. Confermare che si desidera eseguire l'operazione.

Risultati

- La configurazione corrente viene eliminata, distruggendo tutti i dati esistenti sull'array di storage.
- Tutti i dischi non sono assegnati.

Configurare il banner di accesso

È possibile creare un banner di accesso che viene presentato agli utenti prima di stabilire le sessioni in Gestore di sistema di SANtricity. Il banner può includere un avviso e un messaggio di consenso.

A proposito di questa attività

Quando si crea un banner, questo viene visualizzato prima della schermata di accesso in una finestra di dialogo.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Nella sezione **Generale**, selezionare **Configura banner di accesso**.

   Viene visualizzata la finestra di dialogo Configura banner di accesso.

3. Inserire il testo che si desidera visualizzare nel banner di accesso.

   Non utilizzare tag HTML o altri tag di markup per la formattazione.

4. Fare clic su **Save** (Salva).

Risultati

La volta successiva che gli utenti accedono a System Manager, il testo viene visualizzato in una finestra di dialogo. Gli utenti devono fare clic su **OK** per passare alla schermata di accesso.

Gestire i timeout delle sessioni

È possibile configurare i timeout in Gestore di sistema di SANtricity, in modo che le sessioni inattive degli utenti vengano disconnesse dopo un determinato periodo di tempo.

A proposito di questa attività

Per impostazione predefinita, il timeout della sessione per System Manager è di 30 minuti. È possibile regolare l'orario oppure disattivare completamente i timeout della sessione.

Se Access Management viene configurato utilizzando le funzionalità SAML (Security Assertion Markup Language) incorporate nell'array, potrebbe verificarsi un timeout di sessione quando la sessione SSO dell'utente raggiunge il limite massimo. Questo potrebbe verificarsi prima del timeout della sessione di System Manager.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Nella sezione **Generale**, selezionare **attiva/Disattiva timeout sessione**.

   Viene visualizzata la finestra di dialogo **Enable/Disable Session Timeout** (attiva/Disattiva timeout sessione).

3. Utilizzare i comandi per aumentare o diminuire il tempo in minuti.

   Il timeout minimo che è possibile impostare per System Manager è di 15 minuti.

Per disattivare i timeout della sessione, deselezionare la casella di controllo **Imposta la durata…**.

4. Fare clic su **Save** (Salva).

Modificare le impostazioni della cache per lo storage array

Per tutti i volumi nell'array di storage, è possibile regolare le impostazioni della memoria cache per lo spurgo e le dimensioni dei blocchi.

A proposito di questa attività

La memoria cache è un'area di storage volatile temporaneo sul controller, che ha un tempo di accesso più rapido rispetto ai supporti del disco. Per ottimizzare le prestazioni della cache, è possibile regolare le seguenti impostazioni:

Impostazione della cache	Descrizione
Avvia il vampate di cache a richiesta	Start demand cache wlushing specifica la percentuale di dati non scritti nella cache che attiva un write-on della cache (scrittura su disco). Per impostazione predefinita, il vampate della cache viene avviato quando i dati non scritti raggiungono il 80% della capacità. Una percentuale più elevata è una buona scelta per gli ambienti con operazioni principalmente di scrittura, in modo che le nuove richieste di scrittura possano essere elaborate dalla cache senza dover accedere al disco. Le impostazioni più basse sono migliori in ambienti in cui l'i/o è irregolare (con burst di dati), in modo che il sistema scarichi frequentemente la cache tra burst di dati. Tuttavia, una percentuale iniziale inferiore al 80% può causare una riduzione delle performance.
Dimensione del blocco della cache	La dimensione del blocco della cache determina la dimensione massima di ciascun blocco della cache, che è un'unità organizzativa per la gestione della cache. Per impostazione predefinita, la dimensione del blocco è 32 KiB. System Manager consente di impostare la dimensione del blocco della cache su 4, 8, 16 o 32 KiB. Le applicazioni utilizzano blocchi di dimensioni diverse, che hanno un impatto sulle performance dello storage. Una dimensione inferiore è una buona scelta per file system o applicazioni di database. Una dimensione maggiore è ideale per le applicazioni che generano i/o sequenziale, come ad esempio i contenuti multimediali.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Change cache Settings** (Modifica impostazioni cache).

   Viene visualizzata la finestra di dialogo Change cache Settings (Modifica impostazioni cache).

3. Regolare i seguenti valori:
   - **Start demand cache wlushing** — scegliere una percentuale appropriata per l'i/o utilizzato nel proprio ambiente. Se si sceglie un valore inferiore al 80%, si potrebbe notare una riduzione delle performance.
   - **Cache block size** — Scegli una dimensione adatta alle tue applicazioni.

4. Fare clic su **Save** (Salva).

Impostare il reporting sulla connettività host

È possibile attivare il reporting della connettività host in modo che lo storage array monitoraggi continuamente la connessione tra i controller e gli host configurati, quindi avvisa l'utente in caso di interruzione della connessione. Questa funzione è attivata per impostazione predefinita.

A proposito di questa attività

Se si disattiva il reporting sulla connettività host, il sistema non monitora più i problemi di connettività o di driver multipath con un host collegato allo storage array.

> La disattivazione del reporting sulla connettività host disattiva anche il bilanciamento automatico del carico, che monitora e bilancia l'utilizzo delle risorse del controller.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Enable/Disable host Connectivity Reporting** (attiva/Disattiva report connettività host).

   Il testo sotto questa opzione indica se è attivata o disattivata.

   Viene visualizzata una finestra di dialogo di conferma.

3. Fare clic su **Sì** per continuare.

   Selezionando questa opzione, è possibile attivare o disattivare la funzione.

Impostare il bilanciamento automatico del carico

La funzione di bilanciamento automatico del carico garantisce che il traffico i/o in entrata dagli host sia gestito e bilanciato dinamicamente tra entrambi i controller. Questa funzione è attivata per impostazione predefinita, ma è possibile disattivarla da System Manager.

A proposito di questa attività

Quando il bilanciamento automatico del carico è attivato, esegue le seguenti funzioni:

- Monitora e bilancia automaticamente l'utilizzo delle risorse dei controller.
- Regola automaticamente la proprietà del controller del volume quando necessario, ottimizzando in tal modo la larghezza di banda i/o tra gli host e lo storage array.

È possibile disattivare il bilanciamento automatico del carico sull'array di storage per i seguenti motivi:

- Non si desidera modificare automaticamente la proprietà del controller di un determinato volume per bilanciare il carico di lavoro.
- Si opera in un ambiente altamente ottimizzato in cui la distribuzione del carico è appositamente configurata per ottenere una distribuzione specifica tra i controller.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Enable/Disable Automatic Load Balancing** (attiva/Disattiva bilanciamento automatico del carico).

   Il testo sotto questa opzione indica se la funzione è attualmente attivata o disattivata.

   Viene visualizzata una finestra di dialogo di conferma.

3. Confermare facendo clic su **Sì** per continuare.

   Selezionando questa opzione, è possibile attivare o disattivare la funzione.

   > Se questa funzione viene spostata da Disabled (disattivata) a Enabled (attivata), viene attivata automaticamente anche la funzione di reporting della connettività host.

Modificare il tipo di host predefinito

Utilizzare l'impostazione Change Default host Operating System (Modifica sistema operativo host predefinito) per modificare il tipo di host predefinito a livello di array di storage. In genere, è necessario modificare il tipo di host predefinito prima di connettere gli host all'array di storage o quando si collegano altri host.

A proposito di questa attività

Tenere presenti le seguenti linee guida:

- Se tutti gli host che si desidera connettere all'array di storage hanno lo stesso sistema operativo (ambiente host omogeneo), modificare il tipo di host in modo che corrisponda al sistema operativo.
- Se si prevede di collegare host con sistemi operativi diversi allo storage array (ambiente host eterogeneo), modificare il tipo di host in modo che corrisponda alla maggior parte dei sistemi operativi degli host.

  Ad esempio, se si connettono otto host diversi all'array di storage e sei di questi host eseguono un sistema operativo Windows, è necessario selezionare Windows come tipo di sistema operativo host predefinito.

- Se la maggior parte degli host connessi dispone di diversi sistemi operativi, impostare il tipo di host su Factory Default (impostazione predefinita).

  Ad esempio, se si collegano otto host diversi all'array di storage e due di questi host eseguono un sistema operativo Windows, tre eseguono un sistema operativo VMware, Altri tre sistemi operativi Linux sono in esecuzione, è necessario selezionare Factory Default (predefinito) come tipo di sistema operativo host predefinito.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Change Default host Operating System Type** (Modifica tipo di sistema operativo host predefinito).
3. Selezionare il tipo di sistema operativo host che si desidera utilizzare come predefinito.
4. Fare clic su **Cambia**.

Attivare o disattivare l'interfaccia di gestione legacy

È possibile attivare o disattivare l'interfaccia di gestione legacy (Symbol), un metodo di comunicazione tra lo storage array e il client di gestione.

A proposito di questa attività

Per impostazione predefinita, l'interfaccia di gestione legacy è attiva. Se la si disattiva, l'array di storage e il client di gestione utilizzeranno un metodo di comunicazione più sicuro (API REST su https); tuttavia, alcuni strumenti e attività potrebbero risentirne se la funzione è disattivata.

> Per il sistema storage EF600, questa funzione è disattivata per impostazione predefinita.

L'impostazione influisce sulle operazioni come segue:

- **On** (impostazione predefinita) — impostazione richiesta per la configurazione del mirroring con CLI e altri strumenti, come l'adattatore OCI.
- **Off** — impostazione richiesta per applicare la riservatezza nelle comunicazioni tra lo storage array e il client di gestione e per accedere a strumenti esterni. Impostazione consigliata per la configurazione di un server di directory (LDAP).

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Change Management Interface** (interfaccia di gestione delle modifiche).
3. Nella finestra di dialogo, fare clic su **Sì** per continuare.

FAQ

Che cos'è la cache del controller?

La cache del controller è uno spazio di memoria fisica che ottimizza due tipi di operazioni di i/o (input/output): Tra controller e host e tra controller e dischi.

Per i trasferimenti di dati in lettura e scrittura, gli host e i controller comunicano tramite connessioni ad alta velocità. Tuttavia, le comunicazioni dal back-end del controller ai dischi sono più lente, perché i dischi sono dispositivi relativamente lenti.

Quando la cache del controller riceve i dati, il controller riconosce alle applicazioni host che i dati sono ora memorizzati. In questo modo, le applicazioni host non devono attendere che l'i/o venga scritto su disco. Le applicazioni possono invece continuare a lavorare. I dati memorizzati nella cache sono facilmente accessibili anche dalle applicazioni server, eliminando la necessità di letture aggiuntive del disco per accedere ai dati.

La cache del controller influisce sulle prestazioni complessive dello storage array in diversi modi:

- La cache funge da buffer, in modo che i trasferimenti di dati su host e disco non debbano essere sincronizzati.
- I dati per un'operazione di lettura o scrittura dall'host potrebbero trovarsi nella cache di un'operazione precedente, eliminando così la necessità di accedere al disco.
- Se viene utilizzato il caching in scrittura, l'host può inviare comandi di scrittura successivi prima che i dati di un'operazione di scrittura precedente vengano scritti su disco.

- Se il prefetch della cache è attivato, l'accesso in lettura sequenziale è ottimizzato. Il prefetch della cache rende più probabile che un'operazione di lettura trovi i propri dati nella cache, invece di leggere i dati dal disco.

> **Possibile perdita di dati** — se si attiva l'opzione **Write caching without batteries** e non si dispone di un alimentatore universale per la protezione, si potrebbero perdere i dati. Inoltre, è possibile perdere i dati se non si dispone di batterie del controller e si attiva l'opzione **Write caching without batteries**.

Cos'è il vampate di cache?

Quando la quantità di dati non scritti nella cache raggiunge un determinato livello, il controller scrive periodicamente i dati memorizzati nella cache su un disco. Questo processo di scrittura è chiamato "vampate".

Il controller utilizza due algoritmi per il flushing della cache: Basato sulla domanda e basato sull'età. Il controller utilizza un algoritmo basato sulla domanda fino a quando la quantità di dati memorizzati nella cache non scende al di sotto della soglia di scaricamento della cache. Per impostazione predefinita, un'operazione di svuotamento inizia quando il 80% della cache è in uso.

In System Manager, è possibile impostare la soglia "Start demand cache flushing" per supportare al meglio il tipo di i/o utilizzato nell'ambiente. In un ambiente che è principalmente operazioni di scrittura, è necessario impostare la percentuale "Start demand cache wlushing" alta per aumentare la probabilità che qualsiasi nuova richiesta di scrittura possa essere elaborata dalla cache senza dover passare al disco. Un'impostazione di percentuale elevata limita il numero di lavaggi della cache in modo che nella cache rimanga più dati, aumentando così la possibilità di più accessi alla cache.

In un ambiente in cui l'i/o è irregolare (con burst di dati), è possibile utilizzare un basso flushing della cache in modo che il sistema scarichi frequentemente la cache tra burst di dati. In un ambiente i/o diverso che elabora una varietà di carichi, o quando il tipo di carichi non è noto, impostare la soglia al 50% come una buona base intermedia. Tenere presente che se si sceglie una percentuale iniziale inferiore al 80%, le prestazioni potrebbero essere ridotte perché i dati necessari per una lettura host potrebbero non essere disponibili. La scelta di una percentuale inferiore aumenta anche il numero di scritture su disco necessarie per mantenere il livello di cache, aumentando così l'overhead del sistema.

L'algoritmo basato sull'età specifica il periodo di tempo durante il quale i dati di scrittura possono rimanere nella cache prima che possano essere trasferiti sui dischi. I controller utilizzano l'algoritmo basato sull'età fino al raggiungimento della soglia di scaricamento della cache. L'impostazione predefinita è 10 secondi, ma questo periodo di tempo viene conteggiato solo durante i periodi di inattività. Non è possibile modificare i tempi di scaricamento in System Manager; è invece necessario utilizzare il comando **Set Storage Array** nell'interfaccia della riga di comando (CLI).

> **Possibile perdita di dati** — se si attiva l'opzione **Write caching without batteries** e non si dispone di un alimentatore universale per la protezione, si potrebbero perdere i dati. Inoltre, è possibile perdere i dati se non si dispone di batterie del controller e si attiva l'opzione **Write caching without batteries**.

Che cos'è la dimensione del blocco della cache?

Il controller dell'array di storage organizza la cache in "blocchi", ovvero blocchi di memoria che possono essere di 8, 16, 32 KiB. Tutti i volumi sul sistema storage condividono lo stesso spazio cache; pertanto, i volumi possono avere una sola

dimensione del blocco cache.

Le applicazioni utilizzano blocchi di dimensioni diverse, che possono avere un impatto sulle performance dello storage. Per impostazione predefinita, la dimensione del blocco in System Manager è 32 KiB, ma è possibile impostare il valore su 8, 16, 32 KiB. Una dimensione inferiore è una buona scelta per file system o applicazioni di database. Una dimensione maggiore è una buona scelta per le applicazioni che richiedono un grande trasferimento di dati, l'i/o sequenziale o un'elevata larghezza di banda, come ad esempio le applicazioni multimediali.

Quando è necessario sincronizzare gli orologi degli array di storage?

È necessario sincronizzare manualmente gli orologi del controller nell'array di storage se si nota che gli indicatori di data e ora visualizzati in System Manager non sono allineati con quelli visualizzati nel client di gestione (il computer che accede a System Manager tramite il browser). Questa attività è necessaria solo se NTP (Network Time Protocol) non è attivato in System Manager.

> Si consiglia vivamente di utilizzare un server NTP invece di sincronizzare manualmente gli orologi. NTP sincronizza automaticamente gli orologi con un server esterno utilizzando SNTP (Simple Network Time Protocol).

È possibile controllare lo stato della sincronizzazione dalla finestra di dialogo Synchronize Storage Array Blocks (Sincronizza blocchi array di storage), disponibile nella pagina System (sistema). Se gli orari visualizzati nella finestra di dialogo non corrispondono, eseguire una sincronizzazione. È possibile visualizzare periodicamente questa finestra di dialogo, che indica se le visualizzazioni dell'ora dei clock del controller sono state separate e non sono più sincronizzate.

Che cos'è il reporting sulla connettività host?

Quando il reporting sulla connettività host è attivato, lo storage array monitora continuamente la connessione tra i controller e gli host configurati, quindi avvisa l'utente in caso di interruzione della connessione.

In caso di cavi allentati, danneggiati o mancanti o di altri problemi con l'host, potrebbero verificarsi interruzioni della connessione. In queste situazioni, il sistema potrebbe aprire un messaggio Recovery Guru:

- **Host Redundancy Lost** — si apre se uno dei controller non riesce a comunicare con l'host.
- **Host Type Incorrect (tipo host errato)** — si apre se il tipo di host non è specificato correttamente nell'array di storage, con conseguenti problemi di failover.

È possibile disattivare la funzione di reporting della connettività host in situazioni in cui il riavvio di un controller potrebbe richiedere più tempo del timeout di connessione. La disattivazione di questa funzione elimina i messaggi Recovery Gurus.

> La disattivazione del reporting sulla connettività host disattiva anche il bilanciamento automatico del carico, che monitora e bilancia l'utilizzo delle risorse del controller. Tuttavia, se si riattiva il reporting sulla connettività host, la funzione di bilanciamento automatico del carico non viene riattivata automaticamente.

System (sistema): Impostazioni iSCSI

Concetti

Terminologia iSCSI

Scopri in che modo i termini iSCSI si applicano al tuo storage array.

Termine	Descrizione
CAP	Il metodo CHAP (Challenge Handshake Authentication Protocol) convalida l'identità di destinazioni e iniziatori durante il collegamento iniziale. L'autenticazione si basa su una chiave di sicurezza condivisa denominata CHAP*secret*.
Controller	Un controller è costituito da una scheda, firmware e software. Controlla i dischi e implementa le funzioni di System Manager.
DHCP	Il protocollo DHCP (Dynamic host Configuration Protocol) è un protocollo utilizzato sulle reti IP (Internet Protocol) per la distribuzione dinamica dei parametri di configurazione della rete, ad esempio gli indirizzi IP.
IB	InfiniBand (IB) è uno standard di comunicazione per la trasmissione dei dati tra server e sistemi storage dalle performance elevate.
Risposta PING ICMP	ICMP (Internet Control message Protocol) è un protocollo utilizzato dai sistemi operativi dei computer collegati in rete per inviare messaggi. I messaggi ICMP determinano se un host è raggiungibile e quanto tempo occorre per ottenere i pacchetti da e verso tale host.
IQN	Un identificatore IQN (iSCSI Qualified Name) è un nome univoco per un iSCSI Initiator o una destinazione iSCSI.
Er	ISER (iSCSI Extensions for RDMA) è un protocollo che estende il protocollo iSCSI per il funzionamento sui trasporti RDMA, come InfiniBand o Ethernet.
ISNS	Internet Storage Name Service (iSNS) è un protocollo che consente il rilevamento, la gestione e la configurazione automatici dei dispositivi iSCSI e Fibre Channel sulle reti TCP/IP.
Indirizzo MAC	Gli identificatori di controllo dell'accesso ai supporti (indirizzi MAC) vengono utilizzati da Ethernet per distinguere tra canali logici separati che collegano due porte sulla stessa interfaccia di rete di trasporto fisica.
Client di gestione	Un client di gestione è il computer in cui è installato un browser per accedere a System Manager.

Termine	Descrizione
MTU	Una MTU (Maximum Transmission Unit) è il pacchetto o frame di dimensioni maggiori che può essere inviato in una rete.
RDMA	RDMA (Remote Direct Memory Access) è una tecnologia che consente ai computer di rete di scambiare dati nella memoria principale senza coinvolgere il sistema operativo di entrambi i computer.
Sessione di rilevamento senza nome	Quando l'opzione per le sessioni di rilevamento senza nome è attivata, gli iniziatori iSCSI non devono specificare l'IQN di destinazione per recuperare le informazioni del controller.

Come fare

Configurare le porte iSCSI

Se il controller include una connessione host iSCSI, è possibile configurare le impostazioni della porta iSCSI dalla pagina System (sistema).

Prima di iniziare

- Il controller deve includere porte iSCSI; in caso contrario, le impostazioni iSCSI non sono disponibili.
- È necessario conoscere la velocità di rete (la velocità di trasferimento dei dati tra le porte e l'host).

> Le impostazioni e le funzioni iSCSI vengono visualizzate solo se lo storage array supporta iSCSI.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **iSCSI Settings** (Impostazioni iSCSI), selezionare **Configure iSCSI Ports** (Configura porte iSCSI).

   > L'opzione **Configure iSCSI Ports** (Configura porte iSCSI) viene visualizzata solo se System Manager rileva le porte iSCSI sul controller.

3. Selezionare il controller con le porte iSCSI che si desidera configurare.
4. Nell'elenco a discesa, selezionare la porta che si desidera configurare, quindi fare clic su **Avanti**.
5. Selezionare le impostazioni della porta di configurazione, quindi fare clic su **Avanti**.

   Per visualizzare tutte le impostazioni della porta, fare clic sul collegamento **Mostra altre impostazioni della porta** a destra della finestra di dialogo.

Dettagli campo

Impostazione della porta	Descrizione
Attiva IPv4 / attiva IPv6	Selezionare una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6. Se si desidera disattivare l'accesso alla porta, deselezionare entrambe le caselle di controllo.
Porta TCP in ascolto (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire un nuovo numero di porta. La porta di ascolto è il numero di porta TCP utilizzato dal controller per rilevare gli accessi iSCSI dagli iniziatori iSCSI host. La porta di ascolto predefinita è 3260. Immettere 3260 o un valore compreso tra 49152 e 65535.
Dimensione MTU (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire una nuova dimensione in byte per l'unità di trasmissione massima (MTU). La dimensione massima predefinita dell'unità di trasmissione (MTU) è di 1500 byte per frame. Immettere un valore compreso tra 1500 e 9000.
Abilitare le risposte PING ICMP	Selezionare questa opzione per attivare il protocollo ICMP (Internet Control message Protocol). I sistemi operativi dei computer collegati in rete utilizzano questo protocollo per inviare messaggi. Questi messaggi ICMP determinano se un host è raggiungibile e quanto tempo occorre per ottenere i pacchetti da e verso tale host.

Se si seleziona **Enable IPv4** (attiva IPv4), dopo aver fatto clic su **Next** (Avanti) viene visualizzata una finestra di dialogo per la selezione delle impostazioni IPv4. Se si seleziona **Enable IPv6** (attiva IPv6*), dopo aver fatto clic su **Next** (Avanti) viene visualizzata una finestra di dialogo per la selezione delle impostazioni IPv6. Se sono state selezionate entrambe le opzioni, viene visualizzata prima la finestra di dialogo per le impostazioni IPv4, quindi dopo aver fatto clic su **Avanti**, viene visualizzata la finestra di dialogo per le impostazioni IPv6.

6. Configurare le impostazioni IPv4 e/o IPv6, automaticamente o manualmente. Per visualizzare tutte le impostazioni delle porte, fare clic sul collegamento **Mostra altre impostazioni** a destra della finestra di dialogo.

Dettagli campo

Impostazione della porta	Descrizione
Ottenere automaticamente la configurazione	Selezionare questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Selezionare questa opzione, quindi inserire un indirizzo statico nei campi. (Se lo si desidera, è possibile tagliare e incollare gli indirizzi nei campi). Per IPv4, includere la subnet mask di rete e il gateway. Per IPv6, includere l'indirizzo IP instradabile e l'indirizzo IP del router.
Abilitare il supporto VLAN (disponibile facendo clic su **Mostra altre impostazioni**).	Selezionare questa opzione per attivare una VLAN e inserire il relativo ID. Una VLAN è una rete logica che si comporta come se fosse fisicamente separata da altre LAN (Local Area Network) fisiche e virtuali supportate dagli stessi switch, dagli stessi router o da entrambi.
Abilitare la priorità ethernet (disponibile facendo clic su **Mostra altre impostazioni**).	Selezionare questa opzione per attivare il parametro che determina la priorità di accesso alla rete. Utilizzare il dispositivo di scorrimento per selezionare una priorità compresa tra 1 (più bassa) e 7 (più alta). In un ambiente LAN (Local Area Network) condiviso, ad esempio Ethernet, molte stazioni potrebbero entrare in contatto per l'accesso alla rete. L'accesso avviene in base all'ordine di arrivo e all'ordine di arrivo. Due stazioni potrebbero tentare di accedere alla rete contemporaneamente, causando la disattivazione di entrambe le stazioni e l'attesa prima di riprovare. Questo processo è ridotto al minimo per Ethernet commutata, in cui una sola stazione è collegata a una porta dello switch.

7. Fare clic su **fine**.

Configurare l'autenticazione iSCSI

Per una maggiore sicurezza in una rete iSCSI, è possibile impostare l'autenticazione tra controller (destinazioni) e host (iniziatori). System Manager utilizza il metodo Challenge Handshake Authentication Protocol (CHAP), che convalida l'identità di destinazioni e iniziatori durante il collegamento iniziale. L'autenticazione si basa su una chiave di sicurezza condivisa denominata CHAP *secret*.

Prima di iniziare

È possibile impostare il segreto CHAP per gli iniziatori (host iSCSI) prima o dopo aver impostato il segreto CHAP per le destinazioni (controller). Prima di seguire le istruzioni di questa attività, è necessario attendere che gli host abbiano stabilito prima una connessione iSCSI, quindi impostare il segreto CHAP sui singoli host. Una volta effettuate le connessioni, i nomi IQN degli host e i relativi segreti CHAP vengono elencati nella finestra di dialogo per l'autenticazione iSCSI (descritta in questa attività) e non è necessario immetterli manualmente.

A proposito di questa attività

È possibile selezionare uno dei seguenti metodi di autenticazione:

- **Autenticazione unidirezionale** — utilizzare questa impostazione per consentire al controller di autenticare l'identità degli host iSCSI (autenticazione unidirezionale).
- **Autenticazione bidirezionale** — utilizzare questa impostazione per consentire al controller e agli host iSCSI di eseguire l'autenticazione (autenticazione bidirezionale). Questa impostazione fornisce un secondo livello di sicurezza consentendo al controller di autenticare l'identità degli host iSCSI e, a sua volta, agli host iSCSI di autenticare l'identità del controller.

> Le impostazioni e le funzioni iSCSI vengono visualizzate nella pagina Settings (Impostazioni) solo se lo storage array supporta iSCSI.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **iSCSI settings**, fare clic su **Configure Authentication** (Configura autenticazione).

   Viene visualizzata la finestra di dialogo **Configure Authentication** (Configura autenticazione), che mostra il metodo attualmente impostato. Inoltre, indica se alcuni host hanno configurato segreti CHAP.

3. Selezionare una delle seguenti opzioni:
   - **Nessuna autenticazione** — se non si desidera che il controller autentichi l'identità degli host iSCSI, selezionare questa opzione e fare clic su **fine**. La finestra di dialogo si chiude e la configurazione è terminata.
   - **Autenticazione unidirezionale** — per consentire al controller di autenticare l'identità degli host iSCSI, selezionare questa opzione e fare clic su **Avanti** per visualizzare la finestra di dialogo Configura CHAP di destinazione.
   - **Autenticazione bidirezionale** — per consentire sia al controller che agli host iSCSI di eseguire l'autenticazione, selezionare questa opzione e fare clic su **Avanti** per visualizzare la finestra di dialogo Configura CHAP di destinazione.
4. Per l'autenticazione unidirezionale o bidirezionale, immettere o confermare il segreto CHAP per il controller (la destinazione). Il segreto CHAP deve essere compreso tra 12 e 57 caratteri ASCII stampabili.

   > Se il segreto CHAP per il controller è stato configurato in precedenza, i caratteri nel campo vengono mascherati. Se necessario, è possibile sostituire i caratteri esistenti (i nuovi caratteri non vengono mascherati).

5. Effettuare una delle seguenti operazioni:
   - Se si sta configurando l'autenticazione *unidirezionale*, fare clic su **fine**. La finestra di dialogo si chiude e la configurazione è terminata.
   - Se si sta configurando l'autenticazione *bidirezionale*, fare clic su **Avanti** per visualizzare la finestra di dialogo Configure Initiator CHAP.
6. Per l'autenticazione bidirezionale, immettere o confermare un segreto CHAP per uno qualsiasi degli host iSCSI (gli iniziatori), che può essere compreso tra 12 e 57 caratteri ASCII stampabili. Se non si desidera configurare l'autenticazione bidirezionale per un determinato host, lasciare vuoto il campo **Initiator CHAP Secret**.

   > Se il segreto CHAP per un host è stato configurato in precedenza, i caratteri nel campo vengono mascherati. Se necessario, è possibile sostituire i caratteri esistenti (i nuovi caratteri non vengono mascherati).

7. Fare clic su **fine**.

Risultati

L'autenticazione avviene durante la sequenza di login iSCSI tra i controller e gli host iSCSI, a meno che non sia stata specificata alcuna autenticazione.

Abilitare le impostazioni di rilevamento iSCSI

È possibile attivare le impostazioni relative al rilevamento dei dispositivi di storage in una rete iSCSI. Le impostazioni di rilevamento di destinazione consentono di registrare le informazioni iSCSI dell'array di storage utilizzando il protocollo iSNS (Internet Storage Name Service) e di determinare se consentire sessioni di rilevamento senza nome.

Prima di iniziare

Se il server iSNS utilizza un indirizzo IP statico, tale indirizzo deve essere disponibile per la registrazione iSNS. Sono supportati sia IPv4 che IPv6.

A proposito di questa attività

È possibile attivare le seguenti impostazioni relative al rilevamento iSCSI:

- **Abilitare il server iSNS per registrare una destinazione** — quando abilitato, lo storage array registra il proprio iSCSI Qualified Name (IQN) e le informazioni sulle porte dal server iSNS. Questa impostazione consente il rilevamento iSNS, in modo che un iniziatore possa recuperare le informazioni IQN e sulla porta dal server iSNS.
- **Enable unnamed Discovery sessions** (attiva sessioni di rilevamento senza nome) — quando sono attivate sessioni di rilevamento senza nome, l'iniziatore (host iSCSI) non deve fornire l'IQN del controller di destinazione durante la sequenza di accesso per una connessione di tipo Discovery. Se disattivati, gli host devono fornire l'IQN per stabilire una sessione di rilevamento per il controller. Tuttavia, l'IQN di destinazione è sempre richiesto per una sessione normale (i/o Bearing). La disattivazione di questa impostazione può impedire agli host iSCSI non autorizzati di connettersi al controller utilizzando solo il relativo indirizzo IP.

> Le impostazioni e le funzioni iSCSI vengono visualizzate nella pagina Settings (Impostazioni) solo se lo storage array supporta iSCSI.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **iSCSI settings** (Impostazioni iSCSI), fare clic su **View/Edit Target Discovery Settings** (Visualizza/Modifica impostazioni rilevamento destinazione).

   Viene visualizzata la finestra di dialogo **Target Discovery Settings** (Impostazioni rilevamento destinazione). Sotto la voce **Enable iSNS server**… la finestra di dialogo indica se il controller è già registrato.

3. Per registrare il controller, selezionare **Enable iSNS server to register my target**, quindi selezionare una delle seguenti opzioni:
   - **Ottieni automaticamente la configurazione dal server DHCP** — selezionare questa opzione se si desidera configurare il server iSNS utilizzando un server DHCP (Dynamic host Configuration Protocol). Tenere presente che se si utilizza questa opzione, tutte le porte iSCSI del controller devono essere configurate per utilizzare anche DHCP. Se necessario, aggiornare le impostazioni della porta iSCSI del controller per attivare questa opzione.

> Affinché il server DHCP fornisca l'indirizzo del server iSNS, è necessario configurare il server DHCP in modo che utilizzi l'opzione 43 — "Vendor Specific Information". Questa opzione deve contenere l'indirizzo IPv4 del server iSNS nei byte di dati 0xa-0xd (10-13).

- **Specificare manualmente la configurazione statica** — selezionare questa opzione se si desidera inserire un indirizzo IP statico per il server iSNS. (Se lo si desidera, è possibile tagliare e incollare gli indirizzi nei campi). Nel campo, immettere un indirizzo IPv4 o IPv6. Se sono stati configurati entrambi, IPv4 è l'impostazione predefinita. Immettere anche una porta TCP in attesa (utilizzare il valore predefinito 3205 o immettere un valore compreso tra 49152 e 65535).

4. Per consentire allo storage array di partecipare a sessioni di rilevamento senza nome, selezionare **Enable unnamed Discovery sessions** (attiva sessioni di rilevamento senza nome).
   - Se attivato, gli iniziatori iSCSI non devono specificare l'IQN di destinazione per recuperare le informazioni del controller.
   - Se disattivata, le sessioni di rilevamento vengono impedite a meno che l'iniziatore non fornisca l'IQN di destinazione. La disattivazione delle sessioni di rilevamento senza nome offre una maggiore sicurezza.
5. Fare clic su **Save** (Salva).

Risultati

Quando System Manager tenta di registrare il controller con il server iSNS, viene visualizzata una barra di avanzamento. Questo processo potrebbe richiedere fino a cinque minuti.

Visualizzare i pacchetti di statistiche iSCSI

È possibile visualizzare i dati relativi alle connessioni iSCSI allo storage array.

A proposito di questa attività

System Manager mostra questi tipi di statistiche iSCSI. Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **Ethernet MAC statistics** — fornisce statistiche per il controllo dell'accesso ai supporti (MAC). MAC fornisce anche un meccanismo di indirizzamento chiamato indirizzo fisico o indirizzo MAC. L'indirizzo MAC è un indirizzo univoco assegnato a ciascun adattatore di rete. L'indirizzo MAC consente di inviare pacchetti di dati a una destinazione all'interno della sottorete.
- **Ethernet TCP/IP statistics** — fornisce le statistiche per TCP/IP, ovvero il protocollo TCP (Transmission Control Protocol) e il protocollo Internet (IP) per il dispositivo iSCSI. Con TCP, le applicazioni sugli host collegati in rete possono creare connessioni tra loro, attraverso le quali possono scambiare dati in pacchetti. L'IP è un protocollo orientato ai dati che comunica i dati attraverso una rete interconnessa a commutazione di pacchetto. Le statistiche IPv4 e IPv6 vengono visualizzate separatamente.
- **Statistiche Local Target/Initiator (protocollo)** — Mostra le statistiche per la destinazione iSCSI, che fornisce l'accesso a livello di blocco ai relativi supporti di storage, e mostra le statistiche iSCSI per lo storage array quando viene utilizzato come iniziatore nelle operazioni di mirroring asincrono.
- **DCBX Statistiche degli stati operativi** — Visualizza gli stati operativi delle varie funzioni Data Center Bridging Exchange (DCBX).
- **LLDP TLV statistics** — Visualizza le statistiche LLDP (link Layer Discovery Protocol) Type Length Value (TLV).
- **DCBX TLV statistics** — Visualizza le informazioni che identificano le porte host degli array di storage in un ambiente Data Center Bridging (DCB). Queste informazioni vengono condivise con i peer di rete per scopi di identificazione e funzionalità.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Selezionare **View iSCSI Statistics Packages** (Visualizza pacchetti di statistiche iSCSI).
3. Fare clic su una scheda per visualizzare i diversi set di statistiche.
4. **Opzionale:** per impostare la linea di base, fare clic su **Imposta nuova linea di base**.

   L'impostazione della linea di base consente di impostare un nuovo punto di partenza per la raccolta delle statistiche. Per tutte le statistiche iSCSI viene utilizzata la stessa linea di base.

Visualizzare le sessioni iSCSI

È possibile visualizzare informazioni dettagliate sulle connessioni iSCSI allo storage array. Le sessioni iSCSI possono essere eseguite con host o array di storage remoti in una relazione di mirroring asincrona.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Selezionare **View/End iSCSI Sessions** (Visualizza/termina sessioni iSCSI).

   Viene visualizzato un elenco delle sessioni iSCSI correnti.

3. Per visualizzare ulteriori informazioni su una sessione iSCSI specifica, selezionare una sessione, quindi fare clic su **View Details** (Visualizza dettagli).

Dettagli campo

Elemento	Descrizione
SSID (Session Identifier)	Stringa esadecimale che identifica una sessione tra un iSCSI Initiator e una destinazione iSCSI. L'SSID è composto dall'ISID e dal TPGT.
ID sessione iniziatore (ISID)	Parte iniziatore dell'identificatore di sessione. L'iniziatore specifica l'ISID durante l'accesso.
Gruppo di portali di destinazione	La destinazione iSCSI.
Tag del gruppo di portali di destinazione (TPGT)	La parte di destinazione dell'identificatore di sessione. Identificatore numerico a 16 bit per un gruppo di portali di destinazione iSCSI.
Nome iSCSI iniziatore	Il nome univoco mondiale dell'iniziatore.
Etichetta iSCSI iniziatore	L'etichetta utente impostata in System Manager.
Alias iSCSI iniziatore	Un nome che può essere associato anche a un nodo iSCSI. L'alias consente a un'organizzazione di associare una stringa intuitiva al nome iSCSI. Tuttavia, l'alias non sostituisce il nome iSCSI. L'alias iSCSI iniziatore può essere impostato solo sull'host, non in System Manager
Host	Server che invia input e output allo storage array.
ID connessione (CID)	Un nome univoco per una connessione all'interno della sessione tra l'iniziatore e la destinazione. L'iniziatore genera questo ID e lo presenta alla destinazione durante le richieste di accesso. L'ID di connessione viene visualizzato anche durante le disconnessioni che chiudono le connessioni.
Identificatore della porta Ethernet	La porta del controller associata alla connessione.
Indirizzo IP iniziatore	L'indirizzo IP dell'iniziatore.
Parametri di accesso negoziati	I parametri che vengono transatti durante l'accesso alla sessione iSCSI.
Metodo di autenticazione	La tecnica per autenticare gli utenti che desiderano accedere alla rete iSCSI. I valori validi sono **CHAP** e **None**.
Metodo di digest dell'intestazione	La tecnica per mostrare i possibili valori di intestazione per la sessione iSCSI. HeaderDigest e DataDigest possono essere **None** o **CRC32C**. Il valore predefinito per entrambi è **None**.

Elemento	Descrizione
Metodo di data digest	La tecnica per mostrare i possibili valori dei dati per la sessione iSCSI. HeaderDigest e DataDigest possono essere **None** o **CRC32C**. Il valore predefinito per entrambi è **None**.
Numero massimo di connessioni	Il maggior numero di connessioni consentite per la sessione iSCSI. Il numero massimo di connessioni può essere compreso tra 1 e 4. Il valore predefinito è **1**.
Alias di destinazione	L'etichetta associata alla destinazione.
Alias iniziatore	Etichetta associata all'iniziatore.
Indirizzo IP di destinazione	L'indirizzo IP della destinazione per la sessione iSCSI. I nomi DNS non sono supportati.
R2T iniziale	Lo stato iniziale pronto per il trasferimento. Lo stato può essere **Sì** o **No**.
Lunghezza massima del burst	Il payload SCSI massimo in byte per questa sessione iSCSI. La lunghezza massima del burst può essere compresa tra 512 e 262,144 (256 KB). Il valore predefinito è **262,144 (256 KB)**.
Lunghezza del primo burst	Il payload SCSI in byte per i dati non richiesti per questa sessione iSCSI. La lunghezza del primo burst può essere compresa tra 512 e 131,072 (128 KB). Il valore predefinito è **65,536 (64 KB)**.
Tempo di attesa predefinito	Il numero minimo di secondi di attesa prima di tentare di stabilire una connessione dopo la chiusura o la reimpostazione della connessione. Il valore predefinito del tempo di attesa può essere compreso tra 0 e 3600. Il valore predefinito è **2**.
Tempo di conservazione predefinito	Il numero massimo di secondi in cui la connessione è ancora possibile in seguito a una interruzione della connessione o a un ripristino della connessione. Il tempo di conservazione predefinito può essere compreso tra 0 e 3600. Il valore predefinito è **20**.
R2T massimo in sospeso	Il numero massimo di "pronti per i trasferimenti" in sospeso per questa sessione iSCSI. Il valore massimo di ready to transfer può essere compreso tra 1 e 16. Il valore predefinito è **1**.
Livello di ripristino degli errori	Il livello di ripristino degli errori per questa sessione iSCSI. Il valore del livello di ripristino degli errori è sempre impostato su **0**.
Lunghezza massima del segmento di dati di ricezione	La quantità massima di dati che l'iniziatore o la destinazione possono ricevere in qualsiasi PDU (Payload Data Unit) iSCSI.

Elemento	Descrizione
Nome di destinazione	Il nome ufficiale della destinazione (non l'alias). Il nome di destinazione con il formato *iqn*.
Nome dell'iniziatore	Il nome ufficiale dell'iniziatore (non l'alias). Il nome dell'iniziatore che utilizza il formato *iqn* o *eui*.

4. **Opzionale:** per salvare il report in un file, fare clic su **Salva**.

   Il file viene salvato nella cartella Download del browser con il nome file `iscsi-session-connections.txt`.

Terminare la sessione iSCSI

È possibile terminare una sessione iSCSI che non è più necessaria. Le sessioni iSCSI possono essere eseguite con host o array di storage remoti in una relazione di mirroring asincrona.

A proposito di questa attività

È possibile terminare una sessione iSCSI per i seguenti motivi:

- **Accesso non autorizzato** — se un iSCSI Initiator è connesso e non deve avere accesso, è possibile terminare la sessione iSCSI per forzare iSCSI Initiator a disconnettersi dallo storage array. L'iSCSI Initiator potrebbe aver eseguito l'accesso perché era disponibile il metodo di autenticazione None.
- **Downtime del sistema** — se è necessario rimuovere un array di storage e si nota che gli iniziatori iSCSI sono ancora connessi, è possibile terminare le sessioni iSCSI per estrarre gli iniziatori iSCSI dall'array di storage.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Selezionare **View/End iSCSI Sessions** (Visualizza/termina sessioni iSCSI).

   Viene visualizzato un elenco delle sessioni iSCSI correnti.

3. Selezionare la sessione che si desidera terminare
4. Fare clic su **End Session** (fine sessione) e confermare che si desidera eseguire l'operazione.

Configurare iSER su porte InfiniBand

Se il controller include una porta iSER su InfiniBand, è possibile configurare la connessione di rete all'host.

Prima di iniziare

- Il controller deve includere una porta iSER su InfiniBand; in caso contrario, le impostazioni iSER su InfiniBand non sono disponibili in System Manager.
- È necessario conoscere l'indirizzo IP della connessione host.

Fasi

1. Selezionare **Impostazioni › sistema**
2. In **iSER over InfiniBand settings**, selezionare **Configure iSER over InfiniBand ports** (Configura iSER su porte InfiniBand).
3. Fare clic sul controller con la porta iSER su InfiniBand che si desidera configurare. Fare clic su **Avanti**.
4. Nell'elenco a discesa, selezionare la porta HIC che si desidera configurare, quindi immettere l'indirizzo IP dell'host.
5. Fare clic su **fine**.
6. Reimpostare iSER sulla porta InfiniBand facendo clic su **Sì**.

Visualizza le statistiche di iSER su InfiniBand

Se il controller dello storage array include una porta iSER su InfiniBand, è possibile visualizzare i dati relativi alle connessioni host.

A proposito di questa attività

System Manager mostra i seguenti tipi di statistiche iSER su InfiniBand. Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **Statistiche di destinazione locale (protocollo)** — fornisce statistiche per la destinazione iSER su InfiniBand, che mostra l'accesso a livello di blocco ai propri supporti di storage.
- **Statistiche dell'interfaccia iSER su InfiniBand** — fornisce statistiche per tutte le porte iSER sull'interfaccia InfiniBand, che includono statistiche sulle prestazioni e informazioni sugli errori di collegamento associate a ciascuna porta dello switch.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Selezionare **Visualizza statistiche iSER su InfiniBand**.
3. Fare clic su una scheda per visualizzare i diversi set di statistiche.
4. **Opzionale:** per impostare la linea di base, fare clic su **Imposta nuova linea di base**.

   L'impostazione della linea di base consente di impostare un nuovo punto di partenza per la raccolta delle statistiche. La stessa linea di base viene utilizzata per tutte le statistiche iSER su InfiniBand.

FAQ

Cosa accade quando si utilizza un server iSNS per la registrazione?

Quando si utilizzano le informazioni del server iSNS (Internet Storage Name Service), è possibile configurare gli host (iniziatori) in modo che interrogino il server iSNS per recuperare le informazioni dal server di destinazione (controller).

Questa registrazione fornisce al server iSNS le informazioni relative al nome qualificato iSCSI (IQN) e alla porta del controller e consente di eseguire query tra gli iniziatori (host iSCSI) e le destinazioni (controller).

Quali metodi di registrazione sono supportati automaticamente per iSCSI?

L'implementazione iSCSI supporta il metodo di ricerca iSNS (Internet Storage Name Service) o l'utilizzo del comando Invia destinazioni.

Il metodo iSNS consente il rilevamento iSNS tra gli iniziatori (host iSCSI) e le destinazioni (controller). Il controller di destinazione viene registrato per fornire al server iSNS le informazioni relative a iSCSI Qualified Name (IQN) e porta del controller.

Se non si configura iSNS, l'host iSCSI può inviare il comando Invia destinazioni durante una sessione di rilevamento iSCSI. In risposta, il controller restituisce le informazioni sulla porta (ad esempio, il valore IQN di destinazione, l'indirizzo IP della porta, la porta di ascolto e il gruppo di porte di destinazione). Questo metodo di ricerca non è necessario se si utilizza iSNS, perché l'iniziatore host può recuperare gli IP di destinazione dal server iSNS.

Come si interpretano le statistiche di iSER su InfiniBand?

La finestra di dialogo View iSER over InfiniBand Statistics (Visualizza statistiche iSER su InfiniBand) visualizza le statistiche di destinazione locale (protocollo) e le statistiche dell'interfaccia iSER su InfiniBand (IB). Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **Statistiche di destinazione locale (protocollo)** — fornisce statistiche per la destinazione iSER su InfiniBand, che mostra l'accesso a livello di blocco ai propri supporti di storage.
- **Statistiche dell'interfaccia iSER su InfiniBand** — fornisce statistiche per tutte le porte iSER su InfiniBand sull'interfaccia InfiniBand, che includono statistiche sulle prestazioni e informazioni sugli errori di collegamento associate a ciascuna porta dello switch.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

Cosa devo fare per configurare o diagnosticare iSER su InfiniBand?

La seguente tabella elenca le funzioni di System Manager che è possibile utilizzare per configurare e gestire le sessioni iSER su InfiniBand.

> Le impostazioni di iSER su InfiniBand sono disponibili solo se il controller dello storage array include una porta di gestione host iSER su InfiniBand.

Configurare e diagnosticare iSER su InfiniBand

Azione	Posizione
Configurare iSER su porte InfiniBand	1. Selezionare **hardware**. 2. Selezionare **Mostra retro dello shelf**. 3. Selezionare un controller. 4. Selezionare **Configura iSER su porte InfiniBand**. oppure 1. Selezionare **Impostazioni › sistema**. 2. Scorrere fino a **iSER over InfiniBand settings**, quindi selezionare **Configure iSER over InfiniBand Ports** (Configura iSER su porte InfiniBand).
Visualizza le statistiche di iSER su InfiniBand	1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **iSER over InfiniBand settings**, quindi selezionare **View iSER over InfiniBand Statistics** (Visualizza statistiche iSER su InfiniBand).

System (sistema): Impostazioni NVMe

Concetti

Panoramica di NVMe

Alcuni controller includono una porta per l'implementazione di NVMe (non-volatile Memory Express) su fabric. NVMe consente comunicazioni dalle performance elevate tra gli host e lo storage array.

Che cos'è NVMe?

NVM sta per "memoria non volatile" ed è la memoria persistente utilizzata in molti tipi di dispositivi di storage. *NVMe* (NVM Express) è un'interfaccia o protocollo standardizzato progettato specificamente per le comunicazioni multi-coda ad alte prestazioni con i dispositivi NVM.

Che cos'è NVMe sui fabric?

NVMe over Fabrics (NVMe-of) è una specifica tecnologica che consente il trasferimento di dati e comandi basati su messaggi NVMe tra un computer host e lo storage in rete. Un host può accedere a un array di storage NVMe (chiamato *sottosistema*) utilizzando un fabric. I comandi NVMe sono abilitati e incapsulati nei layer di astrazione di trasporto sia sul lato host che sul lato del sottosistema. Questo estende l'interfaccia NVMe dalle performance elevate end-to-end dall'host allo storage e standardizza e semplifica il set di comandi.

Lo storage NVMe-of viene presentato a un host come dispositivo di storage a blocchi locale. Il volume (denominato *namespace*) può essere montato su un file system come con qualsiasi altro dispositivo di storage a blocchi. È possibile utilizzare l'API REST, SMcli o Gestore di sistema di SANtricity per eseguire il provisioning dello storage in base alle esigenze.

Che cos'è un NQN (NVMe Qualified Name)?

NQN (NVMe Qualified Name) viene utilizzato per identificare la destinazione dello storage remoto. Il nome qualificato NVMe per l'array di storage viene sempre assegnato dal sottosistema e non può essere modificato. Esiste un solo NVMe Qualified Name per l'intero array. La lunghezza massima del nome qualificato NVMe è di 223 caratteri. È possibile confrontarlo con un nome qualificato iSCSI.

Che cos'è un namespace e un ID namespace?

Uno spazio dei nomi è l'equivalente di un'unità logica in SCSI, che si riferisce a un volume nell'array. L'ID dello spazio dei nomi (NSID) equivale a un numero di unità logica (LUN) in SCSI. L'NSID viene creato al momento della creazione dello spazio dei nomi e può essere impostato su un valore compreso tra 1 e 255.

Che cos'è un controller NVMe?

Analogamente a un Nexus SCSI i_T, che rappresenta il percorso dall'iniziatore dell'host alla destinazione del sistema di storage, un controller NVMe creato durante il processo di connessione dell'host fornisce un percorso di accesso tra un host e gli spazi dei nomi nell'array di storage. Un NQN per l'host più un identificatore di porta host identificano in modo univoco un controller NVMe. Sebbene un controller NVMe possa essere associato solo a un singolo host, può accedere a più spazi dei nomi.

È possibile configurare gli host a cui accedere e impostare l'ID dello spazio dei nomi per l'host utilizzando Gestione di sistema di SANtricity. Quindi, quando viene creato il controller NVMe, viene creato e utilizzato l'elenco degli ID dello spazio dei nomi accessibili dal controller NVMe per configurare le connessioni consentite.

Terminologia NVMe

Scopri in che modo i termini NVMe si applicano al tuo storage array.

Termine	Descrizione
InfiniBand	InfiniBand (IB) è uno standard di comunicazione per la trasmissione dei dati tra server e sistemi storage dalle performance elevate.
Namespace	Uno spazio dei nomi è uno storage NVM formattato per l'accesso a blocchi. È analogo a un'unità logica in SCSI, che si riferisce a un volume nell'array di storage.
ID spazio dei nomi	L'ID dello spazio dei nomi è l'identificatore univoco del controller NVMe per lo spazio dei nomi e può essere impostato su un valore compreso tra 1 e 255. È analogo a un numero di unità logica (LUN) in SCSI.
NQN	NVMe Qualified Name (NQN) viene utilizzato per identificare la destinazione dello storage remoto (lo storage array).
NVM	La memoria non volatile (NVM) è una memoria persistente utilizzata in molti tipi di dispositivi di storage.

Termine	Descrizione
NVMe	NVMe (non-volatile Memory Express) è un'interfaccia progettata per i dispositivi di storage basati su flash, come ad esempio i dischi SSD. NVMe riduce l'overhead di i/o e include miglioramenti delle performance rispetto alle interfacce dei dispositivi logici precedenti.
NVMe-of	NVMe-of (non-volatile Memory Express over Fabrics) è una specifica che consente ai comandi e ai dati NVMe di trasferire in rete tra un host e lo storage.
Controller NVMe	Durante il processo di connessione all'host viene creato un controller NVMe. Fornisce un percorso di accesso tra un host e gli spazi dei nomi nell'array di storage.
Coda NVMe	Una coda viene utilizzata per il passaggio di comandi e messaggi sull'interfaccia NVMe.
Sottosistema NVMe	Lo storage array con una connessione host NVMe.
RDMA	L'accesso remoto diretto alla memoria (RDMA) consente uno spostamento dei dati più diretto all'interno e all'esterno di un server implementando un protocollo di trasporto nell'hardware della scheda di interfaccia di rete (NIC).
ROCE	RDMA over Converged Ethernet (RoCE) è un protocollo di rete che consente l'accesso remoto diretto alla memoria (RDMA) su una rete Ethernet.
SSD	I dischi a stato solido (SSD) sono dispositivi di storage che utilizzano la memoria a stato solido (flash) per memorizzare i dati in modo persistente. Gli SSD emulano i dischi rigidi convenzionali e sono disponibili con le stesse interfacce utilizzate dai dischi rigidi.

Come fare

Configurare NVMe sulle porte InfiniBand

Se il controller include una connessione NVMe su InfiniBand, è possibile configurare le impostazioni della porta NVMe dalla pagina System (sistema).

Prima di iniziare

- Il controller deve includere una porta host NVMe over InfiniBand; in caso contrario, le impostazioni NVMe over InfiniBand non sono disponibili in System Manager.
- È necessario conoscere l'indirizzo IP della connessione host.

> Le impostazioni e le funzioni NVMe over InfiniBand vengono visualizzate solo se il controller dello storage array include una porta NVMe over InfiniBand.

Fasi

1. Selezionare **Impostazioni › sistema**.

2. In **NVMe over InfiniBand settings**, selezionare **Configure NVMe over InfiniBand ports** (Configura NVMe su porte InfiniBand).
3. Selezionare il controller con la porta NVMe over InfiniBand che si desidera configurare. Fare clic su **Avanti**.
4. Selezionare la porta HIC che si desidera configurare dall'elenco a discesa, quindi immettere l'indirizzo IP.

   Se si configura un array di storage EF600 con un HIC da 200 GB, questa finestra di dialogo visualizza due campi IP Address (Indirizzo IP), uno per una porta fisica (esterna) e uno per una porta virtuale (interna). È necessario assegnare un indirizzo IP univoco a entrambe le porte. Queste impostazioni consentono all'host di stabilire un percorso tra ciascuna porta e di ottenere le massime prestazioni dall'HIC. Se non si assegna un indirizzo IP alla porta virtuale, l'HIC funziona a circa la metà della velocità.

5. Fare clic su **fine**.
6. Ripristinare la porta NVMe over InfiniBand facendo clic su **Sì**.

Configurare NVMe sulle porte RoCE

Se il controller include una connessione per NVMe su RoCE (RDMA over Converged Ethernet), è possibile configurare le impostazioni della porta NVMe dalla pagina System (sistema).

Prima di iniziare

- Il controller deve includere un NVMe su una porta host RoCE; in caso contrario, le impostazioni NVMe su RoCE non sono disponibili in System Manager.
- È necessario conoscere l'indirizzo IP della connessione host.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **NVMe over ROCE settings**, selezionare **Configure NVMe over ROCE ports** (Configura NVMe su porte ROCE).
3. Selezionare il controller con la porta NVMe over RoCE che si desidera configurare. Fare clic su **Avanti**.
4. Selezionare la porta HIC che si desidera configurare dall'elenco a discesa. Fare clic su **Avanti**.
5. Configurare le impostazioni della porta.

   Per visualizzare tutte le impostazioni della porta, fare clic sul collegamento **Mostra altre impostazioni della porta** a destra della finestra di dialogo.

Dettagli campo

Impostazione della porta	Descrizione
Velocità della porta ethernet configurata	Selezionare la velocità che corrisponde alla velocità del modulo SFP sulla porta.
Attiva IPv4 / attiva IPv6	Selezionare una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6. Se si desidera disattivare l'accesso alla porta, deselezionare entrambe le caselle di controllo.
Dimensione MTU (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire una nuova dimensione in byte per l'unità di trasmissione massima (MTU). La dimensione massima predefinita dell'unità di trasmissione (MTU) è di 1500 byte per frame. Immettere un valore compreso tra 1500 e 9000.

Se si seleziona **Enable IPv4** (attiva IPv4), dopo aver fatto clic su **Next** (Avanti) viene visualizzata una finestra di dialogo per la selezione delle impostazioni IPv4. Se si seleziona **Enable IPv6** (attiva IPv6*), dopo aver fatto clic su **Next** (Avanti) viene visualizzata una finestra di dialogo per la selezione delle impostazioni IPv6. Se sono state selezionate entrambe le opzioni, viene visualizzata prima la finestra di dialogo per le impostazioni IPv4, quindi dopo aver fatto clic su **Avanti**, viene visualizzata la finestra di dialogo per le impostazioni IPv6.

1. Configurare le impostazioni IPv4 e/o IPv6, automaticamente o manualmente.

Dettagli campo

Impostazione della porta	Descrizione
Ottenere automaticamente la configurazione	Selezionare questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Selezionare questa opzione, quindi inserire un indirizzo statico nei campi. (Se lo si desidera, è possibile tagliare e incollare gli indirizzi nei campi). Per IPv4, includere la subnet mask di rete e il gateway. Per IPv6, includere l'indirizzo IP instradabile e l'indirizzo IP del router. Se si configura un array di storage EF600 con un HIC da 200 GB, questa finestra di dialogo visualizza due serie di campi per i parametri di rete, uno per una porta fisica (esterna) e uno per una porta virtuale (interna). È necessario assegnare parametri univoci per entrambe le porte. Queste impostazioni consentono all'host di stabilire un percorso tra ciascuna porta e di ottenere le massime prestazioni dall'HIC. Se non si assegna un indirizzo IP alla porta virtuale, l'HIC funziona a circa la metà della velocità.

2. Fare clic su **fine**.

Visualizza le statistiche NVMe over Fabrics

È possibile visualizzare i dati relativi alle connessioni NVMe over Fabrics allo storage array.

A proposito di questa attività

System Manager mostra questi tipi di statistiche NVMe over Fabrics. Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **NVMe Subsystem statistics** — Mostra le statistiche del controller NVMe e della relativa coda. Il controller NVMe fornisce un percorso di accesso tra un host e gli spazi dei nomi nell'array di storage. È possibile esaminare le statistiche del sottosistema NVMe per elementi quali errori di connessione, ripristini e arresti.
- **RDMA Interface statistics** — fornisce statistiche per tutte le porte NVMe over Fabrics sull'interfaccia RDMA, che includono statistiche sulle performance e informazioni sugli errori di collegamento associate a ciascuna porta dello switch. Questa scheda viene visualizzata solo quando sono disponibili porte NVMe over Fabrics.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Selezionare **View NVMe over Fabrics Statistics** (Visualizza statistiche NVMe over Fabrics).
3. **Opzionale:** per impostare la linea di base, fare clic su **Imposta nuova linea di base**.

   L'impostazione della linea di base consente di impostare un nuovo punto di partenza per la raccolta delle statistiche. La stessa linea di base viene utilizzata per tutte le statistiche NVMe.

FAQ

Come si interpretano le statistiche NVMe sulle fabric?

La finestra di dialogo View NVMe over Fabrics Statistics (Visualizza statistiche NVMe su fabric) visualizza le statistiche per il sottosistema NVMe e l'interfaccia RDMA. Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **NVMe Subsystem statistics** — Mostra le statistiche del controller NVMe e della relativa coda. Il controller NVMe fornisce un percorso di accesso tra un host e gli spazi dei nomi nell'array di storage. È possibile esaminare le statistiche del sottosistema NVMe per elementi quali errori di connessione, ripristini e arresti. Per ulteriori informazioni su queste statistiche, fare clic su **Visualizza legenda per le intestazioni delle tabelle**.
- **RDMA Interface statistics** — fornisce statistiche per tutte le porte NVMe over Fabrics sull'interfaccia RDMA, che includono statistiche sulle performance e informazioni sugli errori di collegamento associate a ciascuna porta dello switch. Questa scheda viene visualizzata solo quando sono disponibili porte NVMe over Fabrics. Per ulteriori informazioni sulle statistiche, fare clic su **Visualizza legenda per le intestazioni delle tabelle**.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

Quali altre operazioni è necessario eseguire per configurare o diagnosticare NVMe su InfiniBand?

La seguente tabella elenca le funzioni di System Manager che è possibile utilizzare per configurare e gestire le sessioni NVMe su InfiniBand.

> Le impostazioni NVMe over InfiniBand sono disponibili solo se il controller dello storage array include una porta NVMe over InfiniBand.

Configurare e diagnosticare NVMe su InfiniBand

Azione	Posizione
Configurare NVMe sulle porte InfiniBand	1. Selezionare **hardware**. 2. Selezionare **Mostra retro dello shelf**. 3. Selezionare un controller. 4. Selezionare **Configura NVMe su porte InfiniBand**. oppure 1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **NVMe over InfiniBand settings**, quindi selezionare **Configure NVMe over InfiniBand Ports** (Configura NVMe su porte InfiniBand).
Visualizza le statistiche NVMe su InfiniBand	1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **NVMe over InfiniBand Settings**, quindi selezionare **View NVMe over Fabrics Statistics** (Visualizza statistiche NVMe over Fabrics).

Quali altre operazioni è necessario eseguire per configurare o diagnosticare NVMe su RoCE?

È possibile configurare e gestire NVMe su RoCE dalle pagine hardware e impostazioni.

> Le impostazioni NVMe over RoCE sono disponibili solo se il controller dello storage array include una porta NVMe over RoCE.

Configurare e diagnosticare NVMe su RoCE

Azione	Posizione
Configurare NVMe sulle porte RoCE	1. Selezionare **hardware**. 2. Selezionare **Mostra retro dello shelf**. 3. Selezionare un controller. 4. Selezionare **Configure NVMe over RoCE ports** (Configura NVMe su porte RoCE). oppure 1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **NVMe over RoCE settings**, quindi selezionare **Configure NVMe over RoCE Ports** (Configura NVMe su porte RoCE).
Visualizza le statistiche NVMe over Fabrics	1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **NVMe over RoCE settings**, quindi selezionare **View NVMe over Fabrics Statistics** (Visualizza statistiche NVMe over Fabrics).

Perché sono presenti due indirizzi IP per una porta fisica?

Lo storage array EF600 può includere due HICS, uno esterno e uno interno.

In questa configurazione, l'HIC esterno è collegato a un HIC interno ausiliario. Ciascuna porta fisica a cui è possibile accedere dall'HIC esterno dispone di una porta virtuale associata dall'HIC interno.

Per ottenere prestazioni massime di 200 GB, è necessario assegnare un indirizzo IP univoco per le porte fisiche e virtuali in modo che l'host possa stabilire connessioni a ciascuna porta. Se non si assegna un indirizzo IP alla porta virtuale, l'HIC funziona a circa la metà della velocità.

Perché esistono due set di parametri per una porta fisica?

Lo storage array EF600 può includere due HICS, uno esterno e uno interno.

In questa configurazione, l'HIC esterno è collegato a un HIC interno ausiliario. Ciascuna porta fisica a cui è possibile accedere dall'HIC esterno dispone di una porta virtuale associata dall'HIC interno.

Per ottenere prestazioni massime di 200 GB, è necessario assegnare i parametri per le porte fisiche e virtuali in modo che l'host possa stabilire connessioni a ciascuna porta. Se non si assegnano parametri alla porta virtuale, l'HIC funziona a circa la metà della velocità.

Sistema: Funzionalità aggiuntive

Concetti

Come funzionano le funzionalità aggiuntive

I componenti aggiuntivi sono funzionalità non incluse nella configurazione standard di System Manager e potrebbero richiedere una chiave per l'attivazione. Una funzione

aggiuntiva può essere una singola funzionalità premium o un pacchetto di funzionalità.

I seguenti passaggi forniscono una panoramica sull'attivazione di una funzionalità Premium o Feature Pack:

1. Ottenere le seguenti informazioni:
   - Numero di serie dello chassis e Feature Enable Identifier, che identificano l'array di storage per la funzione da installare. Questi elementi sono disponibili in System Manager.
   - Codice di attivazione della funzione, disponibile sul sito del supporto al momento dell'acquisto della funzione.
2. Per ottenere la chiave funzione, contattare il proprio provider di storage o accedere al sito di attivazione delle funzionalità Premium. Fornire il numero di serie dello chassis, l'identificatore di abilitazione e il codice funzione per l'attivazione.
3. Utilizzando System Manager, attivare la funzionalità Premium o il Feature Pack utilizzando il file delle chiavi funzione.

Terminologia delle funzionalità aggiuntive

Scopri in che modo i termini delle funzionalità aggiuntive si applicano al tuo storage array.

Termine	Descrizione
Identificatore di abilitazione della funzione	Feature Enable Identifier è una stringa univoca che identifica lo storage array specifico. Questo identificatore garantisce che, quando si ottiene la funzionalità premium, venga associata solo a quel particolare array di storage. Questa stringa viene visualizzata sotto Add-Ons nella pagina System (sistema).
File delle chiavi di funzione	Un file Feature Key è un file ricevuto per lo sblocco e l'attivazione di una funzionalità Premium o Feature Pack.
Feature Pack	Un Feature Pack è un bundle che modifica gli attributi degli array di storage (ad esempio, la modifica del protocollo da Fibre Channel a iSCSI). I Feature Pack richiedono una chiave speciale per attivarli.
Funzionalità Premium	Una funzione premium è un'opzione aggiuntiva che richiede una chiave per attivarla. Non è incluso nella configurazione standard di System Manager.

Come fare

Ottenere un file delle chiavi di funzione

Per attivare una funzionalità o un Feature Pack premium sull'array di storage, è necessario prima ottenere un file delle chiavi delle funzioni. Una chiave è associata a un solo array di storage.

A proposito di questa attività

Questa attività descrive come raccogliere le informazioni necessarie per la funzione e inviare una richiesta per un file delle chiavi di funzione. Le informazioni richieste includono:

- Numero di serie dello chassis

- Identificatore di abilitazione della funzione
- Codice di attivazione della funzione

Fasi

1. In System Manager, individuare e registrare il numero di serie dello chassis. Per visualizzare questo numero di serie, passare il mouse sul riquadro Support Center.
2. In System Manager, individuare Feature Enable Identifier. Accedere a **Impostazioni › sistema**, quindi scorrere verso il basso fino a **componenti aggiuntivi**. Cercare **Feature Enable Identifier**. Annotare il numero per l'identificatore di abilitazione della funzione.
3. Individuare e registrare il codice per l'attivazione della funzione. Per i pacchetti di funzionalità, questo codice viene fornito nelle istruzioni appropriate per l'esecuzione della conversione.

   Le istruzioni NetApp sono disponibili all'interno del sito "Centro di documentazione dei sistemi NetApp e-Series".

   Per le funzioni Premium, è possibile accedere al codice di attivazione dal sito del supporto, come indicato di seguito:

   a. Accedere a. "Supporto NetApp".
   b. Accedere a **licenze software** per il prodotto in uso.
   c. Inserire il numero di serie dello chassis dello storage array, quindi fare clic su **Go**.
   d. Cercare i codici di attivazione delle funzioni nella colonna **chiave di licenza**.
   e. Annotare il codice di attivazione della funzione desiderata.
4. Richiedere un file delle chiavi hardware inviando un'e-mail o un documento di testo al fornitore dello storage con le seguenti informazioni: Numero di serie dello chassis, identificativo di abilitazione e codice per l'attivazione delle funzioni.

   È inoltre possibile visitare il sito Web all'indirizzo "Attivazione della licenza NetApp: Attivazione della funzionalità Premium dello storage Array" e inserire le informazioni richieste per ottenere la funzionalità o il feature pack. (Le istruzioni su questo sito sono relative alle funzioni premium, non ai pacchetti di funzionalità).

Al termine

Se si dispone di un file delle chiavi delle funzioni, è possibile attivare la funzionalità Premium o il Feature Pack.

Abilitare una funzione premium

Una funzione premium è un'opzione aggiuntiva che richiede una chiave per l'attivazione.

Prima di iniziare

- È stata ottenuta una chiave funzione. Se necessario, contattare il supporto tecnico per ottenere una chiave.
- Il file delle chiavi è stato caricato sul client di gestione (il sistema con un browser per l'accesso a System Manager).

A proposito di questa attività

Questa attività descrive come utilizzare System Manager per attivare una funzione Premium.

> Se si desidera disattivare una funzione Premium, è necessario utilizzare il comando Disable Storage Array Feature (Disattiva funzionalità array di storage) (`disable storageArray (featurePack | feature=featureAttributeList)`) Nell'interfaccia della riga di comando (CLI).

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **componenti aggiuntivi**, selezionare **attiva funzionalità Premium**.

   Viene visualizzata la finestra di dialogo Enable a Premium Feature (attiva una funzione Premium).

3. Fare clic su **Browse**, quindi selezionare il file delle chiavi.

   Il nome del file viene visualizzato nella finestra di dialogo.

4. Fare clic su **Enable** (attiva).

Abilitare il Feature Pack

Un Feature Pack è un bundle che modifica gli attributi degli array di storage (ad esempio, la modifica del protocollo da Fibre Channel a iSCSI). I Feature Pack richiedono una chiave speciale per l'abilitazione.

Prima di iniziare

- Sono state seguite le istruzioni appropriate per l'esecuzione della conversione e la preparazione del sistema per i nuovi attributi dell'array di storage.

  > Le istruzioni di conversione sono disponibili all'interno del sito "Centro di documentazione dei sistemi NetApp e-Series".

- Lo storage array non è in linea, quindi non vi accedono host o applicazioni.
- Viene eseguito il backup di tutti i dati.
- È stato ottenuto un file Feature Pack.

  Il file del Feature Pack viene caricato sul client di gestione (il sistema con un browser per l'accesso a System Manager).

> È necessario pianificare una finestra di manutenzione del downtime e interrompere tutte le operazioni di i/o tra l'host e i controller. Inoltre, tenere presente che non è possibile accedere ai dati sull'array di storage fino a quando la conversione non è stata completata correttamente.

A proposito di questa attività

Questa attività descrive come utilizzare System Manager per attivare un Feature Pack. Al termine, riavviare lo storage array.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **componenti aggiuntivi**, selezionare **Cambia Feature Pack**.

3. Fare clic su **Browse**, quindi selezionare il file delle chiavi.

   Il nome del file viene visualizzato nella finestra di dialogo.

4. Digitare **CHANGE** nel campo.
5. Fare clic su **Cambia**.

   Viene avviata la migrazione dei Feature Pack e i controller vengono riavviati. I dati della cache non scritti vengono cancellati, il che garantisce l'assenza di attività i/O. Entrambi i controller si riavviano automaticamente per rendere effettivo il nuovo Feature Pack. Una volta completato il riavvio, lo storage array torna allo stato di risposta.

Scaricare l'interfaccia a riga di comando (CLI)

Da System Manager è possibile scaricare il pacchetto dell'interfaccia a riga di comando (CLI). La CLI fornisce un metodo basato su testo per la configurazione e il monitoraggio degli array di storage. Comunica tramite https e utilizza la stessa sintassi della CLI disponibile nel pacchetto software di gestione installato esternamente. Non è richiesta alcuna chiave per scaricare la CLI.

Prima di iniziare

- Sul sistema di gestione in cui si intende eseguire i comandi CLI deve essere disponibile Java Runtime Environment (JRE), versione 8 e successive.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **componenti aggiuntivi**, selezionare **interfaccia riga di comando**.

   Il pacchetto ZIP viene scaricato nel browser.

3. Salvare il file ZIP nel sistema di gestione in cui si desidera eseguire i comandi CLI per l'array di storage, quindi estrarre il file.

   È ora possibile eseguire i comandi CLI da un prompt del sistema operativo, ad esempio il prompt di DOS C:. Un riferimento al comando CLI è disponibile nel menu Help (Guida) in alto a destra dell'interfaccia utente di System Manager.

Sistema: 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 a **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 a **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 a **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.

Termine	Descrizione
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.
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 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 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 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 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:
   - **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). Il numero di porta più comune utilizzato per le comunicazioni del server di gestione delle chiavi è 5696.
   - **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.
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 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 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 protezione).

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 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).

> 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 › sistemi**.
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.
   - **Numero della porta KMIP** — inserire il numero della porta utilizzata 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 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.

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. **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.

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 a **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).
- Se si sta reimpostando un disco NVMe bloccato, è necessario inserire l'ID di sicurezza del disco. Per individuare l'ID di sicurezza, rimuovere fisicamente l'unità e individuare la stringa PSID (massimo 32 caratteri) sull'etichetta dell'unità. Assicurarsi che il disco sia reinstallato prima di avviare l'operazione.

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

La finestra Drive Settings (Impostazioni disco) contiene informazioni sugli attributi Drive Security (protezione disco). "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).

Gestione degli accessi

Concetti

Come funziona Access Management

La gestione degli accessi è un metodo per stabilire l'autenticazione dell'utente in Gestione di sistema di SANtricity.

La configurazione di Access Management e l'autenticazione dell'utente funzionano come segue:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni di amministratore della sicurezza.

   > Per il primo accesso, il nome utente `admin` viene visualizzato automaticamente e non può essere modificato. Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema.

2. L'amministratore accede a Access Management nell'interfaccia utente. Lo storage array è preconfigurato per l'utilizzo dei ruoli utente locali, ovvero un'implementazione delle funzionalità RBAC (role-based access control).
3. L'amministratore configura uno o più dei seguenti metodi di autenticazione:
   - **Ruoli utente locali** — l'autenticazione viene gestita tramite funzionalità RBAC applicate nell'array di storage. I ruoli utente locali includono profili utente predefiniti e ruoli con autorizzazioni di accesso specifiche. Gli amministratori possono utilizzare questi ruoli utente locali come singolo metodo di autenticazione o in combinazione con un servizio di directory. Non è necessaria alcuna configurazione, ad eccezione dell'impostazione delle password per gli utenti.

- **Servizi di directory** — l'autenticazione viene gestita tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft. Un amministratore si connette al server LDAP, quindi esegue il mapping degli utenti LDAP ai ruoli utente locali incorporati nell'array di storage.
- **SAML** — l'autenticazione viene gestita tramite un provider di identità (IdP) utilizzando il linguaggio SAML (Security Assertion Markup Language) 2.0. Un amministratore stabilisce la comunicazione tra il sistema IdP e l'array di storage, quindi mappa gli utenti IdP ai ruoli utente locali integrati nell'array di storage.

4. L'amministratore fornisce agli utenti le credenziali di accesso per System Manager.
5. Gli utenti accedono al sistema inserendo le proprie credenziali.

> Se l'autenticazione viene gestita con SAML e SSO (Single Sign-on), il sistema potrebbe ignorare la finestra di dialogo di accesso di System Manager.

Durante l'accesso, il sistema esegue le seguenti attività in background:

- Autentica il nome utente e la password rispetto all'account utente.
- Determina le autorizzazioni dell'utente in base ai ruoli assegnati.
- Fornisce all'utente l'accesso alle attività nell'interfaccia utente.
- Visualizza il nome utente nella parte superiore destra dell'interfaccia.

Attività disponibili in System Manager

L'accesso alle attività dipende dai ruoli assegnati a un utente, che includono:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol).
- **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Un'attività non disponibile viene visualizzata in grigio o non viene visualizzata nell'interfaccia utente. Ad esempio, un utente con il ruolo Monitor può visualizzare tutte le informazioni sui volumi, ma non può accedere alle funzioni per la modifica di tale volume. Le schede relative a funzioni come **Copy Services** e **Add to workload** non saranno visualizzate; sono disponibili solo **View/Edit Settings**.

Limitazioni in Gestione unificata di SANtricity e Gestione dello storage di SANtricity

Se SAML è configurato per un array di storage, gli utenti non possono rilevare o gestire lo storage per tale array dalle interfacce di gestione unificata dello storage SANtricity o SANtricity.

Una volta configurati i ruoli utente locali e i servizi di directory, gli utenti devono immettere le credenziali prima di eseguire una delle seguenti funzioni:

- Ridenominazione dello storage array

- Aggiornamento del firmware del controller
- Caricamento della configurazione di uno storage array
- Esecuzione di uno script
- Tentativo di eseguire un'operazione attiva quando una sessione non utilizzata è scaduta

Terminologia per la gestione degli accessi

Scopri come si applicano i termini di Access Management al tuo storage array.

Termine	Descrizione
Active Directory	Active Directory (ad) è un servizio di directory Microsoft che utilizza LDAP per le reti di dominio Windows.
Binding	Le operazioni BIND vengono utilizzate per autenticare i client nel server di directory. Il binding in genere richiede credenziali di account e password, ma alcuni server consentono operazioni di binding anonime.
CIRCA	Un'autorità di certificazione (CA) è un'entità attendibile che emette documenti elettronici, denominati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti Web, consentendo connessioni sicure tra client e server.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli autori degli attacchi di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e l'identità dell'entità attendibile che certifica (firma) queste informazioni.
IDP	Un provider di identità (IdP) è un sistema esterno utilizzato per richiedere le credenziali a un utente e per determinare se tale utente è autenticato correttamente. È possibile configurare IdP in modo da fornire l'autenticazione a più fattori e utilizzare qualsiasi database utente, ad esempio Active Directory. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP.
LDAP	LDAP (Lightweight Directory Access Protocol) è un protocollo applicativo per l'accesso e la manutenzione dei servizi informativi di directory distribuiti. Questo protocollo consente a numerose applicazioni e servizi diversi di connettersi al server LDAP per la convalida degli utenti.
RBAC	RBAC (role-based access control) è un metodo per regolare l'accesso alle risorse di computer o di rete in base ai ruoli dei singoli utenti. I controlli RBAC vengono applicati all'array di storage e includono ruoli predefiniti.
SAML	SAML (Security Assertion Markup Language) è uno standard basato su XML per l'autenticazione e l'autorizzazione tra due entità. SAML consente l'autenticazione a più fattori, in cui gli utenti devono fornire due o più elementi per dimostrare la propria identità (ad esempio, una password e un'impronta digitale). La funzionalità SAML integrata dello storage array è conforme a SAML2.0 per l'asserzione, l'autenticazione e l'autorizzazione dell'identità.

Termine	Descrizione
SP	Un service provider (SP) è un sistema che controlla l'autenticazione e l'accesso degli utenti. Quando Access Management è configurato con SAML, lo storage array agisce come service provider per richiedere l'autenticazione al provider di identità.
SSO	SSO (Single Sign-on) è un servizio di autenticazione che consente a un set di credenziali di accesso di accedere a più applicazioni.

Autorizzazioni per i ruoli mappati

Le funzionalità RBAC (role-based access control) applicate all'array di storage includono profili utente predefiniti con uno o più ruoli mappati. Ogni ruolo include le autorizzazioni per l'accesso alle attività in Gestore di sistema di SANtricity.

I profili utente e i ruoli mappati sono accessibili dal menu **Impostazioni[Gestione accessi > ruoli utente locali]** nell'interfaccia utente di System Manager.

I ruoli forniscono agli utenti l'accesso alle attività, come segue:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol).
- **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Se un utente non dispone delle autorizzazioni per una determinata attività, tale attività viene visualizzata in grigio o non viene visualizzata nell'interfaccia utente.

Gestione degli accessi con ruoli utente locali

Per la gestione degli accessi, gli amministratori possono utilizzare le funzionalità RBAC (role-based access control) applicate nell'array di storage. Queste funzionalità sono denominate "ruoli utente locali".

Workflow di configurazione

I ruoli utente locali sono preconfigurati per lo storage array. Per utilizzare i ruoli utente locali per l'autenticazione, gli amministratori possono:

1. Un amministratore effettua l'accesso a Gestione di sistema di SANtricity con un profilo utente che include le autorizzazioni di amministratore della sicurezza.

   Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema.

2. Un amministratore esamina i profili utente predefiniti e non modificabili.
3. **Opzionale:** l'amministratore assegna nuove password per ogni profilo utente.
4. Gli utenti accedono al sistema con le credenziali assegnate.

Gestione

Quando si utilizzano solo ruoli utente locali per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modificare le password.
- Impostare una lunghezza minima per le password.
- Consentire agli utenti di effettuare l'accesso senza password.

Gestione degli accessi con servizi di directory

Per la gestione degli accessi, gli amministratori possono utilizzare un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft.

Workflow di configurazione

Se nella rete vengono utilizzati un server LDAP e un servizio di directory, la configurazione funziona come segue:

1. Un amministratore effettua l'accesso a Gestione di sistema di SANtricity con un profilo utente che include le autorizzazioni di amministratore della sicurezza.

   Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema.

2. L'amministratore inserisce le impostazioni di configurazione per il server LDAP. Le impostazioni includono il nome di dominio, l'URL e le informazioni sull'account di binding.
3. Se il server LDAP utilizza un protocollo sicuro (LDAPS), l'amministratore carica una catena di certificati CA (Certificate Authority) per l'autenticazione tra il server LDAP e lo storage array.
4. Una volta stabilita la connessione al server, l'amministratore associa i gruppi di utenti ai ruoli dell'array di storage. Questi ruoli sono predefiniti e non possono essere modificati.
5. L'amministratore verifica la connessione tra il server LDAP e lo storage array.
6. Gli utenti accedono al sistema con le credenziali LDAP/Directory Services assegnate.

Gestione

Quando si utilizzano i servizi di directory per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Aggiungere un server di directory.
- Modificare le impostazioni del server di directory.
- Associare gli utenti LDAP ai ruoli utente locali.
- Rimuovere un server di directory.

Gestione degli accessi con SAML

Per la gestione degli accessi, gli amministratori possono utilizzare le funzionalità SAML (Security Assertion Markup Language) 2.0 integrate nell'array.

Workflow di configurazione

La configurazione SAML funziona come segue:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni di amministratore della sicurezza.

   > Il `admin` L'utente ha accesso completo a tutte le funzioni di System Manager.

2. L'amministratore accede alla scheda **SAML** in Gestione accessi.
3. Un amministratore configura le comunicazioni con il provider di identità (IdP). Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è autenticato correttamente. Per configurare le comunicazioni con lo storage array, l'amministratore scarica il file di metadati IdP dal sistema IdP, quindi utilizza System Manager per caricare il file nello storage array.
4. Un amministratore stabilisce una relazione di trust tra il service provider e l'IdP. Un service provider controlla l'autorizzazione dell'utente; in questo caso, il controller nell'array di storage agisce come service provider. Per configurare le comunicazioni, l'amministratore utilizza System Manager per esportare un file di metadati del service provider per ciascun controller. Dal sistema IdP, l'amministratore importa i file di metadati nell'IdP.

   > Gli amministratori devono inoltre assicurarsi che IdP supporti la capacità di restituire un ID nome all'autenticazione.

5. L'amministratore associa i ruoli dell'array di storage agli attributi dell'utente definiti nell'IdP. A tale scopo, l'amministratore utilizza System Manager per creare le mappature.
6. L'amministratore verifica l'accesso SSO all'URL IdP. Questo test garantisce che lo storage array e IdP possano comunicare.

   > Una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

7. Da System Manager, l'amministratore abilita SAML per lo storage array.
8. Gli utenti accedono al sistema con le proprie credenziali SSO.

Gestione

Quando si utilizza SAML per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modificare o creare nuove mappature dei ruoli
- Esportare i file del provider di servizi

Restrizioni di accesso

Quando SAML è attivato, gli utenti non possono rilevare o gestire lo storage per quell'array dalle interfacce di gestione unificata dello storage SANtricity o SANtricity.

Inoltre, i seguenti client non possono accedere ai servizi e alle risorse degli array di storage:

- Finestra Enterprise Management (EMW)
- Interfaccia a riga di comando (CLI)
- Client Software Developer Kit (SDK)
- Client in-band
- Client REST API per l'autenticazione di base HTTP
- Effettuare l'accesso utilizzando l'endpoint REST API standard

Come fare

Visualizzare i ruoli utente locali

Dalla scheda Local User Roles (ruoli utente locali), è possibile visualizzare le mappature dei profili utente ai ruoli predefiniti. Questi mapping fanno parte del RBAC (role-based access control) applicato nell'array di storage.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

I profili utente e le mappature non possono essere modificati. È possibile modificare solo le password.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **ruoli utente locali**.

   I profili utente sono mostrati nella tabella:

   - **Root admin** (admin) — Super amministratore che ha accesso a tutte le funzioni del sistema. Questo profilo utente include tutti i ruoli.
   - **Storage admin** (storage) — l'amministratore responsabile di tutto il provisioning dello storage. Questo profilo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor.
   - **Security admin** (sicurezza) — l'utente responsabile della configurazione della sicurezza, inclusa la gestione degli accessi, la gestione dei certificati e le funzioni dei dischi abilitati alla sicurezza. Questo profilo utente include i seguenti ruoli: Security Admin e Monitor.
   - **Support admin** (support) — l'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo profilo utente include i seguenti ruoli: Support Admin e Monitor.
   - **Monitor** (monitor) — utente con accesso in sola lettura al sistema. Questo profilo utente include solo il ruolo Monitor.

Modificare le password

È possibile modificare le password utente per ciascun profilo utente in Gestione accessi.

Prima di iniziare

- Devi essere connesso come amministratore locale, che include le autorizzazioni di amministratore root.
- È necessario conoscere la password dell'amministratore locale.

A proposito di questa attività

Quando si sceglie una password, tenere presenti le seguenti linee guida:

- Le nuove password utente locali devono soddisfare o superare l'impostazione corrente per una password minima (in Visualizza/Modifica impostazioni).
- Le password distinguono tra maiuscole e minuscole.
- Gli spazi finali non vengono rimossi dalle password quando vengono impostati. Fare attenzione a includere spazi se inclusi nella password.
- Per una maggiore sicurezza, utilizzare almeno 15 caratteri alfanumerici e modificare la password frequentemente.

> La modifica della password in System Manager viene modificata anche nell'interfaccia della riga di comando (CLI). Inoltre, le modifiche apportate alla password causano l'interruzione della sessione attiva dell'utente.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare un utente dalla tabella.

   Il pulsante Change Password (Modifica password) diventa disponibile.

4. Selezionare **Change Password** (Modifica password).

   Viene visualizzata la finestra di dialogo Change Password (Modifica password).

5. Se non è stata impostata alcuna lunghezza minima per le password utente locali, selezionare la casella per richiedere all'utente selezionato di immettere una password per accedere all'array di storage, quindi digitare la nuova password per l'utente selezionato.
6. Immettere la password dell'amministratore locale, quindi fare clic su **Change** (Modifica).

Risultati

Se l'utente è attualmente connesso, la modifica della password provoca l'interruzione della sessione attiva dell'utente.

Modificare le impostazioni della password utente locale

È possibile impostare la lunghezza minima richiesta per tutte le password utente locali nuove o aggiornate sull'array di storage. È inoltre possibile consentire agli utenti locali di accedere allo storage array senza inserire una password.

Prima di iniziare

- Devi essere connesso come amministratore locale, che include le autorizzazioni di amministratore root.

A proposito di questa attività

Tenere presenti queste linee guida quando si imposta la lunghezza minima per le password utente locali:

- Le modifiche apportate non influiscono sulle password utente locali esistenti.
- La lunghezza minima richiesta per le password utente locali deve essere compresa tra 0 e 30 caratteri.
- Le nuove password utente locali devono soddisfare o superare l'impostazione di lunghezza minima corrente.
- Non impostare una lunghezza minima per la password se si desidera che gli utenti locali accedano allo storage array senza immettere una password.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare il pulsante **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo **Local User Password Settings** (Impostazioni password utente locale).

4. Effettuare una delle seguenti operazioni:
   - Per consentire agli utenti locali di accedere allo storage array *senza* inserire una password, deselezionare la casella di controllo "Richiedi almeno tutte le password utente locali".
   - Per impostare una lunghezza minima della password per tutte le password utente locali, selezionare la casella di controllo "Richiedi almeno tutte le password utente locali", quindi utilizzare la casella di selezione per impostare la lunghezza minima richiesta per tutte le password utente locali.

     Le nuove password utente locali devono soddisfare o superare l'impostazione corrente.

5. Fare clic su **Save** (Salva).

Aggiungere il server di directory

Per configurare l'autenticazione per la gestione degli accessi, è possibile stabilire comunicazioni tra lo storage array e un server LDAP, quindi mappare i gruppi di utenti LDAP ai ruoli predefiniti dell'array.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali del server LDAP devono essere disponibili, inclusi il nome di dominio, l'URL del server e, facoltativamente, il nome utente e la password dell'account BIND.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del server LDAP deve essere installata sul computer locale.

A proposito di questa attività

L'aggiunta di un server di directory è un processo in due fasi. Immettere innanzitutto il nome di dominio e l'URL. Se il server utilizza un protocollo sicuro, è necessario caricare anche un certificato CA per l'autenticazione se è firmato da un'autorità di firma non standard. Se si dispone delle credenziali per un account BIND, è anche possibile immettere il nome e la password dell'account utente. Quindi, mappare i gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.

> Durante la procedura di aggiunta di un server LDAP, l'interfaccia di gestione legacy viene disattivata. L'interfaccia di gestione legacy (Symbol) è un metodo di comunicazione tra lo storage array e il client di gestione. Se disattivato, lo storage array e il client di gestione utilizzano un metodo di comunicazione più sicuro (REST API over https).

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Dalla scheda **Directory Services**, selezionare **Add Directory Server** (Aggiungi server di directory).

   Viene visualizzata la finestra di dialogo Add Directory Server (Aggiungi server di directory).

3. Nella scheda **Server Settings** (Impostazioni server), immettere le credenziali per il server LDAP.

Dettagli campo

Impostazione	Descrizione
Impostazioni di configurazione	Dominio/i
Immettere il nome di dominio del server LDAP. Per più domini, inserire i domini in un elenco separato da virgole. Il nome di dominio viene utilizzato nel login (*nome utente@dominio*) per specificare il server di directory da autenticare.	URL del server
Immettere l'URL per l'accesso al server LDAP nel formato `ldap[s]://host:*port*`.	Carica certificato (opzionale)

Impostazione	Descrizione
Questo campo viene visualizzato solo se è stato specificato un protocollo LDAPS nel campo URL server sopra riportato. Fare clic su **Browse** (Sfoglia) e selezionare un certificato CA da caricare. Si tratta del certificato attendibile o della catena di certificati utilizzata per l'autenticazione del server LDAP.	Account BIND (opzionale)
Inserire un account utente di sola lettura per le query di ricerca sul server LDAP e per la ricerca all'interno dei gruppi. Immettere il nome dell'account in formato LDAP. Ad esempio, se l'utente bind è chiamato "bindacct", è possibile immettere un valore come "CN=bindacct,CN=Users,DC=cpoc,DC=local".	Password bind (opzionale)

Impostazione	Descrizione
Questo campo viene visualizzato quando si immette un account BIND. Immettere la password per l'account BIND.	Verificare la connessione al server prima di aggiungerli
Selezionare questa casella di controllo per assicurarsi che lo storage array possa comunicare con la configurazione del server LDAP immessa. Il test si verifica dopo aver fatto clic su **Add** (Aggiungi) nella parte inferiore della finestra di dialogo. Se questa casella di controllo è selezionata e il test non riesce, la configurazione non viene aggiunta. È necessario risolvere l'errore o deselezionare la casella di controllo per saltare il test e aggiungere la configurazione.	**Impostazioni dei privilegi**
Ricerca DN base	Immettere il contesto LDAP per la ricerca degli utenti, in genere sotto forma di `CN=Users, DC=copc, DC=local`.
Attributo Username	Inserire l'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.
Attributo/i di gruppo	Inserire un elenco di attributi di gruppo nell'utente, che viene utilizzato per il mapping gruppo-ruolo. Ad esempio: `memberOf, managedObjects`.

4. Fare clic sulla scheda **mappatura ruolo**.
5. Assegnare i gruppi LDAP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

Dettagli campo

Impostazione	Descrizione
Mapping	DN gruppo
Specificare il nome distinto del gruppo (DN) per il gruppo di utenti LDAP da mappare.	Ruoli

Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

1. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.
2. Al termine delle mappature, fare clic su **Aggiungi**.

   Il sistema esegue una convalida, assicurandosi che lo storage array e il server LDAP possano comunicare. Se viene visualizzato un messaggio di errore, selezionare le credenziali inserite nella finestra di dialogo e, se necessario, immettere nuovamente le informazioni.

Modificare le impostazioni del server di directory e le mappature dei ruoli

Se in precedenza è stato configurato un server di directory in Access Management, è possibile modificarne le impostazioni in qualsiasi momento. Le impostazioni includono le informazioni di connessione al server e i mapping gruppo-ruolo.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- È necessario definire un server di directory.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Directory Services**.
3. Se sono stati definiti più server, selezionare il server che si desidera modificare dalla tabella.
4. Selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo **Directory Server Settings** (Impostazioni server directory).

5. Nella scheda **Server Settings** (Impostazioni server), modificare le impostazioni desiderate.

Impostazione	Descrizione
Impostazioni di configurazione	Dominio/i
I nomi di dominio dei server LDAP. Per più domini, inserire i domini in un elenco separato da virgole. Il nome di dominio viene utilizzato nel login (*nome utente @dominio*) per specificare il server di directory da autenticare.	URL del server
L'URL per l'accesso al server LDAP nel formato `ldap[s]://host:*port*`.	Account BIND (opzionale)
L'account utente di sola lettura per le query di ricerca sul server LDAP e per la ricerca all'interno dei gruppi.	Password bind (opzionale)
La password per l'account BIND. (Questo campo viene visualizzato quando viene inserito un account BIND).	Verificare la connessione al server prima di salvare

Impostazione	Descrizione
Verifica che lo storage array possa comunicare con la configurazione del server LDAP. Il test si verifica dopo aver fatto clic su **Save** (Salva) nella parte inferiore della finestra di dialogo. Se questa casella di controllo è selezionata e il test non riesce, la configurazione non viene modificata. È necessario risolvere l'errore o deselezionare la casella di controllo per saltare il test e modificare nuovamente la configurazione.	**Impostazioni dei privilegi**
Ricerca DN base	Il contesto LDAP per la ricerca degli utenti, in genere sotto forma di `CN=Users, DC=copc, DC=local`.
Attributo Username	L'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.
Attributo/i di gruppo	Un elenco di attributi di gruppo sull'utente, utilizzato per il mapping gruppo-ruolo. Ad esempio: `memberOf, managedObjects`.

6. Nella scheda **role Mapping**, modificare la mappatura desiderata.

Impostazione	Descrizione
Mapping	DN gruppo
Il nome di dominio del gruppo di utenti LDAP da mappare.	Ruoli

> Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

7. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.
8. Fare clic su **Save** (Salva).

Risultati

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la

sessione utente corrente.

Rimuovere il server di directory

Per interrompere la connessione tra un server di directory e lo storage array, è possibile rimuovere le informazioni sul server dalla pagina Access Management. È possibile eseguire questa attività se è stato configurato un nuovo server e si desidera rimuovere quello precedente.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la sessione utente corrente.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Directory Services**.
3. Dall'elenco, selezionare il server di directory che si desidera eliminare.
4. Fare clic su **Rimuovi**.

   Viene visualizzata la finestra di dialogo **Remove Directory Server** (Rimuovi server di directory).

5. Tipo `remove` Nel campo, quindi fare clic su **Rimuovi**.

   Le impostazioni di configurazione del server di directory, le impostazioni dei privilegi e i mapping dei ruoli vengono rimossi. Gli utenti non possono più accedere con le credenziali da questo server.

Configurare SAML

Per configurare l'autenticazione per Access Management, è possibile utilizzare le funzionalità SAML (Security Assertion Markup Language) integrate nell'array di storage. Questa configurazione stabilisce una connessione tra un provider di identità e lo storage provider.

A proposito di questa attività

Un provider di identità (IdP) è un sistema esterno utilizzato per richiedere le credenziali a un utente e per determinare se tale utente è autenticato correttamente. È possibile configurare IdP in modo da fornire l'autenticazione a più fattori e utilizzare qualsiasi database utente, ad esempio Active Directory. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP. Un service provider (SP) è un sistema che controlla l'autenticazione e l'accesso degli utenti. Quando Access Management è configurato con SAML, lo storage array agisce come service provider per richiedere l'autenticazione al provider di identità. Per stabilire una connessione tra IdP e lo storage array, è necessario condividere i file di metadati tra queste due entità. Quindi, mappare le entità utente IdP ai ruoli degli array di storage. Infine, prima di attivare SAML, è necessario verificare la connessione e gli accessi SSO.

SAML e Directory Services. Se si attiva SAML quando Directory Services è configurato come metodo di autenticazione, SAML sostituisce Directory Services in System Manager. Se si disattiva SAML in un secondo momento, la configurazione dei servizi di directory torna alla configurazione precedente.

Modifica e disattivazione. una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

La configurazione dell'autenticazione SAML è una procedura multi-step.

Fase 1: Caricare il file di metadati IdP

Per fornire allo storage array le informazioni di connessione IdP, importare i metadati IdP in System Manager.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- Un amministratore IdP ha configurato un sistema IdP.
- Un amministratore IdP ha garantito che IdP supporti la capacità di restituire un ID nome all'autenticazione.
- Un amministratore ha garantito che i clock del server IdP e del controller siano sincronizzati (tramite un server NTP o regolando le impostazioni del clock del controller).
- Un file di metadati IdP viene scaricato dal sistema IdP ed è disponibile sul sistema locale utilizzato per accedere a System Manager.

A proposito di questa attività

In questa attività, si carica un file di metadati da IdP in System Manager. Il sistema IdP ha bisogno di questi metadati per reindirizzare le richieste di autenticazione all'URL corretto e per validare le risposte ricevute. È necessario caricare un solo file di metadati per l'array di storage, anche se sono presenti due controller.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.

   La pagina visualizza una panoramica delle fasi di configurazione.

3. Fare clic sul collegamento **Import Identity Provider (IdP) file**.

   Viene visualizzata la finestra di dialogo **Import Identity Provider file** (Importa file provider di identità).

4. Fare clic su **Browse** (Sfoglia) per selezionare e caricare il file di metadati IdP copiato nel sistema locale.

   Dopo aver selezionato il file, viene visualizzato l'ID entità IdP.

5. Fare clic su **Importa**.

Fase 2: Esportare i file del provider di servizi

Per stabilire una relazione di trust tra IdP e l'array di storage, importare i metadati del service provider nell'IdP.

Prima di iniziare

- Si conosce l’indirizzo IP o il nome di dominio di ciascun controller dell’array di storage.

A proposito di questa attività

In questa attività, si esportano i metadati dai controller (un file per ciascun controller). L’IdP ha bisogno di questi metadati per stabilire una relazione di trust con i controller e per elaborare le richieste di autorizzazione. Il file include informazioni come il nome di dominio del controller o l’indirizzo IP, in modo che l’IdP possa comunicare con i service provider.

Fasi

1. Fare clic sul collegamento **Export Service Provider Files**.

   Viene visualizzata la finestra di dialogo **Export Service Provider Files** (Esporta file provider di servizi).

2. Inserire l’indirizzo IP o il nome DNS del controller nel campo **Controller A**, quindi fare clic su **Export** per salvare il file di metadati nel sistema locale. Se lo storage array include due controller, ripetere questo passaggio per il secondo controller nel campo **Controller B**.

   Dopo aver fatto clic su **Esporta**, i metadati del provider di servizi vengono scaricati nel sistema locale. Prendere nota della posizione in cui è memorizzato il file.

3. Dal sistema locale, individuare i file di metadati del provider di servizi esportati.

   Per ciascun controller è disponibile un file in formato XML.

4. Dal server IdP, importare i file di metadati del provider di servizi per stabilire la relazione di trust. È possibile importare i file direttamente o inserire manualmente le informazioni del controller dai file.

Fase 3: Mappare i ruoli

Per fornire agli utenti l’autorizzazione e l’accesso a System Manager, è necessario mappare gli attributi utente IdP e le appartenenze ai gruppi ai ruoli predefiniti dell’array di storage.

Prima di iniziare

- Un amministratore IdP ha configurato gli attributi utente e l’appartenenza al gruppo nel sistema IdP.
- Il file di metadati IdP viene importato in System Manager.
- Un file di metadati del service provider per ciascun controller viene importato nel sistema IdP per la relazione di trust.

A proposito di questa attività

In questa attività, si utilizza System Manager per associare i gruppi IdP ai ruoli utente locali.

Fasi

1. Fare clic sul collegamento per la mappatura dei ruoli di System Manager.

   Viene visualizzata la finestra di dialogo mappatura ruoli.

2. Assegnare gli attributi e i gruppi degli utenti IdP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

Dettagli campo

Impostazione	Descrizione
Mapping	Attributo dell'utente
Specificare l'attributo (ad esempio, "membro di") per il gruppo SAML da mappare.	Valore dell'attributo
Specificare il valore dell'attributo per il gruppo da mappare.	Ruoli

> Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

3. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.

   > I mapping dei ruoli possono essere modificati dopo l'attivazione di SAML.

4. Una volta completate le mappature, fare clic su **Save** (Salva).

Fase 4: Verifica dell'accesso SSO

Per garantire che il sistema IdP e lo storage array possano comunicare, è possibile eseguire un test di accesso SSO. Questo test viene eseguito anche durante la fase finale per l'abilitazione di SAML.

Prima di iniziare

- Il file di metadati IdP viene importato in System Manager.
- Un file di metadati del service provider per ciascun controller viene importato nel sistema IdP per la relazione di trust.

Fasi

1. Selezionare il collegamento **Test SSO Login**.

   Viene visualizzata una finestra di dialogo per l'immissione delle credenziali SSO.

2. Immettere le credenziali di accesso per un utente con permessi di amministratore della sicurezza e di monitoraggio.

   Viene visualizzata una finestra di dialogo durante il test dell'accesso.

3. Cercare il messaggio Test Successful (Test riuscito). Se il test viene completato correttamente, passare alla fase successiva per l'abilitazione di SAML.

   Se il test non viene completato correttamente, viene visualizzato un messaggio di errore con ulteriori informazioni. Assicurarsi che:

- L'utente appartiene a un gruppo con autorizzazioni per Security Admin e Monitor.
- I metadati caricati per il server IdP sono corretti.
- Gli indirizzi del controller nei file di metadati SP sono corretti.

Fase 5: Abilitare SAML

Il passaggio finale consiste nell'abilitare l'autenticazione utente SAML.

Prima di iniziare

- Il file di metadati IdP viene importato in System Manager.
- Un file di metadati del service provider per ciascun controller viene importato nel sistema IdP per la relazione di trust.
- È stata configurata almeno una mappatura dei ruoli Monitor e Security Admin.

A proposito di questa attività

Questa attività descrive come completare la configurazione SAML per l'autenticazione dell'utente. Durante questo processo, il sistema richiede anche di verificare un accesso SSO. Il processo di test di accesso SSO è descritto nel passaggio precedente.

> **Modifica e disattivazione.** una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

Fasi

1. Dalla scheda **SAML**, selezionare il collegamento **Enable SAML** (attiva SAML).

   Viene visualizzata la finestra di dialogo **Confirm Enable SAML** (Conferma abilitazione SAML).

2. Tipo `enable`, Quindi fare clic su **Enable** (attiva).
3. Immettere le credenziali utente per un test di accesso SSO.

Risultati

Una volta attivato SAML, il sistema termina tutte le sessioni attive e inizia l'autenticazione degli utenti tramite SAML.

Modificare le mappature dei ruoli SAML

Se in precedenza è stato configurato SAML per Access Management, è possibile modificare le mappature dei ruoli tra i gruppi IdP e i ruoli predefiniti dell'array di storage.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- Un amministratore IdP ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- SAML è configurato e abilitato.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.

2. Selezionare la scheda **SAML**.
3. Selezionare **mappatura ruolo**.

   Viene visualizzata la finestra di dialogo **mappatura ruolo**.

4. Assegnare gli attributi e i gruppi degli utenti IdP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

   Prestare attenzione a non rimuovere le autorizzazioni mentre SAML è attivato, altrimenti si perde l'accesso a System Manager.

   Dettagli campo

Impostazione	Descrizione
Mapping	Attributo dell'utente
Specificare l'attributo (ad esempio, "membro di") per il gruppo SAML da mappare.	Valore dell'attributo
Specificare il valore dell'attributo per il gruppo da mappare.	Ruoli

   Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

1. **Opzionale:** fare clic su **Aggiungi un'altra mappatura** per immettere più mappature gruppo-ruolo.
2. Fare clic su **Save** (Salva).

Risultati

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la sessione utente corrente.

Esportare i file del provider di servizi SAML

Se necessario, è possibile esportare i metadati del service provider per lo storage array e reimportare i file nel sistema IdP (Identity Provider).

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- SAML è configurato e abilitato.

A proposito di questa attività

In questa attività, si esportano i metadati dai controller (un file per ciascun controller). L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con i controller ed elaborare le richieste di autenticazione. Il

file include informazioni come il nome di dominio del controller o l'indirizzo IP che IdP può utilizzare per l'invio delle richieste.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.
3. Selezionare **Esporta**.

   Viene visualizzata la finestra di dialogo **Export Service Provider Files** (Esporta file provider di servizi).

4. Per ciascun controller, fare clic su **Export** (Esporta) per salvare il file di metadati nel sistema locale.

   > I campi dei nomi di dominio per ciascun controller sono di sola lettura.

   Prendere nota della posizione in cui è memorizzato il file.

5. Dal sistema locale, individuare i file di metadati del provider di servizi esportati.

   Per ciascun controller è disponibile un file in formato XML.

6. Dal server IdP, importare i file di metadati del provider di servizi. È possibile importare i file direttamente o inserire manualmente le informazioni del controller.
7. Fare clic su **Chiudi**.

Visualizzare l'attività del registro di audit

Visualizzando i registri di controllo, gli utenti con autorizzazioni di amministratore della sicurezza possono monitorare le azioni degli utenti, gli errori di autenticazione, i tentativi di accesso non validi e la durata della sessione utente.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro di controllo**.

   L'attività del registro di controllo viene visualizzata in formato tabulare, che include le seguenti colonne di informazioni:

   - **Data/ora** — Timestamp di quando lo storage array ha rilevato l'evento (in GMT).
   - **Username** — Nome utente associato all'evento. Per qualsiasi azione non autenticata sull'array di storage, viene visualizzato "N/A" come nome utente. Le azioni non autenticate potrebbero essere attivate dal proxy interno o da qualche altro meccanismo.
   - **Status Code** — Codice di stato HTTP dell'operazione (200, 400, ecc.) e testo descrittivo associato all'evento.
   - **URL a cui si accede** — URL completo (incluso host) e stringa di query.
   - **Client IP Address** — Indirizzo IP del client associato all'evento.

- **Origine** — origine di registrazione associata all'evento, che può essere System Manager, CLI, Web Services o Support Shell.

3. Utilizzare le selezioni nella pagina Registro audit per visualizzare e gestire gli eventi.

Dettagli della selezione

Selezione	Descrizione
Mostra gli eventi del…	Limita gli eventi visualizzati in base all'intervallo di date (ultime 24 ore, ultimi 7 giorni, ultimi 30 giorni o un intervallo di date personalizzato).
Filtro	Limita gli eventi visualizzati dai caratteri immessi nel campo. Utilizzare le virgolette ("") per una corrispondenza esatta della parola, immettere `OR` per restituire una o più parole, oppure inserire un trattino (--) per omettere le parole.
Aggiornare	Selezionare **Refresh** (Aggiorna) per aggiornare la pagina agli eventi più recenti.
Visualizza/Modifica impostazioni	Selezionare **Visualizza/Modifica impostazioni** per aprire una finestra di dialogo che consente di specificare un criterio di log completo e il livello di azioni da registrare.
Eliminare gli eventi	Selezionare **Elimina** per aprire una finestra di dialogo che consente di rimuovere gli eventi precedenti dalla pagina.
Mostra/Nascondi colonne	Fare clic sull'icona della colonna **Mostra/Nascondi** per selezionare colonne aggiuntive da visualizzare nella tabella. Le colonne aggiuntive includono: • **Method** — il metodo HTTP (AD esempio, POST, GET, DELETE, ecc.). • **Comando CLI eseguito** — comando CLI (grammatica) eseguito per richieste CLI sicure. • **CLI Return Status** — un codice di stato CLI o una richiesta di file di input dal client. • **Symbol procedure** — procedura di simbolo eseguita. • **SSH Event Type** — tipo di eventi Secure Shell (SSH), come login, logout e login_fail. • **SSH Session PID** — numero ID del processo della sessione SSH. • **SSH Session Duration(s)** — il numero di secondi in cui l'utente ha effettuato l'accesso.
Attiva/disattiva filtri colonna	Fare clic sull'icona **Alterna** per aprire i campi di filtraggio per ciascuna colonna. Immettere i caratteri all'interno di un campo colonna per limitare gli eventi visualizzati da tali caratteri. Fare nuovamente clic sull'icona per chiudere i campi di filtraggio.
Annulla le modifiche	Fare clic sull'icona **Annulla** per ripristinare la configurazione predefinita della tabella.

Selezione	Descrizione
Esportare	Fare clic su **Export** (Esporta) per salvare i dati della tabella in un file CSV (comma Separated Value).

Definire i criteri del registro di controllo

È possibile modificare il criterio di sovrascrittura e i tipi di eventi registrati nel registro di controllo.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

Questa attività descrive come modificare le impostazioni del registro di controllo, che includono il criterio per la sovrascrittura degli eventi precedenti e il criterio per la registrazione dei tipi di evento.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro audit**.
3. Selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo **Impostazioni registro di controllo**.

4. Modificare il criterio di sovrascrittura o i tipi di eventi registrati.

Dettagli campo

Impostazione	Descrizione
Sovrascrivere il criterio	Determina il criterio per la sovrascrittura di eventi precedenti quando viene raggiunta la capacità massima: • **Consente di sovrascrivere gli eventi meno recenti nel registro di controllo quando il registro di controllo è pieno** — sovrascrive gli eventi precedenti quando il registro di controllo raggiunge 50,000 record. • **Richiedere l'eliminazione manuale degli eventi del registro di controllo** — specifica che gli eventi non verranno cancellati automaticamente; viene invece visualizzato un avviso di soglia in corrispondenza della percentuale impostata. Gli eventi devono essere cancellati manualmente. Se il criterio di sovrascrittura è disattivato e le voci del registro di controllo raggiungono il limite massimo, l'accesso a System Manager viene negato agli utenti senza autorizzazioni di amministratore della sicurezza. Per ripristinare l'accesso al sistema agli utenti senza autorizzazioni di amministratore della sicurezza, un utente assegnato al ruolo di amministratore della protezione deve eliminare i vecchi record di eventi. I criteri di sovrascrittura non si applicano se un server syslog è configurato per l'archiviazione dei registri di controllo.
Livello di azioni da registrare	Determina i tipi di eventi da registrare: • **Registra solo eventi di modifica** — Mostra solo gli eventi in cui un'azione dell'utente comporta la modifica del sistema. • **Registra tutti gli eventi di modifica e di sola lettura** — Mostra tutti gli eventi, inclusa un'azione dell'utente che comporta la lettura o il download delle informazioni.

5. Fare clic su **Save** (Salva).

Eliminare gli eventi dal registro di controllo

È possibile cancellare il registro di controllo degli eventi precedenti, rendendo più gestibile la ricerca tra gli eventi. È possibile salvare gli eventi precedenti in un file CSV (comma-Separated Values) al momento dell'eliminazione.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

Questa attività descrive come rimuovere i vecchi eventi dal registro di controllo.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro di controllo**.
3. Selezionare **Delete** (Elimina).

   Viene visualizzata la finestra di dialogo Delete Audit Log.

4. Selezionare o immettere il numero di eventi meno recenti che si desidera eliminare.
5. Se si desidera esportare gli eventi cancellati in un file CSV (scelta consigliata), mantenere la casella di controllo selezionata. Quando si fa clic su **Delete** (Elimina) nella fase successiva, viene richiesto di inserire un nome e una posizione per il file. In caso contrario, se non si desidera salvare gli eventi in un file CSV, fare clic sulla casella di controllo per deselezionarla.
6. Fare clic su **Delete** (Elimina).

   Viene visualizzata una finestra di dialogo di conferma.

7. Tipo `delete` Nel campo, quindi fare clic su **Delete** (Elimina).

   Gli eventi meno recenti vengono rimossi dalla pagina Registro di controllo.

Configurare il server syslog per i registri di controllo

Se si desidera archiviare i registri di controllo su un server syslog esterno, è possibile configurare le comunicazioni tra tale server e lo storage array. Una volta stabilita la connessione, i registri di controllo vengono salvati automaticamente nel server syslog.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- L'indirizzo del server syslog, il protocollo e il numero di porta devono essere disponibili. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se il server utilizza un protocollo sicuro (ad esempio TLS), è necessario che nel sistema locale sia disponibile un certificato dell'autorità di certificazione (CA). I certificati CA identificano i proprietari dei siti Web per connessioni sicure tra server e client.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Dalla scheda **Registro di controllo**, selezionare **Configura server Syslog**.

   Viene visualizzata la finestra di dialogo **Configura server Syslog**.

3. Fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo **Add Syslog Server** (Aggiungi server Syslog).

4. Inserire le informazioni relative al server, quindi fare clic su **Aggiungi**.

- **Indirizzo server** — immettere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- **Protocol** (protocollo) — selezionare un protocollo dall'elenco a discesa (ad esempio TLS, UDP o TCP).
- **Carica certificato (opzionale)** — se è stato selezionato il protocollo TLS e non è stato ancora caricato un certificato CA firmato, fare clic su **Sfoglia** per caricare un file di certificato. I registri di controllo non vengono archiviati in un server syslog senza un certificato attendibile.

> Se il certificato diventa non valido in un secondo momento, l'handshake TLS avrà esito negativo. Di conseguenza, un messaggio di errore viene inviato al registro di controllo e i messaggi non vengono più inviati al server syslog. Per risolvere questo problema, è necessario correggere il certificato sul server syslog e andare al menu **Impostazioni[Registro audit > Configura server Syslog > Test tutti]**.

- **Port** — inserire il numero di porta del ricevitore syslog.

  Dopo aver fatto clic su **Add** (Aggiungi), viene visualizzata la finestra di dialogo **Configure Syslog Servers** (Configura server Syslog) e il server syslog configurato.

5. Per verificare la connessione del server con lo storage array, selezionare **Test All**.

Risultati

Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti.

Modificare le impostazioni del server syslog per i record del registro di controllo

È possibile modificare le impostazioni del server syslog utilizzato per l'archiviazione dei registri di controllo e caricare un nuovo certificato CA per il server.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- L'indirizzo del server syslog, il protocollo e il numero di porta devono essere disponibili. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se si sta caricando un nuovo certificato CA, il certificato deve essere disponibile nel sistema locale.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Dalla scheda **Registro di controllo**, selezionare **Configura server Syslog**.

   I server syslog configurati vengono visualizzati nella pagina.

3. Per modificare le informazioni sul server, selezionare l'icona **Edit** (matita) a destra del nome del server, quindi apportare le modifiche desiderate nei seguenti campi:
   - **Server Address** — inserire un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
   - **Protocol** (protocollo) — selezionare un protocollo dall'elenco a discesa (ad esempio TLS, UDP o TCP).
   - **Port** — inserire il numero di porta del ricevitore syslog.
4. Se il protocollo è stato modificato nel protocollo TLS sicuro (da UDP o TCP), fare clic su **Import Trusted Certificate** (Importa certificato attendibile) per caricare un certificato CA.

5. Per verificare la nuova connessione con lo storage array, selezionare **Test All**.

Risultati

Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti.

FAQ

Perché non riesco ad accedere?

Se si riceve un errore durante il tentativo di accesso a System Manager, esaminare queste possibili cause.

Gli errori di accesso a System Manager possono verificarsi per uno dei seguenti motivi:

- Il nome utente o la password immessi non sono corretti.
- Privilegi insufficienti.
- Il server di directory (se configurato) potrebbe non essere disponibile. In questo caso, provare ad accedere con un ruolo utente locale.
- Si è tentato di accedere più volte senza successo, attivando la modalità di blocco. Attendere 10 minuti per eseguire nuovamente l'accesso.
- È stata attivata una condizione di blocco e il registro di controllo potrebbe essere pieno. Accedere a Gestione accessi ed eliminare i vecchi eventi dal registro di controllo.
- L'autenticazione SAML è attivata. Aggiornare il browser per accedere.

Gli errori di accesso a un array di storage remoto per le attività di mirroring possono verificarsi per uno dei seguenti motivi:

- La password immessa non è corretta.
- Si è tentato di accedere più volte senza successo, attivando la modalità di blocco. Attendere 10 minuti per effettuare nuovamente l'accesso.
- È stato raggiunto il numero massimo di connessioni client utilizzate sul controller. Verificare la presenza di più utenti o client.

Cosa occorre sapere prima di aggiungere un server di directory?

Prima di aggiungere un server di directory in Access Management, assicurarsi di soddisfare i seguenti requisiti.

- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali del server LDAP devono essere disponibili, inclusi il nome di dominio, l'URL del server e, facoltativamente, il nome utente e la password dell'account BIND.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del server LDAP deve essere installata sul computer locale.

Cosa occorre sapere sulla mappatura dei ruoli degli array di storage?

Prima di mappare i gruppi ai ruoli, consultare le seguenti linee guida.

Le funzionalità RBAC (role-based access control) integrate dello storage array includono i seguenti ruoli:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol).
- **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Servizi di directory

Se si utilizza un server LDAP (Lightweight Directory Access Protocol) e servizi di directory, assicurarsi che:

- Un amministratore ha definito i gruppi di utenti nel servizio di directory.
- Si conoscono i nomi di dominio del gruppo per i gruppi di utenti LDAP.
- Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

SAML

Se si utilizzano le funzionalità SAML (Security Assertion Markup Language) integrate nell'array di storage, assicurarsi che:

- Un amministratore del provider di identità (IdP) ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- Conosci i nomi dei membri del gruppo.
- Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

Quali strumenti di gestione esterni potrebbero essere interessati da questa modifica?

Quando si apportano alcune modifiche in System Manager, ad esempio la commutazione dell'interfaccia di gestione o l'utilizzo di SAML per un metodo di autenticazione, l'utilizzo di alcuni strumenti e funzionalità esterni potrebbe essere limitato.

Interfaccia di gestione

Gli strumenti che comunicano direttamente con l'interfaccia di gestione legacy (Symbol), come il provider SMI-S SANtricity o OnCommand Insight (OCI), non funzionano se non è attivata l'impostazione dell'interfaccia di gestione legacy. Inoltre, non è possibile utilizzare i comandi CLI legacy o eseguire operazioni di mirroring se questa impostazione è disattivata.

Per ulteriori informazioni, contatta il supporto tecnico.

Autenticazione SAML

Quando SAML è attivato, i seguenti client non possono accedere ai servizi e alle risorse dell'array di storage:

- Finestra Enterprise Management (EMW)
- Interfaccia a riga di comando (CLI)
- Client Software Developer Kit (SDK)
- Client in-band
- Client REST API per l'autenticazione di base HTTP
- Effettuare l'accesso utilizzando l'endpoint REST API standard

Per ulteriori informazioni, contatta il supporto tecnico.

Cosa occorre sapere prima di configurare e abilitare SAML?

Prima di configurare e attivare le funzionalità SAML (Security Assertion Markup Language) per l'autenticazione, assicurarsi di soddisfare i seguenti requisiti e comprendere le restrizioni SAML.

Requisiti

Prima di iniziare, assicurarsi che:

- Nella rete è configurato un provider di identità (IdP). Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è autenticato correttamente. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP.
- Un amministratore IdP ha configurato gli attributi e i gruppi utente nel sistema IdP.
- Un amministratore IdP ha garantito che IdP supporti la capacità di restituire un ID nome all'autenticazione.
- Un amministratore ha garantito che i clock del server IdP e del controller siano sincronizzati (tramite un server NTP o regolando le impostazioni del clock del controller).
- Un file di metadati IdP viene scaricato dal sistema IdP e disponibile sul sistema locale utilizzato per accedere a System Manager.
- Si conosce l'indirizzo IP o il nome di dominio di ciascun controller dell'array di storage.

Restrizioni

Oltre ai requisiti sopra indicati, assicurati di comprendere le seguenti restrizioni:

- Una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza. Si consiglia di testare gli accessi SSO prima di attivare SAML nella fase finale di configurazione. (Il sistema esegue anche un test di accesso SSO prima di attivare SAML).
- Se si disattiva SAML in futuro, il sistema ripristina automaticamente la configurazione precedente (ruoli utente locali e/o servizi di directory).
- Se i servizi di directory sono attualmente configurati per l'autenticazione dell'utente, SAML sovrascrive tale configurazione.
- Quando SAML è configurato, i seguenti client non possono accedere alle risorse degli array di storage:
  - Finestra Enterprise Management (EMW)
  - Interfaccia a riga di comando (CLI)
  - Client Software Developer Kit (SDK)

- Client in-band
- Client REST API per l'autenticazione di base HTTP
- Effettuare l'accesso utilizzando l'endpoint REST API standard

Quali tipi di eventi vengono registrati nel registro di controllo?

Il registro di controllo può registrare gli eventi di modifica o gli eventi di modifica e di sola lettura.

A seconda delle impostazioni del criterio, vengono visualizzati i seguenti tipi di eventi:

- **Eventi di modifica** — azioni dell'utente da System Manager che comportano modifiche al sistema, come il provisioning dello storage.
- **Eventi di modifica e sola lettura** — azioni dell'utente che comportano modifiche al sistema, nonché eventi che comportano la visualizzazione o il download di informazioni, come la visualizzazione delle assegnazioni dei volumi.

Cosa occorre sapere prima di configurare un server syslog?

È possibile archiviare i registri di controllo su un server syslog esterno.

Prima di configurare un server syslog, tenere presenti le seguenti linee guida.

- Assicurarsi di conoscere l'indirizzo del server, il protocollo e il numero della porta. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se il server utilizza un protocollo sicuro (ad esempio TLS), è necessario che nel sistema locale sia disponibile un certificato dell'autorità di certificazione (CA). I certificati CA identificano i proprietari dei siti Web per connessioni sicure tra server e client.
- Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti.
- Le impostazioni dei criteri di sovrascrittura (disponibili in **View/Edit Settings**) non influiscono sulla gestione dei registri con una configurazione del server syslog.
- I registri di controllo seguono il formato di messaggistica RFC 5424.

Il server syslog non riceve più registri di controllo. Cosa devo fare?

Se è stato configurato un server syslog con un protocollo TLS, il server non può ricevere messaggi se il certificato non è valido per qualsiasi motivo. Nel registro di controllo viene visualizzato un messaggio di errore relativo al certificato non valido.

Per risolvere questo problema, è necessario innanzitutto correggere il certificato per il server syslog. Una volta stabilita una catena di certificati valida, accedere al **Impostazioni › Registro di controllo › Configura server Syslog › Test tutti**.

Certificati

Concetti

Come funzionano i certificati

I certificati sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet.

I certificati garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, privatamente e inalterate, solo tra il server e il client specificati. Con System Manager è possibile gestire i certificati tra il browser di un sistema di gestione host (che funge da client) e i controller di un sistema storage (che funge da server).

Un certificato può essere firmato da un'autorità attendibile o autofirmato. "Firmare" significa semplicemente che qualcuno ha convalidato l'identità del proprietario e determinato che i loro dispositivi possono essere affidabili. Gli array di storage vengono forniti con un certificato autofirmato generato automaticamente su ciascun controller. È possibile continuare a utilizzare i certificati autofirmati oppure ottenere certificati firmati dalla CA per una connessione più sicura tra i controller e i sistemi host.

> Sebbene i certificati firmati dalla CA forniscano una migliore protezione di sicurezza (ad esempio, prevenendo gli attacchi man-in-the-middle), richiedono anche tariffe che possono essere costose se si dispone di una rete di grandi dimensioni. Al contrario, i certificati autofirmati sono meno sicuri, ma sono gratuiti. Pertanto, i certificati autofirmati vengono utilizzati più spesso per ambienti di test interni, non in ambienti di produzione.

Certificati firmati

Un certificato firmato viene convalidato da un'autorità di certificazione (CA), un'organizzazione di terze parti fidata. I certificati firmati includono i dettagli sul proprietario dell'entità (in genere, un server o un sito Web), la data di emissione e scadenza del certificato, i domini validi per l'entità e una firma digitale composta da lettere e numeri.

Quando si apre un browser e si inserisce un indirizzo Web, il sistema esegue un processo di verifica dei certificati in background per determinare se si sta effettuando la connessione a un sito Web che include un certificato valido firmato dalla CA. In genere, un sito protetto con un certificato firmato include un'icona a forma di lucchetto e una designazione https nell'indirizzo. Se si tenta di connettersi a un sito Web che non contiene un certificato firmato dalla CA, il browser visualizza un avviso che indica che il sito non è sicuro.

La CA esegue le operazioni necessarie per verificare l'identità dell'utente durante il processo dell'applicazione. Potrebbero inviare un'e-mail all'azienda registrata, verificare l'indirizzo aziendale ed eseguire una verifica HTTP o DNS. Una volta completato il processo applicativo, la CA invia i file digitali da caricare su un sistema di gestione host. In genere, questi file includono una catena di attendibilità, come segue:

- Root — nella parte superiore della gerarchia si trova il certificato root, che contiene una chiave privata utilizzata per firmare altri certificati. La directory principale identifica un'organizzazione CA specifica. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.
- Intermedio — i certificati intermedi si diramano dalla radice. La CA emette uno o più certificati intermedi per fungere da intermediario tra certificati di server e root protetti.
- Server — nella parte inferiore della catena si trova il certificato del server, che identifica l'entità specifica dell'utente, ad esempio un sito Web o un altro dispositivo. Ogni controller di uno storage array richiede un certificato server separato.

Certificati autofirmati

Ogni controller dell'array di storage include un certificato preinstallato e autofirmato. Un certificato autofirmato è simile a un certificato firmato dalla CA, ad eccezione del fatto che è convalidato dal proprietario dell'entità anziché da una terza parte. Come un certificato firmato dalla CA, un certificato autofirmato contiene una propria chiave privata e garantisce inoltre che i dati siano crittografati e inviati tramite una connessione HTTPS tra un server e un client. Tuttavia, un certificato autofirmato non utilizza la stessa catena di attendibilità di un certificato firmato dalla CA.

I certificati autofirmati non sono "trusted" dai browser. Ogni volta che si tenta di connettersi a un sito Web che contiene solo un certificato autofirmato, il browser visualizza un messaggio di avviso. È necessario fare clic su un collegamento nel messaggio di avviso che consente di accedere al sito Web; in questo modo, si accetta essenzialmente il certificato autofirmato.

Certificati utilizzati per il server di gestione delle chiavi

Se si utilizza un server di gestione delle chiavi esterno con la funzione Drive Security, è anche possibile gestire i certificati per l'autenticazione tra il server e i controller.

Terminologia del certificato

I seguenti termini si applicano alla gestione dei certificati.

Termine	Descrizione
CIRCA	Un'autorità di certificazione (CA) è un'entità attendibile che emette documenti elettronici, denominati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti Web, consentendo connessioni sicure tra client e server.
CSR	Una richiesta di firma del certificato (CSR) è un messaggio inviato da un richiedente a un'autorità di certificazione (CA). La CSR convalida le informazioni richieste dalla CA per il rilascio di un certificato.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli autori degli attacchi di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e l'identità dell'entità attendibile che certifica (firma) queste informazioni.
Catena di certificati	Gerarchia di file che aggiunge un livello di protezione ai certificati. In genere, la catena include un certificato root nella parte superiore della gerarchia, uno o più certificati intermedi e i certificati server che identificano le entità.
Certificato del client	Per la gestione delle chiavi di sicurezza, un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa fidarsi dei propri indirizzi IP.
Certificato intermedio	Uno o più certificati intermedi si diramano dalla directory principale nella catena di certificati. La CA emette uno o più certificati intermedi per fungere da intermediario tra certificati di server e root protetti.

Termine	Descrizione
Certificato del server di gestione delle chiavi	Per la gestione delle chiavi di sicurezza, un certificato del server di gestione delle chiavi convalida il server, in modo che lo storage array possa fidarsi del proprio indirizzo IP.
Archivio chiavi	Un keystore è un repository sul sistema di gestione host che contiene chiavi private, insieme alle chiavi pubbliche e ai certificati corrispondenti. Queste chiavi e certificati identificano le proprie entità, ad esempio i controller.
Server OCSP	Il server OCSP (Online Certificate Status Protocol) determina se l'autorità di certificazione (CA) ha revocato i certificati prima della data di scadenza pianificata, quindi impedisce all'utente di accedere a un server se il certificato viene revocato.
Certificato root	Il certificato root si trova nella parte superiore della gerarchia nella catena del certificato e contiene una chiave privata utilizzata per firmare altri certificati. La directory principale identifica un'organizzazione CA specifica. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.
Certificato firmato	Certificato convalidato da un'autorità di certificazione (CA). Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Inoltre, un certificato firmato include i dettagli relativi al proprietario dell'entità (in genere, un server o un sito Web) e una firma digitale composta da lettere e numeri. Un certificato firmato utilizza una catena di trust e quindi viene utilizzato più spesso negli ambienti di produzione. Definito anche "certificato firmato da CA" o "certificato di gestione".
Certificato autofirmato	Un certificato autofirmato viene validato dal proprietario dell'entità. Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Include anche una firma digitale composta da lettere e numeri. Un certificato autofirmato non utilizza la stessa catena di attendibilità di un certificato firmato dalla CA e, di conseguenza, viene spesso utilizzato negli ambienti di test. Detto anche certificato "preinstallato".
Certificato del server	Il certificato del server si trova nella parte inferiore della catena di certificati. Identifica l'entità specifica dell'utente, ad esempio un sito Web o un altro dispositivo. Ogni controller di un sistema storage richiede un certificato server separato.

Come fare

USA certificati firmati CA per i controller

È possibile ottenere certificati con firma CA per comunicazioni sicure tra i controller e il browser utilizzato per l'accesso a System Manager.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

A proposito di questa attività

L'utilizzo dei certificati firmati dalla CA è una procedura in tre fasi.

Fase 1: Completare e inviare una CSR per i controller

È necessario innanzitutto generare un file CSR (Certificate Signing Request) per ciascun controller nell'array di storage, quindi inviare i file a un'autorità di certificazione (CA).

Prima di iniziare

- È necessario conoscere l'indirizzo IP o il nome DNS di ciascun controller.

A proposito di questa attività

La CSR fornisce informazioni sull'organizzazione, l'indirizzo IP o il nome DNS del controller e una coppia di chiavi che identifica il server Web nel controller. Durante questa attività, viene generato un file CSR se nell'array di storage è presente un solo controller e due file CSR se sono presenti due controller.

> Non generare una nuova CSR dopo l'invio alla CA. Quando si genera una CSR, il sistema crea una coppia di chiavi private e pubbliche. La chiave pubblica fa parte della CSR, mentre la chiave privata viene conservata nell'archivio chiavi. Quando si ricevono i certificati firmati e li si importano nel keystore, il sistema garantisce che sia le chiavi private che quelle pubbliche siano la coppia originale. Pertanto, non è necessario generare una nuova CSR dopo averla inoltrata alla CA. In tal caso, i controller generano nuove chiavi e i certificati ricevuti dalla CA non funzioneranno.

Fasi

1. Selezionare **Impostazioni › certificati**.
2. Dalla scheda **Array Management** (Gestione array), selezionare **complete CSR** (completa CSR).

   > Se viene visualizzata una finestra di dialogo che richiede di accettare un certificato autofirmato per il secondo controller, fare clic su **Accetta certificato autofirmato** per continuare.

3. Inserire le seguenti informazioni, quindi fare clic su **Avanti**:
   - **Organizzazione** — il nome completo e legale della tua azienda o organizzazione. Includere i suffissi, ad esempio Inc. O Corp.
   - **Unità organizzativa (opzionale)** — la divisione dell'organizzazione che gestisce il certificato.
   - **Città/Località** — la città in cui si trova il tuo storage array o il tuo business.
   - **Stato/Regione (opzionale)** — Stato o regione in cui si trova lo storage array o l'azienda.
   - **Codice ISO del Paese** — Codice ISO (International Organization for Standardization) a due cifre del Paese, ad esempio USA.

   > Alcuni campi potrebbero essere precompilati con le informazioni appropriate, ad esempio l'indirizzo IP del controller. Non modificare i valori prepopolati a meno che non si sia certi che siano errati. Ad esempio, se non è stata ancora completata una CSR, l'indirizzo IP del controller viene impostato su "localhost". In questo caso, è necessario modificare "localhost" con il nome DNS o l'indirizzo IP del controller.

4. Verificare o inserire le seguenti informazioni sul controller A nell'array di storage:
   - **Controller A common name** — per impostazione predefinita viene visualizzato l'indirizzo IP o il nome DNS del controller A. Assicurarsi che l'indirizzo sia corretto; deve corrispondere esattamente a quello

immesso per accedere a System Manager nel browser.

- **Controller A alternate IP addresses** — se il nome comune è un indirizzo IP, è possibile inserire eventuali indirizzi IP o alias aggiuntivi per il controller A. Per più voci, utilizzare un formato delimitato da virgole.
- **Controller A alternate DNS Names** — se il nome comune è un nome DNS, inserire eventuali nomi DNS aggiuntivi per il controller A. Per più voci, utilizzare un formato delimitato da virgole. Se non sono presenti nomi DNS alternativi, ma è stato immesso un nome DNS nel primo campo, copiarlo qui. Se lo storage array dispone di un solo controller, il pulsante **Finish** è disponibile. Se lo storage array ha due controller, il pulsante **Next** (Avanti) è disponibile.

> Non fare clic sul collegamento **Ignora questo passaggio** quando si crea una richiesta CSR. Questo collegamento viene fornito in situazioni di ripristino degli errori. In rari casi, una richiesta CSR potrebbe non riuscire su un controller, ma non sull'altro. Questo collegamento consente di saltare la fase per la creazione di una richiesta CSR sul controller A, se già definita, e passare alla fase successiva per la creazione di una richiesta CSR sul controller B.

5. Se è presente un solo controller, fare clic su **fine**. Se sono presenti due controller, fare clic su **Avanti** per immettere le informazioni relative al controller B (come sopra), quindi fare clic su **fine**.

   Per un singolo controller, un file CSR viene scaricato nel sistema locale. Per i controller doppi, vengono scaricati due file CSR. La posizione della cartella del download dipende dal browser in uso.

6. Individuare i file CSR scaricati. La posizione della cartella dipende dal browser.
7. Inviare i file CSR a una CA e richiedere i certificati firmati in formato PEM.
8. Attendere che la CA restituisca i certificati, quindi passare a. Fase 2: Importazione dei certificati firmati per i controller.

Fase 2: Importazione dei certificati firmati per i controller

Una volta ricevuti i certificati firmati, vengono importati i file per i controller.

Prima di iniziare

- La CA ha restituito file di certificato firmati.
- I file sono disponibili sul sistema locale.
- Se la CA ha fornito un certificato concatenato (ad esempio, un file .p7b), è necessario decomprimere il file concatenato in singoli file: Il certificato root, uno o più certificati intermedi e i certificati server che identificano i controller. È possibile utilizzare Windows `certmgr` Utility per disimballare i file (fare clic con il pulsante destro del mouse e selezionare **tutte le attività › Esporta**). Una volta completate le esportazioni, viene visualizzato un file CER per ciascun file di certificato nella catena.

A proposito di questa attività

Questa attività descrive come caricare i file dei certificati.

Fasi

1. Selezionare **Impostazioni › certificati**.
2. Dalla scheda **Array Management** (Gestione array), selezionare **Import** (Importa).

   Viene visualizzata una finestra di dialogo per l'importazione dei file di certificato.

3. Fare clic sui pulsanti **Browse** per selezionare prima i file root e intermedi, quindi selezionare ciascun

certificato server per i controller. I file root e intermedi sono gli stessi per entrambi i controller. Solo i certificati server sono univoci per ciascun controller.

I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

   I file vengono caricati e validati.

Risultati

La sessione viene terminata automaticamente. È necessario effettuare nuovamente l'accesso affinché i certificati abbiano effetto. Quando si effettua nuovamente l'accesso, per la sessione viene utilizzato il nuovo certificato firmato dalla CA.

Reimpostare i certificati di gestione

È possibile ripristinare i certificati sui controller dall'utilizzo dei certificati firmati dalla CA ai certificati autofirmati impostati in fabbrica.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- I certificati con FIRMA CA devono essere importati in precedenza.

A proposito di questa attività

La funzione Reset elimina i file di certificato firmati dalla CA corrente da ciascun controller. I controller torneranno quindi a utilizzare certificati autofirmati.

Fasi

1. Selezionare **Impostazioni › certificati**.
2. Dalla scheda **Array Management** (Gestione array), selezionare **Reset** (Ripristina).

   Viene visualizzata la finestra di dialogo Conferma **Ripristina certificati di gestione**.

3. Tipo `reset` Nel campo, quindi fare clic su **Reset**.

   Dopo l'aggiornamento del browser, il browser potrebbe bloccare l'accesso al sito di destinazione e segnalare che il sito utilizza HTTP Strict Transport Security. Questa condizione si verifica quando si torna ai certificati autofirmati. Per eliminare la condizione che sta bloccando l'accesso alla destinazione, è necessario cancellare i dati di navigazione dal browser.

Risultati

I controller tornano a utilizzare certificati autofirmati. Di conseguenza, il sistema richiede agli utenti di accettare manualmente il certificato autofirmato per le sessioni.

Visualizzare le informazioni sul certificato importato

Dalla pagina certificati, è possibile visualizzare il tipo di certificato, l'autorità di emissione e l'intervallo di date valido dei certificati per l'array di storage.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Selezionare una delle schede per visualizzare le informazioni relative ai certificati.

Scheda	Descrizione
Gestione degli array	Visualizzare le informazioni sui certificati firmati dalla CA importati per ciascun controller, inclusi il file root, i file intermedi e i file server.
Affidabile	Visualizza le informazioni su tutti gli altri tipi di certificati importati per i controller. Utilizzare il campo del filtro sotto **Mostra certificati…** per visualizzare i certificati installati dall'utente o preinstallati. • **Installato dall'utente**. Certificati caricati da un utente nell'array di storage, che possono includere certificati attendibili quando il controller agisce come client (anziché come server), certificati LDAPS e certificati Identity Federation. • **Preinstallato**. Certificati autofirmati inclusi con lo storage array.
Gestione delle chiavi	Consente di visualizzare informazioni sui certificati firmati dalla CA importati per un server di gestione delle chiavi esterno.

Importare i certificati per i controller quando agiscono come client

Se il controller rifiuta una connessione perché non è in grado di convalidare la catena di trust per un server di rete, è possibile importare un certificato dalla scheda Trusted che consente al controller (che agisce come client) di accettare le comunicazioni da quel server.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- I file dei certificati vengono installati nel sistema locale.

A proposito di questa attività

Se si desidera consentire a un altro server di contattare i controller (ad esempio, un server LDAP o un server syslog che utilizza TLS), potrebbe essere necessario importare i certificati dalla scheda Trusted.

Fasi

1. Selezionare **Impostazioni › certificati**.
2. Dalla scheda **Trusted**, selezionare **Import** (Importa).

   Viene visualizzata una finestra di dialogo per l'importazione dei file di certificato attendibili.

3. Fare clic su **Browse** (Sfoglia) per selezionare i file di certificato per i controller.

I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

Risultati

I file vengono caricati e validati.

Attiva il controllo della revoca del certificato

È possibile attivare i controlli automatici dei certificati revocati, in modo che un server OCSP (Online Certificate Status Protocol) blocchi gli utenti da connessioni non sicure.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- Su entrambi i controller viene configurato un server DNS, che consente di utilizzare un nome di dominio completo per il server OCSP. Questa attività è disponibile nella pagina hardware.
- Se si desidera specificare il proprio server OCSP, è necessario conoscere l'URL di tale server.

A proposito di questa attività

Il controllo automatico della revoca è utile nei casi in cui la CA ha emesso un certificato in modo errato o una chiave privata è compromessa.

Durante questa attività, è possibile configurare un server OCSP o utilizzare il server specificato nel file del certificato. Il server OCSP determina se la CA ha revocato i certificati prima della data di scadenza pianificata, quindi impedisce all'utente di accedere a un sito se il certificato viene revocato.

Fasi

1. Selezionare **Impostazioni › certificati**.
2. Selezionare la scheda **Trusted**.

   È inoltre possibile attivare il controllo delle revoche dalla scheda **Gestione chiavi**.

3. Fare clic su **attività non comuni**, quindi selezionare **attiva verifica revoca** dal menu a discesa.
4. Selezionare **i want to enable revocation checking**, in modo che nella casella di controllo venga visualizzato un segno di spunta e che nella finestra di dialogo vengano visualizzati altri campi.
5. Nel campo **OCSP responder address** (Indirizzo responder OCSP), è possibile inserire un URL per un server responder OCSP. Se non si immette un indirizzo, il sistema utilizza l'URL del server OCSP dal file del certificato.
6. Fare clic su **Test Address** per verificare che il sistema possa stabilire una connessione all'URL specificato.
7. Fare clic su **Save** (Salva).

Risultati

Se lo storage array tenta di connettersi a un server con un certificato revocato, la connessione viene negata e viene registrato un evento.

Eliminare i certificati attendibili

È possibile eliminare i certificati installati dall'utente precedentemente importati dalla

scheda Trusted.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- Se si sta aggiornando un certificato attendibile con una nuova versione, il certificato aggiornato deve essere importato prima di eliminare il vecchio certificato.

> Prima di importare un certificato sostitutivo, si potrebbe perdere l'accesso a un sistema se si elimina un certificato utilizzato per autenticare i controller e un altro server, ad esempio un server LDAP.

A proposito di questa attività

Questa attività descrive come eliminare i certificati installati dall'utente. I certificati autofirmati preinstallati non possono essere cancellati.

Fasi

1. Selezionare **Impostazioni › certificati**.
2. Selezionare la scheda **Trusted**.

   La tabella mostra i certificati attendibili dell'array di storage.

3. Nella tabella, selezionare il certificato che si desidera rimuovere.
4. Fare clic su **operazioni non comuni › Elimina**

   Viene visualizzata la finestra di dialogo Conferma eliminazione certificato attendibile.

5. Tipo `delete` Nel campo, quindi fare clic su **Delete** (Elimina).

Utilizzare i certificati firmati CA per l'autenticazione con un server di gestione delle chiavi

Per comunicazioni sicure tra un server di gestione delle chiavi e i controller degli array di storage, è necessario configurare i set di certificati appropriati.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

A proposito di questa attività

L'autenticazione tra i controller e un server di gestione delle chiavi è una procedura in due fasi.

Fase 1: Completare e inviare la CSR per l'autenticazione con un server di gestione delle chiavi

È necessario innanzitutto generare un file CSR (Certificate Signing Request), quindi utilizzare la CSR per richiedere un certificato client firmato a un'autorità di certificazione (CA) attendibile dal server di gestione delle chiavi. È inoltre possibile creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

A proposito di questa attività

Questa attività descrive come generare il file CSR, che verrà utilizzato per richiedere un certificato client firmato a una CA attendibile dal server di gestione delle chiavi. 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). Durante questa attività, è necessario fornire informazioni sull'organizzazione.

Fasi

1. Selezionare **Impostazioni › certificati**.
2. Dalla scheda **Key Management** (Gestione chiavi), selezionare **complete CSR** (completa CSR).
3. Inserire le seguenti informazioni:
   - **Nome comune** — un nome che identifica questa CSR, ad esempio il nome dell'array di storage, che verrà visualizzato nei file di certificato.
   - **Organizzazione** — il nome completo e legale della tua azienda o organizzazione. Includere i suffissi, ad esempio Inc. O Corp.
   - **Unità organizzativa (opzionale)** — la divisione dell'organizzazione che gestisce il certificato.
   - **Città/Località** — la città o la località in cui si trova l'organizzazione.
   - **Stato/Regione (opzionale)** — Stato o regione in cui si trova l'organizzazione.
   - **Codice ISO Paese** — Codice ISO (International Organization for Standardization) a due cifre, ad esempio USA, in cui si trova l'organizzazione.
4. Fare clic su **Download**.

   Un file CSR viene salvato nel sistema locale.

5. Richiedere un certificato client firmato a una CA attendibile dal server di gestione delle chiavi.
6. Se si dispone di un certificato client, visitare il sito Web all'indirizzo Fase 2: Importazione dei certificati per il server di gestione delle chiavi.

Fase 2: Importazione dei certificati per il server di gestione delle chiavi

Come fase successiva, importare i certificati per l'autenticazione tra lo storage array e il server di gestione delle chiavi. Esistono due tipi di certificati: Il certificato client convalida i controller dello storage array, mentre il certificato del server di gestione delle chiavi convalida il server.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- Si dispone di un file di certificato client firmato (vedere Fase 1: Completare e inviare la CSR per l'autenticazione con un server di gestione delle chiavi) Ed è stato copiato sull'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 il file di certificato del server 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.

> Per ulteriori informazioni sul certificato del server, consultare la documentazione relativa al server di gestione delle chiavi.

A proposito di questa attività

Questa attività descrive come caricare i file di certificato per l'autenticazione tra i controller degli array di storage e il server di gestione delle chiavi. È necessario caricare sia il file di certificato del client per i controller che il file di certificato del server per il server di gestione delle chiavi.

Fasi

1. Selezionare **Impostazioni › certificati**.
2. Dalla scheda **Key Management** (Gestione chiavi), selezionare **Import** (Importa).

   Viene visualizzata una finestra di dialogo per l'importazione dei file dei certificati.

3. Accanto a **Select client certificate** (Seleziona certificato client), fare clic sul pulsante **Browse** (Sfoglia) per selezionare il file di certificato client per i controller dell'array di storage.

   Il nome del file viene visualizzato nella finestra di dialogo.

4. Accanto a **Select key management server's server certificate**, fare clic sul pulsante **Browse** (Sfoglia) per selezionare il file di certificato del server per il server di gestione delle chiavi.

   Il nome del file viene visualizzato nella finestra di dialogo.

5. Fare clic su **Importa**.

   I file vengono caricati e validati.

Esportare i certificati del server di gestione delle chiavi

È possibile salvare un certificato per un server di gestione delle chiavi nel computer locale.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- I certificati devono essere importati in precedenza.

Fasi

1. Selezionare **Impostazioni › certificati**.
2. Selezionare la scheda **Key Management** (Gestione chiavi).
3. Dalla tabella, selezionare il certificato che si desidera esportare, quindi fare clic su **Esporta**.

   Viene visualizzata la finestra di dialogo Save (Salva).

4. Inserire un nome file e fare clic su **Save** (Salva).

FAQ

Perché viene visualizzata la finestra di dialogo Impossibile accedere ad altri controller?

Quando si eseguono determinate operazioni relative ai certificati CA (ad esempio, l'importazione di un certificato), potrebbe essere visualizzata una finestra di dialogo che

richiede di accettare un certificato autofirmato per il secondo controller.

Negli array di storage con due controller (configurazioni duplex), questa finestra di dialogo viene talvolta visualizzata se Gestione sistema SANtricity non riesce a comunicare con il secondo controller o se il browser non può accettare il certificato durante un determinato momento di un'operazione.

Se viene visualizzata questa finestra di dialogo, fare clic su **Accetta certificato autofirmato** per continuare. Se viene richiesta una password da un'altra finestra di dialogo, immettere la password dell'amministratore utilizzata per accedere a System Manager.

Se questa finestra di dialogo viene visualizzata di nuovo e non è possibile completare un'attività di certificazione, provare una delle seguenti procedure:

- Utilizzare un tipo di browser diverso per accedere a questo controller, accettare il certificato e continuare.
- Accedere al secondo controller con System Manager, accettare il certificato autofirmato, quindi tornare al primo controller e continuare.

Come è possibile sapere quali certificati devono essere caricati in System Manager per la gestione esterna delle chiavi?

Per la gestione esterna delle chiavi, vengono importati due tipi di certificati per l'autenticazione tra lo storage array e il server di gestione delle chiavi in modo che le due entità possano fidarsi l'una dell'altra.

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). Per ottenere un certificato client, utilizzare System Manager per completare una CSR per lo storage array. È quindi possibile caricare la CSR su un server di gestione delle chiavi e generare un certificato client da tale server. Una volta ottenuto un certificato client, copiare il file 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. Recuperare il file di certificato del server dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager.

Cosa devo sapere sulla verifica della revoca dei certificati?

System Manager consente di controllare i certificati revocati utilizzando un server OCSP (Online Certificate Status Protocol), invece di caricare gli elenchi di revoca dei certificati (CRL).

I certificati revocati non devono più essere attendibili. Un certificato potrebbe essere revocato per diversi motivi; ad esempio, se l'autorità di certificazione (CA) ha emesso il certificato in modo errato, una chiave privata è stata compromessa o l'entità identificata non è conforme ai requisiti dei criteri.

Dopo aver stabilito una connessione a un server OCSP in Gestione sistema, lo storage array esegue il controllo delle revoche ogni volta che si connette a un server AutoSupport, a un server EKMS (External Key Management Server), a un server LDAPS (Lightweight Directory Access Protocol over SSL) o a un server Syslog. Lo storage array tenta di validare i certificati di questi server per assicurarsi che non siano stati revocati. Il server restituisce quindi il valore "buono", "revocato" o "sconosciuto" per il certificato. Se il certificato viene revocato o l'array non riesce a contattare il server OCSP, la connessione viene rifiutata.

Se si specifica un indirizzo del responder OCSP in System Manager o nell'interfaccia della riga di comando (CLI), l'indirizzo OCSP trovato nel file del certificato viene sovrascritta.

Per quali tipi di server verrà attivato il controllo delle revoche?

Lo storage array esegue il controllo delle revoche ogni volta che si connette a un server AutoSupport, a un server EKMS (External Key Management Server), a un server LDAPS (Lightweight Directory Access Protocol over SSL) o a un server Syslog.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.