



Proxy dei servizi Web

E-Series Systems

NetApp
March 22, 2024

Sommario

- Proxy dei servizi Web 1
 - Panoramica dei proxy dei servizi web SANtricity 1
 - Scopri di più sui servizi Web 1
 - Installare e configurare 9
 - Gestire l'accesso degli utenti in Web Services Proxy 20
 - Gestire la sicurezza e i certificati in Web Services Proxy 24
 - Gestire i sistemi storage utilizzando Web Services Proxy 26
 - Gestire il polling automatico per le statistiche del proxy dei servizi Web 32
 - Gestire AutoSupport utilizzando il proxy dei servizi Web 33

Proxy dei servizi Web

Panoramica dei proxy dei servizi web SANtricity

Il proxy dei servizi web SANtricity è un server API RESTful installato separatamente su un sistema host per gestire centinaia di sistemi storage NetApp e-Series nuovi e legacy. Il proxy include Gestore unificato di SANtricity, un'interfaccia basata su web che offre funzioni simili.

Panoramica dell'installazione

L'installazione e la configurazione di Web Services Proxy richiede i seguenti passaggi:

1. ["Verifica dei requisiti di installazione e aggiornamento"](#).
2. ["Scaricare e installare il file proxy dei servizi Web"](#).
3. ["Accedere a API e Unified Manager"](#).
4. ["Configurare il proxy dei servizi Web"](#).

Trova ulteriori informazioni

- Unified Manager — l'installazione del proxy include SANtricity Unified Manager, un'interfaccia basata su web che fornisce l'accesso alla configurazione ai più recenti sistemi storage e-Series ed EF-Series. Per ulteriori informazioni, consultare la guida in linea di Unified Manager, disponibile dalla relativa interfaccia utente o dal ["Sito della documentazione del software SANtricity"](#).
- Repository di GitHub — GitHub contiene un repository per la raccolta e l'organizzazione di script di esempio che illustrano l'utilizzo dell'API dei servizi web di NetApp SANtricity. Per accedere al repository, vedere ["Esempi di NetApp WebServices"](#).
- Representational state transfer (REST) — i servizi web sono un'API RESTful che fornisce l'accesso praticamente a tutte le funzionalità di gestione di SANtricity, in modo da avere familiarità con i concetti REST. Per ulteriori informazioni, vedere ["Stili architetturici e progettazione di architetture software basate su rete"](#).
- JavaScript Object Notation (JSON) — poiché i dati all'interno dei servizi Web sono codificati tramite JSON, dovresti avere familiarità con i concetti di programmazione JSON. Per ulteriori informazioni, vedere ["Presentazione di JSON"](#).

Scopri di più sui servizi Web

Panoramica dei servizi Web e di Unified Manager

Prima di installare e configurare il proxy dei servizi Web, leggere la panoramica dei servizi Web e di Gestione unificata di SANtricity.

Servizi Web

Web Services è un'API (Application Programming Interface) che consente di configurare, gestire e monitorare i sistemi storage NetApp e-Series ed EF-Series. Inviando richieste API, è possibile completare flussi di lavoro come configurazione, provisioning e monitoraggio delle performance per i sistemi storage e-Series.

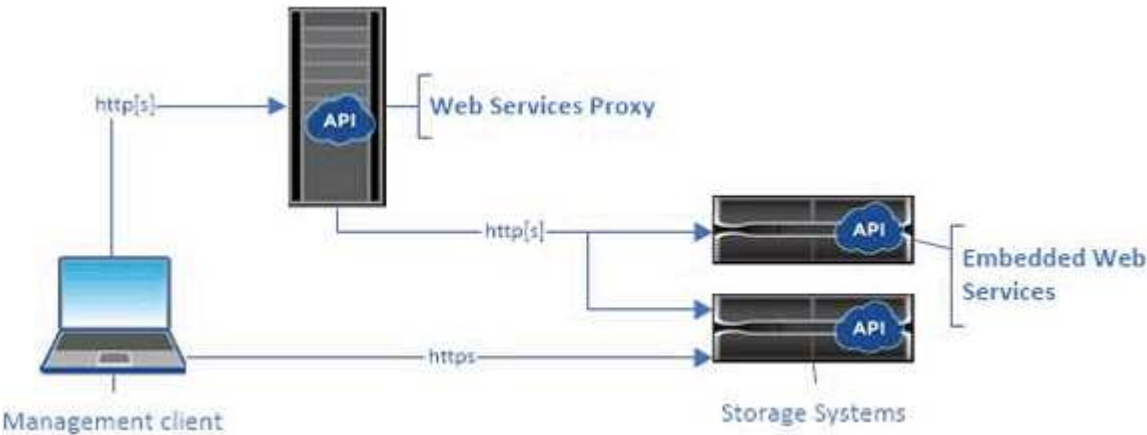
Quando si utilizza l'API dei servizi Web per gestire i sistemi storage, è necessario avere familiarità con quanto segue:

- JavaScript Object Notation (JSON): Poiché i dati all'interno dei servizi Web vengono codificati tramite JSON, è necessario conoscere i concetti di programmazione JSON. Per ulteriori informazioni, vedere ["Presentazione di JSON"](#).
- Representational state transfer (REST): I servizi Web sono un'API RESTful che fornisce accesso a quasi tutte le funzionalità di gestione di SANtricity, per cui dovresti avere familiarità con i concetti REST. Per ulteriori informazioni, vedere ["Stili architetturici e progettazione di architetture software basate su rete"](#).
- Concetti relativi ai linguaggi di programmazione: Java e Python sono i linguaggi di programmazione più comuni utilizzati con l'API dei servizi Web, ma qualsiasi linguaggio di programmazione in grado di effettuare richieste HTTP è sufficiente per l'interazione con l'API.

I servizi Web sono disponibili in due implementazioni:

- **Incorporato** — Un server API RESTful è incorporato in ciascun controller di un sistema storage E2800/EF280 con NetApp SANtricity 11.30 o versioni successive, E5700/EF570 con SANtricity 11.40 o versioni successive e EF300 o EF600 con SANtricity 11.60 o versioni successive. Non è richiesta alcuna installazione.
- **Proxy** — il proxy dei servizi web SANtricity è un server API RESTful installato separatamente su un server Windows o Linux. Questa applicazione basata su host è in grado di gestire centinaia di sistemi storage NetApp e-Series nuovi e legacy. In generale, è necessario utilizzare il proxy per le reti con più di 10 sistemi di storage. Il proxy è in grado di gestire numerose richieste in modo più efficiente rispetto all'API incorporata.

Il nucleo dell'API è disponibile in entrambe le implementazioni.



La seguente tabella fornisce un confronto tra il proxy e la versione integrata.

Considerazione	Proxy	Integrato
Installazione	Richiede un sistema host (Linux o Windows). Il proxy è disponibile per il download all'indirizzo "Sito di supporto NetApp" o su "DockerHub" .	Non è richiesta alcuna installazione o abilitazione.

Considerazione	Proxy	Integrato
Sicurezza	<p>Impostazioni di sicurezza minime per impostazione predefinita.</p> <p>Le impostazioni di sicurezza sono basse, in modo che gli sviluppatori possano iniziare a utilizzare l'API in modo rapido e semplice. Se lo si desidera, è possibile configurare il proxy con lo stesso profilo di protezione della versione integrata.</p>	<p>Impostazioni di protezione elevate per impostazione predefinita.</p> <p>Le impostazioni di sicurezza sono elevate perché l'API viene eseguita direttamente sui controller. Ad esempio, non consente l'accesso HTTP e disattiva tutti i protocolli di crittografia SSL e TLS precedenti per HTTPS.</p>
Gestione centrale	Gestisce tutti i sistemi storage da un unico server.	Gestisce solo il controller su cui è incorporato.

Unified Manager

Il pacchetto di installazione del proxy include Unified Manager, un'interfaccia basata su web che fornisce l'accesso alla configurazione ai più recenti sistemi storage e-Series ed EF-Series, come E2800, E5700, EF300 ed EF600.



Da Unified Manager, è possibile eseguire le seguenti operazioni batch:

- Visualizzare lo stato di più sistemi storage da una vista centrale
- Scoprire più sistemi storage nella tua rete
- Importa le impostazioni da un sistema storage a più sistemi
- Aggiornare il firmware per più sistemi storage

Compatibilità e limitazioni

L'utilizzo del proxy dei servizi Web è soggetto alle seguenti limitazioni e compatibilità.

Considerazione	Compatibilità o restrizione
Supporto HTTP	Il proxy dei servizi Web consente l'utilizzo di HTTP o HTTPS. (La versione integrata dei servizi Web richiede HTTPS per motivi di sicurezza).
Sistemi storage e firmware	Il proxy dei servizi Web è in grado di gestire tutti i sistemi storage e-Series, tra cui una combinazione di sistemi meno recenti e gli ultimi E2800, EF280, E5700, EF570, EF300, E sistemi della serie EF600.

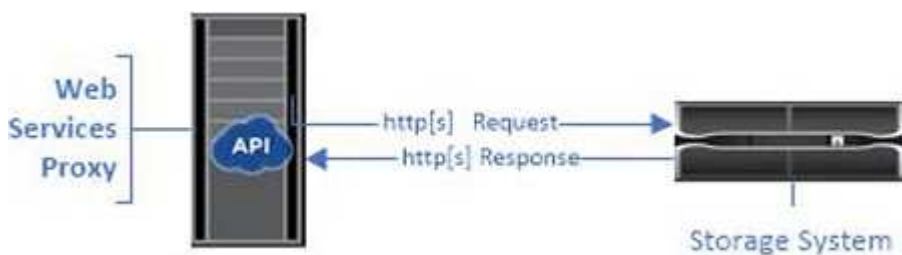
Considerazione	Compatibilità o restrizione
Supporto IP	<p>Il proxy dei servizi Web supporta il protocollo IPv4 o IPv6.</p> <div>  <p>Il protocollo IPv6 potrebbe non funzionare quando il proxy dei servizi Web tenta di rilevare automaticamente l'indirizzo di gestione dalla configurazione del controller. Le possibili cause dell'errore includono problemi durante l'inoltro dell'indirizzo IP o l'attivazione di IPv6 sui sistemi storage ma non sul server.</p> </div>
NVSRAM file name limits	<p>Il proxy dei servizi Web utilizza i nomi dei file NVSRAM per identificare accuratamente le informazioni sulla versione. Pertanto, non è possibile modificare i nomi dei file NVSRAM quando vengono utilizzati con il proxy dei servizi Web. Il proxy dei servizi Web potrebbe non riconoscere un file NVSRAM rinominato come file firmware valido.</p>
Web di Symbol	<p>Symbol Web è un URL nell'API REST. Consente di accedere a quasi tutte le chiamate Symbol. La funzione Symbol fa parte del seguente URL:</p> <pre>http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function</pre> <div>  <p>I sistemi storage disabilitati da Symbol sono supportati tramite il proxy dei servizi Web.</p> </div>

Nozioni di base sulle API

Nell'API dei servizi Web, le comunicazioni HTTP implicano un ciclo di richiesta-risposta.

Elementi URL nelle richieste

Indipendentemente dal linguaggio di programmazione o dallo strumento utilizzato, ogni chiamata all'API dei servizi Web ha una struttura simile, con un URL, un verbo HTTP e un'intestazione Accept.



Tutte le richieste includono un URL, come nell'esempio seguente, e contengono gli elementi descritti nella tabella.

`https://webservices.name.com:8443/devmgr/v2/storage-systems`

Area	Descrizione
Trasporto HTTP <code>https://</code>	<p>Il proxy dei servizi Web attiva l'utilizzo di HTTP o HTTPS.</p> <p>I servizi Web incorporati richiedono HTTPS per motivi di sicurezza.</p>
URL di base e porta <code>webservices.name.com:8443</code>	<p>Ogni richiesta deve essere instradata correttamente a un'istanza attiva dei servizi Web. È richiesto l'FQDN (Fully Qualified Domain Name) o l'indirizzo IP dell'istanza, insieme alla porta di ascolto. Per impostazione predefinita, i servizi Web comunicano tramite la porta 8080 (per HTTP) e la porta 8443 (per HTTPS).</p> <p>Per il proxy dei servizi Web, è possibile modificare entrambe le porte durante l'installazione del proxy o nel file <code>wsconfig.xml</code>. Il conflitto di porte è comune negli host del data center che eseguono varie applicazioni di gestione.</p> <p>Per i servizi Web incorporati, la porta sul controller non può essere modificata; per impostazione predefinita, la porta 8443 consente connessioni sicure.</p>
Percorso API <code>devmgr/v2/storage-systems</code>	<p>Viene inviata una richiesta a una risorsa REST o a un endpoint specifico all'interno dell'API dei servizi Web. La maggior parte degli endpoint è sotto forma di:</p> <p><code>devmgr/v2/<resource>/[id]</code></p> <p>Il percorso API è costituito da tre parti:</p> <ul style="list-style-type: none">• <code>devmgr</code> (Device Manager) è lo spazio dei nomi dell'API dei servizi Web.• <code>v2</code> Indica la versione dell'API a cui si accede. È anche possibile utilizzare <code>utils</code> per accedere agli endpoint di login.• <code>storage-systems</code> è una categoria all'interno della documentazione.

Verbi HTTP supportati

I verbi HTTP supportati includono GET, POST ed DELETE:

- Le richieste GET vengono utilizzate per le richieste di sola lettura.
- Le richieste POST vengono utilizzate per creare e aggiornare oggetti e anche per le richieste di lettura che potrebbero avere implicazioni sulla sicurezza.
- Le richieste DI ELIMINAZIONE vengono in genere utilizzate per rimuovere un oggetto dalla gestione, rimuovere completamente un oggetto o ripristinare lo stato dell'oggetto.



Attualmente, l'API dei servizi Web non supporta PUT o PATCH. È invece possibile utilizzare POST per fornire le funzionalità tipiche di questi verbi.

Accettare le intestazioni

Quando si restituisce un corpo della richiesta, i servizi Web restituiscono i dati in formato JSON (se non diversamente specificato). Alcuni client richiedono per impostazione predefinita "text/html" o qualcosa di simile. In questi casi, l'API risponde con un codice HTTP 406, che indica che non è in grado di fornire dati in questo formato. Come Best practice, devi definire l'intestazione Accept come "application/json" per tutti i casi in cui ti aspetti che JSON sia il tipo di risposta. In altri casi in cui un corpo di risposta non viene restituito (ad esempio, DELETE), la fornitura dell'intestazione Accept non causa effetti indesiderati.

Risposte

Quando viene effettuata una richiesta all'API, una risposta restituisce due informazioni critiche:

- Codice di stato HTTP — indica se la richiesta ha avuto esito positivo.
- Corpo di risposta opzionale - di solito fornisce un corpo JSON che rappresenta lo stato della risorsa o di un corpo fornendo maggiori dettagli sulla natura di un guasto.

È necessario controllare il codice di stato e l'intestazione del tipo di contenuto per determinare l'aspetto del corpo della risposta risultante. Per i codici di stato HTTP 200-203 e 422, Web Services restituisce un corpo JSON con la risposta. Per altri codici di stato HTTP, i servizi Web generalmente non restituiscono un corpo JSON aggiuntivo, perché la specifica non lo consente (204) o perché lo stato è intuitivo. La tabella elenca i codici e le definizioni di stato HTTP comuni. Indica inoltre se le informazioni associate a ciascun codice HTTP vengono restituite in un corpo JSON.

Codice di stato HTTP	Descrizione	Corpo JSON
200 OK	Indica una risposta corretta.	Sì
201 creato	Indica che è stato creato un oggetto. Questo codice viene utilizzato in alcuni rari casi invece dello stato 200.	Sì
202 accettato	Indica che la richiesta è accettata per l'elaborazione come richiesta asincrona, ma è necessario effettuare una richiesta successiva per ottenere il risultato effettivo.	Sì

Codice di stato HTTP	Descrizione	Corpo JSON
203 informazioni non autorevoli	Simile a una risposta 200, ma i servizi Web non possono garantire che i dati siano aggiornati (ad esempio, al momento sono disponibili solo i dati memorizzati nella cache).	Sì
204 Nessun contenuto	Indica un'operazione riuscita, ma non esiste alcun corpo di risposta.	No
400 richiesta errata	Indica che il corpo JSON fornito nella richiesta non è valido.	No
401 non autorizzato	Indica che si è verificato un errore di autenticazione. Non sono state fornite credenziali oppure il nome utente o la password non sono validi.	No
403 proibita	Errore di autorizzazione, che indica che l'utente autenticato non dispone dell'autorizzazione per accedere all'endpoint richiesto.	No
404 non trovato	Indica che non è stato possibile individuare la risorsa richiesta. Questo codice è valido per API inesistenti o risorse inesistenti richieste dall'identificatore.	No
422 entità non elaborabile	Indica che la richiesta è generalmente ben formata, ma i parametri di input non sono validi oppure lo stato del sistema di storage non consente ai servizi Web di soddisfare la richiesta.	Sì
424 dipendenza non riuscita	Utilizzato in Web Services Proxy per indicare che il sistema di storage richiesto non è attualmente accessibile. Pertanto, i servizi Web non possono soddisfare la richiesta.	No
429 troppe richieste	Indica che è stato superato un limite di richiesta e che è necessario eseguire un nuovo processo in un secondo momento.	No

Script di esempio

GitHub contiene un repository per la raccolta e l'organizzazione di script di esempio che illustrano l'utilizzo dell'API dei servizi web NetApp SANtricity. Per accedere al repository, vedere ["Esempi di NetApp WebServices"](#).

Termini e concetti

I seguenti termini si applicano al proxy dei servizi Web.

Termine	Definizione
API	Un'API (Application Programming Interface) è un insieme di protocolli e metodi che consentono agli sviluppatori di comunicare con i dispositivi. L'API dei servizi Web viene utilizzata per comunicare con i sistemi storage e-Series.
ASUP	La funzione ASUP (AutoSupport) raccoglie i dati in un bundle di assistenza clienti e invia automaticamente il file di messaggio al supporto tecnico per la risoluzione dei problemi e l'analisi dei problemi in remoto.
Endpoint	Gli endpoint sono funzioni disponibili attraverso l'API. Un endpoint include un verbo HTTP e il percorso URI. Nei servizi Web, gli endpoint possono eseguire attività come il rilevamento di sistemi storage e la creazione di volumi.
Verbo HTTP	Un verbo HTTP è un'azione corrispondente per un endpoint, ad esempio il recupero e la creazione di dati. Nei servizi Web, i verbi HTTP includono POST, GET ed DELETE.
JSON	JavaScript Object Notation (JSON) è un formato di dati strutturato molto simile a XML, che utilizza un formato minimo e leggibile. I dati all'interno dei servizi Web vengono codificati tramite JSON.

Termine	Definizione
RIPOSO/riposo	<p>REST (Representational state Transfer) è una specifica separata che definisce uno stile architettonico per un'API. Poiché la maggior parte delle API REST non rispetta completamente la specifica, vengono descritte come "reSTful" o "reST-like". In genere, un'API "reSTful" è indipendente dai linguaggi di programmazione e presenta le seguenti caratteristiche:</p> <ul style="list-style-type: none"> • Basato su HTTP, che segue la semantica generale del protocollo • Produttore e consumatore di dati strutturati (JSON, XML, ecc.) • Orientato a oggetti (invece che orientato alle operazioni) <p>I servizi Web sono un'API RESTful che fornisce l'accesso a quasi tutte le funzionalità di gestione di SANtricity.</p>
sistema storage	Un sistema storage è un array e-Series, che include shelf, controller, dischi, software, e firmware.
API di Symbol	Symbol è un'API legacy per la gestione dei sistemi storage e-Series. L'implementazione sottostante dell'API dei servizi Web utilizza Symbol.
Servizi Web	I servizi Web sono API progettate da NetApp per consentire agli sviluppatori di gestire i sistemi storage e-Series. Esistono due implementazioni dei servizi Web: Incorporato nel controller e un proxy separato che può essere installato su Linux o Windows.

Installare e configurare

Verifica dei requisiti di installazione e aggiornamento

Prima di installare Web Services Proxy, esaminare i requisiti di installazione e le considerazioni sull'aggiornamento.

Requisiti di installazione

È possibile installare e configurare il proxy dei servizi Web su un sistema host Windows o Linux.

L'installazione del proxy include i seguenti requisiti.

Requisito	Descrizione
Limitazioni del nome host	Assicurarsi che il nome host del server in cui si desidera installare il proxy dei servizi Web contenga solo lettere ASCII, cifre numeriche e trattini (-). Questo requisito è dovuto a un limite di Java Keytool, utilizzato per generare un certificato autofirmato per il server. Se il nome host del server contiene altri caratteri, ad esempio un carattere di sottolineatura (_), il server Web non verrà avviato dopo l'installazione.
Sistemi operativi	<p>È possibile installare il proxy sui seguenti sistemi operativi:</p> <ul style="list-style-type: none"> • Linux • Windows <p>Per un elenco completo dei sistemi operativi e della compatibilità del firmware, consultare "Tool di matrice di interoperabilità NetApp".</p>
Linux: Considerazioni aggiuntive	Le librerie di base standard Linux (init-functions) sono necessarie per il corretto funzionamento del server Web. È necessario installare i pacchetti lsb/insserv per il sistema operativo in uso. Per ulteriori informazioni, consultare la sezione "pacchetti aggiuntivi richiesti" del file Readme.
Istanze multiple	È possibile installare solo un'istanza di Web Services Proxy su un server; tuttavia, è possibile installare il proxy su più server all'interno della rete.
Pianificazione della capacità	<p>Il proxy dei servizi Web richiede uno spazio adeguato per la registrazione. Assicurarsi che il sistema soddisfi i seguenti requisiti di spazio disponibile su disco:</p> <ul style="list-style-type: none"> • Spazio di installazione richiesto — 275 MB • Spazio minimo di registrazione — 200 MB • Memoria di sistema — 2 GB; lo spazio di heap è di 1 GB per impostazione predefinita <p>È possibile utilizzare uno strumento di monitoraggio dello spazio su disco per verificare lo spazio disponibile su disco per lo storage persistente e la registrazione.</p>
Licenza	Web Services Proxy è un prodotto standalone gratuito che non richiede una chiave di licenza. Tuttavia, si applicano i copyright e i termini del servizio applicabili. Se si installa il proxy in modalità grafica o console, è necessario accettare il Contratto di licenza con l'utente finale (EULA).

Considerazioni sull'upgrade

Se si esegue l'aggiornamento da una versione precedente, tenere presente che alcuni elementi vengono

conservati o rimossi.

- Per il proxy dei servizi Web, le impostazioni di configurazione precedenti vengono conservate. Queste impostazioni includono password utente, tutti i sistemi di storage rilevati, certificati server, certificati attendibili e configurazione del runtime del server.
- Per Unified Manager, tutti i file SANtricity OS precedentemente caricati nel repository vengono rimossi durante l'aggiornamento.

Installare o aggiornare il file proxy dei servizi Web

L'installazione comporta il download del file e l'installazione del pacchetto proxy su un server Linux o Windows. È inoltre possibile aggiornare il proxy seguendo queste istruzioni.

Scaricare i file proxy dei servizi Web

È possibile scaricare il file di installazione e il file Leggimi dalla pagina di download del software del sito del supporto NetApp.

Il pacchetto di download include Web Services Proxy e l'interfaccia di Unified Manager.

Fasi

1. Passare a ["Supporto NetApp - Download"](#).
2. Selezionare **Proxy servizi web e-Series SANtricity**.
3. Seguire le istruzioni per scaricare il file. Assicurarsi di selezionare il pacchetto di download corretto per il server (ad esempio, EXE per Windows; BIN o RPM per Linux).
4. Scaricare il file di installazione sul server in cui si desidera installare il proxy e Unified Manager.

Installazione su server Windows o Linux

È possibile installare Web Services Proxy e Unified Manager utilizzando una delle tre modalità (grafica, console o silenzioso) oppure utilizzando un file RPM (solo Linux).

Prima di iniziare

- ["Esaminare i requisiti di installazione"](#).
- Assicurarsi di aver scaricato il file di installazione corretto (EXE per Windows; BIN per Linux) sul server in cui si desidera installare il proxy e Unified Manager.

Installazione in modalità grafica

È possibile eseguire l'installazione in modalità grafica per Windows o Linux. In modalità grafica, i prompt vengono visualizzati in un'interfaccia di tipo Windows.

Fasi

1. Accedere alla cartella in cui è stato scaricato il file di installazione.
2. Avviare l'installazione per Windows o Linux, come indicato di seguito:
 - Windows — fare doppio clic sul file di installazione:

```
santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe
```

- Linux — eseguire il seguente comando: `santricity_webservices-linux_x64-nn.nn.nn.nnnn.bin`

Nei nomi dei file sopra indicati, `nn.nn.nn.nnnn` rappresenta il numero di versione.

Il processo di installazione viene avviato e viene visualizzata la schermata iniziale del proxy dei servizi Web NetApp SANtricity + Gestore unificato.

3. Seguire le istruzioni a schermo.

Durante l'installazione, viene richiesto di attivare diverse funzioni e di inserire alcuni parametri di configurazione. Se necessario, è possibile modificare una di queste selezioni in un secondo momento nei file di configurazione.



Durante un aggiornamento, non vengono richiesti i parametri di configurazione.

4. Quando viene visualizzato il messaggio Webserver Started (Server Web avviato), fare clic su **OK** per completare l'installazione.

Viene visualizzata la finestra di dialogo Installazione completata.

5. Fare clic sulle caselle di controllo se si desidera avviare Unified Manager o la documentazione API interattiva, quindi fare clic su **fine**.

Installazione in modalità console

È possibile eseguire l'installazione in modalità Console per Windows o Linux. In modalità Console, i prompt vengono visualizzati nella finestra del terminale.

Fasi

1. Eseguire il seguente comando: `<install filename> -i console`

Nel comando precedente, `<install filename>` rappresenta il nome del file di installazione del proxy scaricato (ad esempio: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).



Per annullare l'installazione in qualsiasi momento durante il processo di installazione, digitare `QUIT` al prompt dei comandi.

Viene avviato il processo di installazione e viene visualizzato il messaggio Avvio del programma di installazione — Introduzione.

2. Seguire le istruzioni a schermo.

Durante l'installazione, viene richiesto di attivare diverse funzioni e di inserire alcuni parametri di configurazione. Se necessario, è possibile modificare una di queste selezioni in un secondo momento nei file di configurazione.



Durante un aggiornamento, non vengono richiesti i parametri di configurazione.

3. Una volta completata l'installazione, premere **Invio** per uscire dal programma di installazione.

Installazione in modalità silenziosa

È possibile eseguire l'installazione in modalità silenziosa per Windows o Linux. In modalità silenziosa, nella finestra del terminale non vengono visualizzati messaggi o script di ritorno.

Fasi

1. Eseguire il seguente comando: `<install filename> -i silent`

Nel comando precedente, `<install filename>` rappresenta il nome del file di installazione del proxy scaricato (ad esempio: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

2. Premere **Invio**.

Il completamento del processo di installazione può richiedere alcuni minuti. Una volta completata l'installazione, viene visualizzato un prompt dei comandi nella finestra del terminale.

Installazione del comando RPM (solo Linux)

Per i sistemi Linux compatibili con il sistema di gestione dei pacchetti RPM, è possibile installare il proxy dei servizi Web utilizzando un file RPM opzionale.

Fasi

1. Scaricare il file RPM sul server in cui si desidera installare il proxy e Unified Manager.
2. Aprire una finestra terminale.
3. Immettere il seguente comando:

```
rpm -u santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
```



Nel comando precedente, `nn.nn.nn.nnnn` rappresenta il numero di versione.

Il completamento del processo di installazione può richiedere alcuni minuti. Una volta completata l'installazione, viene visualizzato un prompt dei comandi nella finestra del terminale.

Accedere a API e Unified Manager

I servizi Web includono la documentazione API, che consente di interagire direttamente con L'API REST. Include inoltre Unified Manager, un'interfaccia basata su browser per la gestione di più sistemi storage e-Series.

Accedere all'API dei servizi Web

Dopo aver installato Web Services Proxy, è possibile accedere alla documentazione API interattiva in un browser.

La documentazione API viene eseguita con ogni istanza dei servizi Web ed è disponibile anche in formato PDF statico dal sito del supporto NetApp. Per accedere alla versione interattiva, aprire un browser e immettere l'URL che indica la posizione dei servizi Web (un controller per la versione incorporata o un server per il proxy).



L'API dei servizi Web implementa la specifica OpenAPI (originariamente chiamata specifica Swagger).

Per l'accesso iniziale, utilizzare le credenziali "admin". "Admin" è considerato un super amministratore con accesso a tutte le funzioni e i ruoli.

Fasi

1. Aprire un browser.
2. Inserire l'URL per l'implementazione del proxy o incorporato:

◦ Integrato: `https://<controller>:<port>/devmgr/docs/`

In questo URL, `<controller>` È l'indirizzo IP o FQDN del controller, e. `<port>` è il numero della porta di gestione del controller (il valore predefinito è 8443).

◦ Proxy: `http[s]://<server>:<port>/devmgr/docs/`

In questo URL, `<server>` È l'indirizzo IP o FQDN del server in cui è installato il proxy, e. `<port>` È il numero della porta di ascolto (il valore predefinito è 8080 per HTTP o 8443 per HTTPS).




Se la porta di ascolto è già in uso, il proxy rileva il conflitto e richiede di scegliere un'altra porta di ascolto.

La documentazione API viene aperta nel browser.

3. Una volta aperta la documentazione API interattiva, accedere al menu a discesa in alto a destra della pagina e selezionare **utils**.
4. Fare clic sulla categoria **Login** per visualizzare gli endpoint disponibili.
5. Fare clic sull'endpoint **POST: /Login**, quindi fare clic su **Provalo**.
6. Per il primo accesso, immettere admin come nome utente e password.
7. Fare clic su **Execute** (Esegui).
8. Per accedere agli endpoint per la gestione dello storage, andare al menu a discesa in alto a destra e selezionare **v2**.

Vengono visualizzate le categorie di alto livello per gli endpoint. È possibile esplorare la documentazione API come descritto nella tabella.

Area	Descrizione
Menu a discesa	<p>Nella parte superiore destra della pagina, un menu a discesa fornisce le opzioni per passare dalla versione 2 della documentazione API (V2), all'interfaccia dei simboli (Symbol V2) e alle utility API (utils) per l'accesso.</p> <div><p>Poiché la versione 1 della documentazione API era una versione preliminare e generalmente non disponibile, V1 non è incluso nel menu a discesa.</p></div>

Area	Descrizione
Categorie	La documentazione API è organizzata in base a categorie di alto livello (ad esempio, amministrazione, configurazione). Fare clic su una categoria per visualizzare gli endpoint correlati.
Endpoint	Selezionare un endpoint per visualizzare i percorsi URL, i parametri richiesti, i corpi di risposta e i codici di stato che gli URL potrebbero restituire.
Provalo	<p>Interagire direttamente con l'endpoint facendo clic su Provalo. Questo pulsante viene fornito in ciascuna vista espansa per gli endpoint.</p> <p>Quando si fa clic sul pulsante, vengono visualizzati i campi per l'immissione dei parametri (se applicabile). Immettere i valori e fare clic su Esegui.</p> <p>La documentazione interattiva utilizza JavaScript per inviare la richiesta direttamente all'API; non si tratta di una richiesta di test.</p>

Accedere a Unified Manager

Dopo aver installato Web Services Proxy, è possibile accedere a Unified Manager per gestire più sistemi storage in un'interfaccia basata su web.

Per accedere a Unified Manager, aprire un browser e immettere l'URL che indica la posizione in cui è installato il proxy. Sono supportati i seguenti browser e versioni.

Browser	Versione minima
Google Chrome	79
Microsoft Internet Explorer	11
Microsoft Edge	79
Mozilla Firefox	70
Safari	12

Fasi

1. Aprire un browser e immettere il seguente URL:

```
http[s]://<server>:<port>/um
```

In questo URL, <server> Rappresenta l'indirizzo IP o FQDN del server in cui è installato Web Services

Proxy, e. `<port>` Rappresenta il numero della porta di ascolto (il valore predefinito è 8080 per HTTP o 8443 per HTTPS).

Viene visualizzata la pagina di accesso a Unified Manager.

2. Per il primo accesso, immettere `admin` specificare il nome utente, quindi impostare e confermare una password per l'utente amministratore.

La password può contenere fino a 30 caratteri. Per ulteriori informazioni su utenti e password, consultare la sezione Gestione degli accessi della guida in linea di Unified Manager.

Configurare il proxy dei servizi Web

È possibile modificare le impostazioni di Web Services Proxy per soddisfare i requisiti operativi e di performance specifici per il proprio ambiente.

Arrestare o riavviare il server Web

Il servizio Webserver viene avviato durante l'installazione e viene eseguito in background. Durante alcune attività di configurazione, potrebbe essere necessario arrestare o riavviare il servizio Webserver.

Fasi

1. Effettuare una delle seguenti operazioni:

- Per Windows, accedere al menu **Avvio**, selezionare **Strumenti di amministrazione** > **servizi**, individuare **servizi Web NetApp SANtricity** e selezionare **Interrompi** o **Riavvia**.
- Per Linux, scegliere il metodo per arrestare e riavviare il server Web per la versione del sistema operativo in uso. Durante l'installazione, una finestra di dialogo a comparsa indica quale demone è stato avviato. Ad esempio:

```
web_services_proxy webserver installed and started. You can interact with it
using systemctl start|stop|restart|status web_services_proxy.service
```

Il metodo più comune per interagire con il servizio è l'utilizzo di `systemctl` comandi.

Risolvere i conflitti di porta

Se il proxy dei servizi Web è in esecuzione mentre un'altra applicazione è disponibile all'indirizzo o alla porta definiti, è possibile risolvere il conflitto di porte nel file `wsconfig.xml`.

Fasi

1. Aprire il file `wsconfig.xml` all'indirizzo:
 - (Windows) — `C:/Program Files/NetApp/SANtricity Web Services Proxy`
 - (Linux) — `/opt/netapp/santricity_web_Services_proxy`
2. Aggiungere la seguente riga al file `wsconfig.xml`, in cui `n` è il numero della porta:

```
<sslport clientauth="request">*n*</sslport>
<port>n</port>
```

La tabella seguente mostra gli attributi che controllano le porte HTTP e le porte HTTPS.

Nome	Descrizione	Nodo padre	Attributi	Obbligatorio
config	Il nodo root per la configurazione	Nulla	Versione - la versione dello schema di configurazione è attualmente 1.0.	Sì
slport	La porta TCP in attesa delle richieste SSL. Il valore predefinito è 8443.	config	Clientauth	No
porta	La porta TCP in attesa della richiesta HTTP, per impostazione predefinita, è 8080.	config	-	No

3. Salvare e chiudere il file.

4. Riavviare il servizio Webserver in modo che la modifica abbia effetto.

Configurare il bilanciamento del carico e/o l'alta disponibilità

Per utilizzare il proxy dei servizi Web in una configurazione ad alta disponibilità (ha), è possibile configurare il bilanciamento del carico. In una configurazione ha, in genere, un singolo nodo riceve tutte le richieste mentre le altre sono in stand-by oppure le richieste sono bilanciate in base al carico su tutti i nodi.

Il proxy dei servizi Web può esistere in un ambiente ad alta disponibilità (ha), con la maggior parte delle API che funzionano correttamente indipendentemente dal destinatario della richiesta. I tag e le cartelle dei metadati sono due eccezioni, perché i tag e le cartelle vengono memorizzati in un database locale e non vengono condivisi tra le istanze di Web Services Proxy.

Tuttavia, in una piccola percentuale di richieste si verificano alcuni problemi di tempistica noti. In particolare, un'istanza del proxy può avere dati più recenti più velocemente di una seconda istanza per una piccola finestra. Il proxy dei servizi Web include una configurazione speciale che elimina questo problema di tempistica. Questa opzione non è attivata per impostazione predefinita, perché aumenta il tempo necessario per le richieste di servizio (per la coerenza dei dati). Per attivare questa opzione, è necessario aggiungere una proprietà a un file .INI (per Windows) o .SH (per Linux).

Fasi

1. Effettuare una delle seguenti operazioni:

- Windows: Aprire il file appserver64.ini, quindi aggiungere `Dload-balance.enabled=true` proprietà.

Ad esempio: `vmarg.7=-Dload-balance.enabled=true`

- Linux: Aprire il file webserver.sh, quindi aggiungere `Dload-balance.enabled=true` proprietà.

Ad esempio: `DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`

2. Salvare le modifiche.
3. Riavviare il servizio Webserver in modo che la modifica abbia effetto.

Disattiva il simbolo HTTPS

È possibile disattivare i comandi dei simboli (impostazione predefinita) e inviare comandi tramite una chiamata di procedura remota (RPC). Questa impostazione può essere modificata nel file `wsconfig.xml`.

Per impostazione predefinita, il proxy dei servizi Web invia i comandi dei simboli tramite HTTPS per tutti i sistemi storage della serie E2800 e E5700 con SANtricity OS versione 08.40 o successiva. I comandi Symbol inviati tramite HTTPS vengono autenticati nel sistema di storage. Se necessario, è possibile disattivare il supporto dei simboli HTTPS e inviare comandi tramite RPC. Ogni volta che viene configurato Symbol over RPC, tutti i comandi passivi al sistema di storage vengono abilitati senza autenticazione.



Quando viene utilizzato Symbol over RPC, il proxy dei servizi Web non può connettersi ai sistemi con la porta di gestione dei simboli disattivata.

Fasi

1. Aprire il file `wsconfig.xml` all'indirizzo:
 - (Windows) — `C:/Program Files/NetApp/SANtricity Web Services Proxy`
 - (Linux) — `/opt/netapp/santricity_web_Services_proxy`
2. In `devicemgt.symbolclientstrategy` sostituire `httpsPreferred` valore con `rpcOnly`.

Ad esempio:

```
<env key="devicemgt.symbolclientstrategy">rpcOnly</env>
```

3. Salvare il file.

Configurare la condivisione delle risorse tra origini

È possibile configurare la condivisione delle risorse tra origini (CORS), un meccanismo che utilizza intestazioni HTTP aggiuntive per fornire un'applicazione Web in esecuzione su un'origine per avere l'autorizzazione ad accedere a risorse selezionate da un server di origine diversa.

Il CORS viene gestito dal file `cors.cfg` che si trova nella directory di lavoro. La configurazione CORS è aperta per impostazione predefinita, pertanto l'accesso tra domini non è limitato.

Se non è presente alcun file di configurazione, CORS è aperto. Ma se il file `cors.cfg` è presente, viene utilizzato. Se il file `cors.cfg` è vuoto, non è possibile effettuare una richiesta CORS.

Fasi

1. Aprire il file `cors.cfg` che si trova nella directory di lavoro.
2. Aggiungere le righe desiderate al file.

Ogni riga nel file di configurazione CORS è un modello di espressione regolare da abbinare. L'intestazione di origine deve corrispondere a una riga nel file `cors.cfg`. Se un modello di riga corrisponde all'intestazione di origine, la richiesta è consentita. Viene confrontata l'origine completa, non solo l'elemento host.

3. Salvare il file.

Le richieste vengono associate sull'host e in base al protocollo, ad esempio:

- Associare localhost a qualsiasi protocollo — `*localhost*`
- Corrispondenza localhost solo per HTTPS — `https://localhost*`

Disinstallare il proxy dei servizi Web

Per rimuovere Web Services Proxy e Unified Manager, è possibile utilizzare qualsiasi modalità (file grafico, console, silenzioso o RPM), indipendentemente dal metodo utilizzato per installare il proxy.

Disinstallazione della modalità grafica

È possibile eseguire la disinstallazione in modalità grafica per Windows o Linux. In modalità grafica, i prompt vengono visualizzati in un'interfaccia di tipo Windows.

Fasi

1. Avviare la disinstallazione per Windows o Linux, come indicato di seguito:

- Windows — accedere alla directory che contiene il file di disinstallazione `uninstall_web_Services_proxy`. La directory predefinita si trova nel seguente percorso: `C:/Program Files/NetApp/SANtricity Web Services Proxy/`. Fare doppio clic `uninstall_web_services_proxy.exe`.



In alternativa, è possibile accedere a **pannello di controllo > programmi > Disinstalla un programma**, quindi selezionare "Proxy dei servizi web NetApp SANtricity".

- Linux — accedere alla directory che contiene il file di disinstallazione di Web Services Proxy. La directory predefinita si trova nella seguente posizione:
`/opt/netapp/santricity_web_services_proxy/uninstall_web_services_proxy`

2. Eseguire il seguente comando:

```
uninstall_web_services_proxy -i gui
```

Viene visualizzata la schermata iniziale del proxy dei servizi Web di SANtricity.

3. Nella finestra di dialogo Disinstalla, fare clic su **Disinstalla**.

Viene visualizzata la barra di avanzamento del programma di disinstallazione che mostra lo stato di avanzamento.

4. Quando viene visualizzato il messaggio Uninstall complete (disinstallazione completata), fare clic su **Done** (fine).

Disinstallazione della modalità console

È possibile eseguire la disinstallazione in modalità Console per Windows o Linux. In modalità Console, i prompt vengono visualizzati nella finestra del terminale.

Fasi

1. Accedere alla directory `uninstall_web_Services_proxy`.
2. Eseguire il seguente comando:

```
uninstall_web_services_proxy -i console
```

Viene avviato il processo di disinstallazione.

3. Una volta completata la disinstallazione, premere **Invio** per uscire dal programma di installazione.

Disinstallazione in modalità silenziosa

È possibile eseguire la disinstallazione in modalità silenziosa per Windows o Linux. In modalità silenziosa, nella finestra del terminale non vengono visualizzati messaggi o script di ritorno.

Fasi

1. Accedere alla directory `uninstall_web_Services_proxy`.
2. Eseguire il seguente comando:

```
uninstall_web_services_proxy -i silent
```

Il processo di disinstallazione viene eseguito, ma nella finestra del terminale non vengono visualizzati messaggi o script di ritorno. Una volta disinstallato Web Services Proxy, viene visualizzato un prompt dei comandi nella finestra del terminale.

Disinstallazione del comando RPM (solo Linux)

È possibile utilizzare un comando RPM per disinstallare il proxy dei servizi Web da un sistema Linux.

Fasi

1. Aprire una finestra terminale.
2. Immettere la seguente riga di comando:

```
rpm -e santricity_webservices
```



Il processo di disinstallazione potrebbe lasciare file che non facevano parte dell'installazione originale. Eliminare manualmente questi file per rimuovere completamente il proxy dei servizi Web.

Gestire l'accesso degli utenti in Web Services Proxy

È possibile gestire l'accesso degli utenti alle API dei servizi Web e a Unified Manager per motivi di sicurezza.

Panoramica della gestione degli accessi

La gestione degli accessi include accessi in base al ruolo, crittografia delle password, autenticazione di base e integrazione LDAP.

Accesso in base al ruolo

RBAC (role-based access control) associa gli utenti predefiniti ai ruoli. Ogni ruolo concede le autorizzazioni a un livello specifico di funzionalità.

La tabella seguente descrive ciascun ruolo.

Ruolo	Descrizione
security.admin	SSL e gestione dei certificati.
storage.admin	Accesso completo in lettura/scrittura alla configurazione del sistema storage.
storage.monitor	Accesso in sola lettura per visualizzare i dati del sistema di storage.
support.admin	Accesso a tutte le risorse hardware sui sistemi storage e operazioni di supporto come il recupero ASUP (AutoSupport).

Gli account utente predefiniti sono definiti nel file `users.properties`. È possibile modificare gli account utente modificando direttamente il file `users.properties` o utilizzando le funzioni di gestione degli accessi di Unified Manager.

La tabella seguente elenca gli accessi utente disponibili per il proxy dei servizi Web.

Accesso utente predefinito	Descrizione
amministratore	Un super amministratore che ha accesso a tutte le funzioni e include tutti i ruoli. Per Unified Manager, è necessario impostare la password al primo accesso.
storage	L'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage.admin, support.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
sicurezza	L'utente responsabile della configurazione della sicurezza. Questo utente include i seguenti ruoli: Security.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
supporto	L'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
monitorare	Un utente con accesso di sola lettura al sistema. Questo utente include solo il ruolo storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.

Accesso utente predefinito	Descrizione
rw (legacy per gli array meno recenti)	L'utente rw (lettura/scrittura) include i seguenti ruoli: Storage.admin, support.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
ro (legacy per gli array meno recenti)	L'utente ro (sola lettura) include solo il ruolo storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.

Crittografia della password

Per ciascuna password, è possibile applicare un ulteriore processo di crittografia utilizzando la codifica della password SHA256 esistente. Questo processo di crittografia aggiuntivo applica un set casuale di byte a ciascuna password (SALT) per ogni crittografia hash SHA256. La crittografia SARTed SHA256 viene applicata a tutte le password appena create.



Prima della versione 3.0 di Web Services Proxy, le password venivano crittografate solo tramite l'hashing SHA256. Tutte le password crittografate SHA256 esistenti con solo hash mantengono questa codifica e sono ancora valide nel file users.properties. Tuttavia, le password crittografate SHA256 solo con hash non sono sicure come quelle con crittografia SARTed SHA256.

Autenticazione di base

Per impostazione predefinita, l'autenticazione di base è attivata, il che significa che il server restituisce una sfida di autenticazione di base. Questa impostazione può essere modificata nel file wsconfig.xml.

LDAP

Il protocollo LDAP (Lightweight Directory Access Protocol), un protocollo applicativo per l'accesso e la manutenzione dei servizi informativi di directory distribuiti, è abilitato per il proxy dei servizi Web. L'integrazione LDAP consente l'autenticazione dell'utente e il mapping dei ruoli ai gruppi.

Per informazioni sulla configurazione della funzionalità LDAP, fare riferimento alle opzioni di configurazione nell'interfaccia di Unified Manager o nella sezione LDAP della documentazione API interattiva.

Configurare l'accesso dell'utente

È possibile gestire l'accesso degli utenti applicando una crittografia aggiuntiva alle password, impostando l'autenticazione di base e definendo l'accesso in base al ruolo.

Applicare crittografia aggiuntiva alle password

Per ottenere il massimo livello di sicurezza, è possibile applicare una crittografia aggiuntiva alle password utilizzando la codifica password SHA256 esistente.

Questo processo di crittografia aggiuntivo applica un set casuale di byte a ciascuna password (SALT) per ogni crittografia hash SHA256. La crittografia SARTed SHA256 viene applicata a tutte le password appena create.

Fasi

1. Aprire il file users.properties all'indirizzo:

- (Windows) — C: File di programma/Proxy servizi Web NetApp/SANtricity/data/config
- (Linux) — /opt/netapp/santricity_web_Services_proxy/data/config

2. Immettere nuovamente la password crittografata come testo normale.

3. Eseguire `securepasswd` Utilità della riga di comando per crittografare nuovamente la password o semplicemente riavviare il proxy dei servizi Web. Questa utility viene installata nella directory di installazione principale del proxy dei servizi Web.



In alternativa, è possibile utilizzare le password utente locali e cancellarle ogni volta che vengono modificate le password tramite Unified Manager.

Configurare l'autenticazione di base

Per impostazione predefinita, l'autenticazione di base è attivata, il che significa che il server restituisce una sfida di autenticazione di base. Se lo si desidera, è possibile modificare tale impostazione nel file `wsconfig.xml`.

1. Aprire il file `wsconfig.xml` all'indirizzo:

- (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
- (Linux) — /opt/netapp/santricity_web_Services_proxy

2. Modificare la riga seguente nel file specificando `false` (non abilitato) o `true` (abilitato).

Ad esempio: `<env key="enable-basic-auth">true</env>`

3. Salvare il file.

4. Riavviare il servizio Webserver in modo che la modifica abbia effetto.

Configurare l'accesso in base al ruolo

Per limitare l'accesso degli utenti a funzioni specifiche, è possibile modificare i ruoli specificati per ciascun account utente.

Web Services Proxy include RBAC (role-based access control), in cui i ruoli sono associati a utenti predefiniti. Ogni ruolo concede le autorizzazioni a un livello specifico di funzionalità. È possibile modificare i ruoli assegnati agli account utente modificando direttamente il file `users.properties`.



È inoltre possibile modificare gli account utente utilizzando Access Management in Unified Manager. Per ulteriori informazioni, consultare la guida in linea disponibile con Unified Manager.

Fasi

1. Aprire il file `users.properties`, che si trova in:

- (Windows) — C: File di programma/Proxy servizi Web NetApp/SANtricity/data/config
- (Linux) — /opt/netapp/santricity_web_Services_proxy/data/config

2. Individuare la riga dell'account utente che si desidera modificare (storage, sicurezza, monitor, supporto, rw, o ro).



Non modificare l'utente admin. Si tratta di un super utente con accesso a tutte le funzioni.

3. Aggiungere o rimuovere i ruoli specificati, come desiderato.

I ruoli includono:

- Security.admin — SSL e gestione dei certificati.
- Storage.admin — accesso completo in lettura/scrittura alla configurazione del sistema storage.
- Storage.monitor — accesso in sola lettura per visualizzare i dati del sistema di storage.
- Support.admin — accesso a tutte le risorse hardware sui sistemi storage e operazioni di supporto come il recupero ASUP (AutoSupport).



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

4. Salvare il file.

Gestire la sicurezza e i certificati in Web Services Proxy

Per motivi di sicurezza in Web Services Proxy, è possibile specificare una designazione della porta SSL ed è possibile gestire i certificati. I certificati identificano i proprietari dei siti Web per connessioni sicure tra client e server.

Abilitare SSL

Il proxy dei servizi Web utilizza Secure Sockets Layer (SSL) per la protezione, che viene attivata durante l'installazione. È possibile modificare la designazione della porta SSL nel file wsconfig.xml.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
 - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
 - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Aggiungere o modificare il numero della porta SSL, in modo simile all'esempio seguente:

```
<sslport clientauth="request">8443</sslport>
```

Risultato

Quando il server viene avviato con SSL configurato, il server cerca i file keystore e truststore.

- Se il server non trova un keystore, utilizza l'indirizzo IP del primo indirizzo IPv4 non loopback rilevato per generare un keystore e aggiungere un certificato autofirmato al keystore.
- Se il server non trova un truststore o non viene specificato, il server utilizza il keystore come truststore.

Ignora la convalida del certificato

Per supportare connessioni sicure, il proxy dei servizi Web convalida i certificati dei sistemi di storage rispetto ai propri certificati attendibili. Se necessario, è possibile specificare che il proxy eluderà la convalida prima di connettersi ai sistemi di storage.

Prima di iniziare

- Tutte le connessioni del sistema di storage devono essere sicure.

Fasi

1. Aprire il file `wsconfig.xml` all'indirizzo:
 - (Windows) — `C:/Program Files/NetApp/SANtricity Web Services Proxy`
 - (Linux) — `/opt/netapp/santricity_web_Services_proxy`
2. Invio `true` in `trust.all.arrays` come mostrato nell'esempio:

```
<env key="trust.all.arrays">true</env>
```

3. Salvare il file.

Generare e importare un certificato di gestione host

I certificati identificano i proprietari dei siti Web per connessioni sicure tra client e server. Per generare e importare certificati CA (Certificate Authority) per il sistema host in cui è installato Web Services Proxy, è possibile utilizzare endpoint API.

Per gestire i certificati per il sistema host, eseguire le seguenti attività utilizzando l'API:

- Creare una richiesta di firma del certificato (CSR) per il sistema host.
- Inviare il file CSR a una CA, quindi attendere l'invio dei file di certificato.
- Importare i certificati firmati nel sistema host.



È inoltre possibile gestire i certificati nell'interfaccia di Unified Manager. Per ulteriori informazioni, consultare la guida in linea disponibile in Unified Manager.

Fasi

1. Accedere a ["Documentazione API interattiva"](#).
2. Andare al menu a discesa in alto a destra e selezionare **v2**.
3. Espandere il collegamento **Administration** e scorrere verso il basso fino agli endpoint **/certificates**.
4. Generare il file CSR:
 - a. Selezionare **POST:/certificates**, quindi selezionare **Try it out**.

Il server Web rigenera un certificato autofirmato. È quindi possibile inserire informazioni nei campi per definire il nome comune, l'organizzazione, l'unità organizzativa, l'ID alternativo e altre informazioni utilizzate per generare la CSR.

- b. Aggiungere le informazioni richieste nel riquadro **Example Values** (valori di esempio) per generare un certificato CA valido, quindi eseguire i comandi.



Non chiamare di nuovo **POST:/certificates** o **POST:/certificates/reset**, altrimenti è necessario rigenerare la CSR. Quando si chiama **POST:/certificates** o **POST:/certificates/reset**, si sta generando un nuovo certificato autofirmato con una nuova chiave privata. Se si invia una CSR generata prima dell'ultimo ripristino della chiave privata sul server, il nuovo certificato di protezione non funziona. È necessario generare una nuova CSR e richiedere un nuovo certificato CA.

- c. Eseguire l'endpoint **GET:/certificates/server** per confermare che lo stato corrente del certificato è il

certificato autofirmato con le informazioni aggiunte dal comando **POST:/certificates**.

Il certificato del server (indicato dall'alias `jetty`) è ancora autofirmato a questo punto.

- d. Espandere l'endpoint **POST:/certificates/export**, selezionare **provalo**, immettere un nome di file per il file CSR, quindi fare clic su **Esegui**.
5. Copiare e incollare `fileUrl` in una nuova scheda del browser per scaricare il file CSR, quindi inviare il file CSR a una CA valida per richiedere una nuova catena di certificati del server Web.
6. Quando la CA emette una nuova catena di certificati, utilizzare uno strumento di gestione dei certificati per suddividere i certificati server root, intermedi e Web, quindi importarli nel server proxy dei servizi Web:
 - a. Espandere l'endpoint **POST:/sslconfig/server** e selezionare **Provalo**.
 - b. Immettere un nome per il certificato CA root nel campo **alias**.
 - c. Selezionare **false** nel campo **replaceMainServerCertificate**.
 - d. Individuare e selezionare il nuovo certificato CA principale.
 - e. Fare clic su **Execute** (Esegui).
 - f. Verificare che il caricamento del certificato sia riuscito.
 - g. Ripetere la procedura di caricamento del certificato CA per il certificato intermedio CA.
 - h. Ripetere la procedura di caricamento del certificato per il nuovo file di certificato di sicurezza del server Web, ad eccezione di questa fase, selezionare **true** nell'elenco a discesa **replaceMainServerCertificate**.
 - i. Verificare che l'importazione del certificato di sicurezza del server Web sia riuscita.
 - j. Per confermare che i nuovi certificati root, intermedi e server web sono disponibili nel keystore, eseguire **GET:/certificates/server**.
7. Selezionare ed espandere l'endpoint **POST:/certificates/reload**, quindi selezionare **Try it out**. Quando richiesto, se si desidera riavviare entrambi i controller, selezionare **false**. ("vero" si applica solo nel caso di controller a doppio array). Fare clic su **Execute** (Esegui).

L'endpoint **/certificates/reload** in genere restituisce una risposta http 202 corretta. Tuttavia, il ricaricamento dei certificati truststore e keystore del server Web crea una race condition tra il processo API e il processo di ricarica dei certificati del server Web. In rari casi, il ricaricamento del certificato del server Web può superare l'elaborazione dell'API. In questo caso, il ricaricamento sembra non riuscire anche se è stato completato correttamente. In tal caso, passare comunque alla fase successiva. Se il ricaricamento non è riuscito, anche il passaggio successivo non riesce.

8. Chiudere la sessione corrente del browser sul proxy dei servizi Web, aprire una nuova sessione del browser e verificare che sia possibile stabilire una nuova connessione sicura del browser al proxy dei servizi Web.

Utilizzando una sessione di navigazione in incognito o privata, è possibile aprire una connessione al server senza utilizzare i dati salvati delle sessioni di navigazione precedenti.

Gestire i sistemi storage utilizzando Web Services Proxy

Per gestire i sistemi storage in rete, è necessario prima rilevarli e poi aggiungerli all'elenco di gestione.

Scopri i sistemi storage

È possibile impostare il rilevamento automatico o rilevare manualmente i sistemi storage.

Rilevare automaticamente i sistemi storage

È possibile specificare che i sistemi di storage vengano rilevati automaticamente in rete modificando le impostazioni nel file `wsconfig.xml`. Per impostazione predefinita, il rilevamento automatico IPv6 è disattivato e IPv4 è attivato.

Per aggiungere un sistema storage, è necessario fornire un solo indirizzo IP o DNS di gestione. Il server rileva automaticamente tutti i percorsi di gestione quando i percorsi non sono configurati o sono configurati e ruotabili.



Se si tenta di utilizzare un protocollo IPv6 per rilevare automaticamente i sistemi storage dalla configurazione del controller dopo aver effettuato una connessione iniziale, il processo potrebbe non riuscire. Le possibili cause del guasto includono problemi durante l'inoltro dell'indirizzo IP o l'attivazione di IPv6 sui sistemi storage, ma non sul server.

Prima di iniziare

Prima di attivare le impostazioni di rilevamento IPv6, verificare che l'infrastruttura supporti la connettività IPv6 ai sistemi storage per mitigare eventuali problemi di connessione.

Fasi

1. Aprire il file `wsconfig.xml` all'indirizzo:
 - (Windows) — `C:/Program Files/NetApp/SANtricity Web Services Proxy`
 - (Linux) — `/opt/netapp/santricity_web_Services_proxy`
2. Nelle stringhe di ricerca automatica, modificare le impostazioni da `true` a `false`, come desiderato. Vedere l'esempio seguente.

```
<env key="autodiscover.ipv6.enable">true</env>
```



Quando i percorsi sono configurati, ma non configurati in modo che il server possa instradare verso gli indirizzi, si verificano errori di connessione intermittenti. Se non è possibile impostare gli indirizzi IP in modo che possano essere instradati dall'host, disattivare la funzione di rilevamento automatico (modificare le impostazioni su `false`).

3. Salvare il file.

Rilevare e aggiungere sistemi storage utilizzando endpoint API

È possibile utilizzare gli endpoint API per rilevare e aggiungere sistemi storage all'elenco gestito. Questa procedura crea una connessione di gestione tra il sistema di storage e l'API.



Questa attività descrive come individuare e aggiungere sistemi storage utilizzando l'API REST, in modo da poter gestire questi sistemi nella documentazione API interattiva. Tuttavia, è possibile gestire i sistemi storage in Unified Manager, che offre un'interfaccia di facile utilizzo. Per ulteriori informazioni, consultare la guida in linea disponibile con Unified Manager.

Prima di iniziare

Per i sistemi storage con SANtricity versione 11.30 e successive, l'interfaccia di gestione legacy per Symbol deve essere attivata nell'interfaccia di Gestore di sistema di SANtricity. In caso contrario, gli endpoint di rilevamento non riescono. Per trovare questa impostazione, aprire Gestione sistema e accedere al **Impostazioni > sistema > Impostazioni aggiuntive > interfaccia di gestione delle modifiche**.

Fasi

1. Accedere a ["Documentazione API interattiva"](#).
2. Scopri i sistemi storage come segue:
 - a. Nella documentazione API, assicurarsi che sia selezionato **V2** nell'elenco a discesa, quindi espandere la categoria **Storage-Systems**.
 - b. Fare clic sull'endpoint **POST: /Discovery**, quindi fare clic su **Provalo**.
 - c. Inserire i parametri come descritto nella tabella.

IP startup
IP finale
Sostituire la stringa con l'intervallo di indirizzi IP iniziale e finale per uno o più sistemi di storage in rete.
UseAgents
Impostare questo valore su: <ul style="list-style-type: none">• Vero = utilizza agenti in-band per la scansione di rete.• Falso = non utilizzare agenti in-band per la scansione di rete.
ConnectionTimeout
Inserire i secondi consentiti per la scansione prima che la connessione si esaurisca.
MaxPortsToUse
Immettere un numero massimo di porte utilizzate per la scansione di rete.

- d. Fare clic su **Execute** (Esegui).



Le azioni API vengono eseguite senza richieste dell'utente.

Il processo di rilevamento viene eseguito in background.

- a. Assicurarsi che il codice restituisca 202.
 - b. In **Response Body**, individuare il valore restituito per l'ID richiesta. Per visualizzare i risultati nel passaggio successivo, è necessario l'ID richiesta.
3. Visualizzare i risultati del rilevamento come segue:

- a. Fare clic sull'endpoint **GET: /Discovery**, quindi fare clic su **Provalo**.
- b. Inserire l'ID richiesta dal passaggio precedente. Se si lascia vuoto **ID richiesta**, l'endpoint passa per impostazione predefinita all'ultimo ID richiesta eseguito.
- c. Fare clic su **Execute** (Esegui).
- d. Assicurarsi che il codice restituisca 200.
- e. Nel corpo della risposta, individuare l'ID richiesta e le stringhe per i sistemi di storage. Le stringhe sono simili all'esempio seguente:

```
"storageSystems": [
  {
    "serialNumber": "123456789",
    "wwn": "000A011000AF00000000000001A0C000E",
    "label": "EF570_Array",
    "firmware": "08.41.10.01",
    "nvram": "N5700-841834-001",
    "ipAddresses": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
    ]
  },

```

- f. Annotare i valori per wwn, Label e ipAddresses. Sono necessari per il passaggio successivo.

4. Aggiungere i sistemi storage come segue:

- a. Fare clic sull'endpoint **POST: /Storage-system**, quindi fare clic su **Provalo**.
- b. Inserire i parametri come descritto nella tabella.

id
Immettere un nome univoco per il sistema di storage. È possibile inserire l'etichetta (visualizzata nella risposta per GET: /Discovery), ma il nome può essere qualsiasi stringa scelta. Se non si specifica un valore per questo campo, i servizi Web assegnano automaticamente un identificatore univoco.
ControllerAddresses
Inserire gli indirizzi IP visualizzati nella risposta per GET: /Discovery. Per i controller doppi, separare gli indirizzi IP con una virgola. Ad esempio: "IP address 1", "IP address 2"
validare
Invio true, In modo da poter ricevere la conferma che i servizi Web possono connettersi al sistema di storage.
password

Inserire la password amministrativa per il sistema di storage.

wwn

Inserire il WWN del sistema di storage (visualizzato nella risposta per GET: /Discovery).

- c. Rimuovi tutte le stringhe dopo "enableTrace": true, in modo che l'intero set di stringhe sia simile all'esempio seguente:

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP", "Controller-B-Mgmt_IP"
  ],
  "validate": true,
  "password": "array-admin-password",
  "wwn": "000A011000AF0000000000001A0C000E",
  "enableTrace": true
}
```

- d. Fare clic su **Execute** (Esegui).
- e. Assicurarsi che la risposta del codice sia 201, che indica che l'endpoint è stato eseguito correttamente.

L'endpoint **Post: /Storage-Systems** viene messo in coda. È possibile visualizzare i risultati utilizzando l'endpoint **GET: /Storage-Systems** nella fase successiva.

5. Confermare l'aggiunta dell'elenco, come segue:

- a. Fare clic sull'endpoint **GET: /Storage-system**.

Non sono richiesti parametri.

- b. Fare clic su **Execute** (Esegui).
- c. Assicurarsi che la risposta del codice sia 200, che indica che l'endpoint è stato eseguito correttamente.
- d. Nel corpo della risposta, cercare i dettagli del sistema di storage. I valori restituiti indicano che è stato aggiunto correttamente all'elenco degli array gestiti, in modo simile all'esempio seguente:


```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF00000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
    ]
  }
]
```

Scalare il numero di sistemi storage gestiti

Per impostazione predefinita, l'API può gestire fino a 100 sistemi storage. Se è necessario gestire di più, è necessario superare i requisiti di memoria per il server.

Il server è impostato per utilizzare 512 MB di memoria. Per ogni 100 sistemi storage aggiuntivi della rete, aggiungere 250 MB a tale numero. Non aggiungere più memoria di quella fisicamente disponibile. Consente di aggiungere un numero sufficiente di componenti aggiuntivi per il sistema operativo e altre applicazioni.



La dimensione predefinita della cache è 8,192 eventi. L'utilizzo approssimativo dei dati per la cache degli eventi MEL è di 1 MB per ogni 8,192 eventi. Pertanto, mantenendo le impostazioni predefinite, l'utilizzo della cache dovrebbe essere di circa 1 MB per un sistema storage.



Oltre alla memoria, il proxy utilizza le porte di rete per ciascun sistema di storage. Linux e Windows considerano le porte di rete come handle di file. Come misura di sicurezza, la maggior parte dei sistemi operativi limita il numero di handle di file aperti che un processo o un utente può avere aperto contemporaneamente. In particolare negli ambienti Linux, dove le connessioni TCP aperte sono considerate come handle di file, il proxy dei servizi Web può facilmente superare questo limite. Poiché la correzione dipende dal sistema, fare riferimento alla documentazione del sistema operativo per informazioni su come aumentare questo valore.

Fasi

1. Effettuare una delle seguenti operazioni:
 - In Windows, accedere al file `appserver64.init`. Individuare la linea, `vmarg.3=-Xmx512M`
 - Su Linux, andare al file `webserver.sh`. Individuare la linea, `JAVA_OPTIONS="-Xmx512M"`
2. Per aumentare la memoria, sostituire 512 Con la memoria desiderata in MB.
3. Salvare il file.

Gestire il polling automatico per le statistiche del proxy dei servizi Web

È possibile configurare il polling automatico per tutte le statistiche di dischi e volumi sui sistemi storage rilevati.

Panoramica delle statistiche

Le statistiche forniscono informazioni sui tassi di raccolta dei dati e sulle performance dei sistemi storage.

Il proxy dei servizi Web consente di accedere ai seguenti tipi di statistiche:

- Statistiche raw — contatori totali per i punti dati al momento della raccolta dei dati. Le statistiche raw possono essere utilizzate per operazioni di lettura totali o operazioni di scrittura totali.
- Statistiche analizzate — informazioni calcolate per un intervallo. Esempi di statistiche analizzate sono le operazioni di input/output in lettura (IOPS) al secondo o il throughput in scrittura.

Le statistiche raw sono lineari, in genere richiedono almeno due punti di dati raccolti per ricavare da essi i dati utilizzabili. Le statistiche analizzate sono una derivazione delle statistiche raw, che forniscono metriche importanti. Molti valori che possono essere derivati dalle statistiche raw vengono visualizzati in un formato point-in-time utilizzabile nelle statistiche analizzate per maggiore comodità.

È possibile recuperare le statistiche raw indipendentemente dal fatto che il polling automatico sia attivato o meno. È possibile aggiungere `usecache=true` Stringa di query alla fine dell'URL per recuperare le statistiche memorizzate nella cache dall'ultimo polling. L'utilizzo dei risultati memorizzati nella cache aumenta notevolmente le performance del recupero delle statistiche. Tuttavia, più chiamate a una velocità uguale o inferiore alla cache dell'intervallo di polling configurata recuperano gli stessi dati.

Funzionalità delle statistiche

Il proxy dei servizi Web fornisce endpoint API che consentono il recupero di statistiche di controller e interfacce raw e analizzate da modelli hardware e versioni software supportati.

API Raw Statistics

- `/storage-systems/{system-id}/controller-statistics`
- `/storage-systems/{system-id}/drive-statistics/{optional list of disk ids}`
- `/storage-systems/{system-id}/interface-statistics/{optional list of interface ids}`
- `/storage-systems/{system-id}/volume-statistics/{optional list of volume ids}`

API delle statistiche analizzate

- `/storage-systems/{id}/analysed-controller-statistics/`
- `/storage-systems/{id}/analysed-drive-statistics/{optional list of disk ids}`
- `/storage-systems/{id}/analysed-interface-statistics/{optional list of interface ids}`
- `/storage-systems/{id}/analysed-volume-statistics/{optional list of volume ids}`

Questi URL recuperano le statistiche analizzate dall'ultimo polling e sono disponibili solo quando il polling è attivato. Questi URL includono i seguenti dati input-output:

- Operazioni al secondo
- Throughput in megabyte al secondo
- Tempi di risposta in millisecondi

I calcoli si basano sulle differenze tra le iterazioni di polling statistiche, che sono le misure più comuni delle performance dello storage. Queste statistiche sono preferibili alle statistiche non analizzate.



All'avvio del sistema, non esiste alcuna raccolta di statistiche precedente da utilizzare per calcolare le varie metriche, pertanto le statistiche analizzate richiedono almeno un ciclo di polling dopo l'avvio per restituire i dati. Inoltre, se i contatori cumulativi vengono ripristinati, il ciclo di polling successivo avrà numeri imprevedibili per i dati.

Configurare gli intervalli di polling

Per configurare gli intervalli di polling, modificare il file `wsconfig.xml` in modo da specificare un intervallo di polling in secondi.



Poiché le statistiche sono memorizzate nella cache, potrebbe verificarsi un aumento di circa 1.5 MB di utilizzo della memoria per ciascun sistema di storage.

Prima di iniziare

- I sistemi storage devono essere rilevati dal proxy.

Fasi

1. Aprire il file `wsconfig.xml` all'indirizzo:
 - (Windows) — `C:/Program Files/NetApp/SANtricity Web Services Proxy`
 - (Linux) — `/opt/netapp/santricity_web_Services_proxy`
2. Aggiungere la seguente riga all'interno di `<env-entries>` tag, in cui `n` indica il numero di secondi dell'intervallo tra le richieste di polling:

```
<env key="stats.poll.interval">n</env>
```

Ad esempio, se si inserisce 60, il polling inizia a intervalli di 60 secondi. Ovvero, il sistema richiede l'avvio del polling 60 secondi dopo il completamento del periodo di polling precedente (indipendentemente dalla durata del periodo di polling precedente). Tutte le statistiche sono contrassegnate con l'ora esatta in cui sono state recuperate. Il sistema utilizza l'indicatore orario o la differenza temporale su cui basare il calcolo di 60 secondi.

3. Salvare il file.

Gestire AutoSupport utilizzando il proxy dei servizi Web

È possibile configurare ASUP (AutoSupport), che raccoglie i dati e li invia automaticamente al supporto tecnico per la risoluzione dei problemi e l'analisi dei

problemi in remoto.

Panoramica di ASUP (AutoSupport)

La funzione ASUP (AutoSupport) trasmette automaticamente i messaggi a NetApp in base a criteri manuali e basati su pianificazione.

Ogni messaggio AutoSupport è un insieme di file di log, dati di configurazione, dati di stato e metriche delle performance. Per impostazione predefinita, AutoSupport trasmette i file elencati nella tabella seguente al team di supporto NetApp una volta alla settimana.

Nome file	Descrizione
x-headers-data.txt	Un file .txt contenente le informazioni dell'intestazione X.
manifest.xml	Un file .xml che descrive il contenuto del messaggio.
arraydata.xml	Un file .xml contenente l'elenco dei dati persistenti del client.
appserver-config.txt	Un file .txt contenente i dati di configurazione dell'application server.
wsconfig.txt	Un file .txt contenente i dati di configurazione del servizio Web.
host-info.txt	Un file .txt contenente informazioni sull'ambiente host.
server-logs.7z	Un file .7z contenente tutti i file di log del webserver disponibili.
client-info.txt	Un file .txt con coppie chiave/valore arbitrarie per contatori specifici dell'applicazione, ad esempio accessi a metodi e pagine web.
webservices-profile.json	<p>Questi file contengono i dati del profilo WebServices e i dati statistici di monitoraggio Jersey. Per impostazione predefinita, le statistiche di monitoraggio Jersey sono attivate. È possibile attivarle e disattivarle nel file wsconfig.xml, come indicato di seguito:</p> <ul style="list-style-type: none">• Abilitare: <code><env key="enable.jersey.statistics">true</env></code>• Disattiva: <code><env key="enable.jersey.statistics">false</env></code>

Configurare AutoSupport

AutoSupport è attivato per impostazione predefinita al momento dell'installazione; tuttavia, è possibile modificare tale impostazione o i tipi di consegna.

Attiva o disattiva AutoSupport

La funzione AutoSupport viene attivata o disattivata durante l'installazione iniziale del proxy dei servizi Web, ma è possibile modificarla nel file ASUPConfig.

È possibile attivare o disattivare AutoSupport tramite il file ASUPConfig.xml, come descritto di seguito. In alternativa, è possibile attivare o disattivare questa funzione tramite l'API utilizzando **Configuration** e **POST/asup**, quindi immettendo "true" o "false".

- 1. Aprire il file ASUPConfig.xml nella directory di lavoro.
- 2. Individuare le linee per <asupdata enable="Boolean_value" timestamp="timestamp">
- 3. Invio true (attiva) o. false (disattiva). Ad esempio:

```
<asupdata enabled="false" timestamp="0">
```



La voce relativa all'indicatore data e ora è superflua.

- 4. Salvare il file.

Configurare il metodo di erogazione AutoSupport

È possibile configurare la funzione AutoSupport in modo che utilizzi i metodi di consegna HTTPS, HTTP o SMTP. HTTPS è il metodo di consegna predefinito.

- 1. Accedere al file ASUPConfig.xml nella directory di lavoro.
- 2. Nella stringa, <delivery type="n">, inserire 1, 2 o 3 come descritto nella tabella:

Valore	Descrizione
1	HTTPS (impostazione predefinita) <delivery type="1">
2	HTTP <delivery type="2">
3	SMTP — per configurare correttamente il tipo di recapito AutoSupport su SMTP, è necessario includere l'indirizzo del server di posta SMTP, insieme ai messaggi di posta elettronica dell'utente mittente e destinatario, come nell'esempio seguente: <div><pre><delivery type="3"> <smtp> <mailserver>smtp.example.com</mailserver> <sender>user@example.com</sender> <replyto>user@example.com</replyto> </smtp> </delivery></pre></div>

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.