Web-Services-Proxy

E-Series Systems

NetApp
March 22, 2024

Inhalt

Web-Services-Proxy

SANtricity Web Services Proxy: Überblick

Beim SANtricity Web Services Proxy handelt es sich um einen RESTful API Server, der separat auf einem Host-System installiert wird und auf dem Hunderte neuer und älterer NetApp E-Series Storage-Systeme verwaltet werden. Der Proxy umfasst SANtricity Unified Manager. Dabei handelt es sich um eine webbasierte Schnittstelle mit ähnlichen Funktionen.

Übersicht über die Installation

Zum Installieren und Konfigurieren des Web Services Proxy gehen Sie wie folgt vor:

1. "Installations- und Upgrade-Anforderungen prüfen".
2. "Laden Sie die Web Services Proxy-Datei herunter und installieren Sie sie".
3. "Melden Sie sich bei API und Unified Manager an".
4. "Konfigurieren Sie Web Services Proxy".

Weitere Informationen

- Unified Manager: Die Proxy-Installation umfasst SANtricity Unified Manager, eine webbasierte Schnittstelle mit Konfigurationszugriff auf neuere E-Series und EF-Series Storage-Systeme. Weitere Informationen finden Sie in der Online-Hilfe von Unified Manager, die über seine Benutzeroberfläche oder über die bereitgestellt wird "SANtricity Software-Dokument-Site".
- GitHub Repository — GitHub enthält ein Repository für die Sammlung und Organisation von Beispielskripten, die die Verwendung der NetApp SANtricity Web Services API veranschaulichen. Informationen zum Zugriff auf das Repository finden Sie unter "Beispiele für NetApp Webservices".
- Representational State Transfer (REST) — Webservices sind eine RESTful API, die Zugriff auf praktisch alle SANtricity Management-Funktionen bietet, so dass Sie mit REST-Konzepten vertraut sein sollten. Weitere Informationen finden Sie unter "Architekturstile und das Design netzwerkbasierter Softwarearchitekturen".
- JavaScript Object Notation (JSON) — Da die Daten in Web Services über JSON codiert sind, sollten Sie mit JSON-Programmierkonzepten vertraut sein. Weitere Informationen finden Sie unter "Einführung von JSON".

Erfahren Sie mehr über Web Services

Web Services und Unified Manager im Überblick

Lesen Sie vor der Installation und Konfiguration des Web Services Proxy die Übersicht über Webdienste und SANtricity Unified Manager.

Web-Services

Web Services ist eine API (Application Programming Interface), über die Sie Storage-Systeme der NetApp E-Series und EF-Series konfigurieren, managen und überwachen können. Es werden API-Anfragen gestellt, mit

denen Workflows wie Konfiguration, Bereitstellung und Performance-Monitoring für E-Series Storage-Systeme durchgeführt werden können.

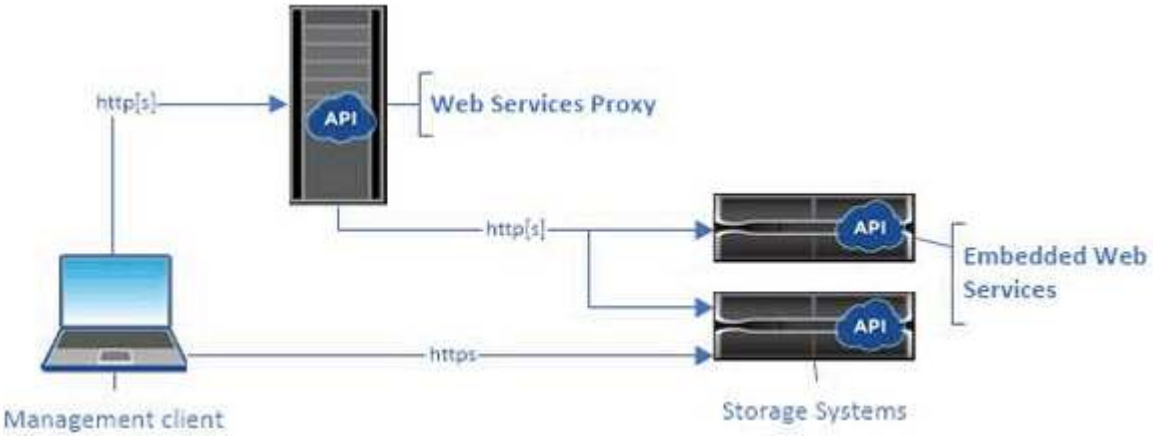
Wenn Sie die Web Services API für das Management von Storage-Systemen verwenden, sollten Sie mit folgenden Informationen vertraut sein:

- JavaScript Object Notation (JSON) – Da die Daten in Web Services über JSON verschlüsselt sind, sollten Sie mit JSON-Programmierkonzepten vertraut sein. Weitere Informationen finden Sie unter "Einführung von JSON".
- Representational State Transfer (REST) – Webservices sind eine RESTful API, die Zugriff auf praktisch alle SANtricity-Managementfunktionen bietet. Sie sollten daher mit REST-Konzepten vertraut sein. Weitere Informationen finden Sie unter "Architekturstile und das Design netzwerkbasierter Softwarearchitekturen".
- Programmiersprachen – Java und Python sind die häufigsten Programmiersprachen, die mit der Web Services API verwendet werden, aber jede Programmiersprache, die HTTP-Anfragen machen kann, reicht für API-Interaktion aus.

Web Services sind in zwei Implementierungen erhältlich:

- **Eingebettet** — Ein RESTful API-Server ist in jeden Controller eines E2800/EF280 Storage-Systems mit NetApp SANtricity 11.30 oder höher, einer E5700/EF570 mit SANtricity 11.40 oder höher und einer EF300 oder EF600 mit SANtricity 11.60 oder höheren Versionen integriert. Es ist keine Installation erforderlich.
- **Proxy** — der SANtricity Web Services Proxy ist ein RESTful API-Server, der separat auf einem Windows- oder Linux-Server installiert wird. Diese Host-basierte Applikation ermöglicht das Management Hunderter neuer und alter NetApp E-Series Storage-Systeme. Im Allgemeinen sollten Sie den Proxy für Netzwerke mit mehr als 10 Speichersystemen verwenden. Der Proxy kann zahlreiche Anforderungen effizienter verarbeiten als die eingebettete API.

Der Core der API ist in beiden Implementierungen verfügbar.



Die folgende Tabelle enthält einen Vergleich des Proxy und der eingebetteten Version.

Überlegungen	Proxy	Eingebettet
Installation	Erfordert ein Host-System (Linux oder Windows). Der Proxy kann unter heruntergeladen werden "NetApp Support Website" Oder auf "DockerHub".	Es ist keine Installation oder Aktivierung erforderlich.

Überlegungen	Proxy	Eingebettet
Sicherheit	Die minimalen Sicherheitseinstellungen sind standardmäßig aktiviert. Die Sicherheitseinstellungen sind gering, sodass Entwickler schnell und einfach mit der API beginnen können. Sie können den Proxy auf Wunsch mit demselben Sicherheitsprofil wie die eingebettete Version konfigurieren.	Hohe Sicherheitseinstellungen sind standardmäßig aktiviert. Sicherheitseinstellungen sind hoch, da die API direkt auf den Controllern ausgeführt wird. So ist beispielsweise kein HTTP-Zugriff möglich, und es werden alle SSL- und älteren TLS-Verschlüsselungsprotokolle für HTTPS deaktiviert.
Zentralisiertes Management	Management aller Storage-Systeme über einen Server	Verwaltet nur den Controller, auf dem er eingebettet ist.

Unified Manager

Das Proxy-Installationspaket umfasst Unified Manager, eine webbasierte Schnittstelle, über die der Konfigurationszugriff auf neuere E-Series und EF-Series Storage-Systeme wie E2800, E5700, EF300 und EF600 Systeme ermöglicht wird.

Von Unified Manager aus können Sie die folgenden Batch-Operationen ausführen:

- Sie können den Status mehrerer Storage-Systeme aus einer zentralen Ansicht anzeigen
- Erkennung mehrerer Storage-Systeme im Netzwerk
- Importieren von Einstellungen von einem Storage-System in mehrere Systeme
- Firmware-Upgrade für mehrere Storage-Systeme

Kompatibilität und Einschränkungen

Die folgenden Kompatibilitätsbeschränkungen und Einschränkungen gelten für die Verwendung des Web Services Proxy.

Überlegungen	Kompatibilität oder Einschränkungen
HTTP-Unterstützung	Der Web Services Proxy ermöglicht die Verwendung von HTTP oder HTTPS. (Die eingebettete Version von Web Services erfordert aus Sicherheitsgründen HTTPS.)
Storage-Systeme und Firmware	Der Web Services Proxy kann alle E-Series Storage-Systeme managen. Dazu zählen eine Mischung aus älteren Systemen und den aktuellen E2800, EF280, E5700, EF570, EF300 Und die Systeme der EF600 Serie.

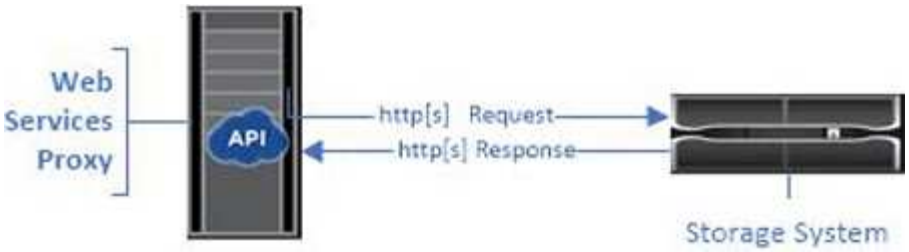
Überlegungen	Kompatibilität oder Einschränkungen
IP-Support	Der Web Services Proxy unterstützt entweder das IPv4-Protokoll oder das IPv6-Protokoll. Das IPv6-Protokoll schlägt möglicherweise fehl, wenn der Web Services Proxy versucht, die Verwaltungsadresse von der Controller-Konfiguration automatisch zu ermitteln. Mögliche Ursachen für den Ausfall sind u. a. Probleme bei der IP-Adressweiterleitung oder bei der Aktivierung von IPv6 auf den Speichersystemen, jedoch nicht auf dem Server.
Einschränkungen bei NVSRAM-Dateinamen	Der Web Services Proxy verwendet NVSRAM-Dateinamen, um Versionsinformationen korrekt zu identifizieren. Daher können Sie NVSRAM-Dateinamen nicht ändern, wenn sie mit dem Web Services Proxy verwendet werden. Der Web Services Proxy erkennt möglicherweise keine umbenannte NVSRAM-Datei als gültige Firmware-Datei.
Symbol Web	Symbol Web ist eine URL in DER REST-API. Sie ermöglicht den Zugriff auf fast alle Symbolrufe. Die Symbolfunktion ist Teil der folgenden URL: `http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function` Symboldeaktivierte Speichersysteme werden über den Web Services Proxy unterstützt.

API-Grundlagen

In der Web Services-API umfasst HTTP-Kommunikation einen Anforderungsantwort-Zyklus.

URL-Elemente in Anforderungen

Unabhängig von der verwendeten Programmiersprache oder dem verwendeten Werkzeug hat jeder Aufruf der Web Services-API eine ähnliche Struktur, mit einer URL, einem HTTP-Verb und einem Accept-Header.



Alle Anforderungen enthalten wie im folgenden Beispiel eine URL und enthalten die in der Tabelle beschriebenen Elemente.

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

Werden	Beschreibung
HTTP-Übertragung `https://`	Der Web Services Proxy ermöglicht die Verwendung von HTTP oder HTTPS. Aus Sicherheitsgründen erfordert die integrierten Webdienste HTTPS.
Basis-URL und Port `webservices.name.com:8443`	Jede Anforderung muss korrekt an eine aktive Instanz von Webservices weitergeleitet werden. Der FQDN (vollständig qualifizierter Domänenname) oder die IP-Adresse der Instanz sind zusammen mit dem Listening-Port erforderlich. Standardmäßig kommuniziert Web Services über Port 8080 (für HTTP) und Port 8443 (für HTTPS). Für den Web Services Proxy können beide Ports während der Proxy-Installation oder in der wsconfig.xml-Datei geändert werden. Port-Konflikte sind auf Datacenter-Hosts üblich, auf denen verschiedene Management-Applikationen ausgeführt werden. Bei den integrierten Webservices kann der Port des Controllers nicht geändert werden. Standardmäßig ist der Port 8443 für sichere Verbindungen verfügbar.

Werden	Beschreibung
API-Pfad `devmgr/v2/storage-systems`	Eine Anforderung wird an eine bestimmte REST-Ressource oder einen bestimmten Endpunkt innerhalb der Web Services-API gestellt. Die meisten Endpunkte sind in Form von: `devmgr/v2/<resource>/[id]` Der API-Pfad besteht aus drei Teilen: • `devmgr` (Device Manager) ist der Namespace der Web Services API. • `v2` Gibt die Version der API an, auf die Sie zugreifen. Sie können auch verwenden `utils` Für den Zugriff auf Anmeldungsendpunkte. • `storage-systems` Ist eine Kategorie innerhalb der Dokumentation.

Unterstützte HTTP-Verben

Unterstützte HTTP-Verben umfassen ABRUFEN, POST und LÖSCHEN:

- GET-Anforderungen werden für schreibgeschützte Anfragen verwendet.
- POST-Requests werden zum Erstellen und Aktualisieren von Objekten sowie für Leseanforderungen verwendet, die möglicherweise Auswirkungen auf die Sicherheit haben.
- LÖSCHANFRAGEN werden normalerweise verwendet, um ein Objekt aus dem Management zu entfernen, ein Objekt vollständig zu entfernen oder den Status des Objekts zurückzusetzen.

> Derzeit unterstützt die Web Services API PUT oder PATCH nicht. Stattdessen können Sie POST verwenden, um die typischen Funktionen für diese Verben bereitzustellen.

Kopfzeilen akzeptieren

Wenn ein Anforderungsentext zurückgegeben wird, gibt Web Services die Daten im JSON-Format zurück (sofern nicht anders angegeben). Bestimmte Clients haben standardmäßig die Anforderung von „`Text/HTML`“ oder etwas ähnlichem. In diesen Fällen antwortet die API mit einem HTTP-Code 406 und bezeichnet, dass sie keine Daten in diesem Format bereitstellen kann. Als Best Practice sollten Sie den Header akzeptieren für alle Fälle als „`Application/json`“ definieren, in denen Sie JSON als Antworttyp erwarten. In anderen Fällen, in denen ein Antwortkörper nicht zurückgegeben wird (z. B. LÖSCHEN), verursacht die Annahme-Kopfzeile keine unbeabsichtigten Auswirkungen.

Antworten

Wenn eine Anfrage an die API gestellt wird, gibt eine Antwort zwei wichtige Informationen zurück:

- HTTP-Statuscode — gibt an, ob die Anforderung erfolgreich war.
- Optionaler Antwortkörper — bietet in der Regel einen JSON-Körper, der den Zustand der Ressource oder eines Körpers darstellt, der mehr Details über die Art eines Fehlers liefert.

Sie müssen den Statuscode und den Inhaltstyp-Header überprüfen, um festzustellen, wie der resultierende Antwortkörper aussieht. Für HTTP-Statuscodes 200-203 und 422 gibt Web Services einen JSON-Text mit der Antwort zurück. Bei anderen HTTP-Statuscodes gibt Web Services in der Regel keinen zusätzlichen JSON-Text zurück, entweder weil die Spezifikation es nicht zulässt (204) oder weil der Status selbsterklärend ist. In der Tabelle sind allgemeine HTTP-Statuscodes und -Definitionen aufgeführt. Sie gibt außerdem an, ob Informationen, die mit den einzelnen HTTP-Codes in einem JSON-Körper verbunden sind, zurückgegeben werden.

HTTP-Statuscode	Beschreibung	JSON-Text
200 OK	Kennzeichnet eine erfolgreiche Antwort.	Ja.
201 Erstellt	Gibt an, dass ein Objekt erstellt wurde. Dieser Code wird in einigen seltenen Fällen anstelle eines 200-Status verwendet.	Ja.
202 Akzeptiert	Gibt an, dass die Anforderung zur Bearbeitung als asynchrone Anforderung akzeptiert wird, Sie müssen jedoch eine nachfolgende Anfrage stellen, um das tatsächliche Ergebnis zu erhalten.	Ja.
203 Nicht-Autorisierende Informationen	Ähnlich wie bei einer Antwort von 200, Webservices können jedoch nicht garantieren, dass die Daten aktuell sind (beispielsweise sind derzeit nur zwischengespeicherte Daten verfügbar).	Ja.
204 Kein Inhalt	Zeigt eine erfolgreiche Operation an, aber es gibt keinen Antwortkörper.	Nein
400 Fehlerhafte Anfrage	Gibt an, dass der in der Anforderung angegebene JSON-Text nicht gültig ist.	Nein
401 Nicht Autorisiert	Zeigt an, dass ein Authentifizierungsfehler aufgetreten ist. Es wurden keine Anmeldedaten angegeben oder der Benutzername oder das Passwort war ungültig.	Nein
403 Verbotene	Ein Autorisierungsfehler, der angibt, dass der authentifizierte Benutzer nicht über die Berechtigung zum Zugriff auf den angeforderten Endpunkt verfügt.	Nein

HTTP-Statuscode	Beschreibung	JSON-Text
404 Nicht Gefunden	Zeigt an, dass die angeforderte Ressource nicht gefunden werden konnte. Dieser Code ist gültig für nicht vorhandene APIs oder nicht vorhandene Ressourcen, die durch die Kennung angefordert werden.	Nein
422 Nicht Verarbeitbare Einheit	Gibt an, dass die Anforderung in der Regel gut geformt ist, jedoch sind die Eingabeparameter ungültig oder der Status des Speichersystems erlaubt Web Services nicht, die Anforderung zu erfüllen.	Ja.
424 Abhängigkeit Fehlgeschlagen	Wird im Web Services Proxy verwendet, um anzuzeigen, dass das angeforderte Speichersystem derzeit nicht verfügbar ist. Daher können Web Services die Anforderung nicht erfüllen.	Nein
429 Zu Viele Anfragen	Gibt an, dass eine Antragsbegrenzung überschritten wurde und zu einem späteren Zeitpunkt erneut versucht werden sollte.	Nein

Beispielskripts

GitHub enthält ein Repository für die Sammlung und Organisation von Beispielskripten, die die Verwendung der NetApp SANtricity Web Services API veranschaulichen. Informationen zum Zugriff auf das Repository finden Sie unter "Beispiele für NetApp Webservices".

Begriffe und Konzepte

Die folgenden Begriffe gelten für den Web Services Proxy.

Laufzeit	Definition
API	Eine API (Application Programming Interface) besteht aus Protokollen und Methoden, die es Entwicklern ermöglichen, mit Geräten zu kommunizieren. Die Web Services API dient zur Kommunikation mit E-Series Storage-Systemen.

Laufzeit	Definition
ASUP	Die AutoSupport (ASUP) Funktion sammelt Daten in einem Kunden-Support-Bundle und sendet die Nachrichtendatei automatisch an den technischen Support, um die Remote-Fehlerbehebung und Problemanalyse zu durchführen.
Endpunkt	Endpunkte sind Funktionen, die über die API verfügbar sind. Ein Endpunkt enthält ein HTTP-Verb sowie den URI-Pfad. In Web Services können Endpunkte Aufgaben wie das Erkennen von Storage-Systemen und das Erstellen von Volumes ausführen.
HTTP-Verb	Ein HTTP-Verb ist eine entsprechende Aktion für einen Endpunkt, wie z. B. das Abrufen und Erstellen von Daten. In Web Services umfassen HTTP-Verben POST, GET und DELETE.
JSON	JavaScript Object Notation (JSON) ist ein strukturiertes Datenformat ähnlich wie XML, das ein minimales, lesbares Format verwendet. Daten in Web Services werden über JSON verschlüsselt.
REST/Ruhe	Representational State Transfer (REST) ist eine lose Spezifikation, die einen Architekturstil für eine API definiert. Da die meisten REST-APIs nicht vollständig der Spezifikation entsprechen, werden sie als „`reSTful`“ oder „`re` ST-Like“ beschrieben. Im Allgemeinen ist eine “reSTful”-API unabhängig von Programmiersprachen und hat die folgenden Eigenschaften: • HTTP-basiert, die der allgemeinen Semantik des Protokolls folgt • Hersteller und Verbraucher strukturierter Daten (JSON, XML, etc.) • Objektorientiert (im Gegensatz zu betriebsorientiert) Web Services ist eine RESTful API, die Zugriff auf nahezu alle SANtricity Managementfunktionen bietet.
Storage-System	Ein Storage-System ist ein E-Series Array, das Shelfs, Controller, Laufwerke, Software Und Firmware.
Symbol-API	Symbol ist eine ältere API für das Management von E-Series Storage-Systemen. Die zugrunde liegende Implementierung der Web Services API verwendet Symbol.

Laufzeit	Definition
Web-Services	Web Services ist eine API, die NetApp für Entwickler zum Management von E-Series Storage-Systemen entwickelt hat. Es gibt zwei Implementierungen von Web Services: Eingebettet in den Controller und einen separaten Proxy, der auf Linux oder Windows installiert werden kann.

Installieren und konfigurieren

Installations- und Upgrade-Anforderungen prüfen

Überprüfen Sie vor der Installation des Web Services Proxy die Installationsanforderungen und die Upgrade-Überlegungen.

Installationsvoraussetzungen

Sie können den Web Services Proxy auf einem Windows- oder Linux-Host-System installieren und konfigurieren.

Die Proxy-Installation umfasst die folgenden Anforderungen.

Anforderungen	Beschreibung
Host-Einschränkungen	Stellen Sie sicher, dass der Hostname des Servers, auf dem Sie den Web Services Proxy installieren möchten, nur ASCII-Buchstaben, numerische Ziffern und Bindestriche (-) enthält. Diese Anforderung ist auf eine Beschränkung von Java Keytool zurückzuführen, das bei der Generierung eines selbst signierten Zertifikats für den Server verwendet wird. Wenn der Hostname Ihres Servers andere Zeichen wie z. B. einen Unterstrich (_) enthält, kann der Webserver nach der Installation nicht gestartet werden.
Betriebssysteme	Sie können den Proxy auf den folgenden Betriebssystemen installieren: • Linux • Windows Eine vollständige Liste der Betriebssysteme und der Firmware-Kompatibilität finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".
Linux: Zusätzliche Überlegungen	Linux Standard Base Bibliotheken (init-Funktionen) sind erforderlich, damit der Webserver ordnungsgemäß funktioniert. Sie müssen die lsb/insserv-Pakete für Ihr Betriebssystem installieren. Weitere Informationen finden Sie im Abschnitt „zusätzliche Pakete erforderlich“ der Readme-Datei.

Anforderungen	Beschreibung
Mehrere Instanzen	Sie können nur eine Instanz von Web Services Proxy auf einem Server installieren. Sie können den Proxy jedoch auf mehreren Servern in Ihrem Netzwerk installieren.
Kapazitätsplanung	Für die Protokollierung von Web Services Proxy ist ausreichend Speicherplatz erforderlich. Stellen Sie sicher, dass Ihr System die folgenden Anforderungen an den verfügbaren Speicherplatz erfüllt: • Erforderlicher Installationsspeicherplatz — 275 MB • Minimaler Protokollierungspeicherplatz — 200 MB • Systemspeicher — 2 GB; Heap-Speicherplatz ist standardmäßig 1 GB Sie können ein Tool zum Monitoring des Festplattenspeichers verwenden, um den verfügbaren Festplattenspeicher für persistenten Speicher und die Protokollierung zu überprüfen.
Lizenz	Der Web Services Proxy ist ein kostenloses eigenständiges Produkt, das keinen Lizenzschlüssel erfordert. Es gelten jedoch geltende Urheberrechte und Nutzungsbedingungen. Wenn Sie den Proxy entweder im Graphical- oder im Konsolenmodus installieren, müssen Sie die Endbenutzer-Lizenzvereinbarung (Endbenutzer License Agreement, EULA) akzeptieren.

Upgrade-Überlegungen

Wenn Sie ein Upgrade von einer vorherigen Version durchführen, beachten Sie, dass einige Elemente beibehalten oder entfernt werden.

- Für den Web Services Proxy bleiben die früheren Konfigurationseinstellungen erhalten. Diese Einstellungen umfassen Benutzerpasswörter, alle erkannten Speichersysteme, Serverzertifikate, vertrauenswürdige Zertifikate und die Konfiguration der Serverlaufzeit.
- Bei Unified Manager werden alle zuvor im Repository geladenen SANtricity-Betriebssystemdateien während des Upgrades entfernt.

Installieren oder Aktualisieren der Web Services Proxy-Datei

Die Installation beinhaltet das Herunterladen der Datei und dann die Installation des Proxy-Pakets auf einem Linux- oder Windows-Server. Sie können den Proxy auch mit diesen Anweisungen aktualisieren.

Laden Sie Web Services Proxy-Dateien herunter

Sie können die Installationsdatei und die Readme-Datei von der Software Download-Seite der NetApp Support-Website herunterladen.

Das Download-Paket umfasst den Web Services Proxy und die Unified Manager-Schnittstelle.

Schritte

1. Gehen Sie zu "NetApp Support – Downloads".
2. Wählen Sie **E-Series SANtricity Web Services Proxy** aus.
3. Befolgen Sie die Anweisungen zum Herunterladen der Datei. Stellen Sie sicher, dass Sie das richtige Download-Paket für Ihren Server auswählen (z. B. EXE für Windows; BIN oder RPM für Linux).
4. Laden Sie die Installationsdatei auf den Server herunter, auf dem Sie den Proxy und Unified Manager installieren möchten.

Installation auf Windows- oder Linux-Server

Sie können den Web Services Proxy und Unified Manager über einen der drei Modi (Graphical, Console oder Silent) oder über eine RPM-Datei (nur Linux) installieren.

Bevor Sie beginnen

- "Installationsanforderungen prüfen".
- Stellen Sie sicher, dass Sie die korrekte Installationsdatei (EXE für Windows; BIN für Linux) auf den Server heruntergeladen haben, auf dem Sie den Proxy und Unified Manager installieren möchten.

Grafikmodus installieren

Sie können die Installation im grafischen Modus für Windows oder Linux ausführen. Im grafischen Modus werden die Aufforderungen in einer Windows-Benutzeroberfläche angezeigt.

Schritte

1. Greifen Sie auf den Ordner zu, in dem Sie die Installationsdatei heruntergeladen haben.
2. Starten Sie die Installation für Windows oder Linux wie folgt:

   - Windows — Doppelklicken Sie auf die Installationsdatei:

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

   - Linux — führen Sie den folgenden Befehl aus: `santricity_webservices-linux_x64-nn.nn.nn.nnnn.bin`

     In den obigen Dateinamen `nn.nn.nn.nnnn` Stellt die Versionsnummer dar.

   Der Installationsprozess wird gestartet und der Begrüßungsbildschirm des NetApp SANtricity Web Services Proxy + Unified Manager wird angezeigt.

3. Befolgen Sie die Anweisungen auf dem Bildschirm.

   Während der Installation werden Sie aufgefordert, mehrere Funktionen zu aktivieren und einige Konfigurationsparameter einzugeben. Bei Bedarf können Sie eine dieser Optionen später in den Konfigurationsdateien ändern.

   > Während eines Upgrades werden keine Konfigurationsparameter angezeigt.

4. Wenn die Meldung Webserver gestartet angezeigt wird, klicken Sie auf **OK**, um die Installation abzuschließen.

   Das Dialogfeld „Installation abgeschlossen“ wird angezeigt.

5. Aktivieren Sie die Kontrollkästchen, wenn Sie Unified Manager oder die interaktive API-Dokumentation starten möchten, und klicken Sie dann auf **Fertig**.

Installation im Konsolenmodus

Sie können die Installation im Konsolenmodus für Windows oder Linux ausführen. Im Konsolenmodus werden die Eingabeaufforderungen im Terminalfenster angezeigt.

Schritte

1. Führen Sie den folgenden Befehl aus: `<install filename> -i console`

   Im obigen Befehl `<install filename>` Gibt den Namen der heruntergeladenen Proxyinstallationsdatei an (z. B.: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

   > Um die Installation während des Installationsvorgangs jederzeit abzubrechen, geben Sie ein `QUIT` An der Eingabeaufforderung.

   Der Installationsprozess wird gestartet, und die Meldung Installer starten — Einleitung wird angezeigt.

2. Befolgen Sie die Anweisungen auf dem Bildschirm.

   Während der Installation werden Sie aufgefordert, mehrere Funktionen zu aktivieren und einige Konfigurationsparameter einzugeben. Bei Bedarf können Sie eine dieser Optionen später in den Konfigurationsdateien ändern.

   > Während eines Upgrades werden keine Konfigurationsparameter angezeigt.

3. Wenn die Installation abgeschlossen ist, drücken Sie **Enter**, um das Installationsprogramm zu beenden.

Installation im Silent-Modus

Sie können die Installation im Silent-Modus für Windows oder Linux ausführen. Im Silent-Modus werden keine Rücksendemeldungen oder -Skripte im Terminalfenster angezeigt.

Schritte

1. Führen Sie den folgenden Befehl aus: `<install filename> -i silent`

   Im obigen Befehl `<install filename>` Gibt den Namen der heruntergeladenen Proxyinstallationsdatei an (z. B.: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

2. Drücken Sie **Enter**.

   Die Installation kann mehrere Minuten in Anspruch nehmen. Nach erfolgreicher Installation wird im Terminalfenster eine Eingabeaufforderung angezeigt.

RPM Command install (nur Linux)

Für Linux-Systeme, die mit dem RPM-Paketverwaltungssystem kompatibel sind, können Sie den Web Services Proxy über eine optionale RPM-Datei installieren.

Schritte

1. Laden Sie die RPM-Datei auf den Server herunter, auf dem Sie den Proxy und Unified Manager installieren

möchten.

2. Öffnen Sie ein Terminal-Fenster.
3. Geben Sie den folgenden Befehl ein:

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

> Im obigen Befehl `nn.nn.nn.nnnn` Stellt die Versionsnummer dar.

Die Installation kann mehrere Minuten in Anspruch nehmen. Nach erfolgreicher Installation wird im Terminalfenster eine Eingabeaufforderung angezeigt.

Melden Sie sich bei API und Unified Manager an

Web Services umfasst die API-Dokumentation, mit der Sie direkt mit DER REST API interagieren können. Das System umfasst zudem Unified Manager, eine browserbasierte Schnittstelle zum Management mehrerer Storage-Systeme der E-Series.

Melden Sie sich bei der Web Services-API an

Nach der Installation des Web Services Proxy können Sie in einem Browser auf die interaktive API-Dokumentation zugreifen.

Die API-Dokumentation läuft mit jeder Instanz von Web Services und ist über die NetApp Support-Website auch im statischen PDF-Format verfügbar. Um auf die interaktive Version zuzugreifen, öffnen Sie einen Browser und geben die URL ein, auf die der Speicherort von Web Services verweist (entweder ein Controller für die eingebettete Version oder ein Server für den Proxy).

> Die Web Services API implementiert die OpenAPI-Spezifikation (ursprünglich Swagger-Spezifikation genannt).

Zur ersten Anmeldung verwenden Sie die „admin“-Anmeldedaten. „Admin“ gilt als Superadministrator mit Zugriff auf alle Funktionen und Rollen.

Schritte

1. Öffnen Sie einen Browser.
2. Geben Sie die URL für die eingebettete oder Proxy-Implementierung ein:
   - Eingebettet: `https://<controller>:<port>/devmgr/docs/`

     In dieser URL `<controller>` Ist die IP-Adresse oder der FQDN des Controllers, und `<port>` Die Management-Port-Nummer des Controllers (standardmäßig 8443).
   - Proxy: `http[s]://<server>:<port>/devmgr/docs/`

     In dieser URL `<server>` Ist die IP-Adresse oder der FQDN des Servers, auf dem der Proxy installiert ist, und `<port>` Ist die Nummer des Listening-Ports (standardmäßig 8080 für HTTP oder 8443 für HTTPS).

     > Wenn der Listening-Port bereits verwendet wird, erkennt der Proxy den Konflikt und fordert Sie auf, einen anderen Listening-Port auszuwählen.

Die API-Dokumentation wird im Browser geöffnet.

3. Wenn die interaktive API-Dokumentation geöffnet wird, gehen Sie zum Dropdown-Menü oben rechts auf der Seite und wählen Sie **utils**.
4. Klicken Sie auf die Kategorie **Login**, um die verfügbaren Endpunkte anzuzeigen.
5. Klicken Sie auf den Endpunkt **POST: /Login** und dann auf **Try it out**.
6. Geben Sie bei der ersten Anmeldung „admin“ für den Benutzernamen und das Kennwort ein.
7. Klicken Sie Auf **Ausführen**.
8. Um auf die Endpunkte für die Speicherverwaltung zuzugreifen, gehen Sie zum Dropdown-Menü oben rechts und wählen Sie **v2**.

   Die übergeordneten Kategorien für Endpunkte werden angezeigt. Sie können die API-Dokumentation wie in der Tabelle beschrieben navigieren.

Werden	Beschreibung
Dropdown-Menü	Rechts oben auf der Seite bietet ein Dropdown-Menü Optionen zum Wechseln zwischen Version 2 der API-Dokumentation (V2), Symbol-Schnittstelle (Symbol V2) und API-Dienstprogrammen (Utils) zur Anmeldung. Da Version 1 der API-Dokumentation ein Vorrecht war und nicht allgemein verfügbar ist, ist V1 nicht im Dropdown-Menü enthalten.
Kategorien	Die API-Dokumentation ist nach übergeordneten Kategorien organisiert (z. B. Administration, Konfiguration). Klicken Sie auf eine Kategorie, um die zugehörigen Endpunkte anzuzeigen.
Endpunkte	Wählen Sie einen Endpunkt aus, um seine URL-Pfade, erforderlichen Parameter, Antwortkörper und Statuscodes anzuzeigen, die die URLs wahrscheinlich zurückgeben werden.
Probieren Sie Es Aus	Interagieren Sie direkt mit dem Endpunkt, indem Sie auf **Try IT Out** klicken. Diese Schaltfläche ist in jeder erweiterten Ansicht für Endpunkte enthalten. Wenn Sie auf die Schaltfläche klicken, werden Felder zur Eingabe von Parametern angezeigt (falls zutreffend). Sie können dann Werte eingeben und auf **Ausführen** klicken. Die interaktive Dokumentation verwendet JavaScript, um die Anfrage direkt an die API zu stellen; es handelt sich nicht um eine Testanforderung.

Melden Sie sich bei Unified Manager an

Nach der Installation des Web Services Proxy können Sie auf Unified Manager zugreifen, um mehrere Speichersysteme in einer webbasierten Schnittstelle zu verwalten.

Um auf Unified Manager zuzugreifen, öffnen Sie einen Browser und geben die URL ein, die auf die installierte Proxy-Adresse verweist. Die folgenden Browser und Versionen werden unterstützt.

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

Schritte

1. Öffnen Sie einen Browser, und geben Sie die folgende URL ein:

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

   In dieser URL `<server>` Stellt die IP-Adresse oder den FQDN des Servers dar, auf dem der Web Services Proxy installiert ist, und `<port>` Gibt die Nummer des Listening-Ports an (standardmäßig 8080 für HTTP oder 8443 für HTTPS).

   Die Anmeldeseite für Unified Manager wird geöffnet.

2. Geben Sie für die erste Anmeldung ein `admin` Geben Sie für den Benutzernamen ein und bestätigen Sie dann ein Passwort für den Admin-Benutzer.

   Das Passwort kann bis zu 30 Zeichen umfassen. Weitere Informationen zu Benutzern und Passwörtern finden Sie im Abschnitt Zugriffsmanagement der Online-Hilfe von Unified Manager.

Konfigurieren Sie Web Services Proxy

Sie können die Web Services Proxy-Einstellungen ändern, um die spezifischen Betriebs- und Performance-Anforderungen für Ihre Umgebung zu erfüllen.

Stoppen oder starten Sie den Webserver neu

Der Webserver-Dienst wird während der Installation gestartet und läuft im Hintergrund. Während einiger Konfigurationsaufgaben müssen Sie den Webserver-Dienst möglicherweise anhalten oder neu starten.

Schritte

1. Führen Sie einen der folgenden Schritte aus:

- Öffnen Sie für Windows das Menü **Start** und wählen Sie MENU:Administrative Tools[Dienste], suchen Sie **NetApp SANtricity Webservices** und wählen Sie dann entweder **Stopp** oder **Neustart** aus.
- Wählen Sie unter Linux die Methode zum Stoppen und Neustarten des Webservers für Ihre Betriebssystemversion aus. Während der Installation wurde in einem Popup-Dialog angezeigt, welcher Daemon gestartet hat. Beispiel:

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

Die am häufigsten verwendete Methode für die Interaktion mit dem Dienst ist die Verwendung `systemctl` Befehle.

Beheben von Port-Konflikten

Wenn der Web Services Proxy ausgeführt wird, während eine andere Anwendung an der definierten Adresse oder dem festgelegten Port verfügbar ist, können Sie den Portkonflikt in der Datei wsconfig.xml beheben.

Schritte

1. Öffnen Sie die Datei wsconfig.xml unter:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_Web_Services_Proxy
2. Fügen Sie der Datei wsconfig.xml die folgende Zeile hinzu, in der *n* die Portnummer ist:

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

   In der folgenden Tabelle werden die Attribute aufgeführt, die HTTP-Ports und HTTPS-Ports steuern.

Name	Beschreibung	Übergeordnetes Node	Merkmale	Erforderlich
Konfigurations	Der Root-Node für die Konfiguration	Null	Version - die Version des Konfigurationsschemas ist derzeit 1.0.	Ja.
Sslport	Der TCP-Port zum Abhören von SSL-Anforderungen. Die Standardeinstellung ist 8443.	Konfigurations	Clientauth	Nein
Port	Der TCP-Port zum Abhören von HTTP-Anfragen ist standardmäßig auf 8080 eingestellt.	Konfigurations	-	Nein

3. Speichern und schließen Sie die Datei.
4. Starten Sie den Webserver-Dienst neu, damit die Änderung wirksam wird.

Konfiguration von Load Balancing und/oder Hochverfügbarkeit

Wenn Sie den Web Services Proxy in einer hochverfügbaren (HA) Konfiguration verwenden möchten, können Sie den Lastausgleich konfigurieren. In einer HA-Konfiguration erhält normalerweise entweder ein einzelner Node alle Anfragen, während die anderen im Standby-Verhältnis sind oder bei den Anforderungen ein Lastausgleich über alle Nodes hinweg erfolgt.

Der Web Services Proxy kann in einer hochverfügbaren (HA) Umgebung vorhanden sein, wobei die meisten APIs unabhängig vom Empfänger der Anfrage korrekt funktionieren. Metadaten-Tags und Ordner sind zwei Ausnahmen, da Tags und Ordner in einer lokalen Datenbank gespeichert und nicht zwischen Web Services Proxy-Instanzen freigegeben werden.

Es gibt jedoch einige bekannte Zeitprobleme, die in einem kleinen Prozentsatz von Anforderungen auftreten. Insbesondere kann eine Instanz des Proxy neuere Daten schneller als eine zweite Instanz für ein kleines Fenster haben. Der Web Services Proxy enthält eine spezielle Konfiguration, die dieses Timing-Problem beseitigt. Diese Option ist standardmäßig nicht aktiviert, da sie die benötigte Zeit für Serviceanfragen erhöht (für Datenkonsistenz). Um diese Option zu aktivieren, müssen Sie einer INI-Datei (für Windows) oder einer .SH-Datei (für Linux) eine Eigenschaft hinzufügen.

Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Windows: Öffnen Sie die Datei appserver64.ini, und fügen Sie dann die hinzu `Dload-balance.enabled=true` Eigenschaft.

     Beispiel: `vmarg.7=-Dload-balance.enabled=true`

   - Linux: Öffnen Sie die Datei webserver.sh, und fügen Sie dann die hinzu `Dload-balance.enabled=true` Eigenschaft.

     Beispiel: `DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`
2. Speichern Sie die Änderungen.
3. Starten Sie den Webserver-Dienst neu, damit die Änderung wirksam wird.

Symbol HTTPS deaktivieren

Sie können Symbolbefehle (Standardeinstellung) deaktivieren und Befehle über einen Remote-Prozeduraufruf (RPC) senden. Diese Einstellung kann in der Datei wsconfig.xml geändert werden.

Standardmäßig sendet der Web Services Proxy für alle Storage-Systeme der E2800 Serie und der E5700 Serie mit SANtricity OS Version 08.40 oder höher Symbolbefehle über HTTPS. Über HTTPS gesendete Symbolbefehle werden an das Speichersystem authentifiziert. Bei Bedarf können Sie die HTTPS-Symbolunterstützung deaktivieren und Befehle über RPC senden. Immer wenn das Symbol über RPC konfiguriert ist, sind alle passiven Befehle des Speichersystems ohne Authentifizierung aktiviert.

> Wenn Symbol über RPC verwendet wird, kann der Web Services Proxy keine Verbindung zu Systemen herstellen, bei denen der Port für die Symbolverwaltung deaktiviert ist.

Schritte

1. Öffnen Sie die Datei wsconfig.xml unter:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_Web_Services_Proxy
2. Im `devicemgt.symbolclientstrategy` Eingabe, ersetzen Sie den `httpsPreferred` Wert mit `rpcOnly`.

   Beispiel:

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

3. Speichern Sie die Datei.

Konfigurieren der Cross-Origin-Ressourcen-Sharing

Sie können CORS (Cross-Origin Resource Sharing) konfigurieren. Hierbei handelt es sich um einen Mechanismus, der zusätzliche HTTP-Header verwendet, um eine Web-Anwendung bereitzustellen, die an einem Ursprung ausgeführt wird und über die Berechtigung zum Zugriff auf ausgewählte Ressourcen von einem Server mit einem anderen Ursprung verfügt.

CORS wird von der Datei cors.cfg im Arbeitsverzeichnis bearbeitet. Die CORS-Konfiguration ist standardmäßig geöffnet, sodass der bereichsübergreifende Zugriff nicht eingeschränkt ist.

Wenn keine Konfigurationsdatei vorhanden ist, ist CORS geöffnet. Aber wenn die Datei cors.cfg vorhanden ist, wird sie verwendet. Wenn die Datei cors.cfg leer ist, können Sie keine CORS-Anforderung erstellen.

Schritte

1. Öffnen Sie die Datei cors.cfg, die sich im Arbeitsverzeichnis befindet.
2. Fügen Sie die gewünschten Zeilen der Datei hinzu.

   Jede Zeile in der CORS-Konfigurationsdatei ist ein regelmäßiges Ausdrucksmuster, das übereinstimmen muss. Die Ursprungsüberschrift muss mit einer Zeile in der Datei cors.cfg übereinstimmen. Wenn ein Linienmuster mit der Ursprungsüberschrift übereinstimmt, ist die Anforderung zulässig. Der vollständige Ursprung wird verglichen, nicht nur das Host-Element.

3. Speichern Sie die Datei.

Anforderungen werden auf dem Host und dem Protokoll zugeordnet, z. B.:

- Localhost mit jedem Protokoll abstimmen — `*localhost*`
- Localhost nur für HTTPS abstimmen — `https://localhost*`

Deinstallieren Sie Web Services Proxy

Um Web Services Proxy und Unified Manager zu entfernen, können Sie jeden beliebigen Modus verwenden (Graphical, Console, Silent oder RPM-Datei), unabhängig von der Methode, die Sie zum Installieren des Proxy verwendet haben.

Grafikmodus deinstallieren

Sie können die Deinstallation im grafischen Modus für Windows oder Linux ausführen. Im grafischen Modus werden die Aufforderungen in einer Windows-Benutzeroberfläche angezeigt.

Schritte

1. Starten Sie die Deinstallation für Windows oder Linux wie folgt:
   - Windows — Gehen Sie zu dem Verzeichnis, das die Deinstallationsdatei uninstall_Web_Services_Proxy enthält. Das Standardverzeichnis befindet sich an folgender Adresse: C:/Program Files/NetApp/SANtricity Web Services Proxy/. Doppelklicken `uninstall_web_services_proxy.exe`.

     Alternativ können Sie zu **Systemsteuerung › Programme › Programm deinstallieren** und dann „NetApp SANtricity Web Services Proxy“ wählen.

   - Linux — Gehen Sie zum Verzeichnis, das die Deinstallationsdatei für Web Services Proxy enthält. Das Standardverzeichnis befindet sich an der folgenden Stelle: `/opt/netapp/santricity_web_services_proxy/uninstall_web_services_proxy`
2. Führen Sie den folgenden Befehl aus:

   ```
   uninstall_web_services_proxy -i gui
   ```

   Der Startbildschirm für SANtricity Webdienste-Proxy wird angezeigt.

3. Klicken Sie im Dialogfeld Deinstallieren auf **Deinstallieren**.

   Die Fortschrittsanzeige „Uninstaller“ wird angezeigt und zeigt den Fortschritt an.

4. Wenn die Meldung „Deinstallation abgeschlossen“ angezeigt wird, klicken Sie auf **Fertig**.

Deinstallieren des Konsolenmodus

Sie können die Deinstallation im Konsolenmodus für Windows oder Linux ausführen. Im Konsolenmodus werden die Eingabeaufforderungen im Terminalfenster angezeigt.

Schritte

1. Gehen Sie zum Verzeichnis uninstall_Web_Services_Proxy.
2. Führen Sie den folgenden Befehl aus:

   ```
   uninstall_web_services_proxy -i console
   ```

   Der Deinstallationsprozess wird gestartet.

3. Wenn die Deinstallation abgeschlossen ist, drücken Sie **Enter**, um das Installationsprogramm zu beenden.

Deinstallation im Silent-Modus

Sie können die Deinstallation im Silent-Modus für Windows oder Linux ausführen. Im Silent-Modus werden keine Rücksendemeldungen oder -Skripte im Terminalfenster angezeigt.

Schritte

1. Gehen Sie zum Verzeichnis uninstall_Web_Services_Proxy.
2. Führen Sie den folgenden Befehl aus:

   ```
   uninstall_web_services_proxy -i silent
   ```

Der Deinstallationsprozess wird ausgeführt, es werden jedoch keine Rücksendemeldungen oder Skripte im Terminalfenster angezeigt. Nachdem Web Services Proxy erfolgreich deinstalliert wurde, wird im Terminalfenster eine Eingabeaufforderung angezeigt.

RPM-Befehl deinstallieren (nur Linux)

Sie können den Befehl RPM verwenden, um Web Services Proxy von einem Linux-System zu deinstallieren.

Schritte

1. Öffnen Sie ein Terminal-Fenster.
2. Geben Sie die folgende Befehlszeile ein:

```
rpm -e santricity_webservices
```

> Beim Deinstallationsprozess können Dateien verbleiben, die nicht zur ursprünglichen Installation gehören. Löschen Sie diese Dateien manuell, um Web Services Proxy vollständig zu entfernen.

Benutzerzugriff in Web Services Proxy verwalten

Sie können den Benutzerzugriff auf die Web Services-API und Unified Manager für Sicherheitszwecke verwalten.

Überblick über Zugriffsmanagement

Zum Zugriffsmanagement gehören rollenbasierte Anmeldedaten, Passwortverschlüsselung, grundlegende Authentifizierung und LDAP-Integration.

Rollenbasierter Zugriff

Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) ordnet vordefinierte Benutzer Rollen zu. Jede Rolle gewährt Berechtigungen für eine bestimmte Funktionsebene.

In der folgenden Tabelle werden die einzelnen Rollen beschrieben.

Rolle	Beschreibung
Sicherheit.admin	SSL- und Zertifikatmanagement
Storage.Administration	Vollständiger Lese-/Schreibzugriff auf die Konfiguration des Storage-Systems.
Storage.Monitor	Schreibgeschützter Zugriff auf die Anzeige von Storage-Systemdaten.
Support.Administration	Zugriff auf alle Hardware-Ressourcen auf Storage-Systemen und Supportvorgänge, z. B. Abruf von AutoSupport (ASUP)

Standardbenutzerkonten sind in der Datei users.properties definiert. Sie können Benutzerkonten ändern, indem Sie die Datei users.properties direkt ändern oder die Zugriffsverwaltungsfunktionen in Unified Manager

verwenden.

In der folgenden Tabelle sind die für den Web Services Proxy verfügbaren Benutzeranmeldungen aufgeführt.

Vordefinierte Benutzeranmeldung	Beschreibung
Admin	Ein Superadministrator, der Zugriff auf alle Funktionen hat und alle Rollen enthält. Für Unified Manager müssen Sie das Passwort bei der ersten Anmeldung festlegen.
Storage	Der Administrator, der für die gesamte Storage-Provisionierung verantwortlich ist. Dieser Benutzer umfasst die folgenden Rollen: Storage.admin, Support.admin und Storage.Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
Sicherheit	Der für die Sicherheitskonfiguration verantwortliche Benutzer. Dieser Benutzer enthält die folgenden Rollen: Security.admin und Storage.Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
Support	Der Benutzer ist für Hardware-Ressourcen, Ausfalldaten und Firmware-Upgrades verantwortlich. Dieser Benutzer enthält die folgenden Rollen: Support.admin und Storage.Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
Überwachen	Ein Benutzer mit schreibgeschütztem Zugriff auf das System. Dieser Benutzer enthält nur die Rolle Storage.Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
rw (alt für ältere Arrays)	der rw-Benutzer (Lese/Schreib) umfasst die folgenden Rollen: Storage.admin, Support.admin und Storage.Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
ro (Altsysteme für ältere Arrays)	Der Benutzer ro (schreibgeschützt) enthält nur die Rolle „Storage.Monitor“. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.

Kennwortverschlüsselung

Für jedes Passwort können Sie einen zusätzlichen Verschlüsselungsvorgang mit der vorhandenen SHA256-Kennwortkodierung anwenden. Bei diesem zusätzlichen Verschlüsselungsverfahren wird für jede SHA256-Hash-Verschlüsselung ein zufälliger Byte-Satz auf jedes Passwort (Salt) angewendet. Die SHA256-Verschlüsselung wird auf alle neu erstellten Passwörter angewendet.

> Vor der Veröffentlichung von Web Services Proxy 3.0 wurden Passwörter nur über SHA256 Hashing verschlüsselt. Alle vorhandenen SHA256-Hash-only-verschlüsselten Passwörter behalten diese Codierung und sind weiterhin unter der Datei users.properties gültig. Allerdings sind SHA256-Hash-only-verschlüsselte Passwörter nicht so sicher wie die Passwörter mit gesalzter SHA256-Verschlüsselung.

Grundlegende Authentifizierung

Standardmäßig ist die Basisauthentifizierung aktiviert, was bedeutet, dass der Server eine grundlegende Authentifizierungsaufgabe zurückgibt. Diese Einstellung kann in der Datei wsconfig.xml geändert werden.

LDAP

Lightweight Directory Access Protocol (LDAP), ein Anwendungsprotokoll für den Zugriff auf verteilte Verzeichnisinformationsdienste und die Wartung, ist für den Web Services Proxy aktiviert. Die LDAP-Integration ermöglicht die Benutzerauthentifizierung und Zuordnung von Rollen zu Gruppen.

Informationen zum Konfigurieren der LDAP-Funktionalität finden Sie in den Konfigurationsoptionen der Unified Manager-Schnittstelle oder im LDAP-Abschnitt der interaktiven API-Dokumentation.

Konfigurieren Sie den Benutzerzugriff

Sie können den Benutzerzugriff verwalten, indem Sie zusätzliche Verschlüsselung auf Passwörter anwenden, grundlegende Authentifizierungsvorgaben festlegen und rollenbasierten Zugriff festlegen.

Wenden Sie die zusätzliche Verschlüsselung auf Passwörter an

Um die höchste Sicherheitsstufe zu erreichen, können Sie mithilfe der vorhandenen SHA256-Kennwortkodierung zusätzliche Verschlüsselung für Passwörter anwenden.

Bei diesem zusätzlichen Verschlüsselungsverfahren wird für jede SHA256-Hash-Verschlüsselung ein zufälliger Byte-Satz auf jedes Passwort (Salt) angewendet. Die SHA256-Verschlüsselung wird auf alle neu erstellten Passwörter angewendet.

Schritte

1. Öffnen Sie die Datei users.properties unter:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\Data\config
   - (Linux) — /opt/netapp/santricity_Web_Services_Proxy/Daten/config
2. Geben Sie das verschlüsselte Kennwort als Klartext erneut ein.
3. Führen Sie die aus `securepasswds` Befehlszeilendienstprogramm zum Reverschlüsseln des Passworts oder einfach den Web Services Proxy neu starten. Dieses Dienstprogramm wird im Stamminstallationsverzeichnis für den Web Services Proxy installiert.

> Alternativ können Sie lokale Benutzerpasswörter einfach salzen und hashen, wenn die Kennwortänderungen über Unified Manager vorgenommen werden.

Konfigurieren Sie die grundlegende Authentifizierung

Standardmäßig ist die Basisauthentifizierung aktiviert, was bedeutet, dass der Server eine grundlegende Authentifizierungsaufgabe zurückgibt. Sie können diese Einstellung bei Bedarf in der Datei wsconfig.xml ändern.

1. Öffnen Sie die Datei wsconfig.xml unter:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_Web_Services_Proxy
2. Ändern Sie die folgende Zeile in der Datei, indem Sie false (nicht aktiviert) oder true (aktiviert) angeben.

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

3. Speichern Sie die Datei.
4. Starten Sie den Webserver-Dienst neu, damit die Änderung wirksam wird.

Konfigurieren Sie den rollenbasierten Zugriff

Um den Benutzerzugriff auf bestimmte Funktionen zu beschränken, können Sie ändern, welche Rollen für jedes Benutzerkonto angegeben sind.

Der Web Services Proxy umfasst eine rollenbasierte Zugriffssteuerung (RBAC), in der Rollen vordefinierten Benutzern zugeordnet werden. Jede Rolle gewährt Berechtigungen für eine bestimmte Funktionsebene. Sie können die Rollen ändern, die Benutzerkonten zugewiesen sind, indem Sie die Datei users.properties direkt ändern.

> Sie können Benutzerkonten auch über die Zugriffsverwaltung in Unified Manager ändern. Weitere Informationen finden Sie in der Online-Hilfe von Unified Manager.

Schritte

1. Öffnen Sie die Datei users.properties unter:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\Data\config
   - (Linux) — /opt/netapp/santricity_Web_Services_Proxy/Daten/config
2. Suchen Sie die Zeile für das zu ändernde Benutzerkonto (Speicherung, Sicherheit, Überwachung, Unterstützung, rw, Oder ro).

   > Ändern Sie den Admin-Benutzer nicht. Dies ist ein Superuser mit Zugriff auf alle Funktionen.

3. Fügen Sie die angegebenen Rollen nach Bedarf hinzu oder entfernen Sie sie.

   Hier einige Funktionen:

   - Security.admin — SSL- und Zertifikatmanagement.
   - Storage.admin – vollständiger Lese-/Schreibzugriff auf die Konfiguration des Storage-Systems.
   - Storage.Monitor: Schreibgeschützter Zugriff zur Anzeige von Storage-Systemdaten
   - Support.admin – Zugriff auf alle Hardware-Ressourcen in Storage-Systemen und Supportvorgänge, z. B. Abruf von AutoSupport (ASUP)

   > Die Rolle „Storage.Monitor“ ist für alle Benutzer, einschließlich des Administrators, erforderlich.

4. Speichern Sie die Datei.

Verwalten von Sicherheit und Zertifikaten in Web Services Proxy

Für die Sicherheit im Web Services Proxy können Sie eine SSL-Port-Bezeichnung angeben und Zertifikate verwalten. Zertifikate identifizieren Website-Eigentümer für sichere Verbindungen zwischen Clients und Servern.

Aktivieren Sie SSL

Der Web Services Proxy verwendet Secure Sockets Layer (SSL) für die Sicherheit, die während der Installation aktiviert ist. Sie können die SSL-Portbezeichnung in der Datei wsconfig.xml ändern.

Schritte

1. Öffnen Sie die Datei wsconfig.xml unter:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_Web_Services_Proxy
2. Fügen Sie die SSL-Portnummer hinzu oder ändern Sie sie, ähnlich dem folgenden Beispiel:

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

Ergebnis

Wenn der Server mit konfiguriertem SSL gestartet wird, sucht der Server nach den KeyStore- und Truststore-Dateien.

- Wenn der Server keinen Schlüsselspeicher findet, verwendet der Server die IP-Adresse der ersten erkannten nicht-Loopback-IPv4-Adresse, um einen Schlüsselspeicher zu generieren und anschließend ein selbstsigniertes Zertifikat zum Schlüsselspeicher hinzuzufügen.
- Wenn der Server keinen Truststore findet oder der Truststore nicht angegeben wird, verwendet der Server den Schlüsselspeicher als Truststore.

Zertifikatvalidierung umgehen

Um sichere Verbindungen zu unterstützen, überprüft der Web Services Proxy die Zertifikate der Speichersysteme' anhand der eigenen vertrauenswürdigen Zertifikate. Bei Bedarf können Sie festlegen, dass der Proxy diese Validierung umgehen kann, bevor Sie eine Verbindung zu den Speichersystemen herstellen.

Bevor Sie beginnen

- Alle Verbindungen des Storage-Systems müssen sicher sein.

Schritte

1. Öffnen Sie die Datei wsconfig.xml unter:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_Web_Services_Proxy
2. Eingabe `true` Im `trust.all.arrays` Eintrag, wie im Beispiel gezeigt:

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

3. Speichern Sie die Datei.

Generieren und Importieren eines Host-Managementzertifikats

Zertifikate identifizieren Website-Eigentümer für sichere Verbindungen zwischen Clients und Servern. Zum Generieren und Importieren von Zertifikatszertifikaten (Certificate Authority, CA) für das Hostsystem, auf dem

der Web Services Proxy installiert ist, können Sie API-Endpunkte verwenden.

Zum Verwalten von Zertifikaten für das Hostsystem führen Sie die folgenden Aufgaben mithilfe der API durch:

- Erstellen Sie eine Zertifikatsignierungsanforderung (CSR) für das Hostsystem.
- Senden Sie die CSR-Datei an eine CA, und warten Sie dann, bis sie Ihnen die Zertifikatdateien senden.
- Importieren Sie die signierten Zertifikate in das Hostsystem.

> Sie können Zertifikate auch in der Unified Manager-Oberfläche verwalten. Weitere Informationen finden Sie in der Online-Hilfe von Unified Manager.

Schritte

1. Melden Sie sich bei an "Interaktive API-Dokumentation".
2. Gehen Sie zum Dropdown-Menü oben rechts und wählen Sie dann **v2**.
3. Erweitern Sie den Link **Administration** und scrollen Sie nach unten zu den **/Certificates** -Endpunkten.
4. CSR-Datei generieren:
   a. Wählen Sie **POST:/Zertifikate**, und wählen Sie dann **Probieren Sie es aus**.

      Der Webserver generiert ein selbstsigniertes Zertifikat erneut. Anschließend können Sie Informationen in die Felder eingeben, um den allgemeinen Namen, die Organisation, die Organisationseinheit, die alternative ID und andere Informationen zu definieren, die zur Generierung des CSR verwendet werden.

   b. Fügen Sie die erforderlichen Informationen im Fensterbereich **Beispielwerte** hinzu, um ein gültiges CA-Zertifikat zu erstellen, und führen Sie dann die Befehle aus.

      > Rufen Sie **POST:/Certificates** oder **POST:/Certificates/Reset** nicht wieder an, oder Sie müssen den CSR erneut generieren. Wenn Sie **POST:/Certificates** oder **POST:/Certificates/Reset** anrufen, generieren Sie ein neues selbstsigniertes Zertifikat mit einem neuen privaten Schlüssel. Wenn Sie einen CSR senden, der vor dem letzten Zurücksetzen des privaten Schlüssels auf dem Server generiert wurde, funktioniert das neue Sicherheitszertifikat nicht. Sie müssen einen neuen CSR erstellen und ein neues CA-Zertifikat anfordern.

   c. Führen Sie den Endpunkt **GET:/Certificates/Server** aus, um zu bestätigen, dass der aktuelle Zertifikatsstatus das selbstsignierte Zertifikat mit den Informationen ist, die vom Befehl **POST:/Certificates** hinzugefügt werden.

      Das Serverzertifikat (gekennzeichnet durch den Alias `jetty`) Ist an dieser Stelle noch selbstsigniert.

   d. Erweitern Sie den Endpunkt **POST:/Zertifikate/Export**, wählen Sie **Probieren Sie es aus**, geben Sie einen Dateinamen für die CSR-Datei ein und klicken Sie dann auf **Ausführen**.
5. Kopieren Sie die, und fügen Sie sie ein `fileUrl` In eine neue Browser-Registerkarte, um die CSR-Datei herunterzuladen, und dann senden Sie die CSR-Datei an eine gültige CA, um eine neue Web-Server-Zertifikatskette anfordern.
6. Wenn die CA eine neue Zertifikatskette ausgibt, verwenden Sie ein Zertifikatmanager-Tool, um die Stammzertifikate, die Zwischenzertifikate und den Webserver auszulösen und diese dann auf den Web Services Proxy-Server zu importieren:
   a. Erweitern Sie den Endpunkt **POST:/sslconfig/Server** und wählen Sie **Try it out** aus.

b. Geben Sie im Feld **Alias** einen Namen für das CA-Stammzertifikat ein.

c. Wählen Sie im Feld **ersetzungMainServerCertificate** die Option **false** aus.

d. Navigieren Sie zum neuen CA-Stammzertifikat, und wählen Sie es aus.

e. Klicken Sie Auf **Ausführen**.

f. Vergewissern Sie sich, dass der ZertifikatUpload erfolgreich war.

g. Wiederholen Sie das Verfahren zum Hochladen des CA-Zertifikats für das Zertifizierungsstellenzertifikat.

h. Wiederholen Sie das Verfahren zum Hochladen des Zertifikats für die neue Web-Server-Sicherheitszertifikatdatei. Mit Ausnahme dieses Schritts wählen Sie in der Dropdown-Liste **ersetzenMainServerCertificate** die Option **true** aus.

i. Bestätigen Sie, dass der Import des Webserversicherheitszertifikats erfolgreich war.

j. Um zu bestätigen, dass die neuen Root-, Zwischenprodukt- und Webserver-Zertifikate im Schlüsselspeicher verfügbar sind, führen Sie **GET:/Zertifikate/Server** aus.

7. Wählen und erweitern Sie den Endpunkt **POST:/Zertifikate/reload** und wählen Sie dann **Try it out** aus. Wenn Sie dazu aufgefordert werden, ob Sie beide Controller neu starten möchten oder nicht, wählen Sie **false** aus. („true“ gilt nur für Dual Array Controller.) Klicken Sie Auf **Ausführen**.

   Der Endpunkt **/certificates/reload** gibt in der Regel eine erfolgreiche HTTP 202-Antwort zurück. Allerdings erzeugt der Reload des Web-Server Trustore und Keystore-Zertifikate eine Race-Bedingung zwischen dem API-Prozess und dem Web-Server-Zertifikat-Reload-Prozess. In seltenen Fällen kann das Reload des Webservers-Zertifikats die API-Verarbeitung überschlagen. In diesem Fall scheint das Neuladen zu fehlschlagen, obwohl es erfolgreich abgeschlossen wurde. In diesem Fall fahren Sie trotzdem mit dem nächsten Schritt fort. Wenn das Neuladen tatsächlich fehlgeschlagen ist, schlägt auch der nächste Schritt fehl.

8. Schließen Sie die aktuelle Browser-Sitzung am Web Services Proxy, öffnen Sie eine neue Browser-Sitzung und bestätigen Sie, dass eine neue sichere Browser-Verbindung zum Web Services Proxy hergestellt werden kann.

   Durch die Verwendung einer Inkognito- oder privaten Browsersitzung können Sie eine Verbindung zum Server öffnen, ohne gespeicherte Daten aus vorherigen Browsersitzungen zu verwenden.

Managen Sie Speichersysteme über Web Services Proxy

Um Storage-Systeme im Netzwerk zu managen, müssen Sie sie zunächst ermitteln und dann der Management-Liste hinzufügen.

Storage-Systeme erkennen

Sie können die automatische Erkennung festlegen oder Storage-Systeme manuell ermitteln.

Automatische Erkennung von Storage-Systemen

Sie können festlegen, dass Speichersysteme automatisch im Netzwerk erkannt werden, indem Sie die Einstellungen in der Datei wsconfig.xml ändern. Standardmäßig ist die automatische IPv6-Erkennung deaktiviert und IPv4 aktiviert.

Sie müssen nur eine Management-IP- oder DNS-Adresse angeben, um ein Storage-System hinzuzufügen. Der Server erkennt automatisch alle Verwaltungspfade, wenn die Pfade entweder nicht konfiguriert oder die Pfade

konfiguriert und drehbar sind.

> Wenn Sie versuchen, ein IPv6-Protokoll zu verwenden, um Speichersysteme nach der ersten Verbindung automatisch von der Controller-Konfiguration zu erkennen, schlägt der Vorgang möglicherweise fehl. Mögliche Ursachen für den Ausfall sind u. a. Probleme bei der IP-Adressweiterleitung oder bei der Aktivierung von IPv6 auf den Speichersystemen, die jedoch nicht auf dem Server aktiviert werden.

Bevor Sie beginnen

Bevor Sie die IPv6-Erkennungseinstellungen aktivieren, überprüfen Sie, ob Ihre Infrastruktur die IPv6-Konnektivität zu den Speichersystemen unterstützt, um eventuelle Verbindungsprobleme zu beheben.

Schritte

1. Öffnen Sie die Datei wsconfig.xml unter:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_Web_Services_Proxy
2. Ändern Sie in den Zeichenketten für die automatische Erkennung die Einstellungen von `true` Bis `false`, Nach Wunsch. Siehe das folgende Beispiel.

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

> Wenn die Pfade konfiguriert, aber nicht so konfiguriert sind, dass der Server zu den Adressen weiterleiten kann, treten intermittierende Verbindungsfehler auf. Wenn Sie die IP-Adressen nicht vom Host als routingfähig festlegen können, deaktivieren Sie die automatische Erkennung (ändern Sie die Einstellungen in `false`).

3. Speichern Sie die Datei.

Storage-Systeme mit API-Endpunkten erkennen und hinzufügen

Über API-Endpunkte können Storage-Systeme ermittelt und der Liste gemanagt hinzugefügt werden. Durch dieses Verfahren wird eine Managementverbindung zwischen dem Storage-System und der API erstellt.

> In dieser Aufgabe wird beschrieben, wie Storage-Systeme mithilfe der REST API ermittelt und hinzugefügt werden. So können Sie diese Systeme in der interaktiven API-Dokumentation managen. Es ist jedoch möglicherweise sinnvoll, Storage-Systeme im Unified Manager zu managen, wodurch eine benutzerfreundliche Oberfläche bereitgestellt wird. Weitere Informationen finden Sie in der Online-Hilfe von Unified Manager.

Bevor Sie beginnen

Bei Storage-Systemen mit SANtricity Version 11.30 und höher muss über die SANtricity System Manager-Schnittstelle die alte Managementoberfläche für Symbol aktiviert sein. Andernfalls schlagen die Endpunkte der Erkennung fehl. Sie können diese Einstellung finden, indem Sie System Manager öffnen und dann im Menü:Einstellungen[System > zusätzliche Einstellungen > Managementoberfläche ändern] wechseln.

Schritte

1. Melden Sie sich bei an "Interaktive API-Dokumentation".
2. Storage-Systeme erkennen Sie wie folgt:

a. Stellen Sie aus der API-Dokumentation sicher, dass **V2** in der Dropdown-Liste ausgewählt ist, und erweitern Sie dann die Kategorie **Storage-Systeme**.

b. Klicken Sie auf den Endpunkt **POST: /Discovery** und dann auf **Probieren Sie es aus**.

c. Geben Sie die Parameter ein, wie in der Tabelle beschrieben.

StartIP EndIP
Ersetzen Sie die Zeichenfolge durch den Start- und Endbereich der IP-Adresse für ein oder mehrere Speichersysteme im Netzwerk.
Einsatzagenten
Setzen Sie diesen Wert auf: • True = in-Band-Agenten für den Netzwerkscan verwenden. • False = Verwenden Sie keine bandinternen Agenten für den Netzwerkscan.
Verbindungs-Timeout
Geben Sie die Sekunden ein, die für den Scan zulässig sind, bevor die Verbindung unterbrochen wird.
MaxPortsToUse
Geben Sie eine maximale Anzahl von Ports ein, die für die Netzwerküberprüfung verwendet werden.

d. Klicken Sie Auf **Ausführen**.

> API-Aktionen werden ohne Benutzeraufforderungen ausgeführt.

Die Bestandsaufnahme wird im Hintergrund ausgeführt.

a. Stellen Sie sicher, dass der Code eine 202 zurückgibt.

b. Suchen Sie unter **Response Body** den für die Anforderungs-ID zurückgegebenen Wert. Im nächsten Schritt müssen Sie die Anfrage-ID anzeigen.

3. Zeigen Sie die Ergebnisse der Bestandsaufnahme an:

a. Klicken Sie auf den Endpunkt **GET: /Discovery** und dann auf **Try it out**.

b. Geben Sie die Anforderungs-ID im vorherigen Schritt ein. Wenn Sie die **Anfrage-ID** leer lassen, wird standardmäßig die letzte ausgeführte Anforderungs-ID verwendet.

c. Klicken Sie Auf **Ausführen**.

d. Stellen Sie sicher, dass der Code 200 zurückgegeben wird.

e. Suchen Sie im Antwortkörper Ihre Anfrage-ID und die Strings für storageSystems. Die Zeichenfolgen sehen dem folgenden Beispiel ähnlich aus:

```
"storageSystems": [
    {
      "serialNumber": "123456789",
      "wwn": "000A011000AF0000000000001A0C000E",
      "label": "EF570_Array",
      "firmware": "08.41.10.01",
      "nvsram": "N5700-841834-001",
      "ipAddresses": [
        "10.xxx.xx.213",
        "10.xxx.xx.214"
      ],
```

f. Notieren Sie sich die Werte für wwn, Label und ipAddresses. Sie brauchen sie für den nächsten Schritt.

4. Fügen Sie Storage-Systeme wie folgt hinzu:
   a. Klicken Sie auf den Endpunkt **POST: /Storage-System** und dann auf **Try it out**.
   b. Geben Sie die Parameter ein, wie in der Tabelle beschrieben.

id
Geben Sie einen eindeutigen Namen für dieses Speichersystem ein. Sie können die Beschriftung eingeben (die in der Antwort für GET: /Discovery angezeigt wird), aber der Name kann eine beliebige Zeichenfolge sein, die Sie auswählen. Wenn Sie für dieses Feld keinen Wert angeben, weist Web Services automatisch eine eindeutige Kennung zu.
ControllerAddresses
Geben Sie die IP-Adressen ein, die in der Antwort für GET: /Discovery angezeigt werden. Trennen Sie bei Dual-Controllern die IP-Adressen durch Komma. Beispiel: `"IP address 1","IP address 2"`
Validieren
Eingabe `true`, So können Sie die Bestätigung erhalten, dass Web Services eine Verbindung zum Speichersystem herstellen können.
Passwort
Geben Sie das Administratorpasswort für das Speichersystem ein.
wwn
Geben Sie den WWN des Storage-Systems ein (wird in der Antwort für GET: /Discovery angezeigt).

c. Danach alle Strings entfernen `"enableTrace": true`, Damit der gesamte String-Satz dem folgenden Beispiel ähnelt:

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

d. Klicken Sie Auf **Ausführen**.

e. Stellen Sie sicher, dass die Codeantwort 201 ist, was darauf hinweist, dass der Endpunkt erfolgreich ausgeführt wurde.

   Der Endpunkt **Post: /Storage-Systems** befindet sich in der Warteschlange. Im nächsten Schritt können Sie die Ergebnisse mit dem Endpunkt **GET: /Storage-Systems** anzeigen.

5. Bestätigen Sie das Hinzufügen der Liste wie folgt:

   a. Klicken Sie auf den Endpunkt **GET: /Storage-System**.

      Es sind keine Parameter erforderlich.

   b. Klicken Sie Auf **Ausführen**.

   c. Stellen Sie sicher, dass die Codeantwort 200 ist, was bedeutet, dass der Endpunkt erfolgreich ausgeführt wurde.

   d. Suchen Sie im Antwortkörper nach den Details des Speichersystems. Die zurückgegebenen Werte zeigen an, dass sie erfolgreich zur Liste der verwalteten Arrays hinzugefügt wurde, ähnlich wie im folgenden Beispiel:

```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "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"
  ]
  }
]
```


Skalieren Sie die Anzahl an gemanagten Storage-Systemen vertikal

Standardmäßig kann die API bis zu 100 Storage-Systeme verwalten. Wenn Sie mehr verwalten müssen, müssen Sie die Speicheranforderungen für den Server erhöhen.

Der Server ist auf 512 MB Arbeitsspeicher eingestellt. Fügen Sie für jedes 100 zusätzliche Speichersystem in Ihrem Netzwerk 250 MB hinzu. Fügen Sie nicht mehr Speicher hinzu, als Sie physisch haben. Lassen Sie Ihrem Betriebssystem und anderen Anwendungen genügend zusätzliche Kapazität zu.

> Die standardmäßige Cache-Größe beträgt 8,192 Ereignisse. Die ungefähre Datennutzung im MEL-Ereignicache beträgt je 8,192 Ereignisse 1 MB. Daher sollte bei Beibehaltung der Standardeinstellungen der Cache-Bedarf bei einem Storage-System ungefähr 1 MB betragen.

> Zusätzlich zum Arbeitsspeicher verwendet der Proxy für jedes Speichersystem Netzwerkanschlüsse. Linux und Windows betrachten Netzwerkports als Datei-Handles. Als Sicherheitsmaßnahme begrenzen die meisten Betriebssysteme die Anzahl der offenen Datei-Handles, die ein Prozess oder ein Benutzer gleichzeitig geöffnet haben kann. Vor allem in Linux-Umgebungen, in denen offene TCP-Verbindungen als Datei-Handles betrachtet werden, kann der Web Services Proxy dieses Limit leicht überschreiten. Da der Fix systemabhängig ist, sollten Sie in der Dokumentation Ihres Betriebssystems nachschlagen, wie Sie diesen Wert erhöhen können.

Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Gehen Sie unter Windows in die Datei appserver64.init. Suchen Sie die Zeile, `vmarg.3=-Xmx512M`
   - Wählen Sie unter Linux die Datei webserver.sh. Suchen Sie die Zeile, `JAVA_OPTIONS="-Xmx512M"`
2. Um den Speicher zu erhöhen, ersetzen Sie `512` Mit dem gewünschten Arbeitsspeicher in MB.
3. Speichern Sie die Datei.

Verwalten der automatischen Abfrage für Web Services-Proxy-Statistiken

Sie können die automatische Abfrage für alle Festplatten- und Volume-Statistiken auf ermittelte Speichersysteme konfigurieren.

Übersicht über die Statistiken

Statistiken enthalten Informationen zu den Erfassungsraten und der Performance der Storage-Systeme.

Der Web Services Proxy bietet Zugriff auf die folgenden Arten von Statistiken:

- Rohstatistik — Zählwerte für Datenpunkte zum Zeitpunkt der Datenerfassung. Rohdaten können für Lesevorgänge insgesamt oder Schreibvorgänge verwendet werden.
- Analysierte Statistik – berechnete Informationen für ein Intervall Beispiele analysierte Statistiken sind Lese-Input/Output-Operationen (IOPS) pro Sekunde oder Schreibdurchsatz.

Rohdaten sind linear, da sie in der Regel mindestens zwei gesammelte Datenpunkte benötigen, um daraus nutzbare Daten abzuleiten. Die analysierten Statistiken sind eine Ableitung der Rohstatistik, die wichtige Kennzahlen liefert. Viele Werte, die sich aus den Rohstatistiken ergeben können, werden in den analysierten Statistiken für Ihren Komfort in einem nutzbaren Point-in-Time-Format angezeigt.

Sie können RAW-Statistiken abrufen, unabhängig davon, ob die automatische Abfrage aktiviert ist oder nicht. Sie können die hinzufügen `usecache=true` Abfragezeichenfolge am Ende der URL, um zwischengespeicherte Statistiken aus der letzten Umfrage abzurufen. Die Verwendung von gecachten Ergebnissen führt zu einer deutlichen Steigerung der Performance beim Abrufen von Statistiken. Mehrere Anrufe mit einer Rate von mindestens oder gleich dem konfigurierten Abrufintervall Cache werden jedoch dieselben Daten abgerufen.

Statistikfunktion

Der Web Services Proxy bietet API-Endpunkte, die den Abruf von RAW- und analysierten Controller- und Schnittstellenstatistiken von unterstützten Hardware-Modellen und Softwareversionen ermöglichen.

RAW Statistics APIs

- `/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}`

Analysierte Statistik-APIs

- `/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}`

Diese URLs rufen die analysierten Statistiken aus der letzten Umfrage ab und sind nur verfügbar, wenn die Abfrage aktiviert ist. Diese URLs umfassen die folgenden Daten für die Input-Ausgabe:

- Operationen pro Sekunde
- Durchsatz in Megabyte pro Sekunde
- Antwortzeiten in Millisekunden

Die Berechnungen basieren auf den Unterschieden zwischen statistischen Abfrageinterationen, bei denen es sich um die häufigsten Kennzahlen zur Storage-Performance handelt. Diese Statistiken sind den nicht analysierten Statistiken vorzuziehen.

> Wenn das System startet, gibt es keine vorherige Statistiksammlung zur Berechnung der verschiedenen Metriken. Die analysierten Statistiken benötigen also mindestens einen Abfragezyklus nach dem Start, um die Daten zurückzugeben. Wenn die kumulativen Zähler zurückgesetzt werden, enthält der nächste Abfragezyklus zudem unvorhersehbare Zahlen für die Daten.

Konfigurieren von Abfrageintervallen

Um Abfrageintervalle zu konfigurieren, ändern Sie die Datei wsconfig.xml, um ein Abrufintervall in Sekunden festzulegen.

> Da die Statistiken im Arbeitsspeicher zwischengespeichert werden, kann der Speicherverbrauch für jedes Storage-System möglicherweise um ca. 1.5 MB höher liegen.

Bevor Sie beginnen

- Die Speichersysteme müssen vom Proxy erkannt werden.

Schritte

1. Öffnen Sie die Datei wsconfig.xml unter:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_Web_Services_Proxy
2. Fügen Sie die folgende Zeile in das hinzu `<env-entries>` Tag, in dem `n` Ist die Anzahl der Sekunden für das Intervall zwischen Abfragungsanträgen:

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

   Wenn beispielsweise 60 eingegeben wird, beginnt die Abfrage in Intervallen von 60 Sekunden. Das heißt, das System fordert die Abfrage an, 60 Sekunden nach Abschluss des vorherigen Abfragzeitraums zu starten (unabhängig von der Dauer des vorherigen Abfrageperiode). Alle Statistiken werden mit dem genauen Zeitpunkt, zu dem sie abgerufen wurden, zeitlich gestempelt. Das System verwendet den Zeitstempel oder die Zeitdifferenz, auf der die 60-Sekunden-Berechnung basiert.

3. Speichern Sie die Datei.

Verwaltung von AutoSupport über Web Services Proxy

Sie können AutoSupport (ASUP) konfigurieren, der Daten sammelt und diese Daten automatisch an den technischen Support sendet, um Remote-Fehlerbehebung und Problemanalysen zu erstellen.

Übersicht über AutoSupport (ASUP)

Die AutoSupport (ASUP)-Funktion überträgt automatisch basierend auf manuellen und planungsbasierten Kriterien Meldungen an NetApp.

Jede AutoSupport Meldung ist eine Sammlung von Log-Dateien, Konfigurationsdaten, Statusdaten und Performance-Kennzahlen. Standardmäßig überträgt AutoSupport einmal pro Woche die in der folgenden Tabelle aufgeführten Dateien an das NetApp Support-Team.

Dateiname	Beschreibung
x-headers-data.txt	Eine .txt-Datei, die die X-Header-Informationen enthält.
manifest.xml	Eine .XML-Datei, in der der Inhalt der Nachricht aufgeführt ist.
arraydata.xml	Eine .XML-Datei, die die Liste der persistierten Clientdaten enthält.
appserver-config.txt	Eine TXT-Datei, die die Konfigurationsdaten des Anwendungsservers enthält.
wsconfig.txt	Eine TXT-Datei, die die Konfigurationsdaten des Webdienstes enthält.
host-info.txt	Eine .txt-Datei mit Informationen zur Hostumgebung.
Server-logs.7z	Eine .7z-Datei mit jeder verfügbaren Webserver-Protokolldatei.
client-info.txt	Eine .txt-Datei mit beliebigen Schlüssel-/Wertpaaren für anwendungsspezifische Zähler wie Methode- und Webseitentreffer.
Webservices-profile.json	Diese Dateien enthalten Profildaten von Webservices und statistische Daten zur Überwachung von Jersey. Standardmäßig sind Statistiken zur Jersey-Überwachung aktiviert. Sie können diese in der Datei wsconfig.xml wie folgt aktivieren und deaktivieren: • Aktivieren: `<env key="enable.jersey.statistics">true</env>` • Deaktivieren: `<env key="enable.jersey.statistics">false</env>`

Konfigurieren Sie AutoSupport

Bei der Installation ist AutoSupport standardmäßig aktiviert. Sie können diese Einstellung jedoch ändern oder

die Bereitstellungstypen ändern.

Aktivieren oder deaktivieren Sie AutoSupport

Die AutoSupport-Funktion ist während der Erstinstallation des Web Services Proxy aktiviert oder deaktiviert, Sie können diese Einstellung jedoch in der ASUP-Datei ändern.

Sie können AutoSupport über die Datei ASUPConfig.xml aktivieren oder deaktivieren, wie in den nachstehenden Schritten beschrieben. Alternativ können Sie diese Funktion über die API mit **Konfiguration** und **POST/asup** aktivieren oder deaktivieren und dann "true" oder "false" eingeben.

1. Öffnen Sie die Datei ASUPConfig.xml im Arbeitsverzeichnis.
2. Suchen Sie nach den Leitungen für <asupdata enable="Boolean_value" timestamp="timestamp">
3. Eingabe `true` (Aktivieren) oder `false` (Deaktivieren). Beispiel:

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

> Der Zeitstempeleintrag ist überflüssig.

4. Speichern Sie die Datei.

Konfigurieren der AutoSupport-Bereitstellungsmethode

Sie können die AutoSupport-Funktion so konfigurieren, dass HTTPS-, HTTP- oder SMTP-Bereitstellungsmethoden verwendet werden. HTTPS ist die Standardausgabemethode.

1. Auf die Datei ASUPConfig.xml im Arbeitsverzeichnis zugreifen.
2. In der Zeichenfolge, `<delivery type="n">`Geben Sie 1, 2 oder 3 ein, wie in der Tabelle beschrieben:

Wert	Beschreibung
1	**HTTPS** (Standard) <Liefertyp=„1“>
2	**HTTP** <Liefertyp=„2“>

Wert	Beschreibung

3	**SMTP** — um den AutoSupport-Bereitstellungstyp ordnungsgemäß an SMTP zu konfigurieren, müssen Sie die SMTP-Mail-Server-Adresse zusammen mit den E-Mails des Absenders und Empfängers angeben, ähnlich wie im folgenden Beispiel:
	
	`<delivery type="3">`
	`<smtp>`
	`<mailserver>smtp.example.com</mailserver>`
	`<sender>user@example.com</sender>`
	`<replyto>user@example.com</replyto>`
	`</smtp>`
	`</delivery>`