Unified Manager

SANtricity 11.8

NetApp
December 16, 2024

Sommario

Gestione di array multipli con Unified Manager 6

Interfaccia principale

Panoramica dell'interfaccia di Unified Manager

Unified Manager è un'interfaccia basata su web che consente di gestire più array di storage in una singola vista.

Pagina principale

Quando si accede a Unified Manager, la pagina principale si apre su **Gestisci - tutto**. Da questa pagina è possibile scorrere un elenco degli array di storage rilevati nella rete, visualizzarne lo stato ed eseguire operazioni su un singolo array o su un gruppo di array.

Barra laterale di navigazione

È possibile accedere alle funzioni e alle funzioni di Unified Manager dalla barra laterale di navigazione.

Area	Descrizione
Gestire	Scopri gli array di storage nella tua rete, avvia Gestore di sistema SANtricity per un array, importa le impostazioni da un array a più array e gestisci i gruppi di array. Selezionare le caselle di controllo accanto ai nomi degli array per eseguire operazioni su di essi, ad esempio l'importazione delle impostazioni e la creazione di gruppi di array. I puntini di sospensione alla fine di ogni riga forniscono un menu in linea per le operazioni su un singolo array, ad esempio la ridenominazione.
Operazioni	Visualizzare l'avanzamento delle operazioni batch, ad esempio l'importazione delle impostazioni da un array all'altro. Alcune operazioni non sono disponibili quando uno storage array ha uno stato non ottimale.
Gestione dei certificati	Gestire i certificati per l'autenticazione tra browser e client.
Gestione degli accessi	Stabilire l'autenticazione dell'utente per l'interfaccia di Unified Manager.
Supporto	Visualizza le opzioni di supporto tecnico, le risorse e i contatti.

Impostazioni dell'interfaccia e guida

Nella parte superiore destra dell'interfaccia, è possibile accedere alla Guida e ad altra documentazione. È inoltre possibile accedere alle opzioni di amministrazione, disponibili dal menu a discesa accanto al proprio nome di accesso.

Login e password degli utenti

L'utente corrente che ha effettuato l'accesso al sistema viene visualizzato nella parte superiore destra dell'interfaccia.

Per ulteriori informazioni su utenti e password, consulta:

- "Impostare la protezione della password amministratore"
- "Modificare la password admin"
- "Modificare le password per i profili utente locali"

Browser supportati

È possibile accedere a Unified Manager da diversi tipi di browser.

Sono supportati i seguenti browser e versioni.

Browser	Versione minima
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

Il proxy dei servizi Web deve essere installato e disponibile nel browser.

Impostare la protezione della password amministratore

È necessario configurare Unified Manager con una password di amministratore per proteggerla da accessi non autorizzati.

Password amministratore e profili utente

Quando si avvia Unified Manager per la prima volta, viene richiesto di impostare una password di amministratore. Qualsiasi utente che dispone della password di amministratore può apportare modifiche alla configurazione degli array di storage.

Oltre alla password di amministratore, l'interfaccia di Unified Manager include profili utente preconfigurati con uno o più ruoli mappati. Per ulteriori informazioni, vedere "Come funziona Access Management".

Gli utenti e le mappature non possono essere modificati. È possibile modificare solo le password. Per modificare le password, vedere:

- "Modificare la password admin"
- "Modificare le password per i profili utente locali"

Timeout della sessione

Il software richiede la password una sola volta durante una singola sessione di gestione. Per impostazione predefinita, una sessione scade dopo 30 minuti di inattività. A questo punto, è necessario immettere nuovamente la password. Se un altro utente accede al software da un altro client di gestione e modifica la password mentre la sessione è in corso, viene richiesta una password la volta successiva che si tenta di eseguire un'operazione di configurazione o un'operazione di visualizzazione.

Per motivi di sicurezza, è possibile tentare di inserire una password solo cinque volte prima che il software entri in uno stato di "blocco". In questo stato, il software rifiuta i successivi tentativi di immissione della password. Attendere 10 minuti per ripristinare lo stato "normale" prima di inserire nuovamente la password.

È possibile regolare i timeout della sessione o disattivarli del tutto. Per ulteriori informazioni, vedere "Gestire i timeout delle sessioni".

Modificare la password admin

È possibile modificare la password admin utilizzata per accedere a Unified Manager.

Prima di iniziare

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

A proposito di questa attività

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

- 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.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare l'utente **admin** 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 di controllo per richiedere all'utente di immettere una password per accedere al sistema.
6. Immettere la nuova password nei due campi.
7. Immettere la password dell'amministratore locale per confermare l'operazione, quindi fare clic su **Change** (Modifica).

Gestire i timeout delle sessioni

È possibile configurare i timeout per Unified Manager, 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 di Unified 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. Dalla barra dei menu, selezionare la freccia a discesa accanto al nome di accesso utente.
2. Selezionare **Enable/Disable session timeout** (attiva/Disattiva timeout sessione).

   Viene visualizzata la finestra di dialogo attiva/Disattiva timeout sessione.
3. Utilizzare i comandi per aumentare o diminuire il tempo in minuti.

   Il timeout minimo che è possibile impostare è di 15 minuti.

   > Per disattivare i timeout della sessione, deselezionare la casella di controllo **Imposta la durata…**.
4. Fare clic su **Save** (Salva).

Storage array

Panoramica del rilevamento

Per gestire le risorse di storage, è necessario prima rilevare gli array di storage nella rete.

Come si rilevano gli array?

Utilizzare la pagina Add/Discover per trovare e aggiungere gli array di storage che si desidera gestire nella rete aziendale. È possibile rilevare più array o un singolo array. A tale scopo, immettere gli indirizzi IP di rete, quindi Unified Manager tenta di stabilire singole connessioni a ciascun indirizzo IP dell'intervallo.

Scopri di più:

- "Considerazioni per il rilevamento degli array"
- "Scopri più array di storage"
- "Scopri un singolo array"

Come si gestiscono gli array?

Dopo aver individuato gli array, accedere alla pagina **Gestisci - tutto**. Da questa pagina è possibile scorrere

un elenco degli array di storage rilevati nella rete, visualizzarne lo stato ed eseguire operazioni su un singolo array o su un gruppo di array.

Se si desidera gestire un singolo array, selezionarlo e aprire System Manager.

Scopri di più:

- "Considerazioni sull'accesso a System Manager"
- "Gestire un singolo array di storage"
- "Visualizzare lo stato degli array di storage"

Concetti

Considerazioni per il rilevamento degli array

Prima di poter visualizzare e gestire le risorse di storage, Unified Manager deve rilevare gli array di storage che si desidera gestire nella rete aziendale. È possibile rilevare più array o un singolo array.

Rilevamento di più array di storage

Se si sceglie di rilevare più array, immettere un intervallo di indirizzi IP di rete e Unified Manager tenta di stabilire connessioni individuali a ciascun indirizzo IP dell'intervallo. Qualsiasi array di storage raggiunto correttamente viene visualizzato nella pagina Discover e può essere aggiunto al dominio di gestione.

Rilevamento di un singolo storage array

Se si sceglie di rilevare un singolo array, inserire il singolo indirizzo IP per uno dei controller nell'array di storage e quindi aggiungere il singolo array di storage.

> Unified Manager rileva e visualizza solo il singolo indirizzo IP o indirizzo IP all'interno di un intervallo assegnato a un controller. Se a questi controller sono assegnati controller alternativi o indirizzi IP che non rientrano in questo singolo indirizzo IP o intervallo di indirizzi IP, Unified Manager non li rileverà né li visualizzerà. Tuttavia, una volta aggiunto lo storage array, tutti gli indirizzi IP associati vengono rilevati e visualizzati nella vista Manage (Gestione).

Credenziali dell'utente

Nell'ambito del processo di rilevamento, è necessario fornire la password di amministratore per ciascun array di storage che si desidera aggiungere.

Certificati di servizi Web

Nell'ambito del processo di rilevamento, Unified Manager verifica che gli array di storage rilevati utilizzino certificati da un'origine attendibile. Unified Manager utilizza due tipi di autenticazione basata su certificati per tutte le connessioni stabilite con il browser:

- **Certificati attendibili**

  Per gli array rilevati da Unified Manager, potrebbe essere necessario installare certificati attendibili aggiuntivi forniti dall'autorità di certificazione.

  Utilizzare il pulsante **Importa** per importare questi certificati. Se si è connessi a questo array in

precedenza, uno o entrambi i certificati controller sono scaduti, revocati o mancano un certificato root o un certificato intermedio nella relativa catena di certificati. È necessario sostituire il certificato scaduto o revocato o aggiungere il certificato root o intermedio mancante prima di gestire lo storage array.

- **Certificati autofirmati**

  È possibile utilizzare anche certificati autofirmati. Se l'amministratore tenta di rilevare gli array senza importare certificati firmati, Unified Manager visualizza una finestra di dialogo di errore che consente all'amministratore di accettare il certificato autofirmato. Il certificato autofirmato dell'array di storage viene contrassegnato come attendibile e l'array di storage viene aggiunto a Unified Manager.

  Se le connessioni all'array di storage non sono attendibili, selezionare **Annulla** e convalidare la strategia di certificato di sicurezza dell'array di storage prima di aggiungere l'array di storage a Unified Manager.

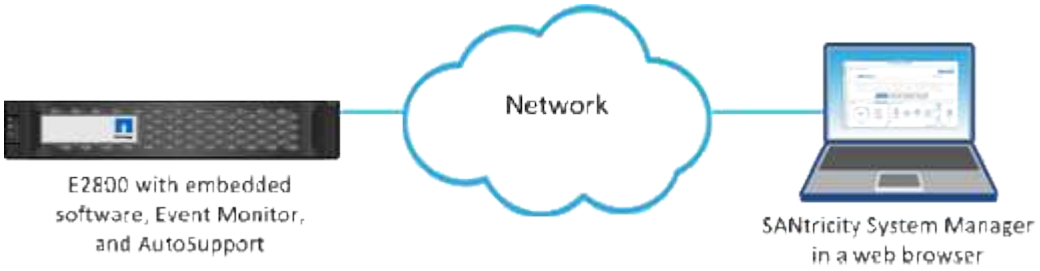
Considerazioni sull'accesso a System Manager

È possibile selezionare uno o più array di storage e utilizzare l'opzione Launch per aprire System Manager quando si desidera configurare e gestire gli array di storage.

System Manager è un'applicazione integrata nei controller, collegata alla rete tramite una porta di gestione Ethernet. Include tutte le funzioni basate su array.

Per accedere a System Manager, è necessario disporre di:

- Uno dei modelli di array elencati di seguito: "Panoramica dell'hardware e-Series"
- Connessione out-of-band a un client di gestione della rete con un browser Web.



Scopri gli array

Scopri più array di storage

Vengono rilevati più array per rilevare tutti gli array di storage nella subnet in cui risiede il server di gestione e aggiungere automaticamente gli array rilevati al dominio di gestione.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore della sicurezza.
- Lo storage array deve essere configurato e configurato correttamente.
- Le password degli array di storage devono essere impostate utilizzando il riquadro Access Management di System Manager.
- Per risolvere i certificati non attendibili, è necessario disporre di file di certificati attendibili provenienti da un'autorità di certificazione (CA) e che i file di certificati siano disponibili nel sistema locale.

Il rilevamento degli array è una procedura multi-step.

Fase 1: Inserire l'indirizzo di rete

Immettere un intervallo di indirizzi di rete per la ricerca nella sottorete locale. Qualsiasi array di storage raggiunto correttamente viene visualizzato nella pagina Discover e potrebbe essere aggiunto al dominio di gestione.

Per interrompere l'operazione di rilevamento per qualsiasi motivo, fare clic su **Stop Discovery** (Interrompi rilevamento).

Fasi

1. Dalla pagina Gestisci, selezionare **Aggiungi/rileva**.

   Viene visualizzata la finestra di dialogo Add/Discover (Aggiungi/rileva).

2. Selezionare il pulsante di opzione **Scopri tutti gli array di storage all'interno di un intervallo di rete**.
3. Inserire l'indirizzo di rete iniziale e quello finale per la ricerca nella sottorete locale, quindi fare clic su **Avvia rilevamento**.

   Viene avviato il processo di rilevamento. Il completamento di questo processo di rilevamento può richiedere alcuni minuti. La tabella nella pagina Discover viene popolata durante il rilevamento degli array di storage.

   > Se non vengono rilevati array gestibili, verificare che gli array di storage siano collegati correttamente alla rete e che gli indirizzi assegnati rientrino nell'intervallo. Fare clic su **New Discovery Parameters** (nuovi parametri di rilevamento) per tornare alla pagina Add/Discover (Aggiungi/rileva).

4. Esaminare l'elenco degli array di storage rilevati.
5. Selezionare la casella di controllo accanto a un array di storage che si desidera aggiungere al dominio di gestione, quindi fare clic su **Avanti**.

   Unified Manager esegue un controllo delle credenziali su ciascun array che si sta aggiungendo al dominio di gestione. Potrebbe essere necessario risolvere eventuali certificati autofirmati e non attendibili associati a tale array.

6. Fare clic su **Avanti** per passare alla fase successiva della procedura guidata.

Fase 2: Risoluzione dei certificati autofirmati durante il rilevamento

Nell'ambito del processo di rilevamento, il sistema verifica che gli array di storage stiano utilizzando certificati da un'origine attendibile.

Fasi

1. Effettuare una delle seguenti operazioni:
   - Se le connessioni agli array di storage rilevati sono attendibili, passare alla scheda successiva della procedura guidata. I certificati autofirmati verranno contrassegnati come attendibili e gli array di storage verranno aggiunti a Unified Manager.
   - Se le connessioni agli array di storage non sono attendibili, selezionare **Annulla** e convalidare la strategia di certificato di sicurezza di ciascun array di storage prima di aggiungerne una a Unified Manager.

2. Fare clic su **Avanti** per passare alla fase successiva della procedura guidata.

Fase 3: Risoluzione dei certificati non attendibili durante il rilevamento

I certificati non attendibili si verificano quando uno storage array tenta di stabilire una connessione sicura a Unified Manager, ma la connessione non viene confermata come sicura. Durante il processo di rilevamento dell'array, è possibile risolvere i certificati non attendibili importando un certificato CA (Certificate Authority) (o certificato firmato da CA) emesso da una terza parte attendibile.

Potrebbe essere necessario installare altri certificati CA attendibili se si verifica una delle seguenti condizioni:

- Di recente è stato aggiunto uno storage array.
- Uno o entrambi i certificati sono scaduti.
- Uno o entrambi i certificati vengono revocati.
- Uno o entrambi i certificati non dispongono di un certificato root o intermedio.

Fasi

1. Selezionare la casella di controllo accanto a qualsiasi array di storage per cui si desidera risolvere i certificati non attendibili, quindi selezionare il pulsante **Importa**.

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

2. Fare clic su **Browse** (Sfoglia) per selezionare i file di certificato per gli array di storage.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

3. Fare clic su **Importa**.

   I file vengono caricati e validati.

   Qualsiasi array di storage con problemi di certificato non attendibili che non sono stati risolti non verrà aggiunto a Unified Manager.

4. Fare clic su **Avanti** per passare alla fase successiva della procedura guidata.

Fase 4: Fornire le password

È necessario immettere le password per gli array di storage che si desidera aggiungere al dominio di gestione.

Fasi

1. Inserire la password per ciascun array di storage che si desidera aggiungere a Unified Manager.
2. **Opzionale:** Associa gli array di storage a un gruppo: Dall'elenco a discesa, seleziona il gruppo desiderato da associare agli array di storage selezionati.
3. Fare clic su **fine**.

Al termine

Gli array di storage vengono aggiunti al dominio di gestione e associati al gruppo selezionato (se specificato).

La connessione di Unified Manager agli array di storage specificati può richiedere alcuni minuti.

Scopri un singolo array

Utilizzare l'opzione Add/Discover Single Storage Array (Aggiungi/rileva singolo array di storage) per rilevare e aggiungere manualmente un singolo array di storage alla rete aziendale.

Prima di iniziare

- Lo storage array deve essere configurato e configurato correttamente.
- Le password degli array di storage devono essere impostate utilizzando il riquadro Access Management di System Manager.

Fasi

1. Dalla pagina Gestisci, selezionare **Aggiungi/rileva**.

   Viene visualizzata la finestra di dialogo Add/Discover (Aggiungi/rileva).

2. Selezionare il pulsante di opzione **Discover a single storage array** (rileva un singolo array di storage).
3. Inserire l'indirizzo IP di uno dei controller nell'array di storage, quindi fare clic su **Avvia rilevamento**.

   La connessione di Unified Manager all'array di storage specificato può richiedere alcuni minuti.

   > Il messaggio Storage Array Not Accessible (Storage Array non accessibile) viene visualizzato quando la connessione all'indirizzo IP del controller specificato non riesce.

4. Se richiesto, risolvere eventuali certificati autofirmati.

   Nell'ambito del processo di rilevamento, il sistema verifica che gli array di storage rilevati stiano utilizzando certificati da un'origine attendibile. Se non riesce a individuare un certificato digitale per un array di storage, richiede di risolvere il certificato non firmato da un'autorità di certificazione (CA) riconosciuta aggiungendo un'eccezione di protezione.

5. Se richiesto, risolvere eventuali certificati non attendibili.

   I certificati non attendibili si verificano quando uno storage array tenta di stabilire una connessione sicura a Unified Manager, ma la connessione non viene confermata come sicura. Risolvi i certificati non attendibili importando un certificato dell'autorità di certificazione (CA) emesso da una terza parte attendibile.

6. Fare clic su **Avanti**.
7. **Opzionale:** associare lo storage array rilevato a un gruppo: Dall'elenco a discesa, selezionare il gruppo desiderato da associare allo storage array.

   Il gruppo "tutti" è selezionato per impostazione predefinita.

8. Inserire la password dell'amministratore per lo storage array che si desidera aggiungere al dominio di gestione, quindi fare clic su **OK**.

Al termine

L'array di storage viene aggiunto a Unified Manager e, se specificato, viene aggiunto anche al gruppo selezionato.

Se è attivata la raccolta automatica dei dati di supporto, i dati di supporto vengono raccolti automaticamente per un array di storage aggiunto.

Gestire gli array

Visualizzare lo stato degli array di storage

Unified Manager visualizza lo stato di ciascun array di storage rilevato.

Accedere alla pagina **Gestisci - tutto**. Da questa pagina è possibile visualizzare lo stato della connessione tra il proxy dei servizi Web e l'array di storage.

Gli indicatori di stato sono descritti nella seguente tabella.

Stato	Indica
Ottimale	Lo storage array si trova in uno stato ottimale. Non ci sono problemi di certificato e la password è valida.
Password non valida	È stata fornita una password dello storage array non valida.
Certificato non attendibile	Una o più connessioni con lo storage array non sono attendibili perché il certificato HTTPS è autofirmato e non è stato importato oppure il certificato è firmato dalla CA e i certificati CA principali e intermedi non sono stati importati.
Richiede attenzione	Si è verificato un problema con lo storage array che richiede l'intervento dell'utente per correggerlo.
Blocco	Lo storage array si trova in uno stato bloccato.
Sconosciuto	Lo storage array non è mai stato contattato. Questo può accadere quando il proxy dei servizi Web si avvia e non ha ancora contattato lo storage array oppure lo storage array non è in linea e non è mai stato contattato dall'avvio del proxy dei servizi Web.
Offline	Il proxy dei servizi Web aveva precedentemente contattato lo storage array, ma ora ha perso tutte le connessioni.

Gestire un singolo array di storage

È possibile utilizzare l'opzione Launch per aprire System Manager basato su browser per uno o più array di storage quando si desidera eseguire operazioni di gestione.

Fasi

1. Dalla pagina Manage (Gestione), selezionare uno o più array di storage che si desidera gestire.
2. Fare clic su **Avvia**.

   Il sistema apre una nuova finestra e visualizza la pagina di accesso di System Manager.

3. Immettere il nome utente e la password, quindi fare clic su **Log in** (Accedi).

Modificare le password degli array di storage

È possibile aggiornare le password utilizzate per visualizzare e accedere agli array di storage in Unified Manager.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore dello storage.
- È necessario conoscere la password corrente per lo storage array, impostata in System Manager.

A proposito di questa attività

In questa attività, immettere la password corrente per uno storage array in modo da potervi accedere in Unified Manager. Questo potrebbe essere necessario se la password dell'array è stata modificata in System Manager e ora deve essere modificata anche in Unified Manager.

Fasi

1. Dalla pagina Manage (Gestione), selezionare uno o più array di storage.
2. Selezionare **operazioni non comuni › fornire password array di storage**.
3. Immettere la password o le password per ciascun array di storage, quindi fare clic su **Save** (Salva).

Rimuovere gli array di storage da Gestione unificata di SANtricity

È possibile rimuovere uno o più array di storage se non si desidera più gestirli da Unified Manager.

A proposito di questa attività

Non è possibile accedere a nessuno degli array di storage rimossi. Tuttavia, è possibile stabilire una connessione a uno degli array di storage rimossi puntando direttamente un browser all'indirizzo IP o al nome host.

La rimozione di uno storage array non influisce in alcun modo sullo storage array o sui relativi dati. Se uno storage array viene rimosso accidentalmente, può essere aggiunto di nuovo.

Fasi

1. Selezionare la pagina **Gestisci**.
2. Selezionare uno o più array di storage che si desidera rimuovere.
3. Selezionare **Uncommon Tasks › Remove storage array**.

   Lo storage array viene rimosso da tutte le viste in Gestione unificata di SANtricity.

Importazione delle impostazioni

Panoramica dell'importazione delle impostazioni

La funzione Import Settings (Impostazioni importazione) consente di eseguire un'operazione batch per importare le impostazioni da un array a più array. Questa funzione consente di risparmiare tempo quando è necessario configurare più array nella rete.

Quali impostazioni è possibile importare?

È possibile importare metodi di avviso, configurazioni AutoSupport, configurazioni dei servizi directory, configurazioni dello storage (come gruppi di volumi e pool) e impostazioni di sistema (come il bilanciamento automatico del carico).

Scopri di più:

- "Come funziona Import Settings (Impostazioni di importazione)"
- "Requisiti per la replica delle configurazioni di storage"

Come si esegue un'importazione in batch?

Su uno storage array da utilizzare come origine, aprire System Manager e configurare le impostazioni desiderate. Quindi, da Unified Manager, accedere alla pagina Manage (Gestione) e importare le impostazioni in uno o più array.

Scopri di più:

- "Importare le impostazioni degli avvisi"
- "Importa impostazioni AutoSupport"
- "Importare le impostazioni dei servizi di directory"
- "Importare le impostazioni di configurazione dello storage"
- "Importare le impostazioni di sistema"

Concetti

Come funziona Import Settings (Impostazioni di importazione)

È possibile utilizzare Unified Manager per importare le impostazioni da un array di storage a più array di storage. La funzione Import Settings (Impostazioni di importazione) è un'operazione batch che consente di risparmiare tempo quando è necessario configurare più array nella rete.

Impostazioni disponibili per l'importazione

È possibile importare le seguenti configurazioni in più array:

- **Alerts** — metodi di avviso per inviare eventi importanti agli amministratori, utilizzando la posta elettronica, un server syslog o un server SNMP.
- **AutoSupport** — funzionalità che monitora lo stato di salute di uno storage array e invia automaticamente i dispatches al supporto tecnico.
- **Servizi di directory** — metodo di autenticazione dell'utente gestito tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft.
- **Configurazione dello storage** — configurazioni relative a:
  - Volumi (solo volumi thick e non repository)
  - Gruppi di volumi e pool
  - Assegnazioni dei dischi hot spare

- **Impostazioni di sistema** — configurazioni relative a:
  - Impostazioni di scansione dei supporti per un volume
  - Impostazioni SSD
  - Bilanciamento automatico del carico (non include il reporting sulla connettività host)

Workflow di configurazione

Per importare le impostazioni, seguire questo flusso di lavoro:

1. Su uno storage array da utilizzare come origine, configurare le impostazioni utilizzando System Manager.
2. Sugli array di storage da utilizzare come destinazione, eseguire il backup della configurazione utilizzando System Manager.
3. Da Unified Manager, accedere alla pagina **Manage** e importare le impostazioni.
4. Dalla pagina **Operations**, esaminare i risultati dell'operazione Import Settings.

Requisiti per la replica delle configurazioni di storage

Prima di importare una configurazione dello storage da uno storage array a un altro, esaminare i requisiti e le linee guida.

Shelf

- Gli shelf in cui risiedono i controller devono essere identici sugli array di origine e di destinazione.
- Gli shelf ID devono essere identici sugli array di origine e di destinazione.
- Gli shelf di espansione devono essere inseriti negli stessi slot con gli stessi tipi di unità (se il disco viene utilizzato nella configurazione, la posizione dei dischi inutilizzati non è importante).

Controller

- Il tipo di controller può essere diverso tra gli array di origine e di destinazione (ad esempio, l'importazione da E2800 a E5700), ma il tipo di enclosure RBOD deve essere identico.
- L'HICS, incluse le funzionalità da dell'host, deve essere identico tra gli array di origine e di destinazione.
- L'importazione da una configurazione duplex a una facciata singola non è supportata; tuttavia, è consentita l'importazione da una facciata singola a una facciata fronte/retro.
- Le impostazioni FDE non sono incluse nel processo di importazione.

Stato

- Gli array di destinazione devono essere nello stato ottimale.
- Non è necessario che l'array di origine sia nello stato ottimale.

Storage

- La capacità del disco può variare tra gli array di origine e di destinazione, a condizione che la capacità del volume sulla destinazione sia superiore a quella dell'origine. (Un array di destinazione potrebbe disporre di unità più recenti e di capacità maggiore che non sarebbero completamente configurate nei volumi dall'operazione di replica).
- Volumi di pool di dischi di almeno 64 TB sull'array di origine impediranno il processo di importazione sulle

destinazioni.

- I volumi thin non sono inclusi nel processo di importazione.

Utilizzare le importazioni in batch

Importare le impostazioni degli avvisi

È possibile importare configurazioni di avviso da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

- Gli avvisi sono configurati in System Manager per lo storage array che si desidera utilizzare come origine (**Impostazioni › Avvisi**).
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).

A proposito di questa attività

Per l'operazione di importazione, è possibile selezionare avvisi e-mail, SNMP o syslog. Le impostazioni importate includono:

- **Avvisi via email** — Indirizzo del server di posta e indirizzi email dei destinatari degli avvisi.
- **Syslog alerts** — un indirizzo del server syslog e una porta UDP.
- **SNMP alerts** — Nome di comunità e indirizzo IP per il server SNMP.

Fasi

1. Nella pagina Manage (Gestione), fare clic su **Import Settings** (Impostazioni importazione).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **Email alerts** (Avvisi email), **SNMP alerts** (Avvisi SNMP) o **Syslog alerts** (Avvisi Syslog), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se Unified Manager non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultati

Gli array di storage di destinazione sono ora configurati per inviare avvisi agli amministratori tramite e-mail, SNMP o syslog.

Importa impostazioni AutoSupport

È possibile importare una configurazione AutoSupport da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

- AutoSupport è configurato in Gestione sistema per lo storage array che si desidera utilizzare come origine (**supporto › Centro di supporto**).
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).

A proposito di questa attività

Le impostazioni importate includono le funzioni separate (AutoSupport di base, AutoSupport on Demand e Diagnostica remota), la finestra di manutenzione, il metodo di erogazione, e pianificazione delle spedizioni.

Fasi

1. Nella pagina Manage (Gestione), fare clic su **Import Settings** (Impostazioni importazione).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Seleziona impostazioni, selezionare **AutoSupport**, quindi fare clic su **Avanti**.

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se Unified Manager non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultati

Gli array di storage di destinazione sono ora configurati con le stesse impostazioni AutoSupport dell'array di origine.

Importare le impostazioni dei servizi di directory

È possibile importare una configurazione di servizi di directory da un array di storage ad altri array di storage. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

- I servizi di directory sono configurati in System Manager per lo storage array che si desidera utilizzare come origine (**Impostazioni › Gestione accessi**).
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).

A proposito di questa attività

Le impostazioni importate includono il nome di dominio e l'URL di un server LDAP (Lightweight Directory Access Protocol), oltre ai mapping dei gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.

Fasi

1. Nella pagina Manage (Gestione), fare clic su **Import Settings** (Impostazioni importazione).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **Directory Services** (servizi directory), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se Unified Manager non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultati

Gli array di storage di destinazione sono ora configurati con gli stessi servizi di directory dell'array di origine.

Importare le impostazioni di sistema

È possibile importare la configurazione di sistema da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

- Le impostazioni di sistema sono configurate in System Manager per lo storage array che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).

A proposito di questa attività

Le impostazioni importate includono le impostazioni di scansione dei supporti per un volume, le impostazioni SSD per i controller e il bilanciamento automatico del carico (non include il reporting della connettività host).

Fasi

1. Nella pagina Manage (Gestione), fare clic su **Import Settings** (Impostazioni importazione).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **System** (sistema), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se Unified Manager non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultati

Gli array di storage di destinazione sono ora configurati con le stesse impostazioni di sistema dell'array di origine.

Importare le impostazioni di configurazione dello storage

È possibile importare la configurazione dello storage da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

- Lo storage viene configurato in Gestore di sistema di SANtricity per l'array di storage che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).

- Gli array di origine e di destinazione devono soddisfare i seguenti requisiti:
  - Gli shelf in cui risiedono i controller devono essere identici.
  - Gli ID degli shelf devono essere identici.
  - Gli shelf di espansione devono essere inseriti negli stessi slot con gli stessi tipi di unità.
  - Il tipo di enclosure RBOD deve essere identico.
  - L'HICS, incluse le funzionalità di Data Assurance dell'host, deve essere identico.
  - Gli array di destinazione devono essere nello stato ottimale.
  - La capacità del volume sull'array di destinazione è maggiore della capacità dell'array di origine.
- Hai compreso le seguenti restrizioni:
  - L'importazione da una configurazione duplex a una facciata singola non è supportata; tuttavia, è consentita l'importazione da una facciata singola a una facciata fronte/retro.
  - Volumi di pool di dischi di almeno 64 TB sull'array di origine impediranno il processo di importazione sulle destinazioni.
  - I volumi thin non sono inclusi nel processo di importazione.

A proposito di questa attività

Le impostazioni importate includono volumi configurati (solo volumi thick e non di repository), gruppi di volumi, pool e assegnazioni di dischi hot spare.

Fasi

1. Nella pagina Manage (Gestione), fare clic su **Import Settings** (Impostazioni importazione).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **Storage Configuration** (Configurazione archiviazione), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se Unified Manager non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultati

Gli array di storage di destinazione sono ora configurati con la stessa configurazione dello storage dell'array di origine.

FAQ

Quali impostazioni verranno importate?

La funzione Import Settings (Impostazioni di importazione) è un'operazione batch che carica le configurazioni da un array di storage a più array di storage. Le impostazioni importate durante questa operazione dipendono dalla configurazione dell'array di storage di origine in System Manager.

È possibile importare le seguenti impostazioni in più array di storage:

- **Avvisi via email** — le impostazioni includono un indirizzo del server di posta e gli indirizzi email dei destinatari degli avvisi.
- **Syslog alerts** — le impostazioni includono un indirizzo del server syslog e una porta UDP.
- **SNMP alerts** — le impostazioni includono un nome di comunità e un indirizzo IP per il server SNMP.
- **AutoSupport** — le impostazioni includono le funzioni separate (AutoSupport di base, AutoSupport on Demand e Diagnostica remota), la finestra di manutenzione, il metodo di erogazione, e pianificazione delle spedizioni.
- **Directory Services** — la configurazione include il nome di dominio e l'URL di un server LDAP (Lightweight Directory Access Protocol), oltre ai mapping dei gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.
- **Configurazione dello storage** — le configurazioni includono volumi (solo volumi thick e non repository), gruppi di volumi, pool e assegnazioni di dischi hot spare.
- **Impostazioni di sistema** — le configurazioni includono le impostazioni di scansione dei supporti per un volume, la cache SSD per i controller e il bilanciamento automatico del carico (non include il reporting della connettività host).

Perché non vengono visualizzati tutti gli array di storage?

Durante l'operazione Import Settings (Impostazioni di importazione), alcuni storage array potrebbero non essere disponibili nella finestra di dialogo di selezione della destinazione.

Gli array di storage potrebbero non essere visualizzati per i seguenti motivi:

- La versione del firmware è inferiore alla 8.50.
- Lo storage array non è in linea.
- Il sistema non è in grado di comunicare con tale array (ad esempio, l'array presenta problemi di certificato, password o rete).

Gruppi di array

Panoramica dei gruppi

Dalla pagina Manage Groups (Gestisci gruppi), è possibile creare un set di gruppi di array di storage per una gestione più semplice.

Cosa sono i gruppi di array?

È possibile gestire l'infrastruttura fisica e virtualizzata raggruppando un set di storage array. È possibile raggruppare gli array di storage per semplificare l'esecuzione dei processi di monitoraggio o reporting.

Esistono due tipi di gruppi:

- **Tutti i gruppi** — il gruppo tutti è il gruppo predefinito e include tutti gli array di storage rilevati nell'organizzazione. È possibile accedere al gruppo All dalla vista principale.
- **User-created group** — Un gruppo creato dall'utente include gli array di storage che si selezionano manualmente per aggiungere a quel gruppo. È possibile accedere ai gruppi creati dall'utente dalla vista principale.

Come si configurano i gruppi?

Dalla pagina Manage Groups (Gestisci gruppi), è possibile creare un gruppo e quindi aggiungere array a tale gruppo.

Scopri di più:

- "Configurare il gruppo di array di storage"

Configurare il gruppo di array di storage

È possibile creare gruppi di storage e quindi aggiungere array di storage ai gruppi.

La configurazione dei gruppi è una procedura in due fasi.

Fase 1: Creare un gruppo

Si crea prima un gruppo. Il gruppo di storage definisce quali dischi forniscono lo storage che costituisce il volume.

Fasi

1. Dalla pagina Manage (Gestisci), selezionare **Manage Groups (Gestisci gruppi) › Create storage array group** (Crea gruppo array di storage).
2. Nel campo **Nome**, digitare un nome per il nuovo gruppo.
3. Selezionare gli array di storage che si desidera aggiungere al nuovo gruppo.
4. Fare clic su **Create** (Crea).

Fase 2: Aggiungere un array di storage al gruppo

È possibile aggiungere uno o più array di storage a un gruppo creato dall'utente.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare il gruppo a cui si desidera aggiungere gli array di storage.
2. Selezionare **Manage Groups › Add storage array to group** (Gestisci gruppi[Aggiungi array di storage al gruppo]).
3. Selezionare gli array di storage che si desidera aggiungere al gruppo.

4. Fare clic su **Aggiungi.**

Rimuovere gli array di storage dal gruppo

È possibile rimuovere uno o più array di storage gestiti da un gruppo se non si desidera più gestirli da un gruppo di storage specifico.

A proposito di questa attività

La rimozione degli array di storage da un gruppo non influisce in alcun modo sull'array di storage o sui relativi dati. Se lo storage array è gestito da System Manager, è comunque possibile gestirlo utilizzando il browser. Se uno storage array viene accidentalmente rimosso da un gruppo, può essere aggiunto di nuovo.

Fasi

1. Dalla pagina Manage (Gestisci), selezionare il **Manage Groups (Gestisci gruppi) › Remove storage array from group** (Rimuovi array di storage dal gruppo).
2. Dal menu a discesa, selezionare il gruppo che contiene gli array di storage che si desidera rimuovere, quindi fare clic sulla casella di controllo accanto a ciascun array di storage che si desidera rimuovere dal gruppo.
3. Fare clic su **Rimuovi**.

Eliminare il gruppo di array di storage

È possibile rimuovere uno o più gruppi di array di storage non più necessari.

A proposito di questa attività

Questa operazione elimina solo il gruppo di array di storage. Gli array di storage associati al gruppo cancellato rimangono accessibili tramite la vista Manage All (Gestisci tutti) o qualsiasi altro gruppo a cui è associato.

Fasi

1. Dalla pagina Manage (Gestisci), selezionare **Manage Groups (Gestisci gruppi) › Delete storage array group** (Elimina gruppo array di storage).
2. Selezionare uno o più gruppi di array di storage che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).

Rinominare il gruppo di array di storage

È possibile modificare il nome di un gruppo di array di storage quando il nome corrente non è più significativo o applicabile.

A proposito di questa attività

Tenere presenti queste linee guida.

- Un nome può essere composto da lettere, numeri e caratteri speciali come sottolineatura (_), trattino (-) e cancelletto (n.). Se si sceglie un altro carattere, viene visualizzato un messaggio di errore. Viene richiesto di scegliere un altro nome.
- Limitare il nome a 30 caratteri. Gli spazi iniziali e finali del nome vengono cancellati.
- Utilizzare un nome univoco e significativo, facile da comprendere e ricordare.
- Evitare nomi o nomi arbitrari che perderebbero rapidamente il loro significato in futuro.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare il gruppo di array di storage che si desidera rinominare.
2. Selezionare **Manage Groups › Rename storage array group** (Gestisci gruppi[Rinomina gruppo array di storage])
3. Nel campo **Nome gruppo**, digitare un nuovo nome per il gruppo.
4. Fare clic su **Rinomina.**

Aggiornamenti

Panoramica di Upgrade Center

Dal Centro aggiornamenti, è possibile gestire il software SANtricity OS e gli aggiornamenti DI NVSRAM per più array di storage.

Come funzionano gli aggiornamenti?

È possibile scaricare il software del sistema operativo più recente e aggiornare uno o più array.

Workflow di upgrade

I seguenti passaggi forniscono un workflow di alto livello per l'esecuzione degli aggiornamenti software.

1. È possibile scaricare il file del software SANtricity OS più recente dal sito del supporto (un collegamento è disponibile da Unified Manager nella pagina del supporto). Salvare il file sul sistema host di gestione (l'host in cui si accede a Unified Manager in un browser), quindi decomprimere il file.
2. In Unified Manager, caricare il file del software del sistema operativo SANtricity e IL file NVSRAM nel repository (un'area del server proxy dei servizi Web in cui sono memorizzati i file). È possibile aggiungere file dal **Centro aggiornamenti › Aggiorna software SANtricity OS o dal Centro aggiornamenti › Gestisci repository software**.
3. Una volta caricati i file nel repository, è possibile selezionare il file da utilizzare nell'aggiornamento. Dalla pagina Aggiorna software SANtricity OS (**Centro aggiornamenti › Aggiorna software SANtricity OS**), selezionare il file del software SANtricity OS e IL file NVSRAM. Dopo aver selezionato un file software, in questa pagina viene visualizzato un elenco di array di storage compatibili. Selezionare quindi gli array di storage che si desidera aggiornare con il nuovo software. (Non è possibile selezionare array incompatibili).
4. È quindi possibile avviare un trasferimento e un'attivazione software immediati oppure scegliere di preparare i file per l'attivazione in un secondo momento. Durante il processo di aggiornamento, Unified Manager esegue le seguenti attività:
   a. Esegue un controllo dello stato degli array di storage per determinare se esistono condizioni che potrebbero impedire il completamento dell'aggiornamento. Se un array non supera il controllo dello stato di salute, è possibile saltare tale array e continuare l'aggiornamento per gli altri oppure interrompere l'intero processo e risolvere i problemi degli array che non hanno superato il test.
   b. Trasferisce i file di aggiornamento a ciascun controller.
   c. Riavvia i controller e attiva il nuovo software SANtricity OS, un controller alla volta. Durante l'attivazione, il file SANtricity OS esistente viene sostituito con il nuovo file.

   È inoltre possibile specificare che il software venga attivato in un secondo momento.

Upgrade immediato o a fasi

È possibile attivare l'aggiornamento immediatamente o eseguirlo in un secondo momento. È possibile scegliere di eseguire l'attivazione in un secondo momento per i seguenti motivi:

- **Ora del giorno** — l'attivazione del software può richiedere molto tempo, quindi potrebbe essere necessario attendere che i carichi di i/o siano più leggeri. A seconda del carico di i/o e delle dimensioni della cache, il completamento di un aggiornamento del controller può richiedere da 15 a 25 minuti. I controller si riavviano e si eseguono il failover durante l'attivazione, pertanto le prestazioni potrebbero essere inferiori al solito fino al completamento dell'aggiornamento.
- **Tipo di pacchetto** — si consiglia di testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri array di storage.

Per attivare il software in fasi, andare al **supporto › Centro di aggiornamento** e fare clic su **attiva** nell'area denominata aggiornamento del software del controller del sistema operativo SANtricity.

Controllo dello stato di salute

Un controllo dello stato di salute viene eseguito come parte del processo di aggiornamento, ma è anche possibile eseguire un controllo dello stato di salute separatamente prima di iniziare (andare al **Upgrade Center › Pre-Upgrade Health Check**).

Il controllo dello stato di salute valuta tutti i componenti del sistema di storage per assicurarsi che l'aggiornamento possa continuare. Le seguenti condizioni potrebbero impedire l'aggiornamento:

- Dischi assegnati non riusciti
- Hot spare in uso
- Gruppi di volumi incompleti
- Operazioni esclusive in esecuzione
- Volumi mancanti
- Controller in stato non ottimale
- Numero eccessivo di eventi del registro eventi
- Errore di convalida del database di configurazione
- Dischi con versioni precedenti di DACstore

Cosa devo sapere prima di eseguire l'aggiornamento?

Prima di eseguire l'upgrade di più array di storage, esaminare le considerazioni chiave come parte della pianificazione.

Versioni correnti

È possibile visualizzare le versioni correnti del software SANtricity OS dalla pagina Gestione di Unified Manager per ogni array di storage rilevato. La versione viene visualizzata nella colonna Software SANtricity OS. Il firmware del controller e LE informazioni SU NVSRAM sono disponibili in una finestra di dialogo a comparsa quando si fa clic sulla versione del sistema operativo SANtricity in ciascuna riga.

Altri componenti che richiedono l'aggiornamento

Nell'ambito del processo di aggiornamento, potrebbe essere necessario aggiornare il driver multipath/failover dell'host o il driver HBA in modo che l'host possa interagire correttamente con i controller.

Per informazioni sulla compatibilità, fare riferimento alla "Matrice di interoperabilità NetApp" . Inoltre, consultare le procedure riportate nelle Express Guide del sistema operativo in uso. Le Express Guide sono disponibili sul sito Web "Documentazione e-Series e SANtricity" .

Controller doppi

Se uno storage array contiene due controller e si dispone di un driver multipath installato, lo storage array può continuare a elaborare l'i/o durante l'aggiornamento. Durante l'aggiornamento, si verifica la seguente procedura:

1. Il controller A esegue il failover di tutti i LUN verso il controller B.
2. L'aggiornamento avviene sul controller A.
3. Il controller A riprende i LUN e tutti i LUN del controller B.
4. L'aggiornamento avviene sul controller B.

Al termine dell'aggiornamento, potrebbe essere necessario ridistribuire manualmente i volumi tra i controller per garantire che i volumi tornino al controller proprietario corretto.

Aggiornare software e firmware

Eseguire un controllo dello stato di salute prima dell'aggiornamento

Un controllo dello stato di salute viene eseguito come parte del processo di aggiornamento, ma è anche possibile eseguire un controllo dello stato di salute separatamente prima di iniziare. Il controllo dello stato di salute valuta i componenti dello storage array per assicurarsi che l'aggiornamento possa continuare.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare **Centro di aggiornamento › controllo stato pre-aggiornamento**.

   Viene visualizzata la finestra di dialogo Pre-Upgrade Health Check (verifica dello stato di salute pre-aggiornamento) che elenca tutti i sistemi storage rilevati.

2. Se necessario, filtrare o ordinare i sistemi storage nell'elenco, in modo da poter visualizzare tutti i sistemi che non sono attualmente nello stato ottimale.
3. Selezionare le caselle di controllo relative ai sistemi storage che si desidera eseguire attraverso il controllo dello stato di salute.
4. Fare clic su **Start**.

   L'avanzamento viene visualizzato nella finestra di dialogo durante l'esecuzione del controllo dello stato di salute.

5. Una volta completato il controllo dello stato di salute, fare clic sui puntini di sospensione (…) a destra di ciascuna riga per visualizzare ulteriori informazioni ed eseguire altre attività.

   Se un array non supera il controllo dello stato di salute, è possibile saltare tale array e continuare l'aggiornamento per gli altri oppure interrompere l'intero processo e risolvere i problemi degli array che non hanno superato il test.

Aggiornare il sistema operativo SANtricity

Aggiorna uno o più storage array con il software più recente e NVSRAM per assicurarti di disporre di tutte le funzionalità più recenti e delle correzioni dei bug. Controller NVSRAM è un file controller che specifica le impostazioni predefinite per i controller.

Prima di iniziare

- I file più recenti del sistema operativo SANtricity sono disponibili sul sistema host in cui sono in esecuzione il proxy dei servizi Web SANtricity e il gestore unificato.
- Si sa se si desidera attivare l'aggiornamento software ora o in una versione successiva.

  È possibile scegliere di eseguire l'attivazione in un secondo momento per i seguenti motivi:

  - **Ora del giorno** — l'attivazione del software può richiedere molto tempo, quindi potrebbe essere necessario attendere che i carichi di i/o siano più leggeri. Il failover dei controller durante l'attivazione potrebbe risultare inferiore al solito fino al completamento dell'aggiornamento.
  - **Tipo di pacchetto** — si consiglia di testare il nuovo software del sistema operativo su un array di storage prima di aggiornare i file su altri array di storage.

> Per eseguire l'aggiornamento alla versione 11.80.x o successiva, i sistemi devono disporre di SANtricity OS 11.70.5.

A proposito di questa attività

> Rischio di perdita di dati o di danneggiamento dello storage array: Non apportare modifiche allo storage array durante l'aggiornamento. Mantenere l'alimentazione dello storage array.

Fasi

1. Se l'array di storage contiene un solo controller o un driver multipath non è in uso, interrompere l'attività i/o dell'array di storage per evitare errori dell'applicazione. Se lo storage array dispone di due controller e si dispone di un driver multipath installato, non è necessario interrompere l'attività di i/O.
2. Dalla vista principale, selezionare **Gestisci**, quindi uno o più array di storage da aggiornare.
3. Selezionare **Centro di aggiornamento › Aggiorna software SANtricity OS**.

   Viene visualizzata la pagina aggiornamento del software SANtricity OS.

4. Scarica il pacchetto software SANtricity OS più recente dal sito di supporto NetApp sul computer locale.

   a. Fare clic su **Aggiungi nuovo file al repository software**.
   b. Fare clic sul collegamento per trovare gli ultimi download del sistema operativo SANtricity*.
   c. Fare clic sul collegamento **Download Latest Release** (Scarica ultima versione).
   d. Seguire le istruzioni rimanenti per scaricare il file del sistema operativo SANtricity e IL file NVSRAM sul computer locale.

   > Il firmware con firma digitale è richiesto nella versione 8.42 e successive. Se si tenta di scaricare il firmware senza firma, viene visualizzato un errore e il download viene interrotto.

5. Selezionare il file del software del sistema operativo e IL file NVSRAM che si desidera utilizzare per

aggiornare i controller:

a. Dall'elenco a discesa **selezionare un file del software SANtricity OS**, selezionare il file del sistema operativo scaricato sul computer locale.

   Se sono disponibili più file, i file vengono ordinati dalla data più recente alla data più vecchia.

   > Il repository software elenca tutti i file software associati al proxy dei servizi Web. Se il file che si desidera utilizzare non viene visualizzato, fare clic sul collegamento **Add new file to software repository** (Aggiungi nuovo file al repository software) per accedere alla posizione in cui si trova il file del sistema operativo che si desidera aggiungere.

a. Dal menu a discesa **Select an NVSRAM file** (Seleziona un file NVSRAM), selezionare il file del controller che si desidera utilizzare.

   Se sono presenti più file, i file vengono ordinati dalla data più recente alla data più vecchia.

6. Nella tabella Compatible Storage Array (matrice di storage compatibile), esaminare gli array di storage compatibili con il file software del sistema operativo selezionato, quindi selezionare gli array da aggiornare.
   - Gli array di storage selezionati nella vista Manage (Gestione) e compatibili con il file del firmware selezionato vengono selezionati per impostazione predefinita nella tabella Compatible Storage Array (array di storage compatibile).
   - Gli array di storage che non possono essere aggiornati con il file del firmware selezionato non sono selezionabili nella tabella degli array di storage compatibili, come indicato dallo stato **incompatibile**.
7. **Opzionale:** per trasferire il file software agli array di storage senza attivarli, selezionare la casella di controllo **trasferire il software del sistema operativo agli array di storage, contrassegnarlo come staged e attivarlo in un secondo momento**.
8. Fare clic su **Start**.
9. A seconda che si sia scelto di attivare ora o successivamente, eseguire una delle seguenti operazioni:
   - Digitare **TRANSFER** per confermare che si desidera trasferire le versioni software del sistema operativo proposte sugli array selezionati per l'aggiornamento, quindi fare clic su **Transfer**.

     Per attivare il software trasferito, selezionare **Upgrade Center › Activate Staged OS Software**.

   - Digitare **UPGRADE** per confermare che si desidera trasferire e attivare le versioni software del sistema operativo proposte sugli array selezionati per l'aggiornamento, quindi fare clic su **Upgrade**.

     Il sistema trasferisce il file software a ciascun array di storage selezionato per l'aggiornamento, quindi attiva il file avviando un riavvio.

     Durante l'operazione di aggiornamento si verificano le seguenti azioni:

   - Durante il processo di aggiornamento viene eseguito un controllo dello stato di salute prima dell'aggiornamento. Il controllo dello stato di salute prima dell'aggiornamento valuta tutti i componenti dell'array di storage per assicurarsi che l'aggiornamento possa continuare.
   - Se un controllo dello stato di salute non riesce per un array di storage, l'aggiornamento si interrompe. È possibile fare clic sui puntini di sospensione (…) E selezionare **Save Log** (Salva registro) per esaminare gli errori. È inoltre possibile scegliere di ignorare l'errore di controllo dello stato di salute e fare clic su **continua** per procedere con l'aggiornamento.
   - È possibile annullare l'operazione di aggiornamento dopo il controllo dello stato di salute prima dell'aggiornamento.

10. **Opzionale:** una volta completato l'aggiornamento, è possibile visualizzare un elenco degli aggiornamenti per uno specifico array di storage facendo clic sui puntini di sospensione (…) E quindi selezionando **Save Log** (Salva registro).

    Il file viene salvato nella cartella Download del browser con il nome `upgrade_log-<date>.json`.

Attivare il software del sistema operativo in fasi

È possibile scegliere di attivare il file software immediatamente o attendere fino a un momento più comodo. Questa procedura presuppone che l'utente abbia scelto di attivare il file software in un secondo momento.

A proposito di questa attività

È possibile trasferire i file del firmware senza attivarli. È possibile scegliere di eseguire l'attivazione in un secondo momento per i seguenti motivi:

- **Ora del giorno** — l'attivazione del software può richiedere molto tempo, quindi potrebbe essere necessario attendere che i carichi di i/o siano più leggeri. I controller si riavviano e si eseguono il failover durante l'attivazione, pertanto le prestazioni potrebbero essere inferiori al solito fino al completamento dell'aggiornamento.
- **Tipo di pacchetto** — si consiglia di testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri array di storage.

> Non è possibile interrompere il processo di attivazione dopo l'avvio.

Fasi

1. Dalla vista principale, selezionare **Gestisci**. Se necessario, fare clic sulla colonna Status (Stato) per ordinare, nella parte superiore della pagina, tutti gli array di storage con lo stato "OS Upgrade (waiting activation)" (aggiornamento del sistema operativo (in attesa di attivazione).
2. Selezionare uno o più array di storage per cui si desidera attivare il software, quindi selezionare **Upgrade Center › Activate Staged OS Software**.

    Durante l'operazione di aggiornamento si verificano le seguenti azioni:

    - Nell'ambito del processo di attivazione viene eseguito un controllo dello stato di salute prima dell'aggiornamento. Il controllo dello stato di salute prima dell'aggiornamento valuta tutti i componenti dell'array di storage per assicurarsi che l'attivazione possa continuare.
    - Se un controllo dello stato di salute non riesce per un array di storage, l'attivazione si interrompe. È possibile fare clic sui puntini di sospensione (…) E selezionare **Save Log** (Salva registro) per esaminare gli errori. È inoltre possibile scegliere di ignorare l'errore di controllo dello stato di salute e fare clic su **continua** per procedere con l'attivazione.
    - È possibile annullare l'operazione di attivazione dopo il controllo dello stato di salute pre-aggiornamento. Una volta completato correttamente il controllo dello stato di salute prima dell'aggiornamento, si verifica l'attivazione. Il tempo necessario per l'attivazione dipende dalla configurazione dello storage array e dai componenti che si stanno attivando.
3. **Opzionale:** una volta completata l'attivazione, è possibile visualizzare un elenco degli elementi attivati per uno specifico array di storage facendo clic sui puntini di sospensione (…) E quindi selezionando **Save Log** (Salva registro).

    Il file viene salvato nella cartella Download del browser con il nome `activate_log-<date>.json`.

Gestire il repository software

Il repository software elenca tutti i file software associati al proxy dei servizi Web.

Se il file che si desidera utilizzare non viene visualizzato, utilizzare l'opzione Gestisci repository software per importare uno o più file SANtricity OS nel sistema host in cui sono in esecuzione il proxy dei servizi Web e Unified Manager. Puoi anche scegliere di eliminare uno o più file SANtricity OS disponibili nel repository software.

Prima di iniziare

Se si stanno aggiungendo file SANtricity OS, assicurarsi che i file del sistema operativo siano disponibili sul sistema locale.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare **Centro di aggiornamento › Gestisci repository software**.

   Viene visualizzata la finestra di dialogo Manage Software Repository (Gestisci repository software).

2. Eseguire una delle seguenti operazioni:

Opzione	Eseguire questa operazione
Importa	a. Fare clic su **Importa.** b. Fare clic su **Browse** (Sfoglia), quindi individuare il percorso in cui si trovano i file del sistema operativo che si desidera aggiungere. I file del sistema operativo hanno un nome file simile a `N2800-830000-000.dlp`. c. Selezionare uno o più file del sistema operativo da aggiungere, quindi fare clic su **Importa**.
Eliminare	a. Selezionare uno o più file del sistema operativo che si desidera rimuovere dal repository software. b. Fare clic su **Delete** (Elimina).

Risultati

Se è stata selezionata l'opzione di importazione, i file vengono caricati e validati. Se si seleziona Delete (Elimina), i file vengono rimossi dal repository software.

Software per sistemi operativi chiari e staged

È possibile rimuovere il software del sistema operativo in fasi per assicurarsi che una versione in sospeso non venga attivata inavvertitamente in un secondo momento. La rimozione del software del sistema operativo in fasi non influisce sulla versione corrente in esecuzione sugli array di storage.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare **Upgrade Center › Cancella software**

sistema operativo in fasi.

Viene visualizzata la finestra di dialogo Clear Staged OS Software (Cancella software per sistemi operativi in fasi) che elenca tutti i sistemi storage rilevati con software o NVSRAM in sospeso.

2. Se necessario, filtrare o ordinare i sistemi di storage nell'elenco, in modo da poter visualizzare tutti i sistemi che dispongono di software in fasi.
3. Selezionare le caselle di controllo relative ai sistemi storage con software in sospeso che si desidera eliminare.
4. Fare clic su **Cancella**.

   Lo stato dell'operazione viene visualizzato nella finestra di dialogo.

Mirroring

Panoramica del mirroring

Utilizza le funzionalità di mirroring per replicare i dati tra uno storage array locale e uno storage array remoto, in modo asincrono o sincrono.

Il mirroring sincrono non è disponibile sul sistema storage EF600 o EF300.

Che cos'è il mirroring?

Le applicazioni SANtricity includono due tipi di mirroring: Asincrono e sincrono. Il mirroring asincrono copia i volumi di dati su richiesta o in base a una pianificazione, riducendo al minimo o evitando i downtime che potrebbero derivare da danneggiamento o perdita dei dati. Il mirroring sincrono replica i volumi di dati in tempo reale per garantire una disponibilità continua.

Scopri di più:

- "Come funziona il mirroring"
- "Terminologia mirrorata"

Come si configura il mirroring?

È possibile configurare il mirroring asincrono o sincrono in Unified Manager, quindi utilizzare System Manager per gestire le sincronizzazioni.

Scopri di più:

- "Flusso di lavoro di configurazione del mirroring"
- "Requisiti per l'utilizzo del mirroring"
- "Creare una coppia asincrona con mirroring"
- "Creare una coppia sincrona con mirroring"

Concetti

Come funziona il mirroring

Unified Manager include opzioni di configurazione per le funzionalità di mirroring di SANtricity, che consentono agli amministratori di replicare i dati tra due array di storage per la protezione dei dati.

Il mirroring sincrono non è disponibile sul sistema storage EF600 o EF300.

Tipi di mirroring

Le applicazioni SANtricity includono due tipi di mirroring: Asincrono e sincrono.

Il mirroring asincrono copia i volumi di dati su richiesta o in base a una pianificazione, riducendo al minimo o evitando i downtime che potrebbero derivare da danneggiamento o perdita dei dati. Il mirroring asincrono acquisisce lo stato del volume primario in un determinato momento e copia solo i dati modificati dall'ultima acquisizione dell'immagine. Il sito primario può essere aggiornato immediatamente e il sito secondario può essere aggiornato in base alla larghezza di banda. Le informazioni vengono memorizzate nella cache e inviate in un secondo momento, man mano che le risorse di rete diventano disponibili. Questo tipo di mirroring è ideale per processi periodici come backup e archiviazione.

Il mirroring sincrono replica i volumi di dati in tempo reale per garantire una disponibilità continua. Lo scopo è quello di raggiungere un obiettivo RPO (Recovery Point Objective) di zero dati persi, grazie alla disponibilità di una copia dei dati importanti in caso di disastro su uno dei due storage array. La copia è identica ai dati di produzione in ogni momento perché ogni volta che viene eseguita una scrittura nel volume primario, viene eseguita una scrittura nel volume secondario. L'host non riceve una conferma che la scrittura è riuscita fino a quando il volume secondario non viene aggiornato con le modifiche apportate sul volume primario. Questo tipo di mirroring è ideale per scopi di business continuity come il disaster recovery.

Differenze tra i tipi di mirroring

La seguente tabella descrive le principali differenze tra i due tipi di mirroring.

Attributo	Asincrono	Sincrono
Metodo di replica	Point-in-time — il mirroring viene eseguito su richiesta o automaticamente in base a una pianificazione definita dall'utente.	Continuo — il mirroring viene eseguito automaticamente in modo continuo, copiando i dati da ogni scrittura host.
Distanza	Supporta lunghe distanze tra gli array. In genere, la distanza è limitata solo dalle funzionalità della rete e dalla tecnologia di estensione del canale.	Limitato a distanze più brevi tra gli array. In genere, la distanza deve essere entro circa 10 km (6.2 miglia) dallo storage array locale per soddisfare i requisiti di latenza e performance applicativa.
Metodo di comunicazione	Una rete IP o Fibre Channel standard.	Solo rete Fibre Channel.
Tipi di volume	Standard o sottile.	Solo standard.

Flusso di lavoro di configurazione del mirroring

È possibile configurare il mirroring asincrono o sincrono in Unified Manager, quindi utilizzare System Manager per gestire le sincronizzazioni.

Workflow di mirroring asincrono

Il mirroring asincrono coinvolge il seguente flusso di lavoro:

1. Eseguire la configurazione iniziale in Unified Manager:
   a. Selezionare lo storage array locale come origine per il trasferimento dei dati.
   b. Creare o selezionare un gruppo di coerenza mirror esistente, che è un contenitore per il volume primario sull'array locale e il volume secondario sull'array remoto. I volumi primario e secondario sono definiti "coppia di mirroring". Se si crea il gruppo di coerenza del mirroring per la prima volta, specificare se si desidera eseguire sincronizzazioni manuali o pianificate.
   c. Selezionare un volume primario dall'array di storage locale, quindi determinarne la capacità riservata. La capacità riservata è la capacità fisica allocata da utilizzare per l'operazione di copia.
   d. Selezionare un array di storage remoto come destinazione del trasferimento, un volume secondario, quindi determinarne la capacità riservata.
   e. Avviare il trasferimento iniziale dei dati dal volume primario al volume secondario. A seconda delle dimensioni del volume, il trasferimento iniziale potrebbe richiedere diverse ore.
2. Verificare l'avanzamento della sincronizzazione iniziale:
   a. In Unified Manager, avviare System Manager per l'array locale.
   b. In System Manager, visualizzare lo stato dell'operazione di mirroring. Una volta completato il mirroring, lo stato della coppia mirrorata è "ottimale".
3. In alternativa, è possibile riprogrammare o eseguire manualmente i trasferimenti di dati successivi in System Manager. Solo i blocchi nuovi e modificati vengono trasferiti dal volume primario al volume secondario.

> Poiché la replica asincrona è periodica, il sistema può consolidare i blocchi modificati e conservare la larghezza di banda della rete. L'impatto sul throughput di scrittura e sulla latenza di scrittura è minimo.

Workflow di mirroring sincrono

Il mirroring sincrono include il seguente flusso di lavoro:

1. Eseguire la configurazione iniziale in Unified Manager:
   a. Selezionare un array di storage locale come origine per il trasferimento dei dati.
   b. Selezionare un volume primario dall'array di storage locale.
   c. Selezionare un array di storage remoto come destinazione per il trasferimento dei dati, quindi selezionare un volume secondario.
   d. Selezionare le priorità di sincronizzazione e risincronizzazione.
   e. Avviare il trasferimento iniziale dei dati dal volume primario al volume secondario. A seconda delle dimensioni del volume, il trasferimento iniziale potrebbe richiedere diverse ore.
2. Verificare l'avanzamento della sincronizzazione iniziale:

a. In Unified Manager, avviare System Manager per l'array locale.

b. In System Manager, visualizzare lo stato dell'operazione di mirroring. Una volta completato il mirroring, lo stato della coppia mirrorata è "ottimale". I due array tentano di rimanere sincronizzati attraverso le normali operazioni. Solo i blocchi nuovi e modificati vengono trasferiti dal volume primario al volume secondario.

3. In alternativa, è possibile modificare le impostazioni di sincronizzazione in System Manager.

> Poiché la replica sincrona è continua, il collegamento di replica tra i due siti deve fornire funzionalità di larghezza di banda sufficienti.

Terminologia mirrorata

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

Termine	Descrizione
Storage array locale	L'array di storage locale è l'array di storage su cui si sta agendo.
Gruppo di coerenza mirror	Un gruppo di coerenza mirror è un contenitore per una o più coppie mirrorate. Per le operazioni di mirroring asincrono, è necessario creare un gruppo di coerenza mirror. Tutte le coppie mirrorate in un gruppo vengono risincronizzate simultaneamente, preservando così un punto di ripristino coerente. Il mirroring sincrono non utilizza gruppi di coerenza mirror.
Coppia mirrorata	Una coppia mirrorata è composta da due volumi, un volume primario e un volume secondario. Nel mirroring asincrono, una coppia mirrorata appartiene sempre a un gruppo di coerenza mirror. Le operazioni di scrittura vengono eseguite prima nel volume primario e poi replicate nel volume secondario. Ogni coppia mirrorata in un gruppo di coerenza mirror condivide le stesse impostazioni di sincronizzazione.
Volume primario	Il volume principale di una coppia mirrorata è il volume di origine da mirrorare.
Storage array remoto	L'array di storage remoto è generalmente designato come sito secondario, che di solito contiene una replica dei dati in una configurazione di mirroring.
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione del servizio di copia e oggetto di storage. Non è direttamente leggibile dall'host. Questi volumi sono necessari per consentire al controller di salvare in modo persistente le informazioni necessarie per mantenere il mirroring in uno stato operativo. Contengono informazioni come i delta log e i dati copy-on-write.
Volume secondario	Il volume secondario di una coppia mirrorata si trova in genere in un sito secondario e contiene una replica dei dati.

Termine	Descrizione
Sincronizzazione	La sincronizzazione avviene alla sincronizzazione iniziale tra lo storage array locale e lo storage array remoto. La sincronizzazione si verifica anche quando i volumi primario e secondario non vengono sincronizzati dopo un'interruzione della comunicazione. Quando il collegamento di comunicazione funziona di nuovo, tutti i dati non replicati vengono sincronizzati con l'array di storage del volume secondario.

Requisiti per l'utilizzo del mirroring

Se si prevede di configurare il mirroring, tenere presenti i seguenti requisiti.

Unified Manager

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Storage array

Il mirroring sincrono non è disponibile sull'array di storage EF600 o EF300.

- È necessario disporre di due array di storage.
- Ogni array di storage deve avere due controller.
- I due storage array devono essere rilevati in Unified Manager.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera eseguire il mirroring.
- Il mirroring asincrono è supportato sui controller con porte host Fibre Channel (FC) o iSCSI, mentre il mirroring sincrono è supportato solo sui controller con porte host FC.

Requisiti di connettività

Il mirroring tramite un'interfaccia FC (asincrona o sincrona) richiede quanto segue:

- Ogni controller dello storage array dedica la porta host FC con il numero più alto alle operazioni di mirroring.
- Se il controller dispone di porte FC di base e porte FC HIC (host Interface Card), la porta con il numero più alto si trova su un HIC. Tutti gli host connessi alla porta dedicata vengono disconnessi e non vengono accettate richieste di accesso all'host. Le richieste di i/o su questa porta vengono accettate solo dai controller che partecipano alle operazioni di mirroring.

- Le porte di mirroring dedicate devono essere collegate a un ambiente fabric FC che supporti le interfacce del servizio di directory e del servizio di nomi. In particolare, FC-al e point-to-point non sono supportati come opzioni di connettività tra i controller che partecipano a relazioni mirror.

Il mirroring tramite un'interfaccia iSCSI (solo asincrona) richiede quanto segue:

- A differenza di FC, iSCSI non richiede una porta dedicata. Quando si utilizza il mirroring asincrono in ambienti iSCSI, non è necessario dedicare alcuna delle porte iSCSI front-end dello storage array per l'utilizzo con il mirroring asincrono; tali porte sono condivise sia per il traffico mirror asincrono che per le connessioni i/o host-to-array.
- Il controller mantiene un elenco di sistemi storage remoti con i quali l'iSCSI Initiator tenta di stabilire una sessione. La prima porta che stabilisce correttamente una connessione iSCSI viene utilizzata per tutte le comunicazioni successive con l'array di storage remoto. Se la comunicazione non riesce, viene tentata una nuova sessione utilizzando tutte le porte disponibili.
- Le porte iSCSI sono configurate a livello di array porta per porta. La comunicazione tra controller per la messaggistica di configurazione e il trasferimento dei dati utilizza le impostazioni globali, incluse le impostazioni per:
  - VLAN: Per comunicare, i sistemi locali e remoti devono avere la stessa impostazione VLAN
  - Porta di ascolto iSCSI
  - Frame jumbo
  - Priorità Ethernet

> La comunicazione tra controller iSCSI deve utilizzare una porta di connessione host e non la porta Ethernet di gestione.

Volumi mirrorati candidati

- Il livello RAID, i parametri di caching e le dimensioni dei segmenti possono essere diversi sui volumi primari e secondari di una coppia mirrorata.

> Per i controller EF600 e EF300, i volumi primari e secondari di una coppia asincrona con mirroring devono corrispondere allo stesso protocollo, livello di vassoio, dimensione del segmento, tipo di sicurezza e livello RAID. Le coppie mirrorate asincrone non idonee non vengono visualizzate nell'elenco dei volumi disponibili.

- Il volume secondario deve essere grande almeno quanto il volume primario.
- Un volume può partecipare a una sola relazione di mirroring.
- Per una coppia sincrona con mirroring, i volumi primario e secondario devono essere volumi standard. Non possono essere volumi thin o volumi snapshot.
- Per il mirroring sincrono, esistono limiti al numero di volumi supportati su un determinato array di storage. Assicurarsi che il numero di volumi configurati sull'array di storage sia inferiore al limite supportato. Quando il mirroring sincrono è attivo, i due volumi di capacità riservata creati vengono conteggiati rispetto al limite di volume.
- Per il mirroring asincrono, il volume primario e il volume secondario devono avere le stesse funzionalità di Drive Security.
  - Se il volume primario è compatibile con FIPS, il volume secondario deve essere compatibile con FIPS.
  - Se il volume primario è compatibile con FDE, il volume secondario deve essere compatibile con FDE.

- Se il volume primario non utilizza Drive Security, il volume secondario non deve utilizzare Drive Security.

Capacità riservata

Mirroring asincrono:

- Un volume a capacità riservata è necessario per un volume primario e per un volume secondario in una coppia mirrorata per la registrazione delle informazioni di scrittura per il ripristino da ripristini del controller e altre interruzioni temporanee.
- Poiché sia il volume primario che il volume secondario di una coppia mirrorata richiedono ulteriore capacità riservata, è necessario assicurarsi di disporre di capacità libera su entrambi gli array di storage nella relazione mirror.

Mirroring sincrono:

- La capacità riservata è necessaria per un volume primario e per un volume secondario per la registrazione delle informazioni di scrittura per il ripristino da ripristini del controller e altre interruzioni temporanee.
- I volumi di capacità riservati vengono creati automaticamente quando viene attivato il mirroring sincrono. Poiché sia il volume primario che il volume secondario di una coppia mirrorata richiedono capacità riservata, è necessario assicurarsi di disporre di una capacità libera sufficiente su entrambi gli array di storage che partecipano alla relazione di mirroring sincrono.

Funzione di protezione del disco

- Se si utilizzano dischi sicuri, il volume primario e il volume secondario devono disporre di impostazioni di sicurezza compatibili. Questa restrizione non viene applicata; pertanto, è necessario verificarla da soli.
- Se si utilizzano dischi sicuri, il volume primario e il volume secondario devono utilizzare lo stesso tipo di disco. Questa restrizione non viene applicata; pertanto, è necessario verificarla da soli.
- Se si utilizza Data Assurance (da), il volume primario e il volume secondario devono avere le stesse impostazioni da.

Configurare il mirroring

Creare una coppia asincrona con mirroring

Per configurare il mirroring asincrono, si crea una coppia mirrorata che include un volume primario sull'array locale e un volume secondario sull'array remoto.

Prima di iniziare

Prima di creare una coppia mirrorata, soddisfare i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Assicurarsi inoltre di soddisfare i seguenti requisiti per gli array e i volumi di storage:

- Ogni array di storage deve avere due controller.

- I due storage array devono essere rilevati in Unified Manager.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera eseguire il mirroring.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel o un'interfaccia iSCSI.
- Sono stati creati i volumi primario e secondario che si desidera utilizzare nella relazione di mirroring asincrono.
- Il volume secondario deve essere grande almeno quanto il volume primario.

A proposito di questa attività

Il processo per creare una coppia asincrona con mirroring è una procedura multi-step.

Fase 1: Creare o selezionare un gruppo di coerenza mirror

In questo passaggio, creare un nuovo gruppo di coerenza mirror o selezionarne uno esistente. Un gruppo di coerenza mirror è un contenitore per i volumi primario e secondario (la coppia mirrorata) e specifica il metodo di risincronizzazione desiderato (manuale o automatico) per tutte le coppie del gruppo.

Fasi

1. Dalla pagina **Manage** (Gestisci), selezionare l'array di storage locale che si desidera utilizzare per l'origine.
2. Selezionare **azioni › Crea coppia di mirroring asincrono**.

   Viene visualizzata la procedura guidata Create Asynchronous Mirrored Pair.

3. Selezionare un gruppo di coerenza mirror esistente o crearne uno nuovo.

   Per selezionare un gruppo esistente, assicurarsi che sia selezionato **un gruppo di coerenza mirror esistente**, quindi selezionare il gruppo dalla tabella. Un gruppo di coerenza può includere più coppie mirrorate.

   Per creare un nuovo gruppo, procedere come segue:

   a. Selezionare **Un nuovo gruppo di coerenza mirror**, quindi fare clic su **Avanti**.
   b. Immettere un nome univoco che descriva meglio i dati sui volumi che verranno mirrorati tra i due array di storage. Un nome può essere composto solo da lettere, numeri e caratteri speciali di sottolineatura (_), trattino (-) e il segno hash (n.). Un nome non può superare i 30 caratteri e non può contenere spazi.
   c. Selezionare l'array di storage remoto su cui si desidera stabilire una relazione mirror con l'array di storage locale.

      Se lo storage array remoto è protetto da password, il sistema richiede una password.

   d. Scegliere se sincronizzare le coppie mirrorate manualmente o automaticamente:
      - **Manuale** — selezionare questa opzione per avviare manualmente la sincronizzazione per tutte le coppie mirrorate all'interno di questo gruppo. Tenere presente che per eseguire una

risincronizzazione in un secondo momento, è necessario avviare System Manager per l'array di storage primario, quindi andare al **Storage › Asynchronous Mirroring**, selezionare il gruppo dalla scheda **Mirror Consistency Groups**, quindi selezionare **More › Manually resincronize**.

- **Automatico** — selezionare l'intervallo desiderato in **minuti**, **ore** o **giorni**, dall'inizio dell'aggiornamento precedente all'inizio dell'aggiornamento successivo. Ad esempio, se l'intervallo di sincronizzazione è impostato su 30 minuti e il processo di sincronizzazione inizia alle 4:00, il processo successivo inizia alle 4:30

e. Selezionare le impostazioni di avviso desiderate:

- Per le sincronizzazioni manuali, specificare la soglia (definita dalla percentuale della capacità rimanente) per la ricezione degli avvisi.
- Per le sincronizzazioni automatiche, è possibile impostare tre metodi di avviso: quando la sincronizzazione non è stata completata in un determinato periodo di tempo, quando i dati del punto di ripristino sull'array remoto sono più vecchi di un limite di tempo specifico e quando la capacità riservata si avvicina a una soglia specifica (definita dalla percentuale della capacità rimanente).

4. Selezionare **Avanti** e andare a Fase 2: Selezionare il volume principale.

Se è stato definito un nuovo gruppo di coerenza mirror, Unified Manager crea prima il gruppo di coerenza mirror sull'array di storage locale, quindi crea il gruppo di coerenza mirror sull'array di storage remoto. È possibile visualizzare e gestire il gruppo di coerenza mirror avviando System Manager per ciascun array.

> Se Unified Manager crea correttamente il gruppo di coerenza mirror sull'array di storage locale, ma non lo crea sull'array di storage remoto, elimina automaticamente il gruppo di coerenza mirror dall'array di storage locale. Se si verifica un errore mentre Unified Manager sta tentando di eliminare il gruppo di coerenza mirror, è necessario eliminarlo manualmente.

Fase 2: Selezionare il volume principale

In questa fase, selezionare il volume primario da utilizzare nella relazione di mirroring e allocare la capacità riservata. Quando si seleziona un volume primario sull'array di storage locale, il sistema visualizza un elenco di tutti i volumi idonei per la coppia mirrorata. I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco.

Tutti i volumi aggiunti al gruppo di coerenza mirror sull'array di storage locale avranno il ruolo principale nella relazione mirror.

Fasi

1. Dall'elenco dei volumi idonei, selezionare un volume che si desidera utilizzare come volume primario, quindi fare clic su **Avanti** per allocare la capacità riservata.
2. Dall'elenco dei candidati idonei, selezionare la capacità riservata per il volume primario.

   Tenere presenti le seguenti linee guida:

   - L'impostazione predefinita per la capacità riservata è il 20% della capacità del volume di base, e di solito questa capacità è sufficiente. Se si modifica la percentuale, fare clic su **Aggiorna candidati**.
   - La capacità richiesta varia in base alla frequenza e alle dimensioni delle scritture i/o nel volume primario e al tempo necessario per mantenere la capacità.
   - In generale, scegliere una capacità più elevata per la capacità riservata se si verifica una o entrambe le seguenti condizioni:
     - Si intende mantenere la coppia mirrorata per un lungo periodo di tempo.

        - Una grande percentuale di blocchi di dati cambierà sul volume primario a causa dell'intensa attività di i/O. Utilizzare dati storici sulle performance o altre utility del sistema operativo per determinare l'attività i/o tipica del volume primario.

3. Selezionare **Avanti** e andare a Fase 3: Selezionare il volume secondario.

Fase 3: Selezionare il volume secondario

In questa fase, selezionare il volume secondario da utilizzare nella relazione di mirroring e allocare la capacità riservata. Quando si seleziona un volume secondario sull'array di storage remoto, il sistema visualizza un elenco di tutti i volumi idonei per la coppia mirrorata. I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco.

Tutti i volumi aggiunti al gruppo di coerenza mirror sull'array di storage remoto avranno il ruolo secondario nella relazione mirror.

Fasi

1. Dall'elenco dei volumi idonei, selezionare un volume che si desidera utilizzare come volume secondario nella coppia mirrorata, quindi fare clic su **Avanti** per allocare la capacità riservata.
2. Dall'elenco dei candidati idonei, selezionare la capacità riservata per il volume secondario.

   Tenere presenti le seguenti linee guida:

   - L'impostazione predefinita per la capacità riservata è il 20% della capacità del volume di base, e di solito questa capacità è sufficiente. Se si modifica la percentuale, fare clic su **Aggiorna candidati**.
   - La capacità richiesta varia in base alla frequenza e alle dimensioni delle scritture i/o nel volume primario e al tempo necessario per mantenere la capacità.
   - In generale, scegliere una capacità più elevata per la capacità riservata se si verifica una o entrambe le seguenti condizioni:
     - Si intende mantenere la coppia mirrorata per un lungo periodo di tempo.
     - Una grande percentuale di blocchi di dati cambierà sul volume primario a causa dell'intensa attività di i/O. Utilizzare dati storici sulle performance o altre utility del sistema operativo per determinare l'attività i/o tipica del volume primario.
3. Selezionare **fine** per completare la sequenza di mirroring asincrono.

Risultati

Unified Manager esegue le seguenti operazioni:

- Avvia la sincronizzazione iniziale tra lo storage array locale e lo storage array remoto.
- Crea la capacità riservata per la coppia mirrorata sull'array di storage locale e sull'array di storage remoto.

> Se il volume sottoposto a mirroring è un volume sottile, solo i blocchi sottoposti a provisioning (capacità allocata anziché capacità riportata) vengono trasferiti al volume secondario durante la sincronizzazione iniziale. In questo modo si riduce la quantità di dati da trasferire per completare la sincronizzazione iniziale.

Creare una coppia sincrona con mirroring

Per configurare il mirroring sincrono, creare una coppia mirrorata che includa un volume primario sull'array locale e un volume secondario sull'array remoto.

Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

Prima di iniziare

Prima di creare una coppia mirrorata, soddisfare i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Assicurarsi inoltre di soddisfare i seguenti requisiti per gli array e i volumi di storage:

- I due storage array che si intende utilizzare per il mirroring vengono rilevati in Unified Manager.
- Ogni array di storage deve avere due controller.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel.
- Sono stati creati i volumi primario e secondario che si desidera utilizzare nella relazione di mirroring sincrono.
- Il volume primario deve essere un volume standard. Non può essere un volume thin o un volume snapshot.
- Il volume secondario deve essere un volume standard. Non può essere un volume thin o un volume snapshot.
- Il volume secondario deve essere grande almeno quanto il volume primario.

A proposito di questa attività

Il processo per creare coppie sincrone mirrorate è una procedura multi-step.

Fase 1: Selezionare il volume principale

In questa fase, selezionare il volume primario da utilizzare nella relazione di mirroring sincrono. Quando si seleziona un volume primario sull'array di storage locale, il sistema visualizza un elenco di tutti i volumi idonei per la coppia mirrorata. I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco. Il volume selezionato contiene il ruolo principale nella relazione mirror.

Fasi

1. Dalla pagina **Manage** (Gestisci), selezionare l'array di storage locale che si desidera utilizzare per l'origine.
2. Selezionare **azioni › Crea coppia sincrona con mirroring**.

   Viene visualizzata la procedura guidata Create Synchronous Mirrored Pair.

3. Dall'elenco dei volumi idonei, selezionare un volume che si desidera utilizzare come volume principale nel mirror.

4. Selezionare **Avanti** e andare a Fase 2: Selezionare il volume secondario.

Fase 2: Selezionare il volume secondario

In questa fase, selezionare il volume secondario da utilizzare nella relazione di mirroring. Quando si seleziona un volume secondario sull'array di storage remoto, il sistema visualizza un elenco di tutti i volumi idonei per la coppia mirrorata. I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco. Il volume selezionato avrà il ruolo secondario nella relazione mirror.

Fasi

1. Selezionare l'array di storage remoto su cui si desidera stabilire una relazione mirror con l'array di storage locale.

   Se lo storage array remoto è protetto da password, il sistema richiede una password.

   - Gli array di storage sono elencati in base al nome dell'array di storage. Se non si è nominato un array di storage, questo verrà elencato come "senza nome".
   - Se lo storage array che si desidera utilizzare non è presente nell'elenco, assicurarsi che sia stato rilevato in Unified Manager.
2. Dall'elenco dei volumi idonei, selezionare un volume che si desidera utilizzare come volume secondario nel mirror.

   Se si sceglie un volume secondario con una capacità superiore a quella del volume primario, la capacità utilizzabile viene limitata alle dimensioni del volume primario.

3. Fare clic su **Avanti** e andare a Fase 3: Selezionare le impostazioni di sincronizzazione.

Fase 3: Selezionare le impostazioni di sincronizzazione

In questa fase, selezionare le impostazioni che determinano la modalità di sincronizzazione dei dati dopo un'interruzione della comunicazione. È possibile impostare la priorità con cui il proprietario del controller del volume primario sincronizza i dati con il volume secondario dopo un'interruzione della comunicazione. È inoltre necessario selezionare il criterio di risincronizzazione, manuale o automatico.

Fasi

1. Utilizzare la barra di scorrimento per impostare la priorità di sincronizzazione.

   La priorità di sincronizzazione determina la quantità di risorse di sistema utilizzate per completare la sincronizzazione iniziale e l'operazione di risincronizzazione dopo un'interruzione della comunicazione rispetto alle richieste di i/o del servizio.

   La priorità impostata in questa finestra di dialogo si applica sia al volume primario che al volume secondario. È possibile modificare la velocità sul volume primario in un secondo momento accedendo a System Manager e selezionando il **Storage › Synchronous Mirroring › More › Edit Settings** (Storage[mirroring sincrono > Altro > Modifica impostazioni).

   Sono disponibili cinque tassi di priorità di sincronizzazione:

   - Più basso
   - Basso
   - Medio

- Alto
- Massimo

  Se la priorità di sincronizzazione è impostata sul tasso più basso, l'attività di i/o ha la priorità e l'operazione di risincronizzazione richiede più tempo. Se la priorità di sincronizzazione è impostata sulla velocità massima, l'operazione di risincronizzazione viene assegnata alla priorità, ma l'attività di i/o per l'array di storage potrebbe risentirne.

2. Scegliere se risincronizzare le coppie mirrorate sull'array di storage remoto manualmente o automaticamente.
   - **Manuale** (opzione consigliata) — selezionare questa opzione per richiedere la ripresa manuale della sincronizzazione dopo il ripristino della comunicazione su una coppia mirrorata. Questa opzione offre la migliore opportunità per il ripristino dei dati.
   - **Automatico** — selezionare questa opzione per avviare la risincronizzazione automaticamente dopo il ripristino della comunicazione su una coppia mirrorata.

     Per riprendere manualmente la sincronizzazione, accedere a System Manager e selezionare **Storage › Synchronous Mirroring**, evidenziare la coppia mirrorata nella tabella e selezionare **Resume** sotto **More**.
3. Fare clic su **fine** per completare la sequenza di mirroring sincrono.

Risultati

Una volta attivato il mirroring, il sistema esegue le seguenti operazioni:

- Avvia la sincronizzazione iniziale tra lo storage array locale e lo storage array remoto.
- Imposta la priorità di sincronizzazione e il criterio di risincronizzazione.
- Riserva la porta con il numero più alto dell'HIC del controller per la trasmissione dei dati mirror.

  Le richieste di i/o ricevute su questa porta vengono accettate solo dal proprietario del controller preferito remoto del volume secondario nella coppia mirrorata. (Sono consentite prenotazioni sul volume primario).

- Crea due volumi di capacità riservata, uno per ciascun controller, che vengono utilizzati per la registrazione delle informazioni di scrittura per il ripristino da ripristini del controller e altre interruzioni temporanee.

  La capacità di ciascun volume è di 128 MiB. Tuttavia, se i volumi sono collocati in un pool, 4 GiB saranno riservati per ogni volume.

Al termine

Accedere a System Manager e selezionare **Home › View Operations in Progress** (Visualizza operazioni in corso) per visualizzare l'avanzamento dell'operazione di mirroring sincrono. Questa operazione può essere lunga e può influire sulle prestazioni del sistema.

FAQ

Cosa è necessario sapere prima di creare un gruppo di coerenza mirror?

Seguire queste linee guida prima di creare un gruppo di coerenza mirror.

Soddisfare i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Assicurarsi inoltre di soddisfare i seguenti requisiti per gli array di storage:

- I due storage array devono essere rilevati in Unified Manager.
- Ogni array di storage deve avere due controller.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel o un'interfaccia iSCSI.

Il mirroring sincrono non è disponibile sul sistema storage EF600 o EF300.

Cosa occorre sapere prima di creare una coppia mirrorata?

Prima di creare una coppia mirrorata, seguire queste linee guida.

- È necessario disporre di due array di storage.
- Ogni array di storage deve avere due controller.
- I due storage array devono essere rilevati in Unified Manager.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera eseguire il mirroring.
- Il mirroring asincrono è supportato sui controller con porte host Fibre Channel (FC) o iSCSI, mentre il mirroring sincrono è supportato solo sui controller con porte host FC.

Il mirroring sincrono non è disponibile sul sistema storage EF600 o EF300.

Perché dovrei modificare questa percentuale?

La capacità riservata corrisponde in genere al 20% del volume di base per le operazioni di mirroring asincrono. Di solito questa capacità è sufficiente.

La capacità necessaria varia in base alla frequenza e alle dimensioni delle scritture i/o nel volume di base e alla durata dell'utilizzo del servizio di copia dell'oggetto di storage. In generale, scegliere una percentuale maggiore per la capacità riservata se sussistono una o entrambe le seguenti condizioni:

- Se la durata di un'operazione di copia del servizio di un oggetto di storage specifico sarà molto lunga.
- Se una grande percentuale di blocchi di dati cambia sul volume di base a causa di un'intensa attività di i/O. Utilizza dati storici sulle performance o altre utility del sistema operativo per determinare l'attività i/o tipica del volume di base.

Perché vengono visualizzati più candidati con capacità riservata?

Se in un pool o gruppo di volumi sono presenti più volumi che soddisfano la percentuale di capacità selezionata per l'oggetto di storage, verranno visualizzati più volumi candidati.

È possibile aggiornare l'elenco dei candidati consigliati modificando la percentuale di spazio su disco fisico che si desidera riservare sul volume di base per le operazioni del servizio di copia. I candidati migliori vengono visualizzati in base alla selezione effettuata.

Perché non vengono visualizzati tutti i volumi?

Quando si seleziona un volume primario per una coppia mirrorata, un elenco mostra tutti i volumi idonei.

I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco. I volumi potrebbero non essere idonei per uno dei seguenti motivi:

- Il volume non è ottimale.
- Il volume sta già partecipando a una relazione di mirroring.
- Per il mirroring sincrono, i volumi primario e secondario di una coppia mirrorata devono essere volumi standard. Non possono essere volumi thin o volumi snapshot.
- Per il mirroring asincrono, i thin volumi devono avere l'espansione automatica abilitata.

> Per i controller EF600 e EF300, i volumi primari e secondari di una coppia asincrona con mirroring devono corrispondere allo stesso protocollo, livello di vassoio, dimensione del segmento, tipo di sicurezza e livello RAID. Le coppie mirrorate asincrone non idonee non vengono visualizzate nell'elenco dei volumi disponibili.

Perché non vengono visualizzati tutti i volumi sull'array di storage remoto?

Quando si seleziona un volume secondario nell'array di storage remoto, un elenco mostra tutti i volumi idonei per la coppia mirrorata.

I volumi non idonei per l'utilizzo non vengono visualizzati nell'elenco. I volumi potrebbero non essere idonei per uno dei seguenti motivi:

- Il volume non è un volume standard, ad esempio un volume snapshot.
- Il volume non è ottimale.
- Il volume sta già partecipando a una relazione di mirroring.
- Per il mirroring asincrono, gli attributi del thin volume tra il volume primario e il volume secondario non corrispondono.
- Se si utilizza Data Assurance (da), il volume primario e il volume secondario devono avere le stesse impostazioni da.

    - Se il volume primario è abilitato da, il volume secondario deve essere abilitato da.
    - Se il volume primario non è abilitato da, il volume secondario non deve essere abilitato da.
- Per il mirroring asincrono, il volume primario e il volume secondario devono avere le stesse funzionalità di Drive Security.
    - Se il volume primario è compatibile con FIPS, il volume secondario deve essere compatibile con FIPS.
    - Se il volume primario è compatibile con FDE, il volume secondario deve essere compatibile con FDE.
    - Se il volume primario non utilizza Drive Security, il volume secondario non deve utilizzare Drive Security.

Qual è l'impatto della priorità di sincronizzazione sulle velocità di sincronizzazione?

La priorità di sincronizzazione definisce il tempo di elaborazione allocato per le attività di sincronizzazione in relazione alle prestazioni del sistema.

Il proprietario del controller del volume primario esegue questa operazione in background. Allo stesso tempo, il proprietario del controller elabora le scritture i/o locali nel volume primario e le scritture remote associate nel volume secondario. Poiché la risincronizzazione distoglie le risorse di elaborazione del controller dall'attività di i/o, la risincronizzazione può avere un impatto sulle prestazioni dell'applicazione host.

Tenere presenti queste linee guida per determinare il tempo necessario per una priorità di sincronizzazione e il modo in cui le priorità di sincronizzazione possono influire sulle prestazioni del sistema.

Sono disponibili i seguenti tassi di priorità:

- Più basso
- Basso
- Medio
- Alto
- Massimo

Il tasso di priorità più basso supporta le prestazioni del sistema, ma la risincronizzazione richiede più tempo. Il tasso di priorità più elevato supporta la risincronizzazione, ma le prestazioni del sistema potrebbero essere compromesse.

Queste linee guida approssimano le differenze tra le priorità.

Tasso di priorità per la sincronizzazione completa	Tempo trascorso rispetto alla massima velocità di sincronizzazione
Più basso	Circa otto volte più a lungo rispetto al tasso di priorità più elevato.
Basso	Circa sei volte più a lungo rispetto al tasso di priorità più elevato.
Medio	Circa tre volte e mezzo fino al tasso di priorità più elevato.
Alto	Circa il doppio rispetto al tasso di priorità più elevato.

Le dimensioni del volume e i carichi della velocità di i/o dell'host influiscono sui confronti dei tempi di sincronizzazione.

Perché si consiglia di utilizzare una policy di sincronizzazione manuale?

La risincronizzazione manuale è consigliata perché consente di gestire il processo di risincronizzazione in modo da offrire la migliore opportunità di recupero dei dati.

Se si utilizza un criterio di risincronizzazione automatica e si verificano problemi di comunicazione intermittente durante la risincronizzazione, i dati sul volume secondario potrebbero essere temporaneamente danneggiati. Una volta completata la risincronizzazione, i dati vengono corretti.

Certificati

Panoramica dei certificati

Gestione certificati consente di creare richieste di firma del certificato (CSR), importare certificati e gestire i certificati esistenti.

Cosa sono i certificati?

I *certificati* sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet. Esistono due tipi di certificati: Un *certificato firmato* viene validato da un'autorità di certificazione (CA) e un *certificato autofirmato* viene validato dal proprietario dell'entità anziché da una terza parte.

Scopri di più:

- "Come funzionano i certificati"
- "Terminologia del certificato"

Come si configurano i certificati?

Da Certificate Management, è possibile configurare i certificati per la stazione di gestione che ospita Unified Manager e importare i certificati per i controller negli array.

Scopri di più:

- "Utilizzare i certificati firmati dalla CA per il sistema di gestione"
- "Importare certificati per gli array"

Concetti

Come funzionano i certificati

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

Certificati firmati

I certificati garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, privatamente e inalterate, solo tra il server e il client specificati. Con Unified Manager, è possibile gestire i certificati per il

browser su un sistema di gestione host e i controller negli array di storage rilevati.

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.

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 disconnettono 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.

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 per Unified Manager

L'interfaccia di Unified Manager viene installata con il proxy dei servizi Web su un sistema host. Quando si apre un browser e si tenta di connettersi a Unified Manager, il browser tenta di verificare che l'host sia un'origine attendibile verificando la presenza di un certificato digitale. Se il browser non individua un certificato firmato dalla CA per il server, viene visualizzato un messaggio di avviso. Da qui, è possibile accedere al sito Web per accettare il certificato autofirmato per la sessione. In alternativa, è possibile ottenere certificati digitali firmati da una CA in modo da non visualizzare più il messaggio di avviso.

Certificati per i controller

Durante una sessione di Unified Manager, potrebbero essere visualizzati ulteriori messaggi di sicurezza quando si tenta di accedere a un controller che non dispone di un certificato firmato dalla CA. In questo caso, è possibile considerare attendibile in modo permanente il certificato autofirmato oppure importare i certificati firmati dalla CA per i controller in modo che il server Web Services Proxy possa autenticare le richieste client in entrata da questi 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 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.
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.

Termine	Descrizione
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.
Truststore	Un truststore è un repository che contiene certificati di terze parti attendibili, ad esempio CA.

Utilizzare i certificati firmati dalla CA per il sistema di gestione

È possibile ottenere e importare certificati firmati dalla CA per un accesso sicuro al sistema di gestione che ospita Unified 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 un file CSR

È necessario innanzitutto generare un file CSR (Certificate Signing Request) che identifichi l'organizzazione e il sistema host in cui sono installati Web Services Proxy e Unified Manager.

In alternativa, è possibile generare un file CSR utilizzando uno strumento come OpenSSL e passare a Fase 2: Inviare il file CSR.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda Management (Gestione), selezionare **complete CSR** (completa CSR).
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 sistema host o l'azienda.
   - **Stato/Regione (opzionale)** — Stato o regione in cui si trova il sistema host o l'azienda.
   - **Codice ISO del Paese** — Codice ISO (International Organization for Standardization) a due cifre del Paese, ad esempio USA.
4. Inserire le seguenti informazioni sul sistema host in cui è installato il proxy dei servizi Web:
   - **Nome comune** — Indirizzo IP o nome DNS del sistema host in cui è installato il proxy dei servizi Web. Assicurarsi che l'indirizzo sia corretto; deve corrispondere esattamente a quello immesso per accedere a Unified Manager nel browser. Non includere http:// o https://. Il nome DNS non può iniziare con un carattere jolly.
   - **Indirizzi IP alternativi** — se il nome comune è un indirizzo IP, è possibile inserire eventuali indirizzi IP o alias aggiuntivi per il sistema host. Per più voci, utilizzare un formato delimitato da virgole.
   - **Nomi DNS alternativi** — se il nome comune è un nome DNS, immettere eventuali nomi DNS aggiuntivi per il sistema host. 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. Il nome DNS non può iniziare con un carattere jolly.
5. Assicurarsi che le informazioni sull'host siano corrette. In caso contrario, i certificati restituiti dalla CA non avranno esito positivo quando si tenta di importarli.
6. Fare clic su **fine**.
7. Andare a Fase 2: Inviare il file CSR.

Fase 2: Inviare il file CSR

Dopo aver creato un file di richiesta di firma del certificato (CSR), lo si invia a un'autorità di certificazione (CA) per ricevere certificati di gestione firmati per il sistema che ospita Unified Manager e Web Services Proxy.

I sistemi e-Series richiedono il formato PEM (codifica ASCII Base64) per i certificati firmati, che include i seguenti tipi di file: .Pem, .crt, .cer o .key.

Fasi

1. Individuare il file CSR scaricato.

   La posizione della cartella del download dipende dal browser in uso.

2. Inviare il file CSR a una CA (ad esempio, VeriSign o DigiCert) e richiedere certificati firmati in formato PEM.

Dopo aver inviato un file CSR alla CA, NON rigenerare un altro file CSR. Ogni volta che si genera una CSR, il sistema crea una coppia di chiavi privata e pubblica. La chiave pubblica fa parte della CSR, mentre la chiave privata viene conservata nell'archivio chiavi del sistema. Quando si ricevono i certificati firmati e li si importano, il sistema garantisce che sia la chiave privata che la chiave pubblica siano la coppia originale. Se le chiavi non corrispondono, i certificati firmati non funzioneranno ed è necessario richiedere nuovi certificati alla CA.

3. Quando la CA restituisce i certificati firmati, passare a Fase 3: Importazione dei certificati di gestione.

Fase 3: Importazione dei certificati di gestione

Dopo aver ricevuto i certificati firmati dall'autorità di certificazione (CA), importare i certificati nel sistema host in cui sono installati Web Services Proxy e l'interfaccia di Unified Manager.

Prima di iniziare

- Sono stati ricevuti certificati firmati dalla CA. Questi file includono il certificato di origine, uno o più certificati intermedi e il certificato del server.
- Se la CA ha fornito un file di 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 il certificato del server. È possibile utilizzare l'utilità Windows `certmgr` per decomprimere i file (fare clic con il pulsante destro del mouse e selezionare **tutte le attività › Esporta**). Si consiglia la codifica base-64. Una volta completate le esportazioni, viene visualizzato un file CER per ciascun file di certificato nella catena.
- I file dei certificati sono stati copiati nel sistema host in cui è in esecuzione il proxy dei servizi Web.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda Management (Gestione), selezionare **Import** (Importa).

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

3. Fare clic su **Browse** (Sfoglia) per selezionare prima i file dei certificati root e intermedi, quindi selezionare il certificato del server. Se la CSR è stata generata da uno strumento esterno, è necessario importare anche il file della chiave privata creato insieme alla CSR.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

Risultati

I file vengono caricati e validati. Le informazioni sul certificato vengono visualizzate nella pagina Gestione certificati.

Reimpostare i certificati di gestione

È possibile ripristinare lo stato originale autofirmato del certificato di gestione.

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 elimina il certificato di gestione corrente dal sistema host in cui sono installati Web Services Proxy e Unified Manager. Una volta ripristinato il certificato, il sistema host torna a utilizzare il certificato autofirmato.

Fasi

1. Selezionare **Impostazioni > certificati**.
2. Selezionare la scheda **Array Management**, quindi selezionare **Reset**.

   Viene visualizzata la finestra di dialogo Conferma ripristino certificato di gestione.

3. Digitare `reset` nel campo, quindi fare clic su **Reimposta**.

   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

Il sistema torna a utilizzare il certificato autofirmato dal server. Di conseguenza, il sistema richiede agli utenti di accettare manualmente il certificato autofirmato per le sessioni.

Utilizzare certificati array

Importare certificati per gli array

Se necessario, è possibile importare i certificati per gli array di storage in modo che possano autenticarsi con il sistema che ospita Unified Manager. I certificati possono essere firmati da un'autorità di certificazione (CA) o autofirmati.

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 importano certificati attendibili, è necessario importarli per i controller degli array di storage utilizzando System Manager.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.

   Questa pagina mostra tutti i certificati segnalati per gli array di storage.

3. Selezionare il **Importa › certificati** per importare un certificato CA oppure il **Importa › certificati array storage autofirmati** per importare un certificato autofirmato.

   Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati…** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.

4. Nella finestra di dialogo, selezionare il certificato e fare clic su **Importa**.

   Il certificato viene caricato e validato.

Eliminare i certificati attendibili

È possibile eliminare uno o più certificati non più necessari, ad esempio un certificato scaduto.

Prima di iniziare

Importare il nuovo certificato prima di eliminarlo.

> Tenere presente che l'eliminazione di un certificato root o intermedio può influire su più array di storage, poiché questi array possono condividere gli stessi file di certificato.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.
3. Selezionare uno o più certificati nella tabella, quindi fare clic su **Elimina**.

   > La funzione **Delete** non è disponibile per i certificati preinstallati.

   Viene visualizzata la finestra di dialogo Conferma eliminazione certificato attendibile.

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

   Il certificato viene rimosso dalla tabella.

Risolvi i certificati non attendibili

I certificati non attendibili si verificano quando uno storage array tenta di stabilire una connessione sicura a Unified Manager, ma la connessione non viene confermata come sicura.

Dalla pagina Certificate (certificato), è possibile risolvere i certificati non attendibili importando un certificato autofirmato dall'array di storage o importando un certificato dell'autorità di certificazione (CA) emesso da una terza parte attendibile.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore della sicurezza.
- Se si intende importare un certificato firmato dalla CA:
  - È stata generata una richiesta di firma del certificato (file CSR) per ciascun controller nell'array di storage e inviata alla CA.
  - La CA ha restituito file di certificato attendibili.
  - I file dei certificati sono disponibili nel sistema locale.

A proposito di questa attività

Potrebbe essere necessario installare altri certificati CA attendibili se si verifica una delle seguenti condizioni:

- Di recente è stato aggiunto uno storage array.
- Uno o entrambi i certificati sono scaduti.

- Uno o entrambi i certificati vengono revocati.
- Uno o entrambi i certificati non dispongono di un certificato root o intermedio.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.

   Questa pagina mostra tutti i certificati segnalati per gli array di storage.

3. Selezionare il **Importa › certificati** per importare un certificato CA oppure il **Importa › certificati array storage autofirmati** per importare un certificato autofirmato.

   Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati…** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.

4. Nella finestra di dialogo, selezionare il certificato, quindi fare clic su **Importa**.

   Il certificato viene caricato e validato.

Gestire i certificati

Visualizzare i certificati

È possibile visualizzare informazioni riepilogative per un certificato, che includono l'organizzazione che utilizza il certificato, l'autorità che ha emesso il certificato, il periodo di validità e le impronte digitali (identificatori univoci).

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 **Certificate Management** (Gestione certificati).
2. Selezionare una delle seguenti schede:
   - **Gestione** — Mostra il certificato per il sistema che ospita il proxy dei servizi Web. Un certificato di gestione può essere autofirmato o approvato da un'autorità di certificazione (CA). Consente un accesso sicuro a Unified Manager.
   - **Trusted** — Mostra i certificati a cui Unified Manager può accedere per storage array e altri server remoti, come un server LDAP. I certificati possono essere emessi da un'autorità di certificazione (CA) o autofirmati.
3. Per visualizzare ulteriori informazioni su un certificato, selezionare la relativa riga, selezionare i puntini di sospensione alla fine della riga, quindi fare clic su **Visualizza** o **Esporta**.

Esportare i certificati

È possibile esportare un certificato per visualizzarne i dettagli completi.

Prima di iniziare

Per aprire il file esportato, è necessario disporre di un'applicazione per il visualizzatore dei certificati.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare una delle seguenti schede:
   - **Gestione** — Mostra il certificato per il sistema che ospita il proxy dei servizi Web. Un certificato di gestione può essere autofirmato o approvato da un'autorità di certificazione (CA). Consente un accesso sicuro a Unified Manager.
   - **Trusted** — Mostra i certificati a cui Unified Manager può accedere per storage array e altri server remoti, come un server LDAP. I certificati possono essere emessi da un'autorità di certificazione (CA) o autofirmati.
3. Selezionare un certificato dalla pagina, quindi fare clic sui puntini di sospensione alla fine della riga.
4. Fare clic su **Esporta**, quindi salvare il file del certificato.
5. Aprire il file nell'applicazione di visualizzazione dei certificati.

Gestione degli accessi

Panoramica sulla gestione degli accessi

Access Management è un metodo per configurare l'autenticazione dell'utente in Unified Manager.

Quali metodi di autenticazione sono disponibili?

Sono disponibili i seguenti metodi di autenticazione:

- **Ruoli utente locali** — l'autenticazione viene gestita tramite funzionalità RBAC (role-based access control). I ruoli utente locali includono profili utente predefiniti e ruoli con autorizzazioni di accesso specifiche.
- **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.
- **SAML** — l'autenticazione viene gestita tramite un provider di identità (IdP) utilizzando SAML 2.0.

Scopri di più:

- "Come funziona Access Management"
- "Terminologia per la gestione degli accessi"
- "Autorizzazioni per i ruoli mappati"
- "SAML"

Come si configura Access Management?

Il software SANtricity è preconfigurato per l'utilizzo dei ruoli utente locali. Se si desidera utilizzare LDAP, è possibile configurarlo nella pagina Gestione accessi.

Scopri di più:

- "Gestione degli accessi con ruoli utente locali"
- "Gestione degli accessi con servizi di directory"
- "Configure SAML (Configura SNMP)"

Concetti

Come funziona Access Management

Utilizzare Access Management per stabilire l'autenticazione dell'utente in Unified Manager.

Workflow di configurazione

La configurazione di Access Management funziona come segue:

1. Un amministratore effettua l'accesso a Unified Manager con un profilo utente che include le autorizzazioni di amministratore di sicurezza.

   Per il primo accesso, il nome utente `admin` viene visualizzato automaticamente e non può essere modificato. L' `admin`utente ha accesso completo a tutte le funzioni del sistema. La password deve essere impostata al primo accesso.

2. L'amministratore accede a Access Management nell'interfaccia utente, che include ruoli utente locali preconfigurati. Questi ruoli sono 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. I ruoli utente locali includono utenti 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 associa gli utenti LDAP ai ruoli utente locali.
   - **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 Unified Manager.
5. Gli utenti accedono al sistema inserendo le proprie credenziali. 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 funzioni dell'interfaccia utente.
   - Visualizza il nome utente nel banner superiore.

Funzioni disponibili in Unified Manager

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

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management.

- **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. 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.

Una funzione non disponibile è disattivata o non viene visualizzata nell'interfaccia utente.

Terminologia per la gestione degli accessi

Scopri come si applicano i termini di Access Management a Unified Manager.

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.
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. Unified Manager include 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.
SSO	SSO (Single Sign-on) è un servizio di autenticazione che consente a un set di credenziali di accesso di accedere a più applicazioni.

Termine	Descrizione
Proxy dei servizi Web	Il proxy dei servizi Web, che fornisce l'accesso tramite meccanismi HTTPS standard, consente agli amministratori di configurare i servizi di gestione per gli array di storage. Il proxy può essere installato su host Windows o Linux. L'interfaccia di Unified Manager è disponibile con Web Services Proxy.

Autorizzazioni per i ruoli mappati

Le funzionalità RBAC (role-based access control) includono utenti predefiniti con uno o più ruoli mappati. Ogni ruolo include le autorizzazioni per l'accesso alle attività in Unified Manager.

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

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management.
- **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. 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 funzione, tale funzione non è disponibile per la selezione o non viene visualizzata nell'interfaccia utente.

Gestione degli accessi con ruoli utente locali

Gli amministratori possono utilizzare le funzionalità RBAC (role-based access control) applicate in Unified Manager. Queste funzionalità sono denominate "ruoli utente locali".

Workflow di configurazione

I ruoli utente locali sono preconfigurati nel sistema. Per utilizzare i ruoli utente locali per l'autenticazione, gli amministratori possono:

1. Un amministratore effettua l'accesso a Unified Manager con un profilo utente che include le autorizzazioni di amministratore di sicurezza.

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

2. Un amministratore esamina i profili utente predefiniti e non modificabili.
3. Facoltativamente, 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

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 Unified Manager con un profilo utente che include le autorizzazioni di amministratore di sicurezza.

   L' `admin`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 il sistema host in cui è installato il proxy dei servizi Web.
4. Una volta stabilita la connessione al server, l'amministratore associa i gruppi di utenti ai ruoli utente locali. Questi ruoli sono predefiniti e non possono essere modificati.
5. L'amministratore verifica la connessione tra il server LDAP e il proxy dei servizi Web.
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.
- Modificare le password.
- Impostare una lunghezza minima per le password.
- Consentire agli utenti di effettuare l'accesso senza password.

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 effettua l'accesso a Unified Manager con un profilo utente che include le autorizzazioni Security Admin.

   L' `admin`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 Unified 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 Unified Manager per esportare un file di metadati del provider di servizi per il controller. Dal sistema IdP, l'amministratore importa il 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 Unified 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 Unified 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 dall'interfaccia precedente di Storage Manager.

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

Utilizzare ruoli utente locali

Visualizzare i ruoli utente locali

Dalla scheda Local User Roles (ruoli utente locali), è possibile visualizzare le mappature degli utenti ai ruoli predefiniti. Questi mapping fanno parte del RBAC (role-based access control) applicato nel proxy dei servizi Web per Unified 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.

A proposito di questa attività

Gli utenti e le mappature non possono essere modificati. È possibile modificare solo le password.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **ruoli utente locali**.

   Gli utenti sono mostrati nella tabella:

   - **Admin** — Amministratore eccellente che ha accesso a tutte le funzioni del sistema. Questo utente include tutti i ruoli.
   - **Storage** — l'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor.
   - **Security** — l'utente responsabile della configurazione della sicurezza, inclusi Access Management e Certificate Management. Questo utente include i seguenti ruoli: Security Admin e Monitor.
   - **Support** — l'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support Admin e Monitor.
   - **Monitor** — un utente con accesso in sola lettura al sistema. Questo utente include solo il ruolo Monitor.
   - **rw** (lettura/scrittura) — questo utente include i seguenti ruoli: Amministratore dello storage, amministratore del supporto e monitor.
   - **Ro** (sola lettura) — questo utente include solo il ruolo Monitor.

Modificare le password per i profili utente locali

È possibile modificare le password utente per ciascun 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.

Fasi

1. Selezionare **Access Management**.
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 di controllo per richiedere all'utente di immettere una password per accedere al sistema.
6. Immettere la nuova password per l'utente selezionato nei due campi.
7. Immettere la password dell'amministratore locale per confermare l'operazione, 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. È inoltre possibile consentire agli utenti locali di accedere al sistema 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 al sistema senza immettere una password.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare **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 al sistema *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).

Utilizzare i servizi di directory

Aggiungere il server di directory

Per configurare l'autenticazione per la gestione degli accessi, è necessario stabilire le comunicazioni tra un server LDAP e l'host che esegue il proxy dei servizi Web per Unified Manager. Quindi, associare i gruppi di utenti LDAP ai ruoli utente locali.

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 utente locali.

Fasi

1. Selezionare **Access Management**.
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 del 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 server
Immettere l'URL per accedere 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 il sistema 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, generalmente sotto forma di `CN=Users, DC=cpoc, 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 del campo

Impostazione	Descrizione
Mapping	DN gruppo
Specificare il nome distinto del gruppo (DN) per il gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata ({}) se non fanno parte di un modello di espressione regolare:[]()<>*+-=!?^	
Ruoli	Fare clic nel campo e selezionare uno dei ruoli utente locali da mappare al DN del gruppo. È necessario selezionare singolarmente ciascun ruolo che si desidera includere per questo gruppo. Il ruolo di monitoraggio è necessario in combinazione con gli altri ruoli per accedere a Gestione unificata di SANtricity. I ruoli mappati includono le seguenti autorizzazioni: • **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza. • **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management. • **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. 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.

Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore.

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

Dettagli del campo

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 server
L'URL per accedere al server LDAP sotto forma di `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 il sistema possa comunicare con la configurazione del server LDAP. Il test si verifica dopo aver fatto clic su **Save** (Salva). 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 ignorare il test e modificare nuovamente la configurazione.	**Impostazioni dei privilegi**
Ricerca DN base	Contesto LDAP per la ricerca degli utenti, generalmente sotto forma di `CN=Users, DC=cpoc, 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.

Dettagli del campo

Impostazione	Descrizione
Mapping	DN gruppo
Il nome di dominio del gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata () se non fanno parte di un modello di espressione regolare: []{}()<>*+-=!?^	
Ruoli	I ruoli da mappare al DN del gruppo. È necessario selezionare singolarmente ciascun ruolo che si desidera includere per questo gruppo. Il ruolo di monitoraggio è necessario in combinazione con gli altri ruoli per accedere a Gestione unificata di SANtricity. I ruoli includono: • **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza. • **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management. • **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. 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.

Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore.

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 il proxy dei servizi Web, è possibile rimuovere le informazioni sul server dalla pagina Gestione accessi. 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 **Access Management**.
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. Digitare `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.

Utilizzare SAML

Configure SAML (Configura SNMP)

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.

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 conoscere l'indirizzo IP o il nome di dominio del controller nell'array di storage.
- 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 la sincronizzazione del clock del controller e del server IdP (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 Unified Manager.

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 Unified Manager. Se si disattiva SAML in un secondo momento, la configurazione dei servizi di directory torna alla configurazione precedente.

Modifica e disabilitazione. 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 Unified Manager. Il sistema IdP ha bisogno di questi metadati per reindirizzare le richieste di autenticazione all'URL corretto e per validare le risposte ricevute.

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 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. L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con il controller ed 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 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.

   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 il file di metadati del Service Provider in formato XML esportato.
4. Dal server IdP, importare il file di metadati del provider di servizi per stabilire la relazione di trust. È possibile importare il file direttamente o inserire manualmente le informazioni del controller dal file.

Fase 3: Mappare i ruoli

Per fornire agli utenti l'autorizzazione e l'accesso a Unified 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 Unified Manager.
- Un file di metadati del service provider per il controller viene importato nel sistema IdP per la relazione di trust.

Fasi

1. Fare clic sul collegamento **mapping dei ruoli di Unified 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 del 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. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escape con una barra rovesciata (\) se non fanno parte di un modello di espressione regolare: \.[]{}()<>*+-=!?^$	
Ruoli	Fare clic nel campo e selezionare uno dei ruoli dell'array di storage da mappare all'attributo. È necessario selezionare singolarmente ciascun ruolo da includere. Per accedere a Unified Manager, è necessario il ruolo di monitoraggio in combinazione con gli altri ruoli. Il ruolo Security Admin è richiesto anche per almeno un gruppo. I ruoli mappati includono le seguenti autorizzazioni: • **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.

Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. Unified 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 Unified Manager.
- Un file di metadati del service provider per il 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.
   - L'indirizzo del controller nei file di metadati SP è corretto.

Fase 5: Abilitare SAML

Il passaggio finale consiste nel 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.

Prima di iniziare

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

Modifica e disabilitazione. 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 Conferma abilitazione SAML.

2. Digitare `enable`, quindi fare clic su **Abilita**.
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 ruoli.

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 Unified Manager.

Dettagli del 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. Unified Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

5. Facoltativamente, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.
6. 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 l'array di storage e reimportare il 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 dal controller. L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con il 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 Esporta file provider di servizi.

4. Fare clic su **Export** (Esporta) per salvare il file di metadati nel sistema locale.

   Il campo del nome di dominio è di sola lettura.

   Prendere nota della posizione in cui è memorizzato il file.

5. Dal sistema locale, individuare il file di metadati del Service Provider in formato XML esportato.
6. Dal server IdP, importare il file di metadati del provider di servizi. È possibile importare il file direttamente o inserire manualmente le informazioni del controller.
7. Fare clic su **Chiudi**.

FAQ

Perché non riesco ad accedere?

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

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

- Il nome utente o la password immessi non sono corretti.
- Privilegi insufficienti.
- Si è tentato di accedere più volte senza successo, attivando la modalità di blocco. Attendere 10 minuti per eseguire nuovamente l'accesso.
- L'autenticazione SAML è attivata. Aggiornare il browser per accedere.

Cosa occorre sapere prima di aggiungere un server di directory?

Prima di aggiungere un server di directory in Access Management, è necessario soddisfare determinati 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, rivedere le linee guida.

Le funzionalità RBAC (role-based access control) includono i seguenti ruoli:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management.
- **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. 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.

> Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore.

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.

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.
- Si conosce il valore dell'attributo per il gruppo da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escape con una barra rovesciata (`\`) se non fanno parte di un modello di espressione regolare:

```
\.[]{}()<>*+-=!?^$|
```

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

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 la sincronizzazione del clock del controller e del server IdP (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 Unified Manager.
- Si conosce l'indirizzo IP o il nome di dominio del controller nell'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 sono gli utenti locali?

Gli utenti locali sono predefiniti nel sistema e includono autorizzazioni specifiche.

Gli utenti locali includono:

- **Admin** — Amministratore eccellente che ha accesso a tutte le funzioni del sistema. Questo utente include tutti i ruoli. La password deve essere impostata al primo accesso.
- **Storage** — l'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Security** — l'utente responsabile della configurazione della sicurezza, inclusi Access Management e Certificate Management. Questo utente include i seguenti ruoli: Security Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Support** — l'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Monitor** — un utente con accesso in sola lettura al sistema. Questo utente include solo il ruolo Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **rw** (lettura/scrittura) — questo utente include i seguenti ruoli: Amministratore dello storage, amministratore del supporto e monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Ro** (sola lettura) — questo utente include solo il ruolo Monitor. Questo account viene disattivato fino a quando non viene impostata una password.

Informazioni sul copyright

Informazioni sul marchio commerciale