SANtricity-Lösungen einsetzen

E-Series storage systems

NetApp
January 20, 2026

Inhalt

SANtricity-Lösungen einsetzen

Web-Services-Proxy

Erfahren Sie mehr über den Webservice-Proxy von SANtricity

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".
- 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

Erfahren Sie mehr über SANtricity Web Services und Unified Manager

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.

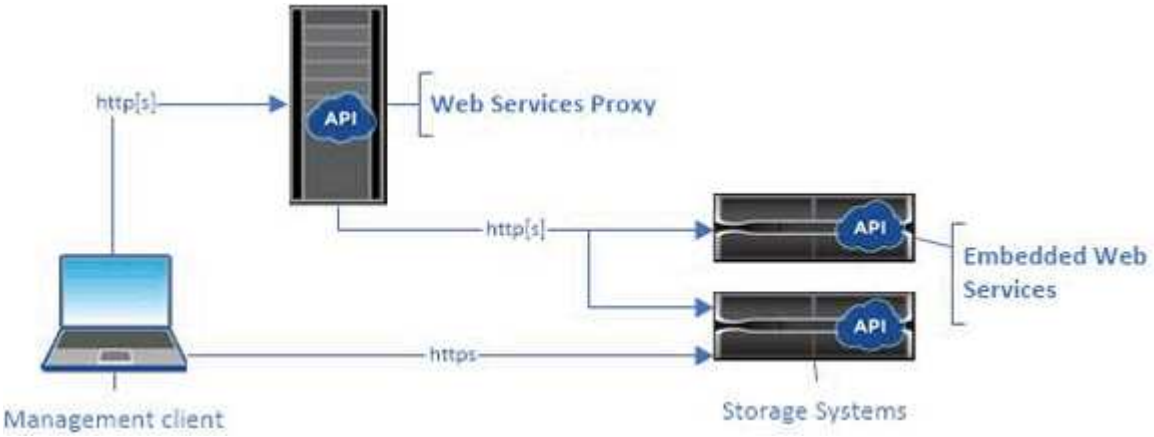
Wenn Sie die Web Services API für das Management von Storage-Systemen verwenden, sollten Sie mit folgenden Informationen vertraut sein:

- 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 auf jedem Controller eines E2800/EF280 Storage-Systems mit NetApp SANtricity 11.30 oder höher, einer E5700/EF570 mit SANtricity 11.40 oder höher, einem EF300 oder EF600 mit SANtricity 11.60 oder höher und einem E4000 mit SANtricity 11.90 oder höher 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

SANtricity Webdienste ProxyKompatibilität 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.

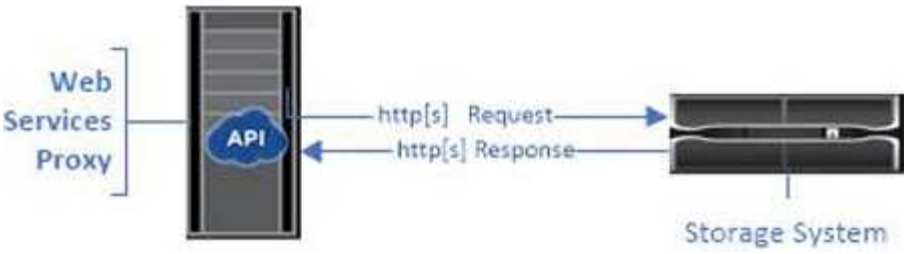
Überlegungen	Kompatibilität oder Einschränkungen
IP-Support	Der Web Services Proxy unterstützt entweder das IPv4-Protokoll oder das IPv6-Protokoll. Das IPv6-Protokoll schlägt möglicherweise fehl, wenn der Web Services Proxy versucht, die Verwaltungsadresse von der Controller-Konfiguration automatisch 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.

Erfahren Sie mehr über die Grundlagen der SANtricity Webdienste-Proxy-API

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

Erfahren Sie mehr über die Terminologie von SANtricity Webservices Proxy

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.
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.

Laufzeit	Definition
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

Überprüfen Sie die Installations- und Upgrade-Anforderungen für den SANtricity-Webdienstproxy

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 Sie die SANtricity Web Services Proxy- und SANtricity Unified Manager-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 der SANtricity Webservices Proxy 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 den SANtricity-Webdienstproxy

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 den SANtricity-Webdienstproxy

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.

Verwalten Sie den Benutzerzugriff im SANtricity-Webdienstproxy

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 Sie die Sicherheit und Zertifikate im SANtricity-Webdienstproxy

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:/ssIconfig/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.

Anmeldesperre

Sie können die Anzahl der Anmeldeversuche für die integrierten und Proxy-Webservices nur über die REST-API konfigurieren. Je nach Ihren Einstellungen wird die Sperrfunktion aktiviert, sobald die Anzahl der Anmeldeversuche für die Webservices überschritten wird.

Schritte

1. Melden Sie sich bei an "Interaktive API-Dokumentation".
2. Gehen Sie zum Dropdown-Menü oben rechts und wählen Sie dann **v2**.
3. Klicken Sie auf den Endpunkt **GET:/settings/Lockout**, um die Sperreinstellungen abzurufen.
4. Klicken Sie auf den Endpunkt **POST:/settings/Lockout**, und klicken Sie dann auf **Try it out**, um die Sperreinstellungen zu konfigurieren.

Verwalten Sie Speichersysteme mithilfe des SANtricity-Webdienstproxys

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 SANtricity-Webdienste-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.

Verwalten Sie AutoSupport mithilfe des SANtricity-Webdienstproxys

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- 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	**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>`

Remote Volume Mirroring

Erfahren Sie mehr über SANtricity Remote Storage Volumes

Verwenden Sie die SANtricity® Funktion Remote Storage Volumes, um Daten von einem Remote-Speichergerät direkt in ein lokales E-Series Volume zu importieren. Diese Funktion optimiert die Prozesse für Geräte-Upgrades und bietet Funktionen zur Datenmigration, mit denen Daten von Geräten der nicht-E-Series auf E-Series Systeme verschoben werden können.

Konfigurationsübersicht

Die Funktion Remote Storage Volumes ist mit SANtricity System Manager für ausgewählte Untermodell-IDs verfügbar. Zur Verwendung dieser Funktion müssen Sie ein Remote-Storage-System und ein E-Series Storage-System konfigurieren, damit sie miteinander kommunizieren können.

Verwenden Sie den folgenden Workflow:

1. "Anforderungen und Einschränkungen prüfen".
2. "Hardware konfigurieren".
3. "Remote-Speicher importieren".

SANtricity-Remote-Speicher-Volumes werden derzeit nicht auf E4000-Systemen unterstützt.

Weitere Informationen

- Die Online-Hilfe von ist auf der Benutzeroberfläche von System Manager oder auf der verfügbar "SANtricity Software-Dokument-Site".
- Weitere technische Informationen zur Funktion Remote Storage Volumes finden Sie im "Technischer Bericht Zu Remote Storage Volumes".

Anforderungen und Einschränkungen für die Verwendung von SANtricity Remote Storage Volumes

Überprüfen Sie vor der Konfiguration der Remote Storage Volumes-Funktion die folgenden Anforderungen und Einschränkungen.

Hardwareanforderungen

Unterstützte Protokolle

Für die erste Version der Funktion Remote Storage Volumes wird nur Unterstützung für iSCSI- und IPv4-Protokolle geboten.

Siehe "NetApp Interoperabilitäts-Matrix-Tool" Sie erhalten aktuelle Informationen zur Unterstützung und Konfiguration zwischen dem Host und dem E-Series (Ziel)-Array, das für die Funktion Remote Storage Volumes verwendet wird.

Storage-Systemanforderungen

Das E-Series Storage-System muss Folgendes umfassen:

- Zwei Controller (Duplexmodus)

- ISCSI-Verbindungen für E-Series Controller zur Kommunikation mit dem Remote-Storage-System über eine oder mehrere iSCSI-Verbindungen
- SANtricity OS 11.71 oder höher
- Remote Storage-Funktion in Submodell-ID (SMID) aktiviert

Das Remote-System kann entweder ein E-Series Storage-System oder ein System eines anderen Anbieters sein. Es müssen iSCSI-fähige Schnittstellen enthalten.

Volume-Anforderungen

Für Importe verwendete Volumes müssen die Anforderungen für Größe, Status und andere Kriterien erfüllen.

Remote Storage Volume

Das Quell-Volume eines Imports wird als „Remote-Storage-Volume“ bezeichnet. Dieses Volume muss die folgenden Kriterien erfüllen:

- Darf nicht Teil eines anderen Imports sein
- Muss einen Online-Status haben

Nach dem Import erstellt die Controller-Firmware im Hintergrund ein Remote-Speicher-Volume. Aufgrund dieses Hintergrundprozesses ist das Remote Storage Volume in System Manager nicht verwaltbar und kann nur für den Importvorgang verwendet werden.

Nach der Erstellung wird das Remote Storage Volume wie jedes andere Standard-Volume des E-Series Systems behandelt. Folgende Ausnahmen gelten:

- Kann als Proxys für das Remote-Speichergerät verwendet werden.
- Kann nicht als Kandidaten für andere Volume-Kopien oder Snapshots verwendet werden.
- Während des Imports kann die Data Assurance-Einstellung nicht geändert werden.
- Es können keine Hosts zugeordnet werden, da sie ausschließlich für den Importvorgang reserviert sind.

Jedes Remote-Storage-Volume ist nur einem Remote-Storage-Objekt zugewiesen. Ein Remote-Storage-Objekt kann jedoch mehreren Remote-Storage Volumes zugewiesen werden. Das Remote Storage Volume wird anhand folgender Elemente eindeutig identifiziert:

- Objekt-ID für Remote-Storage
- LUN-Nummer des Remote-Speichergeräts

Kandidaten für Zielvolumen

Das Ziel-Volume ist das Ziel-Volume auf dem lokalen E-Series System.

Das Ziel-Volume muss die folgenden Kriterien erfüllen:

- Muss ein RAID/DDP-Volume sein.
- Muss eine Kapazität aufweisen, die dem Remote-Storage-Volume entspricht oder größer ist.
- Es müssen Blöcke vorhanden sein, die mit dem Remote-Storage-Volume identisch sind.
- Muss einen gültigen Zustand (optimal) aufweisen.
- Es können keine der folgenden Beziehungen vorhanden sein: Volume-Kopie, Snapshot-Kopien,

asynchrones oder synchrones Spiegeln.

- Keine Neukonfiguration möglich: Dynamische Volume-Erweiterung, dynamische Kapazitätserweiterung, dynamische Segmentgröße, dynamische RAID-Migration, dynamische Kapazitätsreduzierung, Oder Defragmentierung.
- Vor dem Import kann einem Host nicht zugeordnet werden (er kann jedoch nach Importstart zugeordnet werden).
- Flash Read (FRC) kann nicht aktiviert sein.

System Manager überprüft diese Anforderungen automatisch im Assistenten zum Importieren von Remote Storage. Für die Auswahl des Ziel-Volumes werden nur Volumes angezeigt, die alle Anforderungen erfüllen.

Einschränkungen

Die Remote-Speicherfunktion verfügt über folgende Einschränkungen:

- Die Spiegelung muss deaktiviert werden.
- Auf dem Ziel-Volume des E-Series Systems dürfen keine Snapshots vorhanden sein.
- Das Ziel-Volume auf dem E-Series System darf vor dem Start des Imports keinen Hosts zugeordnet werden.
- Auf dem Ziel-Volume des E-Series Systems muss die Ressourcen-Bereitstellung deaktiviert sein.
- Direkte Zuordnungen des Remote-Storage-Volumes zu einem oder mehreren Hosts werden nicht unterstützt.
- Web Services Proxy wird nicht unterstützt.
- ISCSI-CHAP-Schlüssel werden nicht unterstützt.
- SMcli wird nicht unterstützt.
- VMware Datastore wird nicht unterstützt.
- Ein Upgrade von nur einem Speichersystem im Verhältnis-/Importpaar kann zu einem Zeitpunkt durchgeführt werden, an dem ein Importpaar vorhanden ist.

Vorbereitung für Produktionsimporte

Sie sollten vor dem Produktionsimport einen Test oder einen „Probelauf“ durchführen, um die ordnungsgemäße Storage- und Fabric-Konfiguration zu überprüfen.

Viele Variablen können sich auf den Importvorgang und die Abschlusszeit auswirken. Um sicherzustellen, dass ein Produktionsimport erfolgreich ist und eine Schätzung der Dauer erhalten wird, können Sie diese Testimporte verwenden, um sicherzustellen, dass alle Verbindungen wie erwartet funktionieren und der Importvorgang in angemessener Zeit abgeschlossen wird. Anschließend können Sie Anpassungen vornehmen, um die gewünschten Ergebnisse zu erzielen, bevor der Produktionsimport gestartet wird.

Konfigurieren Sie die Hardware für SANtricity Remote Storage Volumes

Das E-Series Storage-System muss so konfiguriert sein, dass es über das unterstützte iSCSI-Protokoll mit dem Remote-Storage-System kommunizieren kann.

Konfiguration von Remote Storage-Gerät und E-Series Array

Bevor Sie mit dem SANtricity System Manager fortfahren, um die Funktion Remote-Speicher-Volumes zu

konfigurieren, gehen Sie wie folgt vor:

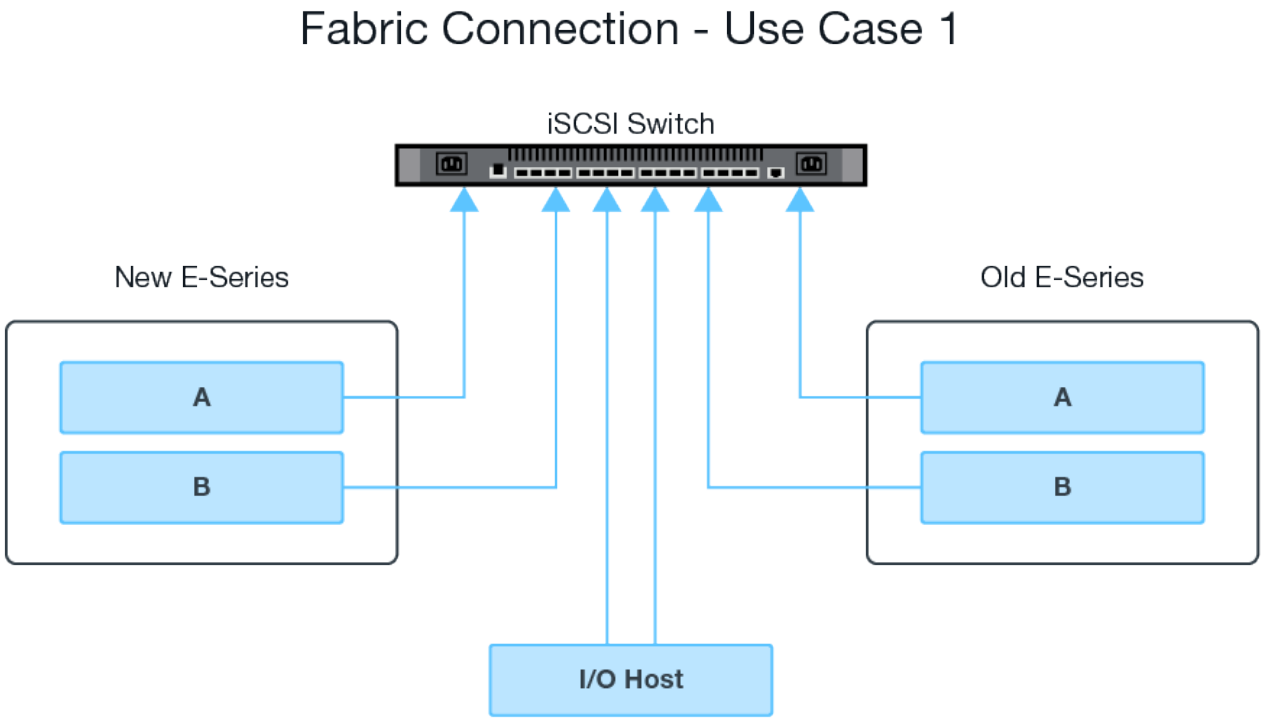
1. Richten Sie manuell eine kabelgebundene Verbindung zwischen dem E-Series System und dem Remote-Storage-System ein, sodass die beiden Systeme für die Kommunikation über iSCSI konfiguriert werden können.
2. Konfigurieren Sie die iSCSI-Ports, sodass das E-Series System und das Remote-Storage-System erfolgreich miteinander kommunizieren können.
3. Beschaffen der IQN des E-Series Systems
4. Machen Sie das E-Series System für das Remote-Storage-System sichtbar. Wenn es sich bei dem Remote-Storage-System um ein E-Series-System handelt, erstellen Sie einen Host mit dem IQN des Ziel-E-Series Systems als Verbindungsinformationen für den Host-Port.
5. Wenn das Remote-Speichergerät von einem Host/einer Applikation verwendet wird:
   - E/A-Vorgänge zum Remote-Speichergerät stoppen.
   - Heben Sie die Zuordnung des Remote-Speichergeräts auf/heben Sie die Bereitstellung auf.
6. Zuordnen des Remote-Storage-Geräts zu dem für das Storage-System der E-Series definierten Host
7. Ermitteln Sie die LUN-Nummer des für die Zuordnung verwendeten Geräts.

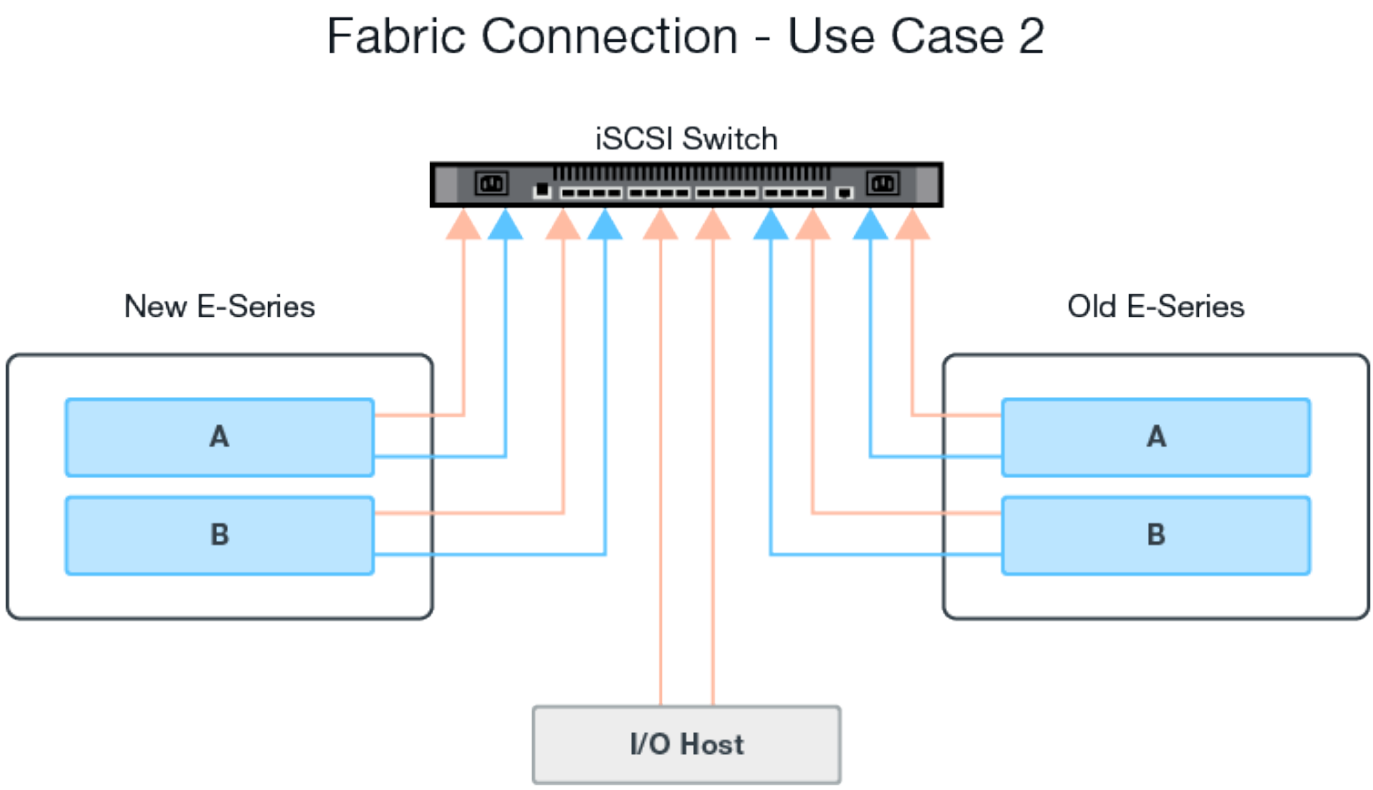
Empfohlen: Sichern Sie das Remote-Quell-Volume, bevor Sie den Importvorgang starten.

Verkabeln Sie die Speicher-Arrays

Im Rahmen des Setups müssen Speicher-Arrays und E/A-Host mit der iSCSI-kompatiblen Schnittstelle verbunden werden.

In den folgenden Diagrammen wird veranschaulicht, wie die Systeme so verkabelt werden, dass sie Remote-Speicher-Volume-Vorgänge über eine iSCSI-Verbindung durchführen.





Konfigurieren Sie die iSCSI-Ports

Sie müssen die iSCSI-Ports konfigurieren, um die Kommunikation zwischen dem Ziel (lokalem E-Series Storage-Array) und der Quelle (Remote-Storage-Array) sicherzustellen.

Die iSCSI-Ports können je nach Subnetz auf mehrere Arten konfiguriert werden. Im Folgenden finden Sie einige Beispiele zum Konfigurieren der iSCSI-Ports für die Verwendung mit der Funktion Remote-Speicher-Volumes.

Quelle A	Quelle B	Ziel A	Ziel B
10.10.1.100/22	10.10.2.100/22	10.10.1.101/22	10.10.2.101/22

Quelle A	Quelle B	Ziel A	Ziel B
10.10.0.100/16	10.10.0.100/16	10.10.0.101/16	10.10.0.101/16

Importieren Sie Remote-Speicher für SANtricity-Remote-Speicher-Volumes

Um einen Storage-Import von einem Remote-System auf ein lokales E-Series Storage-System zu initiieren, verwenden Sie den Assistenten zum Importieren von Remote Storage in der Benutzeroberfläche von SANtricity System Manager.

Was Sie brauchen

- Das E-Series Storage-System muss so konfiguriert sein, dass es mit dem Remote-Storage-System kommunizieren kann. Siehe "Hardware konfigurieren".

- Erfassen Sie für das Remote-Speichersystem die folgenden Informationen:
  - ISCSI-IQN
  - ISCSI-IP-Adressen
  - LUN-Nummer des Remote Storage-Geräts (Quell-Volume)
- Erstellen oder wählen Sie für das lokale E-Series Storage-System ein Volume aus, das für den Datenimport verwendet werden soll. Das Ziel-Volume muss die folgenden Anforderungen erfüllen:
  - Entspricht der Blockgröße des Remote-Speichergeräts (dem Quell-Volume).
  - Verfügt über eine Kapazität, die dem Remote-Speichergerät entspricht oder größer ist.
  - Zustand optimal und verfügbar Eine vollständige Liste der Anforderungen finden Sie unter "Anforderungen und Einschränkungen zu erfüllen".
- Empfohlen: Sichern Sie Volumes auf dem Remote-Speichersystem, bevor Sie den Importvorgang starten.

Über diese Aufgabe

In dieser Aufgabe erstellen Sie eine Zuordnung zwischen dem Remote-Storage-Gerät und einem Volume auf dem lokalen E-Series Storage-System. Wenn Sie die Konfiguration abgeschlossen haben, beginnt der Import.

> Da viele Variablen sich auf den Importvorgang und seine Abschlusszeit auswirken können, sollten Sie zuerst kleinere Importe für „Test“ durchführen. Mit diesen Tests stellen Sie sicher, dass alle Verbindungen wie erwartet funktionieren und dass der Importvorgang in einem angemessenen Zeitraum abgeschlossen wird.

Schritte

1. Klicken Sie im SANtricity System Manager auf **Storage > Remote-Speicher**.
2. Klicken Sie Auf **Remote Storage Importieren**.

   Ein Assistent zum Importieren von Remote-Speicher wird angezeigt.

3. Geben Sie in Schritt 1a des Bedienfelds „Quelle konfigurieren“ Verbindungsinformationen ein.

   a. Geben Sie unter dem Feld **Name** den Namen für das Remote-Speichergerät ein.

   b. Geben Sie unter **iSCSI-Verbindungseigenschaften** für das Remote-Speichergerät Folgendes ein: IQN, IP-Adresse und Portnummer (Standard: 3260).

      Wenn Sie eine weitere iSCSI-Verbindung hinzufügen möchten, klicken Sie auf **+Weitere IP-Adresse hinzufügen**, um eine zusätzliche IP-Adresse für den Remote-Speicher hinzuzufügen. Wenn Sie fertig sind, klicken Sie auf **Weiter**.

   Nachdem Sie auf Weiter geklickt haben, wird Schritt 1b des Bedienfelds „Quelle konfigurieren“ angezeigt.

4. Wählen Sie im Feld **LUN** die gewünschte Quell-LUN für das Remote-Speichergerät aus, und klicken Sie dann auf **Weiter**.

   Das Fenster „Ziel konfigurieren“ wird geöffnet und zeigt Volume-Kandidaten an, die als Ziel für den Import dienen sollen. Einige Volumes werden aufgrund von Blockgröße, Kapazität oder Volume-Verfügbarkeit nicht in der Liste der Kandidaten angezeigt.

5. Wählen Sie aus der Tabelle ein Ziel-Volume auf dem E-Series Storage-System aus. Verwenden Sie bei Bedarf den Schieberegler, um die Importpriorität zu ändern. Klicken Sie Auf **Weiter**. Bestätigen Sie den Vorgang im nächsten Dialogfeld, indem Sie eingeben `continue`, Und dann auf **Weiter** klicken.

Wenn das Ziel-Volume eine Kapazität besitzt, die größer als das Quell-Volume ist, wird diese zusätzliche Kapazität nicht dem mit dem E-Series System verbundenen Host gemeldet. Um die neue Kapazität zu verwenden, müssen Sie auf dem Host nach Abschluss des Importvorgangs eine Dateisystemerweiterung durchführen und die Verbindung trennen.

Nachdem Sie die Konfiguration im Dialogfeld bestätigt haben, wird das Fenster Überprüfung angezeigt.

6. Überprüfen Sie auf dem Bildschirm Überprüfung, ob die angegebenen Einstellungen für Remote-Speicher, Ziel und Import korrekt sind. Klicken Sie auf **Fertig stellen**, um die Erstellung des Remote-Speichers abzuschließen.

   Es wird ein weiteres Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie einen anderen Import starten möchten.

7. Klicken Sie bei Bedarf auf **Ja**, um einen anderen Remote-Speicherimport zu erstellen. Wenn Sie auf Ja klicken, gelangen Sie zu Schritt 1a des Bedienfelds „Quelle konfigurieren“, in dem Sie die vorhandene Konfiguration auswählen oder eine neue hinzufügen können. Wenn Sie keinen weiteren Import erstellen möchten, klicken Sie auf **Nein**, um das Dialogfeld zu schließen.

   Sobald der Importvorgang beginnt, wird das gesamte Zielvolume mit den kopierten Daten überschrieben. Wenn der Host während dieses Prozesses neue Daten auf das Ziel-Volume schreibt, werden diese neuen Daten wieder an das Remote-Gerät (Quell-Volume) übertragen.

8. Zeigen Sie den Fortschritt des Vorgangs im Dialogfeld „Anzeigevorgänge“ im Fenster „Remote-Speicher“ an.

   Wie lange der Importvorgang abgeschlossen werden muss, hängt von der Größe des Remote-Speichersystems, der Prioritätseinstellung für den Import und der Menge der I/O-Last auf beiden Storage-Systemen und den zugehörigen Volumes ab. Nach Abschluss des Imports handelt es sich bei dem lokalen Volume um ein Duplikat des Remote-Speichergeräts.

9. Wenn Sie bereit sind, die Beziehung zwischen den beiden Volumes zu brechen, wählen Sie im Importobjekt in der Ansicht Operationen in Progress **Disconnect** aus. Sobald die Beziehung getrennt ist, kehrt die Performance des lokalen Volumes wieder in den Normalzustand zurück und wird nicht mehr von der Remote-Verbindung beeinträchtigt.

Importfortschritt für SANtricity-Remote-Speicher-Volumes verwalten

Nach Beginn des Importvorgangs können Sie den Fortschritt anzeigen und ausführen.

Auf der Seite „Operations in Progress“ wird für jeden Importvorgang ein Prozentsatz des Fertigstellungsvorgangs und die geschätzte verbleibende Zeit angezeigt. Zu den Aktionen gehören die Änderung der Importpriorität, das Stoppen und Wiederaufnehmen von Vorgängen und das Trennen von dem Vorgang.

Sie können die laufenden Vorgänge auch auf der Startseite anzeigen (**Home > Vorgänge in Bearbeitung anzeigen**).

Schritte

1. Gehen Sie im SANtricity-System-Manager zur Seite Remote-Speicher und wählen Sie **Anzeigevorgänge** aus.

   Das Dialogfeld „laufende Vorgänge“ wird angezeigt.

2. Verwenden Sie bei Bedarf die Links in der Spalte Aktionen, um anzuhalten und fortzufahren, die Priorität zu ändern oder die Verbindung zu einem Vorgang zu trennen.
   - **Priorität ändern** – Wählen Sie **Priorität ändern**, um die Verarbeitungspriorität eines laufenden oder ausstehenden Vorgangs zu ändern. Wenden Sie eine Priorität auf den Vorgang an, und klicken Sie dann auf **OK**.
   - **Stopp** – Wählen Sie **Stopp**, um das Kopieren von Daten vom Remote-Speichergerät anzuhalten. Die Beziehung zwischen dem Importpaar ist noch intakt, und Sie können **Fortsetzen** wählen, wenn Sie bereit sind, den Importvorgang fortzusetzen.
   - **Fortsetzen** – Wählen Sie **Fortsetzen**, um einen angehoppten oder fehlgeschlagenen Prozess zu starten, von dem aus er aufgehört wurde. Wenden Sie dann eine Priorität für den Vorgang „Fortsetzen“ an, und klicken Sie dann auf **OK**.

     Mit dem Vorgang Wiederaufnehmen wird der Import von Anfang an **nicht** neu gestartet. Wenn Sie den Prozess von Anfang an neu starten möchten, müssen Sie **Trennen** auswählen und dann den Import mit dem Assistenten für Remote-Speicher importieren neu erstellen.

   - **Trennen** – Wählen Sie **Trennen**, um die Beziehung zwischen Quell- und Ziel-Volumes für einen Importvorgang zu unterbrechen, der angehalten, beendet oder fehlgeschlagen ist.

Ändern Sie die Einstellungen für die Remote-Speicherverbindung für SANtricity-Remote-Speichervolumes

Über die Option „Einstellungen anzeigen/bearbeiten“ können Sie Verbindungseinstellungen für eine beliebige Remote-Speicherkonfiguration bearbeiten, hinzufügen oder löschen.

Änderungen an Verbindungseigenschaften wirken sich auf laufende Importe aus. Um Unterbrechungen zu vermeiden, nehmen Sie nur Änderungen an Verbindungseigenschaften vor, wenn keine Importe ausgeführt werden.

Schritte

1. Wählen Sie im Bildschirm Remote-Speicherung des SANtricity-System-Managers das gewünschte Objekt für Remote-Speicher im Abschnitt Ergebnisliste aus.
2. Klicken Sie Auf **Einstellungen Anzeigen/Bearbeiten**.

   Der Bildschirm „Remote-Speichereinstellungen“ wird angezeigt.

3. Klicken Sie auf die Registerkarte **Verbindungseigenschaften**.

   Die konfigurierten IP-Adressen- und Porteinstellungen für den Remote-Speicherimport werden angezeigt.

4. Führen Sie eine der folgenden Aktionen aus:
   - **Bearbeiten** – Klicken Sie neben dem entsprechenden Zeilenelement für das entfernte Speicherobjekt auf **Bearbeiten**. Geben Sie die überarbeitete IP-Adresse und/oder Portinformationen in die Felder ein.
   - **Hinzufügen** – Klicken Sie auf **Hinzufügen** und geben Sie dann die neue IP-Adresse und Port-Informationen in die dafür vorgesehenen Felder ein. Klicken Sie zur Bestätigung auf **Hinzufügen** und dann wird die neue Verbindung in der Liste der Remote-Speicherobjekte angezeigt.
   - **Löschen** – Wählen Sie die gewünschte Verbindung aus der Liste aus und klicken Sie dann auf **Löschen**. Bestätigen Sie den Vorgang, indem Sie eingeben `delete` Klicken Sie im dafür vorgesehenen Feld auf **Löschen**. Die Verbindung wird aus der Liste der Remote-Speicherobjekte

entfernt.

5. Klicken Sie Auf **Speichern**.

   Die geänderten Verbindungseinstellungen werden auf das Remote-Speicherobjekt angewendet.

Entfernen Sie das Remote-Speicherobjekt für SANtricity-Remote-Speichervolumes

Nach Abschluss des Imports können Sie ein Remote-Speicherobjekt entfernen, wenn Sie keine Daten mehr zwischen den lokalen und Remote-Geräten kopieren möchten.

Schritte

1. Stellen Sie sicher, dass dem Remote-Speicherobjekt, das Sie entfernen möchten, keine Importe zugeordnet sind.
2. Wählen Sie im Bildschirm Remote-Speicherung des SANtricity-System-Managers das gewünschte Objekt für Remote-Speicher im Abschnitt Ergebnisliste aus.
3. Klicken Sie Auf **Entfernen**.

   Das Dialogfeld „Remote-Speicherverbindung bestätigen“ wird angezeigt.

4. Bestätigen Sie den Vorgang, indem Sie eingeben `remove` Und dann auf **Entfernen** klicken.

   Das ausgewählte entfernte Speicherobjekt wird entfernt.

Storage Plug-in für vCenter

Erfahren Sie mehr über das SANtricity Storage Plug-in für vCenter

Das SANtricity Storage Plug-in für vCenter ermöglicht das integrierte Management von E-Series Storage-Arrays innerhalb einer VMware vSphere Client-Session.

Verfügbare Aufgaben

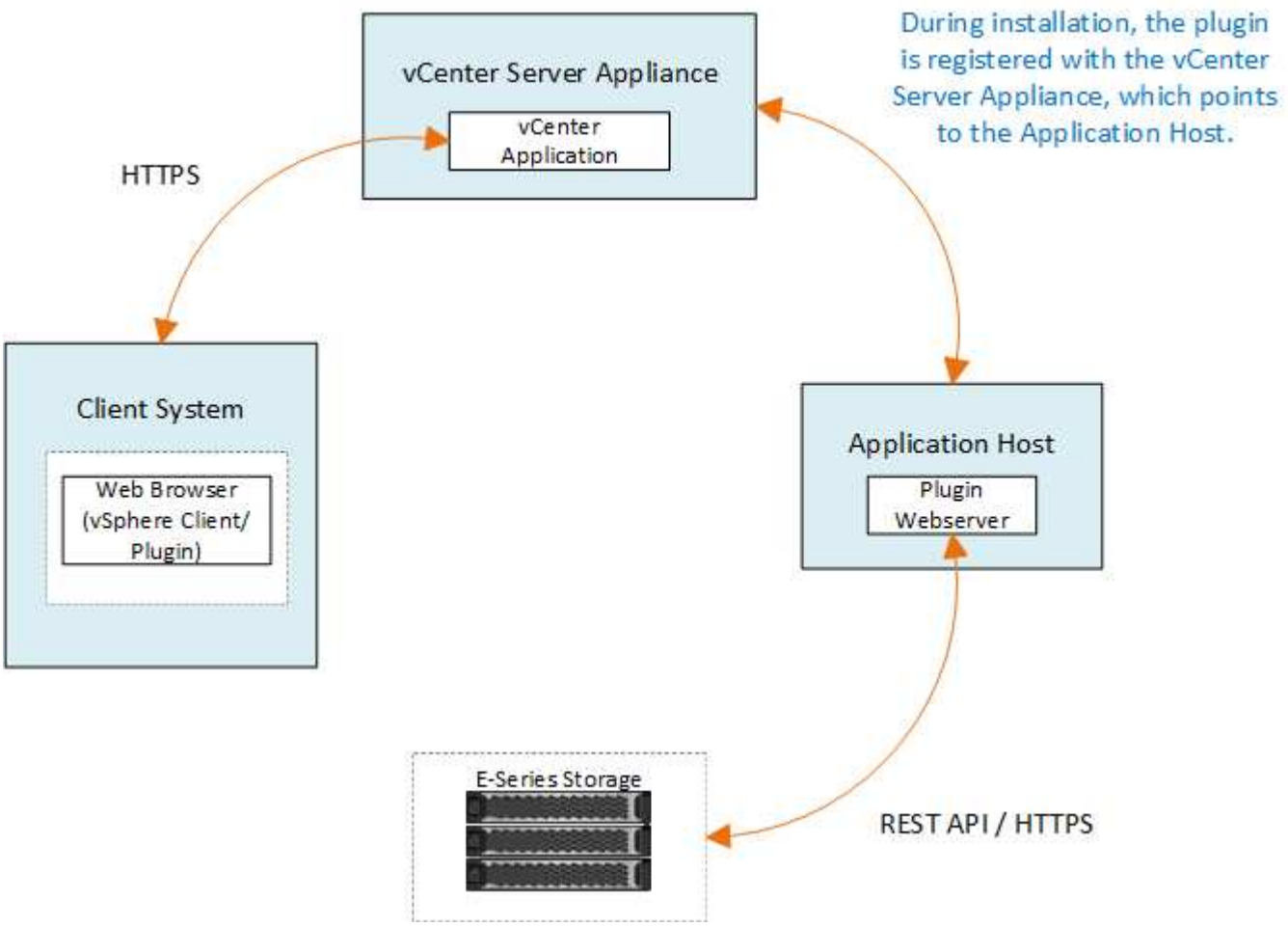
Sie können das Plugin verwenden, um die folgenden Aufgaben auszuführen:

- Anzeigen und Verwalten erkannter Speicher-Arrays im Netzwerk.
- Führen Sie Batch-Vorgänge auf Gruppen mehrerer Storage-Arrays durch.
- Führen Sie Upgrades auf dem Software-Betriebssystem durch.
- Einstellungen von einem Speicher-Array in ein anderes importieren.
- Konfiguration von Volumes, SSD-Cache, Hosts, Host-Clustern, Pools Und Volume-Gruppen.
- Starten Sie die System Manager-Schnittstelle, um zusätzliche Managementaufgaben auf einem Array auszuführen.

> Das Plug-in ist kein direkter Ersatz für die System Manager Schnittstelle, die in jeden Controller für ein Storage Array integriert ist. System Manager bietet zusätzliche Management-Funktionen. Wenn gewünscht, können Sie den System Manager öffnen, indem Sie ein Speicher-Array in der Hauptansicht des Plugins auswählen und dann auf **Start** klicken.

Das Plug-in erfordert eine in der VMware-Umgebung implementierte VMware vCenter Server Appliance und einen Anwendungshost, um den Plug-in-Webserver zu installieren und auszuführen.

Weitere Informationen zur Kommunikation in der vCenter Umgebung finden Sie in der folgenden Abbildung.



Schnittstellenübersicht

Wenn Sie sich beim Plugin anmelden, öffnet sich die Hauptseite zu **Verwalten - Alle**. Auf dieser Seite können Sie alle erkannten Speicher-Arrays im Netzwerk anzeigen und verwalten.

Navigationsleiste rechts in der Seitenleiste

In der Navigationsleiste wird Folgendes angezeigt:

- **Verwalten** — Entdecken Sie Speicher-Arrays in Ihrem Netzwerk, starten Sie System Manager für ein Array, importieren Sie Einstellungen von einem Array auf mehrere Arrays, managen Sie Array-Gruppen, aktualisieren Sie das SANtricity-Betriebssystem und stellen Sie Speicher bereit.
- **Zertifikatverwaltung** — Verwalten von Zertifikaten zur Authentifizierung zwischen Browsern und Clients.
- **Operationen** — Zeigen Sie den Fortschritt von Batch-Operationen, wie das Importieren von Einstellungen von einem Array in ein anderes.

Einige Vorgänge sind nicht verfügbar, wenn ein Speicherarray einen nicht optimalen Status hat.

- **Support** — Technische Support-Optionen, Ressourcen und Kontakte anzeigen.

Unterstützte Browser

Auf das Storage Plug-in für vCenter kann über verschiedene Browsertypen zugegriffen werden. Die folgenden Browser und Versionen werden unterstützt.

- Google Chrome 89 oder höher
- Mozilla Firefox 80 oder höher
- Microsoft Edge 90 oder höher

Benutzerrollen und Berechtigungen

Für den Zugriff auf Aufgaben im Storage Plugin für vCenter muss der Benutzer über Lese-/Schreibberechtigungen verfügen. Standardmäßig verfügen alle definierten VMware vCenter-Benutzer-IDs über keine Berechtigungen zum Ausführen von Aufgaben im Plug-in.

Konfigurationsübersicht

Die Konfiguration umfasst folgende Schritte:

1. "Installieren und registrieren Sie das Plugin".
2. "Konfigurieren Sie die Berechtigungen für den Plugin-Zugriff".
3. "Melden Sie sich bei der Plug-in-Schnittstelle an".
4. "Erkennen Sie Storage-Arrays".
5. "Bereitstellung von Storage".

Weitere Informationen

Weitere Informationen zum Verwalten von Datastores im vSphere Client finden Sie unter "Dokumentation zu VMware vSphere".

Los geht’s

Installations- und Upgrade-Anforderungen für das SANtricity Storage Plug-in für vCenter

Prüfen Sie vor der Installation oder dem Upgrade des SANtricity Storage Plug-ins für vCenter die Installationsanforderungen und die Upgrade-Überlegungen.

Installationsvoraussetzungen

Sie können das Storage Plug-in für vCenter auf einem Windows Host-System installieren und konfigurieren. Die Plugin-Installation umfasst die folgenden Anforderungen.

Anforderungen	Beschreibung
Unterstützte Versionen	• Von der VMware vCenter Server Appliance unterstützte Versionen: 6.7U3J, 7.0U1, 7.0U2, 7.0U3 und 8.0. • NetApp SANtricity OS Version: 11.60.2 oder höher • Unterstützte Applikations-Host-Versionen: Windows 2016, Windows 2019, Windows 2022. Weitere Informationen zur Kompatibilität finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
Mehrere Instanzen	Sie können nur eine Instanz des Speicher-Plug-ins für vCenter auf einem Windows-Host installieren und können es nur bei einem vCSA registrieren.
Kapazitätsplanung	Das Storage Plug-in für vCenter benötigt ausreichend Platz für die Ausführung und Protokollierung. Stellen Sie sicher, dass Ihr System die folgenden Anforderungen an den verfügbaren Speicherplatz erfüllt: • Erforderlicher Installationsspeicherplatz: 275 MB • Speicherplatz – 275 MB + 200 MB (Protokollierung) • Systemspeicher – 1.5 GB
Lizenz	Das Storage Plug-in für vCenter ist ein kostenloses eigenständiges Produkt, für das kein Lizenzschlüssel erforderlich ist. Es gelten jedoch geltende Urheberrechte und Nutzungsbedingungen.

Upgrade-Überlegungen

Wenn Sie ein Upgrade von einer früheren Version durchführen, beachten Sie, dass das Plugin vor dem Upgrade von der vCSA nicht registriert werden muss.

- Während des Upgrades werden die meisten früheren Konfigurationseinstellungen des Plug-ins beibehalten. Diese Einstellungen umfassen Benutzerpasswörter, alle erkannten Speichersysteme, Serverzertifikate, vertrauenswürdige Zertifikate und die Konfiguration der Serverlaufzeit.
- Der Upgrade-Prozess nicht erhalten die **vcenter.properties**-Dateien, so müssen Sie das Plugin vor dem Upgrade zu registrieren. Sobald das Upgrade erfolgreich abgeschlossen wurde, können Sie das Plugin wieder bei der vCSA registrieren.
- Alle zuvor im Repository geladenen SANtricity-OS-Dateien werden während des Upgrades entfernt.

Installieren oder aktualisieren Sie das SANtricity Storage Plug-in für vCenter

Führen Sie diese Schritte aus, um das Storage Plug-in für vCenter zu installieren und die Plugin-Registrierung zu überprüfen. Sie können das Plugin auch mit diesen Anweisungen aktualisieren.

Installationsvoraussetzungen prüfen

Stellen Sie sicher, dass Ihre Systeme die Anforderungen in erfüllen "Installations- und Upgrade-Anforderungen

prüfen".

> Die **vcenter.properties**-Dateien werden durch den Aktualisierungsprozess nicht beibehalten. Wenn Sie ein Upgrade durchführen, müssen Sie die Registrierung des Plugins vor dem Upgrade aufheben. Sobald das Upgrade erfolgreich abgeschlossen wurde, können Sie das Plugin wieder bei der vCSA registrieren.

Installieren Sie die Plug-in-Software

So installieren Sie die Plugin-Software:

1. Kopieren Sie die Installer-Datei auf den Host, der als Anwendungsserver verwendet wird, und greifen Sie dann auf den Ordner zu, in dem Sie das Installationsprogramm heruntergeladen haben.
2. Doppelklicken Sie auf die Installationsdatei:

   ```
   santricity_storage_vcenterplugin-windows_x64-- nn.nn.nn.nnnn.exe
   ```

   Im obigen Dateinamen, `nn.nn.nn.nnnn` Stellt die Versionsnummer dar.

3. Wenn die Installation beginnt, befolgen Sie die Anweisungen auf dem Bildschirm, um 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.

   > Während der Installation werden Sie zur Zertifikatvalidierung aufgefordert. Aktivieren Sie das Kontrollkästchen, wenn Sie die Zertifikatvalidierung zwischen dem Plug-in und den Speicher-Arrays durchsetzen möchten. Bei dieser Durchsetzung werden die Speicherarrayzertifikate auf Vertrauen in das Plug-in geprüft. Wenn die Zertifikate nicht vertrauenswürdig sind, dürfen sie dem Plugin nicht hinzugefügt werden. Wenn Sie die Zertifikatvalidierung überschreiben möchten, deaktivieren Sie das Kontrollkästchen, damit alle Speicher-Arrays mit selbstsignierten Zertifikaten zum Plugin hinzugefügt werden können. Weitere Informationen zu Zertifikaten finden Sie in der Online-Hilfe, die über die Plug-in-Schnittstelle verfügbar ist.

4. Wenn die Meldung Webserver gestartet angezeigt wird, klicken Sie auf **OK**, um die Installation abzuschließen, und klicken Sie dann auf **Fertig**.
5. Überprüfen Sie, ob der Anwendungsserver erfolgreich installiert wurde, indem Sie den Befehl **Services.msc** ausführen.
6. Überprüfen Sie, ob der Application Server (VCP)-Service **NetApp SANtricity Storage Plug-in für vCenter** installiert war und der Service gestartet wurde.

Bei Bedarf können Sie die Einstellungen für Zertifikatvalidierung und Webservice-Port nach der Installation ändern. Öffnen Sie im Installationsverzeichnis die Datei wsconfig.xml. Um die Zertifikatvalidierung auf Speicherarrays zu entfernen, ändern Sie das `env` Schlüssel, `trust.all.arrays`, An `true`. Ändern Sie den Web Services-Port, wenn Sie den ändern möchten `sslport` Wert bis zum gewünschten Portwert im Bereich von 0-65535. Stellen Sie sicher, dass die verwendete Portnummer keine Bindung an einen anderen Prozess hat. Wenn Sie fertig sind, speichern Sie die Änderungen und starten Sie den Plugin Webserver neu. Wenn der Portwert des Plugin-Webservers nach der Registrierung des Plugins in einem vCSA geändert wird, müssen Sie das Plugin unregistrieren und neu registrieren, damit der vCSA auf dem geänderten Port an den Plugin-Webserver kommuniziert.

Registrieren Sie das Plug-in mit einer vCenter Server Appliance

Nachdem die Plugin-Software installiert ist, registrieren Sie das Plugin mit einem vCSA.

Das Plugin kann nur jeweils auf einer vCSA registriert werden. Um sich bei einem anderen vCSA zu registrieren, müssen Sie das Plugin von der aktuellen vCSA deinstallieren und es vom Anwendungs-Host deinstallieren. Sie können dann das Plugin neu installieren und es auf dem anderen vCSA registrieren.

1. Öffnen Sie eine Eingabeaufforderung über die Befehlszeile, und navigieren Sie zum folgenden Verzeichnis:

   ```
   <install directory>\vcenter-register\bin
   ```

2. Führen Sie die Datei **vcenter-Register.bat** aus:
   ```
   vcenter-register.bat ^
   -action registerPlugin ^
   -vcenterHostname <vCenter FQDN> ^
   -username <Administrator username> ^
   ```
3. Überprüfen Sie, ob das Skript erfolgreich war.

Die Protokolle werden in gespeichert `%install_dir%/working/logs/vc-registration.log`.

Überprüfen Sie die Plugin-Registrierung

Nachdem das Plugin installiert und das Registrierungsskript ausgeführt wurde, überprüfen Sie, ob das Plugin bei der vCenter Server Appliance erfolgreich registriert wurde.

1. Öffnen Sie vSphere Client auf der vCenter Server Appliance.
2. Wählen Sie in der Menüleiste Menü:Administrator[Client Plugins].
3. Stellen Sie sicher, dass das Storage Plugin für vCenter als **aktiviert** aufgeführt ist.

   Wenn das Plug-in als deaktiviert aufgeführt wird und eine Fehlermeldung anzeigt, dass es nicht mit dem Anwendungsserver kommunizieren kann, überprüfen Sie, ob die für den Anwendungsserver definierte Portnummer aktiviert ist, um alle Firewalls zu durchlaufen, die verwendet werden könnten. Die standardmäßige Portnummer des Anwendungsservers Transmission Control Protocol (TCP) ist 8445.

Konfigurieren Sie das SANtricity-Speicher-Plugin für vCenter-Zugriffsberechtigungen

Sie können Zugriffsberechtigungen für das Storage Plugin für vCenter konfigurieren, das

Benutzer, Rollen und Berechtigungen umfasst.

Erforderliche vSphere-Berechtigungen prüfen

Um auf das Plug-in im vSphere Client zuzugreifen, müssen Sie einer Rolle zugewiesen werden, die über die entsprechenden vSphere-Berechtigungen verfügt. Benutzer mit der Berechtigung „Datastore konfigurieren“ vSphere haben Lese-Schreib-Zugriff auf das Plugin, während Benutzer mit der Berechtigung „Datastore durchsuchen“ nur Lesezugriff haben. Wenn ein Benutzer keine dieser Berechtigungen hat, zeigt das Plugin eine Meldung „unzureichende Berechtigungen“ an.

Plugin-Zugriffstyp	VSphere-Berechtigung erforderlich
Lesen/Schreiben (Konfigurieren)	Datastore.Configure
Schreibgeschützt (Anzeigen)	Datastore.Durchsuchen

Storage Administrator-Rollen konfigurieren

Um Lese-/Schreibberechtigungen für Plugin-Benutzer bereitzustellen, können Sie eine Rolle erstellen, klonen oder bearbeiten. Weitere Informationen zum Konfigurieren von Rollen im vSphere-Client finden Sie im VMware Doc Center unter folgendem Thema:

- "Erstellen Sie eine benutzerdefinierte Rolle"

Auf Rollenaktionen zugreifen

1. Wählen Sie auf der Startseite des vSphere Clients im Bereich Access Control die Option **Administrator** aus.
2. Klicken Sie im Bereich Zugriffskontrolle auf **Rollen**.
3. Führen Sie eine der folgenden Aktionen aus:
   - **Neue Rolle erstellen**: Klicken Sie auf das Aktionssymbol **Rolle erstellen**.
   - **Clone Role**: Wählen Sie eine vorhandene Rolle aus und klicken Sie auf das Aktionssymbol **Clone Role**.
   - **Vorhandene Rolle bearbeiten**: Wählen Sie eine vorhandene Rolle aus und klicken Sie auf das Aktionssymbol **Rolle bearbeiten**.

Die Administratorrolle kann nicht bearbeitet werden.

Abhängig von der oben genannten Auswahl wird der entsprechende Assistent angezeigt.

Erstellen Sie eine neue Rolle

1. Wählen Sie in der Liste Berechtigungen die Zugriffsberechtigungen aus, die dieser Rolle zugewiesen werden sollen.

   Um schreibgeschützten Zugriff auf das Plugin zu ermöglichen, wählen Sie Menü:Datastore[Browse Datastore]. Um Lese-/Schreibzugriff zu ermöglichen, wählen Sie Menü:Datastore[Configure Datastore].

2. Weisen Sie bei Bedarf andere Berechtigungen für die Liste zu und klicken Sie dann auf **Weiter**.
3. Benennen Sie die Rolle und geben Sie eine Beschreibung ein.
4. Klicken Sie Auf **Fertig Stellen**.

Rolle klonen

1. Benennen Sie die Rolle und geben Sie eine Beschreibung ein.
2. Klicken Sie auf **OK**, um den Assistenten zu beenden.
3. Wählen Sie die geklonte Rolle aus der Liste aus und klicken Sie dann auf **Rolle bearbeiten**.
4. Wählen Sie in der Liste Berechtigungen die Zugriffsberechtigungen aus, die dieser Rolle zugewiesen werden sollen.

   Um schreibgeschützten Zugriff auf das Plugin zu ermöglichen, wählen Sie Menü:Datastore[Browse Datastore]. Um Lese-/Schreibzugriff zu ermöglichen, wählen Sie Menü:Datastore[Configure Datastore].

5. Klicken Sie Auf **Weiter**.
6. Aktualisieren Sie ggf. den Namen und die Beschreibung.
7. Klicken Sie Auf **Fertig Stellen**.

Bearbeiten Sie eine vorhandene Rolle

1. Wählen Sie in der Liste Berechtigungen die Zugriffsberechtigungen aus, die dieser Rolle zugewiesen werden sollen.

   Um schreibgeschützten Zugriff auf das Plugin zu ermöglichen, wählen Sie Menü:Datastore[Browse Datastore]. Um Lese-/Schreibzugriff zu ermöglichen, wählen Sie Menü:Datastore[Configure Datastore].

2. Klicken Sie Auf **Weiter**.
3. Aktualisieren Sie ggf. den Namen oder die Beschreibung.
4. Klicken Sie Auf **Fertig Stellen**.

Legen Sie Berechtigungen für vCenter Server Appliance fest

Nachdem Sie Berechtigungen für eine Rolle festgelegt haben, müssen Sie der vCenter Server Appliance eine Berechtigung hinzufügen. Mit dieser Berechtigung kann ein Benutzer oder eine Gruppe auf das Plugin zugreifen.

1. Wählen Sie aus der Dropdown-Liste Menü die Option **Hosts und Cluster** aus.
2. Wählen Sie die **vCenter Server Appliance** aus dem Bereich Access Control aus.
3. Klicken Sie auf die Registerkarte **Berechtigungen**.
4. Klicken Sie auf das Aktionssymbol **Berechtigung hinzufügen**.
5. Wählen Sie die entsprechende Domäne und den entsprechenden Benutzer/die entsprechende Gruppe aus.
6. Wählen Sie die erstellte Rolle aus, die die Berechtigung zum Lese-/Schreib-Plugin ermöglicht.
7. Aktivieren Sie bei Bedarf die Option **auf Kinder übertragen**.
8. Klicken Sie auf **OK**.

Sie können eine vorhandene Berechtigung auswählen und ändern, um die erstellte Rolle zu verwenden. **Beachten Sie jedoch, dass die Rolle zusammen mit Lese-/Schreib-Plugin-Berechtigungen die gleichen Rechte haben muss, um eine Regress in Berechtigungen zu vermeiden.**

Um auf das Plugin zuzugreifen, müssen Sie sich unter dem Benutzerkonto, das über die Lese-/Schreibberechtigungen für das Plugin verfügt, beim vSphere Client anmelden.

Weitere Informationen zum Verwalten von Berechtigungen finden Sie in den folgenden Themen im VMware Doc Center:

- "Verwalten von Berechtigungen für vCenter-Komponenten"
- "Best Practices für Rollen und Berechtigungen"

Melden Sie sich an und navigieren Sie zum SANtricity Storage Plug-in für vCenter

Sie können sich beim Storage Plugin für vCenter anmelden, um die Benutzeroberfläche zu navigieren.

1. Bevor Sie sich beim Plugin anmelden, stellen Sie sicher, dass Sie einen der folgenden Browser verwenden:
   - Google Chrome 89 oder höher
   - Mozilla Firefox 80 oder höher
   - Microsoft Edge 90 oder höher
2. Melden Sie sich beim vSphere Client unter dem Benutzerkonto an, das über Lese-/Schreibberechtigungen für das Plugin verfügt.
3. Klicken Sie auf der Startseite des vSphere Clients auf **SANtricity Storage Plug-in für vCenter**.

   Das Plugin wird in einem vSphere Client-Fenster geöffnet. Die Hauptseite des Plugins öffnet sich zu **Manage-All**.

4. Greifen Sie über die Navigationsleiste links in der Navigationsleiste auf Storage Management-Aufgaben zu:
   - **Verwalten** – Entdecken Sie Speicher-Arrays in Ihrem Netzwerk, öffnen Sie System Manager für ein Array, importieren Sie Einstellungen von einem Array auf mehrere Arrays, managen Sie Array-Gruppen, aktualisieren Sie die Betriebssystemsoftware und stellen Sie Speicher bereit.
   - **Zertifikatverwaltung** – Verwalten von Zertifikaten zur Authentifizierung zwischen Browsern und Clients.
   - **Operationen** – Anzeigen des Fortschritts von Batch-Operationen, wie z.B. das Importieren von Einstellungen von einem Array in ein anderes.
   - **Support** – Anzeigen von Optionen, Ressourcen und Kontakten zum technischen Support.

Einige Vorgänge sind nicht verfügbar, wenn ein Speicherarray einen nicht optimalen Status hat.

Ermitteln Sie Speicher-Arrays im SANtricity Speicher-Plug-in für vCenter

Um Speicherressourcen anzuzeigen und zu verwalten, müssen Sie die IP-Adressen von Arrays in Ihrem Netzwerk über die Schnittstelle Storage Plug-in für vCenter ermitteln.

Bevor Sie beginnen

- Sie müssen die Netzwerk-IP-Adressen (oder den Adressbereich) der Array-Controller kennen.
- Die Speicher-Arrays müssen ordnungsgemäß eingerichtet und konfiguriert sein, und Sie müssen die Anmeldedaten des Speicher-Arrays (Benutzername und Passwort) kennen.

Schritt 1: Geben Sie Netzwerkadressen für die Ermittlung ein

Schritte

1. Wählen Sie auf der Seite Verwalten die Option **Hinzufügen/Entdecken**.

   Das Dialogfeld Netzwerkadressbereich eingeben wird angezeigt.

2. Führen Sie einen der folgenden Schritte aus:
   - Um ein Array zu ermitteln, wählen Sie die Optionsschaltfläche **Entdecken eines einzelnen Speicherarrays** aus und geben dann die IP-Adresse für einen der Controller im Speicher-Array ein.
   - Um mehrere Speicher-Arrays zu entdecken, wählen Sie die Optionsschaltfläche **Alle Speicher-Arrays in einem Netzwerkbereich** aus. Geben Sie dann die Startnetzwerkadresse und die Netzwerkadresse ein, um das lokale Subnetzwerk zu durchsuchen.
3. Klicken Sie Auf **Erkennung Starten**.

   Beim Beginn des Erkennungsvorgangs werden die Speicher-Arrays im Dialogfeld angezeigt, wenn sie erkannt werden. Der Erkennungsvorgang kann mehrere Minuten dauern.

   Wenn keine verwaltbaren Arrays erkannt werden, überprüfen Sie, ob die Speicher-Arrays ordnungsgemäß mit Ihrem Netzwerk verbunden sind und die zugewiesenen Adressen innerhalb der Reichweite liegen. Klicken Sie auf **Neue Ermittlungsparameter**, um zur Seite Hinzufügen/Entdecken zurückzukehren.

4. Aktivieren Sie das Kontrollkästchen neben einem beliebigen Speicher-Array, das Sie Ihrer Management-Domäne hinzufügen möchten.

   Das System führt für jedes Array, das Sie der Management-Domäne hinzufügen, eine Anmeldeinformationsprüfung durch. Möglicherweise müssen Sie Probleme mit nicht vertrauenswürdigen Zertifikaten beheben, bevor Sie fortfahren.

5. Klicken Sie auf **Weiter**, um mit dem nächsten Schritt im Assistenten fortzufahren.

   Wenn die Speicher-Arrays über gültige Zertifikate verfügen, gehen Sie zu Schritt 3: Geben Sie Passwörter ein.

   Wenn keine Speicherarrays über gültige Zertifikate verfügen, wird das Dialogfeld Selbstsignierte Zertifikate auflösen angezeigt. Gehen Sie zu Schritt 2: Lösen Sie nicht vertrauenswürdige Zertifikate während der Ermittlung.

   Wenn Sie CA-signierte Zertifikate importieren möchten, löschen Sie den Ermittlungsassistenten und klicken Sie im linken Bereich auf **Zertifikatverwaltung**. Weitere Anweisungen finden Sie in der Online-Hilfe.

Schritt 2: Lösen Sie nicht vertrauenswürdige Zertifikate während der Ermittlung

Sie müssen Probleme mit dem Zertifikat lösen, bevor Sie mit der Ermittlung fortfahren.

1. Wenn das Dialogfeld selbst signierte Zertifikate auflösen geöffnet wird, überprüfen Sie die Informationen, die für die nicht vertrauenswürdigen Zertifikate angezeigt werden. Für weitere Informationen können Sie auch auf die Ellipsen am äußersten Ende der Tabelle klicken und im Kontextmenü **Ansicht** wählen.
2. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie den Verbindungen zu den erkannten Speicherarrays vertrauen, klicken Sie auf **Weiter** und klicken Sie dann auf **Ja**, um den nächsten Dialog im Assistenten zu bestätigen. Die selbstsignierten Zertifikate werden als vertrauenswürdig gekennzeichnet und die Speicher-Arrays werden dem Plugin

hinzugefügt.

- Wenn Sie den Verbindungen zu den Speicher-Arrays nicht vertrauen, wählen Sie **Abbrechen** und validieren Sie die Sicherheitszertifikatstrategie jedes Speicherarrays, bevor Sie einen dieser Verbindungen hinzufügen.

3. Klicken Sie auf **Weiter**, um mit dem nächsten Schritt im Assistenten fortzufahren.

Schritt 3: Geben Sie Passwörter ein

Als letzter Schritt zur Ermittlung müssen Sie die Passwörter für die Speicherarrays eingeben, die Sie Ihrer Management-Domäne hinzufügen möchten.

1. Geben Sie für jedes erkannte Array sein Administratorkennwort in die Felder ein.
2. Klicken Sie Auf **Fertig Stellen**.

   Es kann mehrere Minuten dauern, bis das System eine Verbindung zu den angegebenen Speicherarrays herstellt. Nach Abschluss des Prozesses werden die Speicherarrays Ihrer Verwaltungsdomäne hinzugefügt und der ausgewählten Gruppe zugeordnet (falls angegeben).

Stellen Sie Speicher im SANtricity Speicher-Plug-in für vCenter bereit

Zur Bereitstellung von Storage erstellen Sie Volumes, weisen Hosts Volumes zu und weisen Datastores Volumes zu.

Schritt: Volumes erstellen

Volumes sind Daten-Container, die den Speicherplatz auf Ihrem Storage-Array managen und organisieren. Sie erstellen Volumes aus der Speicherkapazität, die auf Ihrem Speicher-Array verfügbar ist, was Ihnen hilft, die Ressourcen Ihres Systems zu organisieren. Das Konzept der "Volumes" ist ähnlich wie die Verwendung von Ordnern/Verzeichnissen auf einem Computer, um Dateien für schnellen Zugriff zu organisieren.

Volumes sind die einzige Datenebene, die Hosts sichtbar ist. In einer SAN-Umgebung werden Volumes den Logical Unit Numbers (LUNs) zugeordnet. Diese LUNs enthalten die Benutzerdaten, auf die über ein oder mehrere der vom Storage-Array unterstützten Host-Zugriffsprotokolle zugegriffen werden kann.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie Menü:Erstellen[Volumes].

   Das Dialogfeld Host auswählen wird angezeigt.

4. Wählen Sie aus der Dropdown-Liste einen bestimmten Host oder Host-Cluster aus, dem Sie Volumes zuweisen möchten, oder wählen Sie aus, zu einem späteren Zeitpunkt den Host oder Host-Cluster zuzuweisen.
5. Um die Volume-Erstellungsreihenfolge für den ausgewählten Host oder Host-Cluster fortzusetzen, klicken Sie auf **Weiter**.

   Das Dialogfeld „Workload auswählen“ wird angezeigt. Ein Workload enthält Volumes mit ähnlichen Eigenschaften, die auf Grundlage des von dem Workload unterstützten Applikationstyps optimiert sind. Sie können einen Workload definieren oder vorhandene Workloads auswählen.

6. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie die Option **Volumes für einen vorhandenen Workload erstellen** aus, und wählen Sie den Workload aus der Dropdown-Liste aus.
   - Wählen Sie die Option **Einen neuen Workload erstellen** aus, um einen neuen Workload für eine unterstützte Anwendung oder für „andere“ Anwendungen zu definieren, und führen Sie anschließend die folgenden Schritte aus:
     i. Wählen Sie in der Dropdown-Liste den Namen der Anwendung aus, für die Sie den neuen Workload erstellen möchten. Wählen Sie einen der „anderen“ Einträge aus, wenn die Anwendung, die Sie für dieses Speicher-Array verwenden möchten, nicht aufgeführt ist.
     ii. Geben Sie einen Namen für den zu erstellenden Workload ein.
7. Klicken Sie Auf **Weiter**. Wenn Ihr Workload einem unterstützten Applikationstyp zugewiesen ist, geben Sie die angeforderten Informationen ein. Andernfalls fahren Sie mit dem nächsten Schritt fort.

   Das Dialogfeld Volumes hinzufügen/bearbeiten wird angezeigt. In diesem Dialogfeld erstellen Sie Volumes aus geeigneten Pools oder Volume-Gruppen. Für jeden infrage kommenden Pool und jede Volume-Gruppe wird die Anzahl der verfügbaren Laufwerke und die gesamte freie Kapazität angezeigt. Für einige applikationsspezifische Workloads zeigt jede qualifizierte Pool- oder Volume-Gruppe die vorgeschlagene Kapazität basierend auf der vorgeschlagenen Volume-Konfiguration und zeigt die verbleibende freie Kapazität in gib an. Für andere Workloads wird die vorgeschlagene Kapazität angezeigt, wenn Sie Volumes zu einem Pool oder einer Volume-Gruppe hinzufügen und die gemeldete Kapazität angeben.

8. Bevor Sie mit dem Hinzufügen von Volumes beginnen, lesen Sie die Richtlinien in der folgenden Tabelle.

Feld	Beschreibung
Freie Kapazität	Da Volumes aus Pools oder Volume-Gruppen erstellt werden, muss der ausgewählte Pool oder die ausgewählte Volume-Gruppe über ausreichende freie Kapazität verfügen.
Data Assurance (da)	Um ein Volume mit einem da-fähigen Volumen zu erstellen, muss die Host-Verbindung, die Sie verwenden möchten, da unterstützen. • Wenn Sie ein DA-fähiges Volume erstellen möchten, wählen Sie einen Pool oder eine Volume-Gruppe aus, die für da geeignet ist (suchen Sie in der Tabelle mit den Kandidaten für Pool- und Volume-Gruppen nach **Ja** neben „da“). • DA-Funktionen werden auf Pool- und Volume-Gruppenebene präsentiert. DA der Schutz auf Fehler überprüft und korrigiert, die auftreten können, wenn Daten durch die Controller an die Laufwerke übertragen werden. Durch die Auswahl eines da-fähigen Pools oder einer Volume-Gruppe für das neue Volume wird sichergestellt, dass Fehler erkannt und behoben werden. • Wenn eine der Host-Verbindungen auf den Controllern im Speicher-Array keine Unterstützung für da bietet, können die zugeordneten Hosts auf da-fähige Volumes keinen Zugriff auf Daten haben.

Feld	Beschreibung
Laufwerkssicherheit	Um ein sicheres Volume zu erstellen, muss für das Storage Array ein Sicherheitsschlüssel erstellt werden. • Wenn Sie ein sicheres Volume erstellen möchten, wählen Sie einen Pool oder eine Volume-Gruppe aus, die sicher ist (suchen Sie in der Tabelle mit den Kandidaten für Pool- und Volume-Gruppen nach **Ja** neben „Secure-fähig“). • Die Sicherheitsfunktionen für die Laufwerksicherheit werden auf Pool- und Volume-Gruppenebene präsentiert. Sichere Laufwerke verhindern unbefugten Zugriff auf die Daten auf einem Laufwerk, das physisch vom Storage-Array entfernt wird. Ein sicheres Laufwerk verschlüsselt Daten während des Schreibvorgangs und entschlüsselt Daten beim Lesen mithilfe eines eindeutigen Verschlüsselungsschlüssels. • Ein Pool oder eine Volume-Gruppe kann sowohl sichere als auch nicht sichere Laufwerke enthalten. Zur Nutzung der Verschlüsselungsfunktionen müssen jedoch alle Laufwerke sicher sein.
Ressourcen-Provisionierung	Um ein Volume mit Ressourcenbereitstellung zu erstellen, müssen alle Laufwerke NVMe-Laufwerke mit der dezugewiesenen oder nicht geschriebenen Option Logical Block Error (DULBE) sein.

9. Wählen Sie eine dieser Aktionen aus, basierend darauf, ob Sie im vorherigen Schritt „Sonstige“ oder einen applikationsspezifischen Workload ausgewählt haben:
   - **Other** – Klicken Sie **Neues Volume hinzufügen** in jedem Pool oder Volume-Gruppe, die Sie verwenden möchten, um ein oder mehrere Volumes zu erstellen.
   - **Anwendungsspezifischer Workload** – Klicken Sie entweder auf **Weiter**, um die vom System empfohlenen Volumes und Merkmale für den ausgewählten Workload zu akzeptieren, oder klicken Sie auf **Volumes bearbeiten**, um die vom System empfohlenen Volumes und Merkmale für den ausgewählten Workload zu ändern, hinzuzufügen oder zu löschen.

     Die folgenden Felder werden angezeigt.

Feld	Beschreibung
Volume-Name	Einem Volume wird während der Volume-Erstellungsreihenfolge ein Standardname zugewiesen. Sie können entweder den Standardnamen akzeptieren oder einen aussagekräftigeren Namen angeben, der die Art der im Volume gespeicherten Daten angibt.

Feld	Beschreibung
Gemeldete Kapazität	Definieren Sie die Kapazität des neuen Volume und der zu verwendenden Kapazitätseinheiten (MiB, gib oder tib). Bei dicken Volumes beträgt die Mindestkapazität 1 MiB, und die maximale Kapazität wird durch die Anzahl und Kapazität der Laufwerke im Pool oder der Volume-Gruppe bestimmt. Die Kapazität in einem Pool wird in Schritten von 4 gib zugewiesen. Kapazitäten, die nicht ein Vielfaches von 4 gib beträgt, werden zugewiesen, aber nicht nutzbar. Um sicherzustellen, dass die gesamte Kapazität nutzbar ist, geben Sie die Kapazität in Schritten von 4 gib an. Wenn eine nicht nutzbare Kapazität vorhanden ist, besteht die einzige Möglichkeit zur Wiederherstellung darin, die Kapazität des Volume zu erhöhen.
Volume-Typ	Wenn Sie „applikationsspezifische Workloads“ ausgewählt haben, wird das Feld Volume-Typ angezeigt. Dies gibt den Volume-Typ an, der für einen applikationsspezifischen Workload erstellt wurde.
Volume-Block-Größe (nur EF300 und EF600)	Zeigt die Block-Größen, die für das Volume erstellt werden können: • 512–512 Byte • 4 KB – 4,096 Byte

Feld	Beschreibung
Segmentgröße	Zeigt die Einstellung für die Segmentgrößen, die nur für Volumes in einer Volume-Gruppe angezeigt wird. Sie können die Segmentgröße ändern, um die Leistung zu optimieren. **Zulässige Segmentgrößen-Übergänge** – das System bestimmt die zulässigen Segmentgrößen-Übergänge. Segmentgrößen, bei denen es sich um unangemessene Übergänge aus der aktuellen Segmentgröße handelt, sind in der Dropdown-Liste nicht verfügbar. Zulässige Übergänge sind in der Regel doppelt oder halb so groß wie das aktuelle Segment. Wenn die aktuelle Volume-Segmentgröße beispielsweise 32 KiB beträgt, ist eine neue Volume-Segmentgröße von entweder 16 KiB oder 64 KiB zulässig. **SSD Cache-fähige Volumes** – Sie können eine 4-KiB-Segmentgröße für SSD Cache-fähige Volumes angeben. Vergewissern Sie sich, dass Sie die 4-KiB-Segmentgröße nur für SSD-Cache-fähige Volumes auswählen, die I/O-Vorgänge mit kleinen Blöcken bearbeiten (beispielsweise 16 KiB-I/O-Blockgrößen oder kleiner). Die Performance könnte beeinträchtigt werden, wenn Sie 4 als Segmentgröße für SSD Cache-fähige Volumes auswählen, die sequenzielle Operationen von großen Blöcken bearbeiten. **Zeit zum Ändern der Segmentgröße** – die Zeit, die zur Änderung der Segmentgröße eines Volumes benötigt wird, hängt von diesen Variablen ab: • Die I/O-Last vom Host • Die Änderungspriorität des Volumes • Die Anzahl der Laufwerke in der Volume-Gruppe • Die Anzahl der Laufwerkskanäle • Die Verarbeitungsleistung der Speicher-Array-Controller Wenn Sie die Segmentgröße für ein Volume ändern, wirkt sich die I/O-Performance auf die I/O-Performance aus, doch die Daten bleiben verfügbar.
Sicher	**Ja** erscheint neben "Secure-fähig" nur dann, wenn die Laufwerke im Pool oder in der Volume-Gruppe verschlüsselungsfähig sind. Die Laufwerkssicherheit verhindert, dass nicht autorisierter Zugriff auf die Daten auf einem Laufwerk erfolgt, das physisch vom Speicher-Array entfernt wird. Diese Option ist nur verfügbar, wenn die Laufwerksicherheit aktiviert wurde und für das Speicher-Array ein Sicherheitsschlüssel eingerichtet wurde. Ein Pool oder eine Volume-Gruppe kann sowohl sichere als auch nicht sichere Laufwerke enthalten. Zur Nutzung der Verschlüsselungsfunktionen müssen jedoch alle Laufwerke sicher sein.
DA	**Ja** erscheint neben „da“ nur dann, wenn die Laufwerke im Pool oder in der Volume-Gruppe Data Assurance (da) unterstützen. DA erhöht die Datenintegrität im gesamten Storage-System. DA ermöglicht es dem Storage-Array, Fehler zu überprüfen, die auftreten können, wenn Daten durch die Controller an die Laufwerke übertragen werden. Die Verwendung von da für das neue Volume stellt sicher, dass alle Fehler erkannt werden.

10. Klicken Sie auf **Weiter**, um mit der Volumenerzeugung für die ausgewählte Anwendung fortzufahren.

11. Lesen Sie im letzten Schritt eine Zusammenfassung der Volumes, die Sie erstellen möchten, und nehmen Sie die erforderlichen Änderungen vor. Um Änderungen vorzunehmen, klicken Sie auf **Zurück**. Wenn Sie mit Ihrer Volumenkonfiguration zufrieden sind, klicken Sie auf **Fertig stellen**.

Schritt: Hostzugriff erstellen und Volumes zuweisen

Ein Host kann manuell erstellt werden:

- **Manuell** – bei der manuellen Hosterstellung verknüpfen Sie Host-Port-IDs, indem Sie sie aus einer Liste auswählen oder manuell eingeben. Nachdem Sie einen Host erstellt haben, können Sie ihm Volumes zuweisen oder einem Host Cluster hinzufügen, wenn Sie den Zugriff auf Volumes freigeben möchten.

Manuelles Erstellen des Hosts

Bevor Sie beginnen

Lesen Sie folgende Richtlinien:

- Sie müssen bereits Storage Arrays in Ihrer Umgebung hinzugefügt oder erkannt haben.
- Sie müssen die dem Host zugeordneten Host-Identifier-Ports definieren.
- Stellen Sie sicher, dass Sie denselben Namen wie den zugewiesenen Systemnamen des Hosts angeben.
- Dieser Vorgang ist nicht erfolgreich, wenn der gewählte Name bereits verwendet wird.
- Die Länge des Namens darf nicht mehr als 30 Zeichen umfassen.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit der Hostverbindung aus.
2. Wählen Sie Menü:Bereitstellung [Hosts konfigurieren].

   Die Seite Hosts konfigurieren wird geöffnet.

3. Klicken Sie auf Menü:Create[Host].

   Das Dialogfeld Host erstellen wird angezeigt.

4. Wählen Sie die entsprechenden Einstellungen für den Host aus.

Feld	Beschreibung
Name	Geben Sie einen Namen für den neuen Host ein.
Host-Betriebssystem-Typ	Wählen Sie aus der Dropdown-Liste das auf dem neuen Host ausgeführte Betriebssystem aus.
Host-Schnittstellentyp	(Optional) Wenn auf Ihrem Speicherarray mehr als eine Host-Schnittstelle unterstützt wird, wählen Sie den Host-Schnittstellentyp aus, den Sie verwenden möchten.

Feld	Beschreibung
Host-Ports	Führen Sie einen der folgenden Schritte aus: • **I/O-Schnittstelle auswählen** — generell sollten sich die Host-Ports angemeldet haben und über die Dropdown-Liste verfügbar sein. Sie können die Host-Port-IDs aus der Liste auswählen. • **Manuelles Hinzufügen** — Wenn eine Host-Port-ID nicht in der Liste angezeigt wird, bedeutet dies, dass der Host-Port nicht angemeldet ist. Mithilfe eines HBA-Dienstprogramms oder des iSCSI-Initiator-Dienstprogramms können die Host-Port-IDs ermittelt und mit dem Host verknüpft werden. Sie können die Host-Port-IDs manuell eingeben oder sie aus dem Dienstprogramm (nacheinander) in das Feld Host-Ports kopieren/einfügen. Sie müssen eine Host-Port-ID gleichzeitig auswählen, um sie dem Host zuzuordnen. Sie können jedoch weiterhin so viele Kennungen auswählen, die dem Host zugeordnet sind. Jede Kennung wird im Feld Host-Ports angezeigt. Bei Bedarf können Sie auch einen Bezeichner entfernen, indem Sie neben ihm die **X**-Option auswählen.
Legen Sie den CHAP-Initiatorschlüssel fest	(Optional) Wenn Sie einen Host-Port mit einem iSCSI-IQN ausgewählt oder manuell eingegeben haben und wenn Sie einen Host benötigen möchten, der versucht, auf das Speicher-Array zuzugreifen, um sich mit dem Challenge Handshake Authentication Protocol (CHAP) zu authentifizieren, aktivieren Sie das Kontrollkästchen **CHAP Initiator Secret** setzen. Gehen Sie für jeden ausgewählten oder manuell eingegebenen iSCSI-Host-Port wie folgt vor: • Geben Sie denselben CHAP-Schlüssel ein, der auf jedem iSCSI-Hostinitiator für die CHAP-Authentifizierung festgelegt wurde. Wenn Sie die gegenseitige CHAP-Authentifizierung verwenden (zwei-Wege-Authentifizierung, die es einem Host ermöglicht, sich am Speicher-Array zu validieren, und damit sich ein Speicher-Array am Host validieren kann), müssen Sie auch den CHAP-Schlüssel für das Speicher-Array bei der Ersteinrichtung oder durch Ändern von Einstellungen festlegen. • Wenn Sie keine Host-Authentifizierung benötigen, lassen Sie das Feld leer. Derzeit wird nur CHAP verwendet.

5. Klicken Sie Auf **Erstellen**.
6. Wenn Sie die Hostinformationen aktualisieren müssen, wählen Sie den Host aus der Tabelle aus und klicken Sie auf **Einstellungen anzeigen/bearbeiten**.

   Nachdem der Host erfolgreich erstellt wurde, erstellt das System für jeden Host-Port, der für den Host konfiguriert wurde (Benutzungsbezeichnung) einen Standardnamen. Der Standard-Alias ist `<Hostname_Port Number>`. Der Standard-Alias für den ersten Port, der für das Host-IPT erstellt wurde, ist beispielsweise `IPT_1`.

7. Als Nächstes müssen Sie ein Volume einem Host oder Host-Cluster zuweisen, damit es für I/O-Vorgänge verwendet werden kann. Wählen Sie Menü:Bereitstellung [Hosts konfigurieren].

Die Seite Hosts konfigurieren wird geöffnet.

8. Wählen Sie den Host oder Host-Cluster aus, dem Sie Volumes zuweisen möchten, und klicken Sie dann auf **Volumes zuweisen**.

   Es wird ein Dialogfeld angezeigt, in dem alle Volumes aufgelistet werden, die zugewiesen werden können. Sie können jede der Spalten sortieren oder etwas in das Filter-Feld eingeben, um bestimmte Volumes einfacher zu finden.

9. Aktivieren Sie das Kontrollkästchen neben jedem Volume, das Sie zuweisen möchten, oder aktivieren Sie das Kontrollkästchen in der Tabellenüberschrift, um alle Volumes auszuwählen.
10. Klicken Sie auf **Zuweisen**, um den Vorgang abzuschließen.

    Das System führt die folgenden Aktionen durch:

    - Das zugewiesene Volume erhält die nächste verfügbare LUN-Nummer. Der Host verwendet die LUN-Nummer für den Zugriff auf das Volume.
    - Der vom Benutzer bereitgestellte Volume-Name wird in den Volume-Listen angezeigt, die dem Host zugeordnet sind. Falls zutreffend, wird das werkseitig konfigurierte Zugriffsvolume auch in den Volume-Listen angezeigt, die dem Host zugeordnet sind.

Schritt 3: Erstellen Sie einen Datastore in vSphere Client

Informationen zum Erstellen eines Datastore im vSphere-Client finden Sie unter "Erstellen Sie einen VMFS-Datenspeicher im vSphere-Client" Thema im VMware Doc Center.

Erhöhung der Kapazität vorhandener Datastores durch Erhöhung der Volume-Kapazität

Sie können die gemeldete Kapazität (die gemeldete Kapazität an Hosts) eines Volumes erhöhen, indem Sie die freie Kapazität nutzen, die in dem Pool bzw. der Volume-Gruppe verfügbar ist.

Bevor Sie beginnen

Stellen Sie sicher, dass:

- Im zugewiesenen Pool bzw. der Volume-Gruppe des Volumes steht genügend freie Kapazität zur Verfügung.
- Das Volume ist optimal und nicht in einem Zustand der Änderung.
- Im Volume werden keine Hot-Spare-Laufwerke verwendet. (Gilt nur für Volumes in Volume-Gruppen.)

> Eine Erhöhung der Kapazität eines Volumens wird nur auf bestimmten Betriebssystemen unterstützt. Wenn Sie die Volume-Kapazität auf einem Host-Betriebssystem erhöhen, das die LUN-Erweiterung nicht unterstützt, kann die erweiterte Kapazität nicht verwendet werden. Sie können die ursprüngliche Volume-Kapazität nicht wiederherstellen.

Schritte

1. Navigieren Sie zum Plug-in in vSphere Client.
2. Wählen Sie im Plug-in das gewünschte Speicher-Array aus.
3. Klicken Sie auf **Provisioning** und wählen Sie **Volumes verwalten**.
4. Wählen Sie das Volumen aus, für das Sie die Kapazität erhöhen möchten, und wählen Sie dann **Kapazität erhöhen**.

Das Dialogfeld Kapazität erhöhen bestätigen wird angezeigt.

5. Wählen Sie **Ja**, um fortzufahren.

   Das Dialogfeld gemeldete Kapazität erhöhen wird angezeigt.

   In diesem Dialogfeld wird die aktuell gemeldete Kapazität des Volumes und die freie Kapazität angezeigt, die im zugeordneten Pool oder der Volume-Gruppe verfügbar ist.

6. Verwenden Sie das Feld * gemeldete Kapazität erhöhen, indem Sie…* hinzufügen, um die Kapazität der aktuell verfügbaren gemeldeten Kapazität hinzuzufügen. Sie können den Kapazitätswert ändern, um entweder in Mebibyte (MiB), Gibibyte (gib) oder Tebibyte (tib) anzuzeigen.
7. Klicken Sie Auf **Erhöhen**.
8. Zeigen Sie den Fensterbereich Letzte Aufgaben an, um den Fortschritt des Vorgangs Kapazitätssteigerung anzuzeigen, der derzeit für das ausgewählte Volume ausgeführt wird. Dieser Vorgang kann langwierig sein und die System-Performance beeinträchtigen.
9. Nachdem die Volume-Kapazität abgeschlossen ist, müssen Sie die VMFS-Größe manuell erhöhen, um sie wie in beschrieben anzupassen "Erhöhen Sie die VMFS-Datenspeicherkapazität im vSphere-Client" Thema im VMware Doc Center.

Erhöhen Sie die Kapazität vorhandener Datastores durch Hinzufügen von Volumes

1. Sie können die Kapazität eines Datastores durch Hinzufügen von Volumes erhöhen. Befolgen Sie die Schritte unter Schritt: Volumes erstellen.
2. Weisen Sie dann die Volumes dem gewünschten Host zu, um die Kapazität des Datenspeichers zu erhöhen.

   Siehe "Erhöhen Sie die VMFS-Datenspeicherkapazität im vSphere-Client" Weitere Informationen finden Sie unter dem VMware Doc Center.

Zeigen Sie den Status Ihres Speichersystems im SANtricity Speicher-Plug-in für vCenter an

Sie können den Systemstatus über das Storage Plug-in für vCenter oder über den vSphere Client anzeigen.

1. Öffnen Sie das Plug-in aus dem vSphere Client.
2. Status aus den folgenden Bereichen anzeigen:
   - **Storage Array Status** — Gehen Sie zum Fenster **Manage-All**. Für jedes erkannte Array wird in der Zeile eine Spalte Status angezeigt.
   - **Operationen in Bearbeitung** — Klicken Sie auf **Operationen** auf der Seitenleiste, um alle lang laufenden Aufgaben, wie das Importieren von Einstellungen, anzuzeigen. Über das Dropdown-Menü Provisioning können Sie auch langlebige Vorgänge anzeigen. Für jeden Vorgang, der im Dialogfeld „laufende Vorgänge“ aufgeführt wird, werden ein Prozentsatz des Fertigstellungsvorgangs und die geschätzte verbleibende Zeit bis zum Abschluss des Vorgangs angezeigt. In einigen Fällen können Sie einen Vorgang anhalten oder eine höhere oder niedrigere Priorität zuweisen. Verwenden Sie die Links in der Spalte Aktionen, um die Priorität für einen Vorgang zu beenden oder zu ändern.

> Lesen Sie alle in den Dialogfeldern angegebenen Vorsichtstexte, insbesondere wenn Sie einen Vorgang unterbrechen.

Operationen, die für das Plugin angezeigt werden können, sind in der folgenden Tabelle aufgelistet. Möglicherweise werden auch weitere Vorgänge in der Benutzeroberfläche von System Manager angezeigt.

Betrieb	Möglicher Status des Vorgangs	Maßnahmen, die Sie ergreifen können
Volume-Erstellung (nur Thick Pool Volumes über 64 tib)	In Bearbeitung	Keine
Volume-Löschen (nur Thick Pool Volumes über 64 tib)	In Bearbeitung	Keine
Hinzufügen von Kapazitäten für den Pool oder die Volume-Gruppe	In Bearbeitung	Keine
Ändern Sie einen RAID-Level für ein Volume	In Bearbeitung	Keine
Reduktion der Kapazität für einen Pool	In Bearbeitung	Keine
Prüfen Sie die verbleibende Zeit für einen IAF-Betrieb (Instant Availability Format) für Pool Volumes	In Bearbeitung	Keine
Prüfen Sie die Datenredundanz einer Volume-Gruppe	In Bearbeitung	Keine
Initialisieren Sie ein Volume	In Bearbeitung	Keine
Höhere Kapazität für ein Volume	In Bearbeitung	Keine
Ändern Sie die Segmentgröße für ein Volume	In Bearbeitung	Keine

Verwalten von Zertifikaten

Erfahren Sie mehr über das Verwalten von Zertifikaten im SANtricity Speicher-Plug-in für vCenter

Die Zertifikatverwaltung im Speicher-Plugin für vCenter ermöglicht die Erstellung von Zertifikatsignierungsanforderungen (CSRs), den Import von Zertifikaten und die Verwaltung vorhandener Zertifikate.

Was sind Zertifikate?

Zertifikate sind digitale Dateien, die Online-Einheiten wie Websites und Server für eine sichere Kommunikation im Internet identifizieren. Sie stellen sicher, dass die Webkommunikation in verschlüsselter Form, privat und unverändert, nur zwischen dem angegebenen Server und dem angegebenen Client übertragen wird. Mit dem Storage Plug-in für vCenter können Sie Zertifikate für den Browser auf einem Host-Managementsystem und die Controller in den ermittelten Speicher-Arrays verwalten.

Ein Zertifikat kann von einer vertrauenswürdigen Behörde signiert werden, oder es kann selbst signiert werden. „Unterzeichnen“ bedeutet einfach, dass jemand die Identität des Besitzers bestätigt und festgestellt hat, dass seine Geräte vertrauenswürdig sind.

Die Storage Arrays werden mit einem automatisch generierten, selbstsignierten Zertifikat auf jedem Controller

ausgeliefert. Sie können weiterhin die selbst signierten Zertifikate verwenden oder CA-signierte Zertifikate für eine sicherere Verbindung zwischen den Controllern und den Host-Systemen erhalten.

> Auch wenn CA-signierte Zertifikate einen besseren Schutz bieten (zum Beispiel die Verhinderung von man-in-the-Middle-Angriffen), verlangen sie auch Gebühren, die teuer sein können, wenn Sie ein großes Netzwerk haben. Im Gegensatz dazu sind selbstsignierte Zertifikate weniger sicher, aber sie sind kostenlos. Daher werden selbst signierte Zertifikate am häufigsten für interne Testumgebungen eingesetzt, nicht in Produktionsumgebungen.

Signierte Zertifikate

Ein signiertes Zertifikat wird von einer Zertifizierungsstelle (CA) validiert, einer vertrauenswürdigen Drittorganisation. Signierte Zertifikate enthalten Angaben über den Eigentümer der Einheit (in der Regel Server oder Website), Datum der Zertifikatausgabe und -Ablauf, gültige Domains für das Unternehmen und eine digitale Signatur bestehend aus Buchstaben und Zahlen.

Wenn Sie einen Browser öffnen und eine Webadresse eingeben, führt Ihr System eine Zertifikatprüfung im Hintergrund durch, um zu bestimmen, ob Sie eine Verbindung zu einer Website herstellen, die ein gültiges, von einer Zertifizierungsstelle signiertes Zertifikat enthält. In der Regel enthält eine mit einem signierten Zertifikat gesicherte Website ein Vorhängeschloss-Symbol und eine https-Bezeichnung in der Adresse. Wenn Sie versuchen, eine Verbindung zu einer Website herzustellen, die kein CA-signiertes Zertifikat enthält, zeigt Ihr Browser eine Warnung an, dass die Website nicht sicher ist.

Die CA führt Schritte durch, um Ihre Identität während des Anwendungsprozesses zu überprüfen. Sie senden möglicherweise eine E-Mail an Ihr registriertes Unternehmen, überprüfen Ihre Geschäftsadresse und führen eine HTTP- oder DNS-Verifizierung durch. Wenn der Anwendungsprozess abgeschlossen ist, sendet die Zertifizierungsstelle digitale Dateien zum Laden auf einem Host-Managementsystem. In der Regel umfassen diese Dateien eine Kette des Vertrauens, wie folgt:

- **Root** — an der Spitze der Hierarchie befindet sich das Stammzertifikat, welches einen privaten Schlüssel enthält, der zum Signieren anderer Zertifikate verwendet wird. Das Root identifiziert eine bestimmte CA-Organisation. Wenn Sie dieselbe Zertifizierungsstelle für alle Netzwerkgeräte verwenden, benötigen Sie nur ein Stammzertifikat.
- **Intermediate** — Abzweigung von der Wurzel sind die Zwischenzertifikate. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten fungieren sollen.
- **Server** — unten in der Kette befindet sich das Server-Zertifikat, welches Ihre spezifische Entität, wie z.B. eine Website oder ein anderes Gerät, identifiziert. Jeder Controller in einem Storage Array benötigt ein separates Serverzertifikat.

Selbstsignierte Zertifikate

Jeder Controller im Speicher-Array verfügt über ein vorinstalliertes, selbstsigniertes Zertifikat. Ein selbst signiertes Zertifikat ähnelt einem CA-signierten Zertifikat, außer dass es vom Eigentümer des Unternehmens anstelle eines Dritten validiert wird. Wie ein Zertifikat mit einer Zertifizierungsstelle enthält auch ein selbstsigniertes Zertifikat einen eigenen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt und über eine HTTPS-Verbindung zwischen einem Server und einem Client gesendet werden.

Selbstsignierte Zertifikate werden von Browsern nicht „vertrauenswürdig“. Jedes Mal, wenn Sie versuchen, eine Verbindung zu einer Website herzustellen, die nur ein selbstsigniertes Zertifikat enthält, wird im Browser eine Warnmeldung angezeigt. Sie müssen in der Warnmeldung auf einen Link klicken, der Ihnen die Nutzung der Website ermöglicht. Dadurch akzeptieren Sie im Wesentlichen das selbstsignierte Zertifikat.

Managementzertifikat

Wenn Sie das Plugin öffnen, versucht der Browser zu überprüfen, ob der Management-Host eine vertrauenswürdige Quelle ist, indem er nach einem digitalen Zertifikat prüft. Wenn der Browser ein von einer Zertifizierungsstelle signiertes Zertifikat nicht findet, wird eine Warnmeldung angezeigt. Von dort aus können Sie auf der Website fortfahren, um das selbstsignierte Zertifikat für diese Sitzung zu akzeptieren. Sie können auch signierte digitale Zertifikate von einer Zertifizierungsstelle beziehen, damit die Warnmeldung nicht mehr angezeigt wird.

Vertrauenswürdige Zertifikate

Während einer Plugin-Sitzung werden möglicherweise zusätzliche Sicherheitsmeldungen angezeigt, wenn Sie versuchen, auf einen Controller zuzugreifen, der kein von einer Zertifizierungsstelle signiertes Zertifikat hat. In diesem Fall können Sie dem selbst signierten Zertifikat dauerhaft vertrauen oder die CA-signierten Zertifikate für die Controller importieren, damit das Plugin eingehende Clientanforderungen von diesen Controllern authentifizieren kann.

Verwenden Sie CA-signierte Zertifikate im SANtricity-Speichermodul für vCenter

Sie können CA-signierte Zertifikate für den sicheren Zugriff auf das Managementsystem abrufen und importieren, das das Storage Plugin für vCenter hostet.

Die Verwendung von CA-signierten Zertifikaten ist ein dreistufiges Verfahren:

- Schritt 1: Eine CSR-Datei ausfüllen.
- Schritt 2: CSR-Datei senden.
- Schritt 3: Import Management Zertifikate.

Schritt 1: Eine CSR-Datei ausfüllen

Sie müssen zuerst eine CSR-Datei (Certificate Signing Request) generieren, die Ihre Organisation und das Host-System identifiziert, auf dem das Plugin ausgeführt wird. Alternativ können Sie eine CSR-Datei mit einem Tool wie OpenSSL generieren und zu überspringen Schritt 2: CSR-Datei senden.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte **Management** die Option **CSR abschließen** aus.
3. Geben Sie die folgenden Informationen ein, und klicken Sie dann auf **Weiter**:
   - **Organisation** — der vollständige, rechtliche Name Ihres Unternehmens oder Ihrer Organisation. Fügen Sie Suffixe wie Inc. Oder Corp. Mit ein
   - **Organisationseinheit (optional)** — die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet.
   - **Stadt/Ort** — die Stadt, in der sich Ihr Hostsystem oder Ihr Geschäft befindet.
   - **Bundesland/Region (optional)** — der Staat oder die Region, in der sich Ihr Hostsystem oder Ihr Geschäft befindet.
   - **Land ISO Code** — der zweistellige ISO-Code Ihres Landes (International Organization for Standardization), wie z. B. die USA.
4. Geben Sie die folgenden Informationen über das Hostsystem ein, auf dem das Plugin ausgeführt wird:
   - **Allgemeiner Name** — die IP-Adresse oder der DNS-Name des Hostsystems, auf dem das Plugin läuft. Stellen Sie sicher, dass diese Adresse korrekt ist; sie muss genau mit dem übereinstimmen, was Sie

eingeben, um auf das Plugin im Browser zugreifen. Verwenden Sie kein http:// oder https://. Der DNS-Name kann nicht mit einem Platzhalter beginnen.

- **Alternative IP-Adressen** — Wenn der allgemeine Name eine IP-Adresse ist, können Sie optional weitere IP-Adressen oder Aliase für das Host-System eingeben. Verwenden Sie für mehrere Einträge ein kommagetrenntes Format.
- **Alternative DNS-Namen** — Wenn der gemeinsame Name ein DNS-Name ist, geben Sie weitere DNS-Namen für das Host-System ein. Verwenden Sie für mehrere Einträge ein kommagetrenntes Format. Falls es keine alternativen DNS-Namen gibt, aber Sie im ersten Feld einen DNS-Namen eingegeben haben, kopieren Sie diesen Namen hier. Der DNS-Name kann nicht mit einem Platzhalter beginnen.

5. Stellen Sie sicher, dass die Host-Informationen richtig sind. Wenn dies nicht der Fall ist, schlagen die von der Zertifizierungsstelle zurückgegebenen Zertifikate fehl, wenn Sie versuchen, sie zu importieren.
6. Klicken Sie Auf **Fertig Stellen**.

Schritt 2: CSR-Datei senden

Nachdem Sie eine CSR-Datei (Certificate Signing Request) erstellt haben, senden Sie die generierte CSR-Datei an eine CA, um signierte Management-Zertifikate für das System zu erhalten, das das Plugin hostet.

Systeme der E-Series erfordern ein PEM-Format (Base64 ASCII-Kodierung) für signierte Zertifikate, das die folgenden Dateitypen umfasst: .Pem, .crt, .cer oder .key.

Schritte

1. Suchen Sie die heruntergeladene CSR-Datei.

   Der Speicherort des Downloads hängt von Ihrem Browser ab.

2. Senden Sie die CSR-Datei an eine CA (z. B. Verisign oder DigiCert), und fordern Sie signierte Zertifikate im PEM-Format an.

> Nachdem Sie eine CSR-Datei an die CA gesendet haben, erstellen SIE keine weitere CSR-Datei erneut.

Immer wenn Sie eine CSR erstellen, erstellt das System ein privates und öffentliches Schlüsselpaar. Der öffentliche Schlüssel ist Teil der CSR, während der private Schlüssel im Schlüsselspeicher des Systems aufbewahrt wird. Wenn Sie die signierten Zertifikate erhalten und importieren, stellt das System sicher, dass sowohl der private als auch der öffentliche Schlüssel das ursprüngliche Paar sind. Wenn die Schlüssel nicht übereinstimmen, funktionieren die signierten Zertifikate nicht und Sie müssen neue Zertifikate von der CA anfordern.

Schritt 3: Import Management Zertifikate

Nachdem Sie von der Zertifizierungsstelle (CA) signierte Zertifikate erhalten haben, importieren Sie die Zertifikate in das Hostsystem, auf dem das Plugin installiert ist.

Bevor Sie beginnen

- Sie müssen über die signierten Zertifikate der Zertifizierungsstelle verfügen. Diese Dateien umfassen das Stammzertifikat, ein oder mehrere Zwischenzertifikate und das Serverzertifikat.
- Wenn die CA eine verkettete Zertifikatdatei (z. B. eine .p7b-Datei) lieferte, müssen Sie die verkettete Datei in einzelne Dateien entpacken: Das Stammzertifikat, ein oder mehrere Zwischenzertifikate und das Serverzertifikat. Sie können das Windows-certmgr-Dienstprogramm zum Entpacken der Dateien verwenden (Rechtsklick und Menü wählen:Alle Aufgaben[Export]). Base-64-Kodierung wird empfohlen. Wenn die Exporte abgeschlossen sind, wird für jede Zertifikatdatei in der Kette eine CER-Datei angezeigt.

- Sie müssen die Zertifikatdateien auf das Hostsystem kopieren, auf dem das Plugin ausgeführt wird.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte * Management* die Option **Import**.

   Es wird ein Dialogfeld zum Importieren der Zertifikatdateien geöffnet.

3. Klicken Sie auf **Durchsuchen**, um zuerst die Stamm- und Zwischenzertifikatdateien auszuwählen und dann das Serverzertifikat auszuwählen. Wenn Sie die CSR aus einem externen Tool generiert haben, müssen Sie auch die private Schlüsseldatei importieren, die zusammen mit der CSR erstellt wurde.

   Die Dateinamen werden im Dialogfeld angezeigt.

4. Klicken Sie Auf **Import**.

Ergebnis

Die Dateien werden hochgeladen und validiert. Die Zertifikatinformationen werden auf der Seite Zertifikatverwaltung angezeigt.

Setzen Sie Managementzertifikate im SANtricity Speicher-Plug-in für vCenter zurück

Für das Managementsystem, das das Storage Plugin für vCenter hostet, können Sie das Managementzertifikat in den ursprünglichen, werkseitig selbstsignierten Zustand zurücksetzen.

Über diese Aufgabe

Mit dieser Aufgabe wird das aktuelle Management-Zertifikat aus dem Hostsystem gelöscht, auf dem das Storage Plugin für vCenter ausgeführt wird. Nach dem Zurücksetzen des Zertifikats wird das Host-System auf das selbstsignierte Zertifikat zurückgesetzt.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte **Verwaltung** die Option **Zurücksetzen**.

   Das Dialogfeld „Zertifikat zurücksetzen bestätigen“ wird geöffnet.

3. Geben Sie Reset in das Feld ein, und klicken Sie dann auf **Zurücksetzen**.

   Nach der Aktualisierung Ihres Browsers kann der Browser den Zugriff auf die Zielseite blockieren und melden, dass die Website HTTP Strict Transport Security verwendet. Diese Bedingung tritt auf, wenn Sie wieder auf selbstsignierte Zertifikate wechseln. Um die Bedingung zu löschen, die den Zugriff auf das Ziel blockiert, müssen Sie die Browserdaten aus dem Browser löschen.

Ergebnis

Das System setzt auf die Verwendung des selbstsignierten Zertifikats des Servers zurück. Das System fordert Benutzer daher auf, das selbstsignierte Zertifikat für ihre Sitzungen manuell anzunehmen.

Importieren Sie Zertifikate für Arrays im SANtricity Speicher-Plugin für vCenter

Bei Bedarf können Zertifikate für die Speicher-Arrays importiert werden, sodass sie sich

mit dem System authentifizieren können, das das Storage Plug-in für vCenter hostet. Zertifikate können von einer Zertifizierungsstelle (CA) signiert oder selbst signiert werden.

Bevor Sie beginnen

Wenn Sie vertrauenswürdige Zertifikate importieren, müssen die Zertifikate für die Speicher-Array-Controller mit System Manager importiert werden.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte * Trusted* aus.

   Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-Arrays gemeldet wurden.

3. Wählen Sie entweder Menü:Import[Certificates], um ein CA-Zertifikat oder Menü zu importieren:Importieren[Self-signierte Speicher-Array-Zertifikate], um ein selbstsigniertes Zertifikat zu importieren.
4. Um die Ansicht einzuschränken, können Sie das Filterfeld **Zertifikate anzeigen verwenden, das…** ist, oder Sie können die Zertifikatzeilen sortieren, indem Sie auf eine der Spaltenüberschrift klicken.
5. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf **Import**.

   Das Zertifikat wird hochgeladen und validiert.

Zeigen Sie Zertifikate im SANtricity Speicher-Plug-in für vCenter an

Sie können zusammenfassende Informationen für ein Zertifikat anzeigen, das die Organisation, die das Zertifikat verwendet, die Behörde, die das Zertifikat ausgestellt hat, den Gültigkeitszeitraum und die Fingerabdrücke (eindeutige Kennungen) umfasst.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie eine der folgenden Registerkarten aus:
   - **Management** — zeigt das Zertifikat für das System, das das Plugin hostet. Ein Managementzertifikat kann von einer Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Es ermöglicht sicheren Zugriff auf das Plugin.
   - **Trusted** — zeigt Zertifikate, auf die das Plugin für Speicher-Arrays und andere Remote-Server zugreifen kann, z. B. einen LDAP-Server. Die Zertifikate können von einer Zertifizierungsstelle (CA) ausgestellt oder selbst signiert werden.
3. Um weitere Informationen zu einem Zertifikat anzuzeigen, wählen Sie seine Zeile aus, wählen Sie die Ellipsen am Zeilenende aus und klicken Sie dann auf **Ansicht** oder **Export**.

Exportieren Sie Zertifikate in das SANtricity-Speichermodul für vCenter

Sie können ein Zertifikat exportieren, um die vollständigen Details anzuzeigen.

Bevor Sie beginnen

Um die exportierte Datei zu öffnen, müssen Sie über eine Zertifikatanzeige-Anwendung verfügen.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie eine der folgenden Registerkarten aus:
   - **Management** — zeigt das Zertifikat für das System, das das Plugin hostet. Ein Managementzertifikat kann von einer Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Es ermöglicht sicheren Zugriff auf das Plugin.
   - **Trusted** — zeigt Zertifikate, auf die das Plugin für Speicher-Arrays und andere Remote-Server zugreifen kann, z. B. einen LDAP-Server. Die Zertifikate können von einer Zertifizierungsstelle (CA) ausgestellt oder selbst signiert werden.
3. Wählen Sie auf der Seite ein Zertifikat aus, und klicken Sie dann am Ende der Zeile auf die Ellipsen.
4. Klicken Sie auf **Exportieren** und speichern Sie dann die Zertifikatdatei.
5. Öffnen Sie die Datei in Ihrer Zertifikatanzeige-Anwendung.

Löschen Sie vertrauenswürdige Zertifikate im SANtricity Speicher-Plugin für vCenter

Sie können ein oder mehrere nicht mehr benötigte Zertifikate löschen, z. B. ein abgelaufenes Zertifikat.

Bevor Sie beginnen

Importieren Sie das neue Zertifikat, bevor Sie das alte löschen.

> Beachten Sie, dass das Löschen eines Root- oder Zwischenzertifikats mehrere Speicher-Arrays beeinflussen kann, da diese Arrays dieselben Zertifikatdateien gemeinsam nutzen können.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte * Trusted* aus.
3. Wählen Sie ein oder mehrere Zertifikate in der Tabelle aus, und klicken Sie dann auf **Löschen**.

   > Die Löschfunktion ist für vorinstallierte Zertifikate nicht verfügbar.

   Das Dialogfeld Vertrauenswürdiges Zertifikat bestätigen wird geöffnet.
4. Bestätigen Sie den Löschvorgang, und klicken Sie dann auf **Löschen**.

   Das Zertifikat wird aus der Tabelle entfernt.

Lösen Sie nicht vertrauenswürdige Zertifikate im SANtricity Speicher-Plug-in für vCenter auf

Auf der Zertifikatsseite können Sie nicht vertrauenswürdige Zertifikate auflösen, indem Sie ein selbstsigniertes Zertifikat aus dem Speicher-Array importieren oder ein Zertifikat der Zertifizierungsstelle importieren, das von einem vertrauenswürdigen Dritten ausgestellt wurde.

Bevor Sie beginnen

Wenn Sie ein Zertifikat importieren möchten, muss Folgendes sichergestellt sein:

- Sie haben für jeden Controller im Speicher-Array eine Zertifikatsignierungsanforderung (.CSR-Datei)

generiert und an die CA gesendet.

- Die CA hat vertrauenswürdige Zertifikatdateien zurückgegeben.
- Die Zertifikatdateien sind auf Ihrem lokalen System verfügbar.

Über diese Aufgabe

Nicht vertrauenswürdige Zertifikate treten auf, wenn ein Speicher-Array versucht, eine sichere Verbindung zum Plugin herzustellen, aber die Verbindung wird nicht als sicher bestätigt. Möglicherweise müssen Sie zusätzliche vertrauenswürdige CA-Zertifikate installieren, wenn eine der folgenden Optionen zutrifft:

- Sie haben kürzlich ein Speicher-Array hinzugefügt.
- Ein oder beide Zertifikate sind abgelaufen oder widerrufen.
- Ein oder beide Zertifikate fehlen ein Stammzertifikat oder ein Zwischenzertifikat.

Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte * Trusted* aus.

   Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-Arrays gemeldet wurden.

3. Wählen Sie entweder Menü:Import[Certificates], um ein CA-Zertifikat oder Menü zu importieren:Importieren[Self-signierte Speicher-Array-Zertifikate], um ein selbstsigniertes Zertifikat zu importieren.
4. Um die Ansicht einzuschränken, können Sie das Filterfeld **Zertifikate anzeigen verwenden, das…** ist, oder Sie können die Zertifikatzeilen sortieren, indem Sie auf eine der Spaltenüberschrift klicken.
5. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf **Import**.

   Das Zertifikat wird hochgeladen und validiert.

Management von Arrays

Erfahren Sie mehr über das Management von Speicher-Arrays im SANtricity Speicher-Plug-in für vCenter

Verwenden Sie die Funktion Add/Discover, um die zu managenden Storage-Arrays im Storage Plug-in für vCenter zu finden und hinzuzufügen. Auf der Seite Verwalten können Sie auch neue Passwörter für diese ermittelten Arrays umbenennen, entfernen und bereitstellen.

Überlegungen bei der Array-Ermittlung

Damit das Plug-in Storage-Ressourcen anzeigen und verwalten kann, müssen Sie die Storage-Arrays ermitteln, die Sie im Netzwerk Ihres Unternehmens managen möchten. Sie können entweder ein oder mehrere Arrays ermitteln und dann hinzufügen.

Mehrere Storage-Arrays

Wenn Sie mehrere Arrays ermitteln möchten, geben Sie einen Netzwerk-IP-Adressbereich ein, und das System versucht dann individuelle Verbindungen zu jeder IP-Adresse in diesem Bereich. Jedes erfolgreich erreichte Storage Array wird im Plug-in angezeigt und Sie können sie dann Ihrer Management-Domäne hinzufügen.

Einzelnes Storage Array

Wenn Sie ein einzelnes Array ermitteln möchten, geben Sie die einzelne IP-Adresse für einen der Controller im Storage Array ein und fügen Sie anschließend dieses Array zur Management-Domäne hinzu.

> Das Plugin erkennt und zeigt nur die einzige IP-Adresse oder IP-Adresse innerhalb eines Bereichs an, der einem Controller zugewiesen ist. Wenn diesen Controllern alternative Controller oder IP-Adressen zugewiesen sind, die außerhalb dieser einzelnen IP-Adresse oder des IP-Adressbereichs liegen, werden sie durch das Plugin nicht ermittelt oder angezeigt. Sobald Sie jedoch das Speicher-Array hinzufügen, werden alle zugehörigen IP-Adressen ermittelt und in der Ansicht Verwalten angezeigt.

Benutzeranmeldeinformationen

Sie müssen für jedes Speicherarray, das Sie hinzufügen möchten, das Administratorkennwort angeben.

Zertifikate

Im Rahmen der Bestandsaufnahme überprüft das System, ob die erkannten Speicher-Arrays Zertifikate von einer vertrauenswürdigen Quelle verwenden. Das System verwendet zwei Arten von zertifikatbasierter Authentifizierung für alle Verbindungen, die es mit dem mit dem Browser herstellt:

- **Vertrauenswürdige Zertifikate** — möglicherweise müssen Sie zusätzliche vertrauenswürdige Zertifikate installieren, die von der Zertifizierungsstelle bereitgestellt werden, wenn ein oder beide Controller-Zertifikate abgelaufen, widerrufen oder ein Zertifikat in der Kette fehlt.
- **Selbstsignierte Zertifikate** — Arrays können auch selbstsignierte Zertifikate verwenden. Wenn Sie versuchen, Arrays zu entdecken, ohne signierte Zertifikate zu importieren, bietet das Plugin einen zusätzlichen Schritt, mit dem Sie das selbstsignierte Zertifikat akzeptieren können. Das selbstsignierte Zertifikat des Speicherarrays wird als vertrauenswürdig markiert und das Speicherarray wird dem Plugin hinzugefügt. Wenn Sie den Verbindungen zum Speicher-Array nicht vertrauen, wählen Sie **Abbrechen** und validieren Sie die Sicherheitszertifikatstrategie des Speicherarrays, bevor Sie das Speicher-Array zum Plugin hinzufügen.

Status des Storage-Arrays

Wenn Sie das Storage Plug-in für vCenter öffnen, wird die Kommunikation mit jedem Speicher-Array hergestellt und der Status jedes Speicher-Arrays wird angezeigt.

Auf der Seite **Verwalten - Alle** können Sie den Status des Speicherarrays und den Status der Speicherarray-Verbindung anzeigen.

Status	Zeigt An
Optimal	Das Storage-Array befindet sich in einem optimalen Zustand. Es gibt keine Zertifikatprobleme und das Passwort ist gültig.
Ungültiges Kennwort	Es wurde ein ungültiges Kennwort für das Speicher-Array angegeben.

Status	Zeigt An
Nicht Vertrauenswürdiges Zertifikat	Eine oder mehrere Verbindungen mit dem Speicher-Array sind nicht vertrauenswürdig, da das HTTPS-Zertifikat entweder selbst signiert ist und noch nicht importiert wurde, oder das Zertifikat eine CA-Signatur hat und die Stamm- und Intermediate-CA-Zertifikate nicht importiert wurden.
Erfordert Aufmerksamkeit	Es liegt ein Problem mit dem Speicher-Array vor, das Ihr Eingreifen erfordert, um es zu beheben.
Verriegeln	Das Storage-Array befindet sich in einem gesperrten Zustand.
Unbekannt	Das Speicher-Array wurde noch nie kontaktiert. Dies kann passieren, wenn das Plugin gestartet wird und noch keinen Kontakt zum Speicher-Array hergestellt hat oder das Speicher-Array offline ist und seit dem Start des Plugins nie kontaktiert wurde.
Offline	Das Plug-in hatte bereits zuvor Kontakt mit dem Storage-Array hergestellt, doch jetzt gingen sämtliche Verbindungen verloren.

Plug-in-Schnittstelle verglichen mit System Manager

Sie können Storage Plug-in für vCenter für grundlegende Betriebsaufgaben in Ihrem Speicher-Array verwenden. Es kann jedoch zu Zeiten kommen, in denen Sie System Manager starten müssen, um Aufgaben auszuführen, die im Plug-in nicht verfügbar sind.

System Manager ist eine eingebettete Anwendung auf dem Controller des Storage-Arrays, die über einen Ethernet-Management-Port mit dem Netzwerk verbunden ist. System Manager enthält alle Array-basierten Funktionen.

Die folgende Tabelle hilft Ihnen bei der Entscheidung, ob Sie die Plug-in-Schnittstelle oder die System Manager-Schnittstelle für eine bestimmte Aufgabe des Speicherarrays verwenden können.

Funktion	Plug-in-Schnittstelle	Benutzeroberfläche von System Manager
Batch-Operationen in Gruppen von mehreren Storage-Arrays	Ja.	Nein Operationen werden auf einem einzelnen Array durchgeführt.
Upgrades für die SANtricity OS Firmware	Ja. Ein oder mehrere Arrays im Batch-Betrieb	Ja. Nur Single Array.
Einstellungen von einem Array in mehrere Arrays importieren	Ja.	Nein
Host- und Host-Cluster-Management (Erstellung, Zuweisung von Volumes, Aktualisierung und Löschen)	Ja.	Ja.

Funktion	Plug-in-Schnittstelle	Benutzeroberfläche von System Manager
Pools und Volume-Gruppen-Management (Erstellung, Aktualisierung, Aktivierung und Löschen)	Ja.	Ja.
Volume-Management (Erstellen, Skalieren, Aktualisieren und Löschen)	Ja.	Ja.
SSD Cache-Management (Erstellen, Aktualisieren und Löschen)	Ja.	Ja.
Spiegelung und Snapshot Management	Nein	Ja.
Hardware-Management (Controller-Status anzeigen, Port-Verbindungen konfigurieren, Controller offline schalten, Hot Spares aktivieren, Laufwerke löschen, Usw.)	Nein	Ja.
Management von Warnmeldungen (E-Mail, SNMP und Syslog)	Nein	Ja.
Sicherheitsschlüsselmanagement	Nein	Ja.
Zertifikatsmanagement für Controller	Nein	Ja.
Zugriffsmanagement für Controller (LDAP, SAML usw.)	Nein	Ja.
AutoSupport Management	Nein	Ja.

Ermitteln Sie Speicher-Arrays im SANtricity Speicher-Plug-in für vCenter

Um Speicherressourcen im Storage Plug-in für vCenter anzuzeigen und zu verwalten, müssen Sie die IP-Adressen von Arrays in Ihrem Netzwerk ermitteln.

Bevor Sie beginnen

- Sie müssen die Netzwerk-IP-Adressen (oder den Adressbereich) der Array-Controller kennen.
- Die Speicher-Arrays müssen ordnungsgemäß eingerichtet und konfiguriert sein.
- Passwörter für das Storage-Array müssen mithilfe der Kachel „System Manager Access Management“ eingerichtet werden.

Über diese Aufgabe

Die Array-Erkennung ist ein mehrstufiges Verfahren:

- Schritt 1: Geben Sie Netzwerkadressen für die Ermittlung ein
- Schritt 2: Lösen Sie nicht vertrauenswürdige Zertifikate während der Ermittlung

- Schritt 3: Geben Sie Passwörter ein

Schritt 1: Geben Sie Netzwerkadressen für die Ermittlung ein

Als erster Schritt zur Ermittlung von Speicherarrays geben Sie eine einzelne IP-Adresse oder eine Reihe von IP-Adressen ein, um im lokalen Teilnetzwerk zu suchen. Die Funktion Hinzufügen/Entdecken öffnet einen Assistenten, der Sie durch den Erkennungsprozess führt.

Schritte

1. Wählen Sie auf der Seite **Verwalten** die Option **Hinzufügen/Entdecken**.

   Das Dialogfeld Netzwerkadressbereich eingeben wird angezeigt.

2. Führen Sie einen der folgenden Schritte aus:
   - Um ein Array zu ermitteln, wählen Sie die Optionsschaltfläche **Entdecken eines einzelnen Speicherarrays** aus und geben dann die IP-Adresse für einen der Controller im Speicher-Array ein.
   - Um mehrere Speicher-Arrays zu entdecken, wählen Sie die Optionsschaltfläche **Alle Speicher-Arrays in einem Netzwerkbereich** aus. Geben Sie dann die Startnetzwerkadresse und die Netzwerkadresse ein, um das lokale Subnetzwerk zu durchsuchen.
3. Klicken Sie Auf **Erkennung Starten**.

   Beim Beginn des Erkennungsvorgangs werden die Speicher-Arrays im Dialogfeld angezeigt, wenn sie erkannt werden. Der Erkennungsvorgang kann mehrere Minuten dauern.

   > Wenn keine verwaltbaren Arrays erkannt werden, überprüfen Sie, ob die Speicher-Arrays ordnungsgemäß mit Ihrem Netzwerk verbunden sind und die zugewiesenen Adressen innerhalb der Reichweite liegen. Klicken Sie auf **Neue Ermittlungsparameter**, um zur Seite Hinzufügen/Entdecken zurückzukehren.

4. Aktivieren Sie das Kontrollkästchen neben einem beliebigen Speicher-Array, das Sie Ihrer Management-Domäne hinzufügen möchten.

   Das System führt eine Anmeldeinformationen für jedes Array aus, das Sie der Management-Domäne hinzufügen. Möglicherweise müssen Sie Probleme mit nicht vertrauenswürdigen Zertifikaten beheben, bevor Sie fortfahren.

5. Klicken Sie auf **Weiter**, um mit dem nächsten Schritt im Assistenten fortzufahren.
6. Wenn die Speicher-Arrays über gültige Zertifikate verfügen, gehen Sie zu Schritt 3: Geben Sie Passwörter ein. Wenn keine Speicherarrays über gültige Zertifikate verfügen, wird das Dialogfeld Selbstsignierte Zertifikate auflösen angezeigt. Gehen Sie zu Schritt 2: Lösen Sie nicht vertrauenswürdige Zertifikate während der Ermittlung. Wenn Sie CA-signierte Zertifikate importieren möchten, löschen Sie die Ermittlungsdialoge und gehen Sie zu "Importieren Sie Zertifikate für Arrays".

Schritt 2: Lösen Sie nicht vertrauenswürdige Zertifikate während der Ermittlung

Falls erforderlich, müssen Sie Zertifikatprobleme beheben, bevor Sie mit dem Erkennungsvorgang fortfahren.

Wenn während der Erkennung Speicherarrays den Status „nicht vertrauenswürdige Zertifikate“ aufweisen, wird das Dialogfeld Selbstsignierte Zertifikate auflösen angezeigt. In diesem Dialogfeld können Sie nicht vertrauenswürdige Zertifikate auflösen oder CA-Zertifikate importieren (siehe "Importieren Sie Zertifikate für Arrays").

Schritte

1. Wenn das Dialogfeld selbst signierte Zertifikate auflösen geöffnet wird, überprüfen Sie die Informationen, die für die nicht vertrauenswürdigen Zertifikate angezeigt werden. Für weitere Informationen können Sie auch auf die Ellipsen am äußersten Ende der Tabelle klicken und im Kontextmenü **Ansicht** wählen.
2. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie den Verbindungen zu den erkannten Speicherarrays vertrauen, klicken Sie auf **Weiter** und klicken Sie dann auf **Ja**, um die nächste Karte im Assistenten zu bestätigen. Die selbstsignierten Zertifikate werden als vertrauenswürdig gekennzeichnet und die Speicher-Arrays werden dem Plugin hinzugefügt.
   - Wenn Sie den Verbindungen zu den Speicher-Arrays nicht vertrauen, wählen Sie **Abbrechen** und validieren Sie die Sicherheitszertifikatstrategie jedes Speicherarrays, bevor Sie eine dieser Verbindungen zum Plugin hinzufügen.

Schritt 3: Geben Sie Passwörter ein

Als letzter Schritt zur Ermittlung müssen Sie die Passwörter für die Speicherarrays eingeben, die Sie Ihrer Management-Domäne hinzufügen möchten.

Schritte

1. Wenn Sie bereits Gruppen für die Arrays konfiguriert haben, können Sie mit dem Dropdown-Menü eine Gruppe für die ermittelten Arrays auswählen.
2. Geben Sie für jedes erkannte Array sein Administratorkennwort in die Felder ein.
3. Klicken Sie Auf **Fertig Stellen**.

> Es kann mehrere Minuten dauern, bis das System eine Verbindung zu den angegebenen Speicherarrays herstellt.

Ergebnis

Die Speicher-Arrays werden Ihrer Management-Domäne hinzugefügt und der ausgewählten Gruppe zugeordnet (falls angegeben).

> Sie können die Option Start verwenden, um den Browser-basierten System Manager für ein oder mehrere Speicher-Arrays zu öffnen, wenn Sie Managementvorgänge ausführen möchten.

Benennen Sie ein Speicher-Array im SANtricity Speicher-Plug-in für vCenter um

Sie können den Namen des Speicher-Arrays ändern, der auf der Seite Verwalten des Speicher-Plug-ins für vCenter angezeigt wird.

Schritte

1. Aktivieren Sie auf der Seite **Verwalten** das Kontrollkästchen links neben dem Namen des Speicherarrays.
2. Wählen Sie die Ellipsen ganz rechts in der Zeile aus, und wählen Sie dann im Popup-Menü die Option **Speicher-Array umbenennen** aus.
3. Geben Sie den neuen Namen ein und klicken Sie auf **Speichern**.

Ändern Sie die Passwörter für Speicher-Arrays im SANtricity Speicher-Plug-in für vCenter

Sie können die Passwörter aktualisieren, die für die Anzeige und den Zugriff auf Speicher-Arrays im Storage Plug-in für vCenter verwendet werden.

Bevor Sie beginnen

Sie müssen das aktuelle Passwort für das Speicher-Array kennen, das in System Manager festgelegt ist.

Über diese Aufgabe

In dieser Aufgabe geben Sie das aktuelle Passwort für ein Speicher-Array ein, damit Sie im Plugin darauf zugreifen können. Dies kann erforderlich sein, wenn das Array-Passwort in System Manager geändert wurde.

Schritte

1. Wählen Sie auf der Seite **Verwalten** ein oder mehrere Speicher-Arrays aus.
2. Menü wählen:Sonstige Aufgaben[Passwörter für Speicherarrays angeben].
3. Geben Sie für jedes Speicherarray das Kennwort oder die Passwörter ein, und klicken Sie dann auf **Speichern**.

Entfernen Sie Speicher-Arrays im SANtricity Speicher-Plug-in für vCenter

Sie können ein oder mehrere Storage Arrays entfernen, wenn Sie es nicht mehr aus dem Storage Plugin für vCenter managen möchten.

Über diese Aufgabe

Sie können nicht auf die von Ihnen entfernenden Speicher-Arrays zugreifen. Sie können jedoch eine Verbindung zu einem der entfernten Speicher-Arrays herstellen, indem Sie einen Browser direkt auf seine IP-Adresse oder den Host-Namen zeigen.

Das Entfernen eines Speicher-Arrays hat keinerlei Auswirkungen auf das Speicher-Array oder seine Daten. Wenn ein Speicher-Array versehentlich entfernt wird, kann es erneut hinzugefügt werden.

Schritte

1. Wählen Sie auf der Seite **Verwalten** ein oder mehrere Speicher-Arrays aus, die Sie entfernen möchten.
2. Menü wählen:Sonstige Aufgaben[Speicher-Arrays entfernen].

   Das Speicher-Array wird aus allen Ansichten in der Plugin-Schnittstelle entfernt.

Starten Sie System Manager über das SANtricity Storage Plug-in für vCenter

Verwenden Sie zum Verwalten eines einzelnen Arrays die Option Starten, um SANtricity System Manager in einem neuen Browser-Fenster zu öffnen.

System Manager ist eine eingebettete Anwendung auf dem Controller des Storage-Arrays, die über einen Ethernet-Management-Port mit dem Netzwerk verbunden ist. System Manager enthält alle Array-basierten Funktionen. Um auf System Manager zugreifen zu können, müssen Sie über eine Out-of-Band-Verbindung mit einem Netzwerkverwaltungs-Client mit einem Webbrowser verfügen.

Schritte

1. Wählen Sie auf der Seite **Verwalten** ein oder mehrere Speicherarrays aus, die Sie verwalten möchten.
2. Klicken Sie Auf **Start**.

   Das System öffnet im Browser eine neue Registerkarte und zeigt dann die Anmeldeseite von System Manager an.

3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie dann auf **Anmelden**.

Einstellungen importieren

Erfahren Sie mehr über die Funktion „Importeinstellungen“ im SANtricity Storage Plugin für vCenter

Die Funktion „Importeinstellungen“ ist ein Batch-Vorgang, mit dem Sie die Einstellungen in einem einzelnen Speicher-Array (der Quelle) auf mehrere Arrays (die Ziele) im Storage Plug-in für vCenter replizieren können.

Für den Import verfügbare Einstellungen

Die folgenden Konfigurationen können von einem Array in ein anderes importiert werden:

- **Alerts** — Alerting-Methoden, um wichtige Ereignisse mithilfe von E-Mail, Syslog-Server oder SNMP-Server an Administratoren zu senden.
- **AutoSupport** — Eine Funktion, die den Zustand eines Speicherarrays überwacht und automatische Entsendungen an den technischen Support sendet.
- **Directory Services** — eine Methode der Benutzerauthentifizierung, die über einen LDAP-Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst, wie Microsoft Active Directory verwaltet wird.
- **Systemeinstellungen** — Konfigurationen in Bezug auf folgende Komponenten:
  - Medien-Scan-Einstellungen für ein Volume
  - SSD-Einstellungen
  - Automatischer Lastausgleich (ohne Berichterstellung für Hostkonnektivität)
- **Speicherkonfiguration** — Konfigurationen im Zusammenhang mit folgenden:
  - Volumes (nur Thick Volumes und nicht Repository Volumes)
  - Volume-Gruppen und -Pools
  - Zuweisung von Hot-Spare-Laufwerken

Konfigurationsworkflow

So importieren Sie Einstellungen:

1. Konfigurieren Sie die Einstellungen in einem Speicher-Array, das als Quelle verwendet werden soll, mit System Manager.
2. Sichern Sie auf den Storage Arrays, die als Ziele verwendet werden sollen, ihre Konfiguration mit System Manager.
3. Gehen Sie von der Plugin-Schnittstelle zur Seite **Verwalten** und importieren Sie die Einstellungen.
4. Überprüfen Sie auf der Seite „Vorgänge“ die Ergebnisse des Vorgangs „Importeinstellungen“.

Anforderungen für die Replizierung von Storage-Konfigurationen

Bevor Sie eine Speicherkonfiguration von einem Speicher-Array in ein anderes importieren, überprüfen Sie die Anforderungen und Richtlinien.

Shelfs

- Die Shelfs, in denen sich die Controller befinden, müssen auf den Quell- und Ziel-Arrays identisch sein.

- Shelf IDs müssen auf den Quell- und Ziel-Arrays identisch sein.
- Erweiterungs-Shelfs müssen in denselben Steckplätzen mit denselben Laufwerktypen bestückt werden (wenn das Laufwerk in der Konfiguration verwendet wird, ist die Position nicht verwendeter Laufwerke unwichtig).

Controller

- Der Controllertyp kann zwischen Quell- und Ziel-Arrays unterschiedlich sein, aber der RBOD-Gehäusetyp muss identisch sein.
- Die HICs, einschließlich der da-Fähigkeiten des Hosts, müssen identisch sein zwischen den Quell- und Ziel-Arrays.
- Der Import von einer Duplex-Konfiguration in eine Simplex-Konfiguration wird nicht unterstützt. Der Import von Simplex in Duplex ist jedoch zulässig.
- FDE-Einstellungen sind beim Importvorgang nicht enthalten.

Status

- Die Ziel-Arrays müssen den optimalen Status haben.
- Das Quell-Array muss nicht im optimalen Status sein.

Storage

- Die Laufwerkskapazität kann zwischen den Quell- und Ziel-Arrays variieren, solange die Volume-Kapazität auf dem Ziel größer ist als die Quelle. (In einem Ziel-Array sind unter Umständen neuere Laufwerke mit höherer Kapazität enthalten, die durch den Replizierungsvorgang nicht vollständig in Volumes konfiguriert wären.)
- Laufwerk-Pool-Volumes mit einer Größe von mindestens 64 TB auf dem Quell-Array verhindern den Importvorgang auf den Zielen.

Importieren Sie Warnmeldungseinstellungen in das SANtricity-Speicher-Plug-in für vCenter

Sie können Alarmkonfigurationen von einem Speicher-Array in andere Speicher-Arrays importieren. Dieser Batch-Betrieb spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Bevor Sie beginnen

Stellen Sie sicher, dass:

- Warnmeldungen werden in System Manager (Menü:Einstellungen[Warnungen]) für das Speicherarray konfiguriert, das als Quelle verwendet werden soll.
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).
- Sie haben die Anforderungen für die Replizierung von Speicherkonfigurationen in überprüft "Überblick über die Einstellungen importieren".

Über diese Aufgabe

Sie können E-Mail-, SNMP- oder Syslog-Warnungen für den Importvorgang auswählen:

- **E-Mail-Benachrichtigungen** — Eine E-Mail-Server-Adresse und die E-Mail-Adressen der Alarmempfänger.

- **Syslog Alerts** — Eine Syslog-Serveradresse und ein UDP-Port.
- **SNMP Alerts** — Ein Community-Name und IP-Adresse für den SNMP-Server.

Schritte

1. Klicken Sie auf der Seite Verwalten auf Menü:Aktionen[Einstellungen importieren].

   Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen entweder **E-Mail-Alarme**, **SNMP-Alarme** oder **Syslog-Warnungen** aus und klicken Sie dann auf **Weiter**.

   Zum Auswählen des Quell-Arrays wird ein Dialogfeld geöffnet.

3. Wählen Sie im Dialogfeld Quelle auswählen das Array mit den zu importierenden Einstellungen aus, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld Ziele auswählen ein oder mehrere Arrays aus, um die neuen Einstellungen zu erhalten.

   Speicher-Arrays mit Firmware unter 8.50 stehen nicht zur Auswahl. Darüber hinaus wird in diesem Dialogfeld kein Array angezeigt, wenn das Plug-in nicht mit diesem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es Probleme mit Zertifikat, Kennwort oder Netzwerk hat).

5. Klicken Sie Auf **Fertig Stellen**.

   Auf der Seite Operationen werden die Ergebnisse des Importvorgangs angezeigt. Wenn der Vorgang fehlschlägt, können Sie auf die Zeile klicken, um weitere Informationen anzuzeigen.

Ergebnis

Die Ziel-Storage-Arrays sind jetzt so konfiguriert, dass sie Warnmeldungen per E-Mail, SNMP oder Syslog an Administratoren senden.

Importieren Sie die AutoSupport-Einstellungen in das SANtricity Speicher-Plug-in für vCenter

Sie können eine AutoSupport-Konfiguration von einem Speicher-Array in andere Speicher-Arrays importieren. Dieser Batch-Betrieb spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Bevor Sie beginnen

Stellen Sie sicher, dass:

- AutoSupport ist in System Manager (Menü:Support[Support Center]) für das Speicherarray konfiguriert, das als Quelle verwendet werden soll.
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).
- Sie haben die Anforderungen für die Replizierung von Speicherkonfigurationen in überprüft "Überblick über die Einstellungen importieren".

Über diese Aufgabe

Zu den importierten Einstellungen gehören die separaten Funktionen (Basic AutoSupport, AutoSupport

OnDemand und Remote Diagnostics), das Wartungsfenster, die Bereitstellungsmethode, Und dem Versandplan.

Schritte

1. Klicken Sie auf der Seite Verwalten auf Menü:Aktionen[Einstellungen importieren].

   Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen **AutoSupport** aus und klicken Sie dann auf **Weiter**.

   Zum Auswählen des Quell-Arrays wird ein Dialogfeld geöffnet.

3. Wählen Sie im Dialogfeld Quelle auswählen das Array mit den zu importierenden Einstellungen aus, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld Ziele auswählen ein oder mehrere Arrays aus, um die neuen Einstellungen zu erhalten.

   Speicher-Arrays mit Firmware unter 8.50 stehen nicht zur Auswahl. Darüber hinaus wird in diesem Dialogfeld kein Array angezeigt, wenn das Plug-in nicht mit diesem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es Probleme mit Zertifikat, Kennwort oder Netzwerk hat).

5. Klicken Sie Auf **Fertig Stellen**.

   Auf der Seite Operationen werden die Ergebnisse des Importvorgangs angezeigt. Wenn der Vorgang fehlschlägt, können Sie auf die Zeile klicken, um weitere Informationen anzuzeigen.

Ergebnis

Die Ziel-Storage-Arrays sind nun mit denselben AutoSupport-Einstellungen wie das Quell-Array konfiguriert.

Importieren Sie die Einstellungen für Verzeichnisdienste im SANtricity-Speichermodul für vCenter

Sie können eine Konfiguration für Verzeichnisdienste von einem Speicher-Array in andere Speicher-Arrays importieren. Dieser Batch-Betrieb spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Bevor Sie beginnen

Stellen Sie sicher, dass:

- Verzeichnisdienste werden in System Manager (Menü:Einstellungen[Zugriffsverwaltung]) für das Speicherarray konfiguriert, das als Quelle verwendet werden soll.
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).
- Sie haben die Anforderungen für die Replizierung von Speicherkonfigurationen in überprüft "Überblick über die Einstellungen importieren".

Über diese Aufgabe

Zu den importierten Einstellungen gehören der Domänenname und die URL eines LDAP-Servers (Lightweight Directory Access Protocol) sowie die Zuordnungen der Benutzergruppen des LDAP-Servers zu den vordefinierten Rollen des Speicher-Arrays.

Schritte

1. Klicken Sie auf der Seite Verwalten auf Menü:Aktionen[Einstellungen importieren].

   Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen die Option **Verzeichnisdienste** aus und klicken Sie dann auf **Weiter**.

   Zum Auswählen des Quell-Arrays wird ein Dialogfeld geöffnet.

3. Wählen Sie im Dialogfeld Quelle auswählen das Array mit den zu importierenden Einstellungen aus, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld Ziele auswählen ein oder mehrere Arrays aus, um die neuen Einstellungen zu erhalten.

   Speicher-Arrays mit Firmware unter 8.50 stehen nicht zur Auswahl. Darüber hinaus wird in diesem Dialogfeld kein Array angezeigt, wenn das Plug-in nicht mit diesem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es Probleme mit Zertifikat, Kennwort oder Netzwerk hat).

5. Klicken Sie Auf **Fertig Stellen**.

   Auf der Seite Operationen werden die Ergebnisse des Importvorgangs angezeigt. Wenn der Vorgang fehlschlägt, können Sie auf die Zeile klicken, um weitere Informationen anzuzeigen.

Ergebnis

Die Ziel-Storage-Arrays sind nun mit denselben Verzeichnisdiensten konfiguriert wie das Quell-Array.

Importieren Sie Systemeinstellungen in das SANtricity-Speichermodul für vCenter

Sie können die Systemeinstellungen von einem Speicher-Array in andere Speicher-Arrays importieren. Dieser Batch-Betrieb spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Bevor Sie beginnen

Stellen Sie sicher, dass:

- Systemeinstellungen sind in System Manager für das Speicherarray konfiguriert, das als Quelle verwendet werden soll.
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).
- Sie haben die Anforderungen für die Replizierung von Speicherkonfigurationen in überprüft "Überblick über die Einstellungen importieren".

Über diese Aufgabe

Importierte Einstellungen umfassen Medien-Scan-Einstellungen für ein Volume, SSD-Einstellungen für Controller und automatischen Lastausgleich (ohne Berichterstellung für Host-Konnektivität).

Schritte

1. Klicken Sie auf der Seite Verwalten auf Menü:Aktionen[Einstellungen importieren].

Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen die Option **System** aus und klicken Sie dann auf **Weiter**.

   Zum Auswählen des Quell-Arrays wird ein Dialogfeld geöffnet.

3. Wählen Sie im Dialogfeld Quelle auswählen das Array mit den zu importierenden Einstellungen aus, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld Ziele auswählen ein oder mehrere Arrays aus, um die neuen Einstellungen zu erhalten.

   Speicher-Arrays mit Firmware unter 8.50 stehen nicht zur Auswahl. Darüber hinaus wird in diesem Dialogfeld kein Array angezeigt, wenn das Plug-in nicht mit diesem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es Probleme mit Zertifikat, Kennwort oder Netzwerk hat).

5. Klicken Sie Auf **Fertig Stellen**.

   Auf der Seite Operationen werden die Ergebnisse des Importvorgangs angezeigt. Wenn der Vorgang fehlschlägt, können Sie auf die Zeile klicken, um weitere Informationen anzuzeigen.

Ergebnis

Die Ziel-Storage-Arrays sind nun mit denselben Systemeinstellungen wie das Quell-Array konfiguriert.

Importieren Sie die Speicherkonfigurationseinstellungen im SANtricity Speicher-Plug-in für vCenter

Sie können die Speicherkonfiguration von einem Speicher-Array in andere Speicher-Arrays importieren. Dieser Batch-Betrieb spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Bevor Sie beginnen

Stellen Sie sicher, dass:

- Storage ist in System Manager für das Storage-Array konfiguriert, das Sie als Quelle verwenden möchten.
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).
- Sie haben die Anforderungen für die Replizierung von Speicherkonfigurationen in überprüft "Überblick über die Einstellungen importieren".
- Quell- und Ziel-Arrays müssen die folgenden Anforderungen erfüllen:
  - Die Shelfs, in denen sich die Controller befinden, müssen identisch sein.
  - Shelf-IDs müssen identisch sein.
  - Erweiterungs-Shelfs müssen in denselben Steckplätzen mit denselben Laufwerkstypen bestückt werden.
  - Der Typ des RBOD-Gehäuses muss identisch sein.
  - Die HICs, einschließlich der Data Assurance-Funktionen des Hosts, müssen identisch sein.
  - Die Ziel-Arrays müssen den optimalen Status haben.

- Die Volume-Kapazität auf dem Ziel-Array ist größer als die Kapazität des Quell-Arrays.

- Sie verstehen die folgenden Einschränkungen:
  - Der Import von einer Duplex-Konfiguration in eine Simplex-Konfiguration wird nicht unterstützt. Der Import von Simplex in Duplex ist jedoch zulässig.
  - Laufwerk-Pool-Volumes mit einer Größe von mindestens 64 TB auf dem Quell-Array verhindern den Importvorgang auf den Zielen.

Über diese Aufgabe

Zu den importierten Einstellungen gehören konfigurierte Volumes (nur Thick- und nicht-Repository-Volumes), Volume-Gruppen, Pools und Hot-Spare-Laufwerkszuordnungen.

Schritte

1. Klicken Sie auf der Seite Verwalten auf Menü:Aktionen[Einstellungen importieren].

   Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen die Option **Speicherkonfiguration** aus und klicken Sie dann auf **Weiter**.

   Zum Auswählen des Quell-Arrays wird ein Dialogfeld geöffnet.

3. Wählen Sie im Dialogfeld Quelle auswählen das Array mit den zu importierenden Einstellungen aus, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Dialogfeld Ziele auswählen ein oder mehrere Arrays aus, um die neuen Einstellungen zu erhalten.

   > Speicher-Arrays mit Firmware unter 8.50 stehen nicht zur Auswahl. Darüber hinaus wird in diesem Dialogfeld kein Array angezeigt, wenn das Plug-in nicht mit diesem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es Probleme mit Zertifikat, Kennwort oder Netzwerk hat).

5. Klicken Sie Auf **Fertig Stellen**.

   Auf der Seite Operationen werden die Ergebnisse des Importvorgangs angezeigt. Wenn der Vorgang fehlschlägt, können Sie auf die Zeile klicken, um weitere Informationen anzuzeigen.

Ergebnis

Die Ziel-Storage-Arrays sind nun mit derselben Storage-Konfiguration wie das Quell-Array konfiguriert.

Managen von Array-Gruppen

Erfahren Sie mehr über das Management von Array-Gruppen im SANtricity Storage Plug-in für vCenter

Sie können Ihre physische und virtualisierte Infrastruktur im Storage Plug-in für vCenter managen, indem Sie eine Reihe von Storage-Arrays gruppieren. Möglicherweise möchten Sie Storage-Arrays gruppieren, um die Ausführung von Überwachungs- oder Reporting-Aufgaben zu erleichtern.

Arten von Speicher-Array-Gruppen:

- **Alle Gruppe** — die All-Gruppe ist die Standardgruppe und umfasst alle Speicher-Arrays, die in Ihrem Unternehmen entdeckt wurden. Auf die Gruppe Alle kann über die Hauptansicht zugegriffen werden.
- **Vom Benutzer erstellte Gruppe** — Eine vom Benutzer erstellte Gruppe enthält die Speicherarrays, die Sie manuell auswählen, um diese Gruppe hinzuzufügen. Auf von Benutzern erstellte Gruppen kann über die Hauptansicht zugegriffen werden.

Erstellen Sie eine Speicher-Array-Gruppe im SANtricity Speicher-Plug-in für vCenter

Sie erstellen Speichergruppen und fügen dann Speicher-Arrays zu den Gruppen hinzu. Die Speichergruppe definiert, welche Laufwerke den Speicher bereitstellen, aus dem das Volume besteht.

Schritte

1. Wählen Sie auf der Seite Verwalten die Option MENU:Gruppen verwalten[Speicherarray-Gruppe erstellen].
2. Geben Sie im Feld **Name** einen Namen für die neue Gruppe ein.
3. Wählen Sie die Speicher-Arrays aus, die Sie der neuen Gruppe hinzufügen möchten.
4. Klicken Sie Auf **Erstellen**.

Fügen Sie Speicher-Array zur Gruppe im SANtricity Speicher-Plugin für vCenter hinzu

Sie können einer vom Benutzer erstellten Gruppe einen oder mehrere Speicher-Arrays hinzufügen.

Schritte

1. Wählen Sie in der Hauptansicht **Verwalten** aus, und wählen Sie dann die Gruppe aus, der Sie Speicher-Arrays hinzufügen möchten.
2. Wählen Sie Menü:Gruppen verwalten[Speicher-Arrays zu Gruppe hinzufügen].
3. Wählen Sie die Speicher-Arrays aus, die Sie der Gruppe hinzufügen möchten.
4. Klicken Sie Auf **Hinzufügen**.

Benennen Sie eine Speicher-Array-Gruppe im SANtricity Speicher-Plug-in für vCenter um

Sie können den Namen einer Speicherarraygruppe ändern, wenn der aktuelle Name nicht mehr aussagekräftig oder zutreffend ist.

Über diese Aufgabe

Berücksichtigen Sie diese Richtlinien bitte.

- Ein Name kann aus Buchstaben, Zahlen und den Sonderzeichen Unterstrich (_), Bindestrich (-) und Pfund (#) bestehen. Wenn Sie andere Zeichen auswählen, wird eine Fehlermeldung angezeigt. Sie werden aufgefordert, einen anderen Namen auszuwählen.
- Beschränken Sie den Namen auf 30 Zeichen. Alle führenden und nachgestellten Leerzeichen im Namen werden gelöscht.
- Verwenden Sie einen eindeutigen, aussagekräftigen Namen, der leicht zu verstehen und zu merken ist.
- Vermeiden Sie beliebige Namen oder Namen, die in Zukunft schnell ihre Bedeutung verlieren würden.

Schritte

1. Wählen Sie in der Hauptansicht **Verwalten** aus, und wählen Sie dann die Speicherarray-Gruppe aus, die Sie umbenennen möchten.
2. Wählen Sie Menü:Gruppen verwalten[Speicherarray-Gruppe umbenennen].
3. Geben Sie im Feld **Gruppenname** einen neuen Namen für die Gruppe ein.
4. Klicken Sie Auf **Umbenennen**.

Entfernen Sie Speicher-Arrays aus einer Gruppe im SANtricity Speicher-Plug-in für vCenter

Sie können ein oder mehrere verwaltete Speicher-Arrays aus einer Gruppe entfernen, wenn Sie sie nicht mehr aus einer bestimmten Speichergruppe verwalten möchten.

Über diese Aufgabe

Das Entfernen von Speicher-Arrays aus einer Gruppe hat keinerlei Auswirkungen auf das Speicher-Array oder seine Daten. Wenn das Storage Array von System Manager gemanagt wird, können Sie es weiterhin mit Ihrem Browser verwalten. Wenn ein Speicher-Array versehentlich aus einer Gruppe entfernt wird, kann es erneut hinzugefügt werden.

Schritte

1. Wählen Sie auf der Seite Verwalten die Option MENU:Gruppen verwalten[Speicher-Arrays aus Gruppe entfernen].
2. Wählen Sie im Dropdown-Menü die Gruppe aus, die die zu entfernenden Speicher-Arrays enthält, und klicken Sie dann auf das Kontrollkästchen neben jedem Speicher-Array, das Sie aus der Gruppe entfernen möchten.
3. Klicken Sie Auf **Entfernen**.

Löschen Sie eine Speicher-Array-Gruppe im SANtricity Speicher-Plug-in für vCenter

Sie können eine oder mehrere Speicherarraygruppen entfernen, die nicht mehr benötigt werden.

Über diese Aufgabe

Bei diesem Vorgang wird nur die Speicherarraygruppe gelöscht. Die der gelöschten Gruppe zugeordneten Speicher-Arrays bleiben über die Ansicht Alle verwalten oder eine andere Gruppe, der sie zugeordnet ist, zugänglich.

Schritte

1. Wählen Sie auf der Seite Verwalten die Option MENU:Gruppen verwalten[Speicherarray-Gruppe löschen].
2. Wählen Sie eine oder mehrere Speicherarray-Gruppen aus, die Sie löschen möchten.
3. Klicken Sie Auf **Löschen**.

Aktualisieren der Betriebssystemsoftware

Erfahren Sie mehr über das Management von SANtricity Software-Upgrades mit dem Storage Plug-in für vCenter

Im Storage Plug-in für vCenter können Sie SANtricity Software und NVSRAM Upgrades für mehrere Storage Arrays desselben Typs managen.

Workflow-Upgrade

Die folgenden Schritte bieten einen grundlegenden Workflow zur Durchführung von Software-Upgrades:

1. Sie laden die neueste SANtricity OS-Datei von der Support-Website herunter. (Ein Link ist auf der Support-Seite verfügbar) Speichern Sie die Datei auf dem Management-Host-System (dem Host, auf den Sie in einem Browser auf das Plugin zugreifen), und entpacken Sie die Datei.
2. Im Plugin können Sie die SANtricity OS-Softwaredatei und die NVSRAM-Datei in das Repository laden (ein Bereich des Servers, auf dem Dateien gespeichert sind).
3. Nachdem die Dateien in das Repository geladen wurden, können Sie die Datei auswählen, die für das Upgrade verwendet werden soll. Wählen Sie auf der Seite Upgrade SANtricity OS Software die Betriebssystemsoftware und die NVSRAM-Datei aus. Nach Auswahl einer Softwaredatei wird auf dieser Seite eine Liste kompatibler Speicher-Arrays angezeigt. Anschließend wählen Sie die Speicher-Arrays aus, die Sie mit der neuen Software aktualisieren möchten. (Sie können nicht inkompatible Arrays auswählen.)
4. Anschließend können Sie eine sofortige Softwareübertragung und -Aktivierung starten oder die Dateien zu einem späteren Zeitpunkt für die Aktivierung aktivieren. Während des Upgrade-Vorgangs führt das Plugin die folgenden Aufgaben aus:
   - Durchführung einer Integritätsprüfung für die Speicher-Arrays, um festzustellen, ob Bedingungen vorhanden sind, die das Upgrade möglicherweise verhindern. Wenn Arrays die Integritätsprüfung nicht bestanden haben, können Sie das jeweilige Array überspringen und das Upgrade für die anderen fortsetzen. Alternativ können Sie den gesamten Prozess beenden und die Arrays, die nicht bestanden haben, beheben.
   - Überträgt die Upgrade-Dateien an jeden Controller.
   - Bootet die Controller neu und aktiviert das neue Betriebssystem, jeweils ein Controller. Während der Aktivierung wird die vorhandene Betriebssystemdatei durch die neue Datei ersetzt.

Sie können auch angeben, dass die Software zu einem späteren Zeitpunkt aktiviert wird.

Upgrade-Überlegungen

Vor dem Upgrade mehrerer Storage-Arrays sollten Sie die wichtigsten Überlegungen in Ihrer Planung durchgehen.

Aktuelle Versionen

Sie können die aktuellen Softwareversionen des SANtricity OS von der Seite Verwalten des Storage Plug-ins für vCenter für jedes erkannte Storage-Array anzeigen. Die Version wird in der Spalte SANtricity OS Software angezeigt. Die Informationen zu Controller-Firmware und NVSRAM finden Sie in einem Popup-Dialogfeld, wenn Sie in jeder Zeile auf die Betriebssystemversion klicken.

Andere Komponenten müssen aktualisiert werden

Im Rahmen des Upgrades müssen Sie eventuell auch den Multipath-/Failover-Treiber oder den HBA-Treiber des Hosts aktualisieren, damit der Host korrekt mit den Controllern interagieren kann. Informationen zur Kompatibilität finden Sie im "Interoperabilitäts-Matrix-Tool".

Dual-Controller

Wenn ein Storage-Array zwei Controller enthält und ein Multipath-Treiber installiert ist, kann das Storage-Array die I/O-Verarbeitung während des Upgrades fortsetzen. Während des Upgrades erfolgt der folgende Vorgang:

1. Controller A Failover aller LUNs zu Controller B
2. Das Upgrade erfolgt bei Controller A
3. Controller A nimmt seine LUNs und alle Controller B LUNs wieder auf.
4. Upgrade erfolgt auf Controller B.

Nach Abschluss des Upgrades müssen Sie Volumes möglicherweise manuell zwischen den Controllern neu verteilen, um sicherzustellen, dass die Volumes wieder zum korrekten Controller zurückkehren.

Führen Sie eine Integritätsprüfung vor dem Upgrade im SANtricity-Speichermodul für vCenter durch

Eine Zustandsprüfung wird im Rahmen des Upgrade-Prozesses ausgeführt, doch vor Beginn kann zusätzlich ein Systemcheck separat durchgeführt werden. Bei der Integritätsprüfung werden Komponenten des Storage-Arrays bewertet, um sicherzustellen, dass das Upgrade fortgesetzt werden kann.

Schritte

1. Wählen Sie in der Hauptansicht **Verwalten** und dann Menü:Upgrade Center[Health Check Pre-Upgrade].

   Das Dialogfeld Integritätsprüfung vor dem Upgrade wird geöffnet und zeigt alle erkannten Speichersysteme an.

2. Filtern oder sortieren Sie bei Bedarf die Speichersysteme in der Liste, sodass Sie alle Systeme, die sich derzeit nicht im optimalen Zustand befinden, anzeigen können.
3. Aktivieren Sie die Kontrollkästchen für die Speichersysteme, die Sie durch die Integritätsprüfung ausführen möchten.
4. Klicken Sie Auf **Start**.

   Der Fortschritt wird im Dialogfeld angezeigt, während die Integritätsprüfung durchgeführt wird.

5. Wenn die Integritätsprüfung abgeschlossen ist, können Sie rechts neben jeder Zeile auf die Ellipsen (…) klicken, um weitere Informationen anzuzeigen und andere Aufgaben auszuführen.

> Wenn Arrays die Integritätsprüfung nicht bestanden haben, können Sie das jeweilige Array überspringen und das Upgrade für die anderen fortsetzen. Alternativ können Sie den gesamten Prozess beenden und die Arrays, die nicht bestanden haben, beheben.

Führen Sie ein Upgrade der SANtricity Software und NVSRAM mit dem Storage Plug-in für vCenter durch

Aktualisieren Sie ein oder mehrere Storage-Arrays mit der neuesten Software und NVSRAM, um sicherzustellen, dass Sie über alle neuesten Funktionen und Fehlerbehebungen verfügen. Der NVSRAM-Controller ist eine Controller-Datei, die die Standardeinstellungen für die Controller angibt.

Bevor Sie beginnen

Stellen Sie sicher, dass:

- Die neuesten SANtricity OS-Dateien sind auf dem Host-System verfügbar, auf dem das Plugin ausgeführt wird.

- Sie wissen, ob Sie Ihr Software-Upgrade jetzt oder später aktivieren möchten. Aus folgenden Gründen können Sie sich später aktivieren:
  - **Tageszeit** — die Aktivierung der Software kann eine lange Zeit dauern, so dass Sie möglicherweise warten möchten, bis I/O-Lasten leichter sind. Der Failover der Controller während der Aktivierung ist möglich, sodass die Performance bis zum Abschluss des Upgrades unter Umständen niedriger ist als üblich.
  - **Art des Pakets** — möglicherweise möchten Sie die neue Betriebssystemsoftware auf einem Speicher-Array testen, bevor Sie die Dateien auf anderen Speicher-Arrays aktualisieren.

Risiko eines Datenverlustes oder eines Schadensrisikos am Speicher-Array — nehmen Sie während des Upgrades keine Änderungen am Speicher-Array vor. Halten Sie den Strom für das Speicher-Array aufrecht.

Schritte

1. Wenn Ihr Storage Array nur einen Controller oder einen Multipath-Treiber enthält, beenden Sie die I/O-Aktivitäten des Storage Arrays, um Applikationsfehler zu vermeiden. Wenn Ihr Storage Array über zwei Controller verfügt und Sie einen Multipath-Treiber installiert haben, müssen Sie die I/O-Aktivität nicht stoppen.
2. Wählen Sie in der Hauptansicht **Verwalten** aus, und wählen Sie dann ein oder mehrere Speicher-Arrays aus, die Sie aktualisieren möchten.
3. Wählen Sie Menü:Upgrade Center[Upgrade > SANtricity OS > Software].

   Die Seite SANtricity OS-Software aktualisieren wird angezeigt.
4. Laden Sie das aktuelle SANtricity OS Softwarepaket von der Support-Website auf Ihren lokalen Computer herunter.
   a. Klicken Sie auf Neue Datei zum Software-Repository hinzufügen
   b. Klicken Sie auf den Link, um die neuesten SANtricity OS Downloads zu finden.
   c. Klicken Sie auf den Link **Letzte Version herunterladen**.
   d. Befolgen Sie die restlichen Anweisungen, um die Betriebssystemdatei und die NVSRAM-Datei auf Ihren lokalen Computer herunterzuladen.

   In Version 8.42 und höher ist digital signierte Firmware erforderlich. Wenn Sie versuchen, nicht signierte Firmware herunterzuladen, wird ein Fehler angezeigt und der Download wird abgebrochen.
5. Wählen Sie die Betriebssystemsoftware und die NVSRAM-Datei aus, die Sie zum Aktualisieren der Controller verwenden möchten:
   a. Wählen Sie im Dropdown-Menü die Betriebssystemdatei aus, die Sie auf Ihren lokalen Computer heruntergeladen haben.

      Wenn mehrere Dateien verfügbar sind, werden die Dateien vom neuesten Datum bis zum ältesten Datum sortiert.

   Das Software-Repository listet alle mit dem Plug-in verbundenen Softwaredateien auf. Wenn die Datei nicht angezeigt wird, die Sie verwenden möchten, klicken Sie auf den Link **Neue Datei zum Software-Repository hinzufügen**, um zu dem Speicherort zu navigieren, an dem sich die Betriebssystemdatei befindet, die Sie hinzufügen möchten.

a. Wählen Sie im Dropdown-Menü **Select an NVSRAM file** die gewünschte Controllerdatei aus.

   Wenn es mehrere Dateien gibt, werden die Dateien vom neuesten Datum bis zum ältesten Datum sortiert.

6. Überprüfen Sie in der Tabelle kompatibler Speicher-Arrays die Speicherarrays, die mit der ausgewählten Betriebssystemsoftware kompatibel sind, und wählen Sie dann die Arrays aus, die aktualisiert werden sollen.
   - Die Speicherarrays, die Sie in der Ansicht Verwalten ausgewählt haben und mit der ausgewählten Firmware-Datei kompatibel sind, werden standardmäßig in der Tabelle kompatible Speicherarrays ausgewählt.
   - Die Speicher-Arrays, die nicht mit der ausgewählten Firmware-Datei aktualisiert werden können, können in der kompatiblen Speicher-Array-Tabelle nicht wie im Status **inkompatibel** angegeben ausgewählt werden.
7. (Optional) um die Software-Datei ohne Aktivierung auf die Speicher-Arrays zu übertragen, wählen Sie das Kontrollkästchen **Betriebssystemsoftware auf die Speicher-Arrays übertragen, als stufenweise markieren und zu einem späteren Zeitpunkt aktivieren** aus.
8. Klicken Sie Auf **Start**.
9. Je nachdem, ob Sie jetzt oder später aktiviert haben, führen Sie einen der folgenden Schritte aus:
   - Typ `TRANSFER` Um zu bestätigen, dass Sie die vorgeschlagene Betriebssystemsoftware auf den Arrays übertragen möchten, die Sie aktualisieren möchten, und klicken Sie dann auf **Transfer**. Um die übertragene Software zu aktivieren, wählen Sie MENU:Upgrade Center[Staged SANtricity OS Software aktivieren].
   - Typ `UPGRADE` Um zu bestätigen, dass Sie die vorgeschlagene Betriebssystemsoftware auf den Arrays übertragen und aktivieren möchten, die Sie für die Aktualisierung ausgewählt haben, und klicken Sie dann auf **Upgrade**.

     Das System überträgt die Softwaredatei auf jedes Speicherarray, das Sie für die Aktualisierung ausgewählt haben, und aktiviert diese Datei durch einen Neustart.

   Während des Aktualisierungsvorgangs treten folgende Aktionen auf:

   - Im Rahmen des Upgrades wird eine Integritätsprüfung vor dem Upgrade ausgeführt. Bei der Integritätsprüfung vor dem Upgrade werden alle Komponenten des Storage Arrays bewertet, um sicherzustellen, dass das Upgrade fortgesetzt werden kann.
   - Wenn eine Integritätsprüfung für ein Speicherarray fehlschlägt, wird das Upgrade abgebrochen. Klicken Sie auf die Ellipsen (…) Und wählen Sie **Protokoll speichern**, um die Fehler zu überprüfen. Sie können auch den Fehler der Integritätsprüfung überschreiben und dann auf **Weiter** klicken, um mit dem Upgrade fortzufahren.
   - Sie können den Upgrade-Vorgang nach der Integritätsprüfung vor dem Upgrade abbrechen.
10. (Optional) Sobald das Upgrade abgeschlossen ist, wird eine Liste der für ein bestimmtes Speicherarray aktualisierten Versionen angezeigt, indem Sie auf die Auslassungspunkte (…) klicken. Und wählen Sie dann **Protokoll speichern**.

    Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `upgrade_log-<date>. json`.

Aktivieren Sie die gestufte Betriebssystemsoftware im SANtricity-Speichermodul für vCenter

Sie können die Software-Datei sofort aktivieren oder bis zu einem angenehmeren Zeitpunkt warten. Bei diesem Verfahren wird davon ausgegangen, dass Sie die Softwaredatei zu einem späteren Zeitpunkt aktivieren.

Über diese Aufgabe

Sie können die Firmware-Dateien übertragen, ohne sie zu aktivieren. Aus folgenden Gründen können Sie sich später aktivieren:

- **Tageszeit** — die Aktivierung der Software kann eine lange Zeit dauern, so dass Sie möglicherweise warten möchten, bis I/O-Lasten leichter sind. Die Controller starten neu und führen einen Failover während der Aktivierung durch. Dadurch kann die Performance bis zum Abschluss des Upgrades unter Umständen niedriger sein als üblich.
- **Paketyp** — möglicherweise möchten Sie die neue Software und Firmware auf einem Speicher-Array testen, bevor Sie die Dateien auf anderen Speicher-Arrays aktualisieren.

Sie können den Aktivierungsvorgang nach dem Start nicht beenden.

Schritte

1. Wählen Sie in der Hauptansicht **Verwalten**. Klicken Sie bei Bedarf auf die Spalte **Status**, um oben auf der Seite alle Speicher-Arrays mit dem Status „Betriebssystem-Upgrade (Aktivierung ausstehend)“ zu sortieren.
2. Wählen Sie ein oder mehrere Speicher-Arrays aus, für die Sie Software aktivieren möchten, und wählen Sie dann Menü:Upgrade Center[Activate Staged SANtricity Software].

   Während des Aktualisierungsvorgangs treten folgende Aktionen auf:

   - Im Rahmen der Aktivierung wird eine Integritätsprüfung vor dem Upgrade ausgeführt. Bei der Integritätsprüfung vor dem Upgrade werden alle Komponenten des Storage-Arrays bewertet, um sicherzustellen, dass die Aktivierung fortgesetzt werden kann.
   - Wenn eine Integritätsprüfung für ein Speicherarray fehlschlägt, wird die Aktivierung angehalten. Klicken Sie auf die Ellipsen (…) Und wählen Sie **Protokoll speichern**, um die Fehler zu überprüfen. Sie können auch den Fehler der Integritätsprüfung überschreiben und dann auf **Weiter** klicken, um mit der Aktivierung fortzufahren.
   - Sie können den Aktivierungsvorgang nach der Integritätsprüfung vor dem Upgrade abbrechen.

     Nach erfolgreichem Abschluss der Integritätsprüfung vor dem Upgrade erfolgt die Aktivierung. Die Aktivierungszeiten hängen von der Konfiguration des Speicherarrays und den Komponenten ab, die Sie aktivieren.

3. (Optional) nach Abschluss der Aktivierung sehen Sie eine Liste der aktivierten Optionen für ein bestimmtes Speicherarray, indem Sie auf die Ellipsen (…) klicken. Und wählen Sie dann **Protokoll speichern**.

   Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `activate_log-<date>.json`.

Löschen Sie die gestufte Betriebssystemsoftware im SANtricity Storage Plug-in für vCenter

Sie können die stufenweise Betriebssystemsoftware entfernen, um sicherzustellen, dass

eine ausstehende Version zu einem späteren Zeitpunkt nicht versehentlich aktiviert wird. Das Entfernen der stufenweisen Betriebssystemsoftware hat keine Auswirkungen auf die aktuelle Version, die auf den Speicher-Arrays ausgeführt wird.

Schritte

1. Wählen Sie in der Hauptansicht **Verwalten** und dann Menü:SANtricity-Upgrade[Staged—Software löschen].

   Das Dialogfeld „Staged SANtricity-Software löschen“ wird geöffnet und listet alle erkannten Speichersysteme mit ausstehender Software oder NVSRAM auf.

2. Filtern oder sortieren Sie die Speichersysteme in der Liste, falls erforderlich, so dass Sie alle Systeme mit stufenweise Software anzeigen können.
3. Aktivieren Sie die Kontrollkästchen für die Speichersysteme mit ausstehender Software, die Sie löschen möchten.
4. Klicken Sie Auf **Löschen**.

   Der Status des Vorgangs wird im Dialogfeld angezeigt.

Managen Sie das Software Repository im SANtricity Storage Plug-in für vCenter

Sie können ein Software-Repository anzeigen und managen, in dem alle Softwaredateien aufgelistet sind, die mit dem Storage Plug-in für vCenter verknüpft sind.

Bevor Sie beginnen

Wenn Sie das Repository zum Hinzufügen von SANtricity OS-Dateien verwenden, stellen Sie sicher, dass die Betriebssystemdateien auf Ihrem lokalen System verfügbar sind.

Über diese Aufgabe

Sie können die Option SANtricity OS Software Repository verwalten verwenden, um eine oder mehrere Betriebssystemdateien auf das Hostsystem zu importieren, auf dem das Plugin ausgeführt wird. Sie können auch wählen, ob Sie eine oder mehrere Betriebssystemdateien löschen möchten, die im Software-Repository verfügbar sind.

Schritte

1. Wählen Sie in der Hauptansicht **Verwalten** und dann Menü:SANtricity-Software-Repository verwalten].

   Das Dialogfeld SANtricity OS Software-Repository verwalten wird angezeigt.

2. Führen Sie eine der folgenden Aktionen aus:
   - **Import:**
     i. Klicken Sie Auf **Import**.
     ii. Klicken Sie auf **Durchsuchen** und navigieren Sie dann zu dem Speicherort, an dem die Betriebssystemdateien gespeichert werden sollen. Betriebssystemdateien haben einen ähnlichen Dateinamen wie `N2800-830000-000.dlp`.
     iii. Wählen Sie eine oder mehrere Betriebssystemdateien aus, die Sie hinzufügen möchten, und klicken Sie dann auf **Import**.
   - **Löschen:**

i. Wählen Sie eine oder mehrere Betriebssystemdateien aus, die Sie aus dem Software-Repository entfernen möchten.

ii. Klicken Sie Auf **Löschen**.

Ergebnis

Wenn Sie den Import ausgewählt haben, werden die Dateien hochgeladen und validiert. Wenn Sie „Löschen“ ausgewählt haben, werden die Dateien aus dem Software-Repository entfernt.

Bereitstellung von Storage

Erfahren Sie mehr über die Bereitstellung von Storage im SANtricity Storage Plug-in für vCenter

Im Storage Plug-in für vCenter können Sie Daten-Container, sogenannte Volumes, erstellen, sodass der Host auf den Storage im Array zugreifen kann.

Volume-Typen und -Eigenschaften

Volumes sind Daten-Container, die den Speicherplatz auf Ihrem Storage-Array managen und organisieren.

Sie erstellen Volumes aus der Speicherkapazität, die auf Ihrem Speicher-Array verfügbar ist, was Ihnen hilft, die Ressourcen Ihres Systems zu organisieren. Das Konzept der "Volumes" ist ähnlich wie die Verwendung von Ordnern/Verzeichnissen auf einem Computer, um Dateien für schnellen Zugriff zu organisieren.

Volumes sind die einzige Datenebene, die Hosts sichtbar ist. In einer SAN-Umgebung werden Volumes den Logical Unit Numbers (LUNs) zugeordnet. Diese LUNs enthalten die Benutzerdaten, auf die über ein oder mehrere der vom Storage Array unterstützten Host-Zugriffsprotokolle zugegriffen werden kann, einschließlich FC, iSCSI und SAS.

Jedes Volume in einem Pool oder Volume-Gruppe kann je nach Art der Daten seine eigenen, individuellen Eigenschaften aufweisen. Einige dieser Eigenschaften sind:

- **Segmentgröße** — Ein Segment ist die Datenmenge in Kilobyte (KiB), die auf einem Laufwerk gespeichert ist, bevor das Speicherarray zum nächsten Laufwerk im Stripe (RAID-Gruppe) wechselt. Die Segmentgröße ist gleich oder kleiner als die Kapazität der Volume-Gruppe. Die Segmentgröße ist festgelegt und kann für Pools nicht geändert werden.
- **Kapazität** — Sie erstellen ein Volume aus der freien Kapazität, die entweder in einem Pool oder einer Volume-Gruppe verfügbar ist. Bevor Sie ein Volume erstellen, muss der Pool oder die Volume-Gruppe bereits vorhanden sein und genügend freie Kapazität zur Erstellung des Volumes haben.
- **Controller-Eigentum** — Alle Speicher-Arrays können einen oder zwei Controller haben. Auf einem Single-Controller-Array wird die Workload eines Volumes von einem einzigen Controller verwaltet. Auf einem Dual-Controller-Array hat ein Volume einen bevorzugten Controller (A oder B), der das Volume „besitzt“. In einer Dual-Controller-Konfiguration wird die Eigentümerschaft von Volumes automatisch mithilfe der Funktion Automatischer Lastausgleich angepasst, um eventuelle Probleme beim Lastenausgleich bei der Workload-Verschiebung zwischen den Controllern zu beheben. Der automatische Lastausgleich ermöglicht einen automatisierten I/O-Workload-Ausgleich und sorgt dafür, dass eingehender I/O-Datenverkehr von den Hosts auf beiden Controllern dynamisch gemanagt und ausgeglichen wird.
- **Volume-Zuweisung** — Sie können Hosts entweder bei der Erstellung des Volumes oder zu einem späteren Zeitpunkt auf ein Volume zugreifen. Der gesamte Host-Zugriff wird über eine LUN (Logical Unit Number) gemanagt. Hosts erkennen LUNs, die wiederum den Volumes zugewiesen sind. Wenn Sie ein Volume mehreren Hosts zuweisen, verwenden Sie eine Clustering-Software, um sicherzustellen, dass das Volume für alle Hosts verfügbar ist.

Der Host-Typ kann bestimmte Einschränkungen für die Anzahl der Volumes haben, auf die der Host zugreifen kann. Beachten Sie diese Einschränkung bei der Erstellung von Volumes zur Verwendung durch einen bestimmten Host.

- **Ressourcen-Provisioning** — für EF600- oder EF300-Speicher-Arrays können Sie festlegen, dass Volumes ohne Hintergrundinitialisierung sofort verwendet werden. Ein vom Ressourcen bereitgestelltes Volume ist ein Thick Volume in einer SSD-Volume-Gruppe oder einem Pool. Dabei wird bei der Erstellung des Volume die Laufwerkskapazität zugewiesen (dem Volume zugewiesen), die Laufwerksblöcke jedoch aufgehoben (nicht zugewiesen).
- **Beschreibenden Name** — Sie können ein Volumen benennen, welchen Namen Sie wollen, aber wir empfehlen, den Namen beschreibend zu machen.

Während der Volume-Erstellung wird jedem Volume Kapazität zugewiesen. Sie erhalten einen Namen, eine Segmentgröße (nur Volume-Gruppen), einen Controller-Besitz und eine Zuweisung von Volume zu Host. Bei Bedarf erfolgt ein automatischer Lastausgleich der Volume-Daten über Controller hinweg.

Kapazität für Volumes

Die Laufwerke in Ihrem Speicher-Array stellen die physische Speicherkapazität für Ihre Daten bereit. Bevor Sie mit dem Speichern von Daten beginnen können, müssen Sie die zugewiesene Kapazität in logischen Komponenten – Pools oder Volume-Gruppen – konfigurieren. Mithilfe dieser Speicherobjekte lassen sich Daten auf dem Speicher-Array konfigurieren, speichern, verwalten und erhalten.

Kapazität zur Erstellung und Erweiterung von Volumes

Sie können Volumes entweder aus der nicht zugewiesenen Kapazität oder aus freien Kapazitäten in einem Pool oder einer Volume-Gruppe erstellen.

- Wenn Sie ein Volume aus nicht zugewiesenen Kapazitäten erstellen, können Sie gleichzeitig einen Pool oder eine Volume-Gruppe und das Volume erstellen.
- Wenn Sie ein Volume aus freier Kapazität erstellen, erstellen Sie ein zusätzliches Volume in einem bereits vorhandenen Pool oder einer Volume-Gruppe.Nachdem Sie die Volume-Kapazität erweitert haben, müssen Sie die Größe des Dateisystems manuell erhöhen, um sie anzupassen. Wie Sie dies tun, hängt von dem Dateisystem ab, das Sie verwenden. Weitere Informationen finden Sie in der Dokumentation Ihres Host-Betriebssystems.

Die Plugin-Schnittstelle bietet keine Option zum Erstellen von Thin Volumes.

Gemeldete Kapazität für Volumes

Die gemeldete Kapazität des Volumes entspricht der Menge der zugewiesenen physischen Speicherkapazität. Es muss die gesamte physische Storage-Kapazität vorhanden sein. Der physisch zugewiesene Speicherplatz entspricht dem Speicherplatz, der dem Host gemeldet wird.

Normalerweise stellen Sie die gemeldete Kapazität des Volumes so ein, dass die maximale Kapazität, die Ihrer Meinung nach das Volume vergrößern wird. Volumes liefern eine hohe und vorhersehbare Performance für Ihre Applikationen, vor allem, weil sämtliche Benutzerkapazitäten reserviert und bei ihrer Erstellung zugewiesen sind.

Kapazitätsgrenzen

Die minimale Kapazität für ein Volume beträgt 1 MiB, und die maximale Kapazität hängt von der Anzahl und Kapazität der Laufwerke im Pool bzw. der Volume-Gruppe ab.

Beachten Sie bei der Erhöhung der gemeldeten Kapazität für ein Volumen die folgenden Richtlinien:

- Sie können bis zu drei Dezimalstellen (z. B. 65.375 gib) angeben.
- Die Kapazität muss kleiner sein als (oder gleich) die maximale in der Volume-Gruppe verfügbar ist. Wenn Sie ein Volume erstellen, wird für die DSS-Migration (Dynamic Segment Size) zusätzliche Kapazität vorab zugewiesen. Die DSS-Migration ist eine Funktion der Software, mit der Sie die Segmentgröße eines Volumes ändern können.
- Volumes mit einer Größe von mehr als 2 tib werden von einigen Host-Betriebssystemen unterstützt (die maximale gemeldete Kapazität wird vom Host-Betriebssystem bestimmt). Tatsächlich unterstützen einige Host-Betriebssysteme bis zu 128 tib Volumes. Weitere Informationen finden Sie in der Dokumentation Ihres Host-Betriebssystems.

Applikationsspezifische Workloads

Wenn Sie ein Volume erstellen, wählen Sie einen Workload aus, um die Storage-Array-Konfiguration für eine bestimmte Applikation anzupassen.

Ein Workload ist ein Storage-Objekt, das eine Applikation unterstützt. Sie können einen oder mehrere Workloads oder Instanzen pro Applikation definieren. Bei einigen Applikationen konfiguriert das System den Workload so, dass er Volumes mit ähnlichen zugrunde liegenden Volume-Merkmalen enthält. Diese Volume-Merkmale werden basierend auf dem Applikationstyp optimiert, den der Workload unterstützt. Wenn Sie beispielsweise einen Workload erstellen, der eine Microsoft SQL Server Applikation unterstützt und anschließend Volumes für diesen Workload erstellt, werden die zugrunde liegenden Volume-Merkmale zur Unterstützung von Microsoft SQL Server optimiert.

Während der Volume-Erstellung werden Sie vom System aufgefordert, Fragen zur Verwendung eines Workloads zu beantworten. Wenn Sie beispielsweise Volumes für Microsoft Exchange erstellen, werden Sie gefragt, wie viele Mailboxen Sie benötigen, wie viele Mailboxen Ihre durchschnittlichen Anforderungen an die Mailbox-Kapazität sind und wie viele Kopien der Datenbank Sie benötigen. Das System erstellt anhand dieser Informationen eine optimale Volume-Konfiguration für Sie, die Sie nach Bedarf bearbeiten können. Optional können Sie diesen Schritt in der Sequenz zur Volume-Erstellung überspringen.

Workload-Typen

Es können zwei unterschiedliche Workload-Typen erstellt werden: Applikationsspezifisch oder sonstige.

- **Applikationsspezifisch** — Wenn Sie Volumes mit einem anwendungsspezifischen Workload erstellen, empfiehlt das System möglicherweise eine optimierte Volume-Konfiguration, um Konflikte zwischen Applikations-Workload I/O und anderem Traffic aus Ihrer Anwendungsinstanz zu minimieren. Volume-Merkmale wie I/O-Typ, Segmentgröße, Controller-Besitz und Lese- und Schreib-Cache werden automatisch für Workloads empfohlen und optimiert, die für die folgenden Applikationstypen erstellt wurden.
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Videoüberwachungsapplikationen
  - VMware ESXi (für Volumes, die mit dem Virtual Machine File System verwendet werden sollen)

    Sie können die empfohlene Volume-Konfiguration überprüfen und die vom System empfohlenen Volumes und Merkmale bearbeiten, hinzufügen oder löschen. Verwenden Sie dazu das Dialogfeld Volumes hinzufügen/bearbeiten.
- **Andere (oder Anwendungen ohne spezifische Unterstützung der Volumenerzeugung)** — Bei anderen

Workloads wird eine Volume-Konfiguration verwendet, die manuell angegeben werden muss, wann ein Workload erstellt werden soll, der nicht mit einer bestimmten Applikation verknüpft ist, oder ob das System keine integrierte Optimierung für die Applikation bietet, die Sie im Storage-Array verwenden möchten. Sie müssen die Volume-Konfiguration manuell über das Dialogfeld Volumes hinzufügen/bearbeiten angeben.

Anzeige von Applikationen und Workloads

Um Anwendungen und Workloads anzuzeigen, starten Sie System Manager. Über diese Schnittstelle können Sie die Informationen anzeigen, die mit einem applikationsspezifischen Workload verknüpft sind. Sie haben verschiedene Möglichkeiten:

- Sie können die Registerkarte Anwendungen & Workloads in der Kachel Volumes auswählen, um die Volumes des Speicherarrays nach Workload gruppiert und den Anwendungstyp, mit dem der Workload verknüpft ist, anzuzeigen.
- Über die Registerkarte Applikationen und Workloads im Tile Performance können Sie Performance-Metriken (Latenz, IOPS und MB) für logische Objekte anzeigen. Die Objekte werden nach Applikation und zugehörieinem Workload gruppiert. Indem Sie diese Performance-Daten in regelmäßigen Abständen erfassen, können Sie Basismessungen vornehmen und Trends analysieren. Dies unterstützt Sie bei der Untersuchung von I/O-Performance-Problemen.

Erstellen Sie Speicher im SANtricity Speicher-Plug-in für vCenter

Im Storage Plug-in für vCenter erstellen Sie Storage, indem Sie zuerst einen Workload für einen bestimmten Applikationstyp erstellen. Als Nächstes wird dem Workload Storage-Kapazität hinzugefügt, indem Volumes mit ähnlichen zugrunde liegenden Volume-Merkmalen erstellt werden.

Schritt: Workloads erstellen

Ein Workload ist ein Storage-Objekt, das eine Applikation unterstützt. Sie können einen oder mehrere Workloads oder Instanzen pro Applikation definieren.

Über diese Aufgabe

Bei einigen Applikationen konfiguriert das System den Workload so, dass er Volumes mit ähnlichen zugrunde liegenden Volume-Merkmalen enthält. Diese Volume-Merkmale werden basierend auf dem Applikationstyp optimiert, den der Workload unterstützt. Wenn Sie beispielsweise einen Workload erstellen, der eine Microsoft SQL Server Applikation unterstützt und anschließend Volumes für diesen Workload erstellt, werden die zugrunde liegenden Volume-Merkmale zur Unterstützung von Microsoft SQL Server optimiert.

Das System empfiehlt nur für die folgenden Applikationstypen eine optimierte Volume-Konfiguration:

- Microsoft SQL Server
- Microsoft Exchange Server
- Videoüberwachung
- VMware ESXi (für Volumes, die mit dem Virtual Machine File System verwendet werden sollen)

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie Menü:Erstellen[Workload].

Das Dialogfeld Anwendungs-Workload erstellen wird angezeigt.

4. Wählen Sie in der Dropdown-Liste den Applikationstyp aus, für den der Workload erstellt werden soll, und geben Sie dann einen Workload-Namen ein.
5. Klicken Sie Auf **Erstellen**.

Schritt: Volumes erstellen

Sie erstellen Volumes, um einem applikationsspezifischen Workload Storage-Kapazität hinzuzufügen und die erstellten Volumes für einen bestimmten Host oder Host-Cluster sichtbar zu machen.

Über diese Aufgabe

Bei den meisten Applikationstypen wird standardmäßig eine benutzerdefinierte Volume-Konfiguration verwendet, während bei anderen Typen eine intelligente Konfiguration bei der Volume-Erstellung angewendet wird. Wenn Sie beispielsweise Volumes für eine Microsoft Exchange Applikation erstellen, werden Sie gefragt, wie viele Mailboxen Sie benötigen, wie viele Mailboxen Ihre durchschnittlichen Anforderungen an die Mailbox-Kapazität sind und wie viele Kopien der Datenbank Sie benötigen. Das System erstellt anhand dieser Informationen eine optimale Volume-Konfiguration für Sie, die Sie nach Bedarf bearbeiten können.

Sie können Volumes über das Menü:Provisioning[Manage Volumes > Create > Volumes] oder über das Menü:Provisioning[Configure Pools and Volume Groups > Create > Volumes] erstellen. Das Verfahren ist bei beiden Auswahlmöglichkeiten identisch.

Der Prozess zur Erstellung eines Volumes ist ein mehrstufiges Verfahren.

Schritt 2a: Wählen Sie Host für ein Volume

Im ersten Schritt können Sie einen bestimmten Host oder Host-Cluster für das Volume auswählen oder den Host später zuweisen.

Bevor Sie beginnen

Stellen Sie sicher, dass:

- Es wurden gültige Hosts oder Host-Cluster definiert (unter Menü:Bereitstellung [Hosts konfigurieren]).
- Für den Host wurden Host-Port-IDs definiert.
- Die Host-Verbindung muss Data Assurance (da) unterstützen, wenn Sie die Erstellung von da-fähigen Volumes planen. Wenn eine der Host-Verbindungen auf den Controllern im Speicher-Array keine Unterstützung für da bietet, können die zugeordneten Hosts auf da-fähige Volumes keinen Zugriff auf Daten haben.

Über diese Aufgabe

Beachten Sie bei der Zuweisung von Volumes die folgenden Richtlinien:

- Das Betriebssystem eines Hosts kann bestimmte Einschränkungen für die Zugriffsmöglichkeiten auf die Anzahl der Volumes haben, auf die der Host zugreifen kann. Beachten Sie diese Einschränkung bei der Erstellung von Volumes zur Verwendung durch einen bestimmten Host.
- Sie können eine Zuweisung für jedes Volume im Storage-Array definieren.
- Zugewiesene Volumes werden von den Controllern im Storage-Array gemeinsam genutzt.
- Die gleiche Logical Unit Number (LUN) kann nicht zweimal von einem Host oder einem Host-Cluster verwendet werden, um auf ein Volume zuzugreifen. Sie müssen eine eindeutige LUN verwenden.
- Wenn Sie den Prozess zum Erstellen von Volumes beschleunigen möchten, können Sie den

Hostzuordnungsschritt überspringen, damit neu erstellte Volumes offline initialisiert werden.

> Die Zuweisung eines Volumes zu einem Host schlägt fehl, wenn Sie versuchen, einem Host-Cluster ein Volume zuzuweisen, das mit einer festgelegten Zuordnung für einen Host in den Host-Clustern in Konflikt steht.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie Menü:Erstellen[Volumes].

   Das Dialogfeld Host auswählen wird angezeigt.

4. Wählen Sie aus der Dropdown-Liste einen bestimmten Host oder Host-Cluster aus, dem Sie Volumes zuweisen möchten, oder wählen Sie aus, zu einem späteren Zeitpunkt den Host oder Host-Cluster zuzuweisen.
5. Um die Volume-Erstellungsreihenfolge für den ausgewählten Host oder Host-Cluster fortzusetzen, klicken Sie auf **Weiter.**

   Das Dialogfeld „Workload auswählen“ wird angezeigt.

Schritt 2b: Wählen Sie einen Workload für ein Volume

Im zweiten Schritt wählen Sie einen Workload aus, um die Storage-Array-Konfiguration für eine bestimmte Applikation wie VMware anzupassen.

Über diese Aufgabe

In dieser Aufgabe wird die Erstellung von Volumes für einen Workload beschrieben. Ein Workload enthält normalerweise Volumes mit ähnlichen Merkmalen, die entsprechend dem von dem Workload unterstützten Applikationstyp optimiert werden. Sie können in diesem Schritt einen Workload definieren oder vorhandene Workloads auswählen.

Beachten Sie folgende Richtlinien:

- Bei der Verwendung eines applikationsspezifische Workloads empfiehlt das System eine optimierte Volume-Konfiguration, um Konflikte zwischen Applikations-Workload-I/O und anderem Datenverkehr aus Ihrer Applikationsinstanz zu minimieren. Sie können die empfohlene Volume-Konfiguration überprüfen und anschließend die vom System empfohlenen Volumes und -Eigenschaften bearbeiten, hinzufügen oder löschen. Verwenden Sie dazu das Dialogfeld Volumes hinzufügen/bearbeiten (im nächsten Schritt verfügbar).
- Bei Verwendung anderer Anwendungstypen legen Sie die Volume-Konfiguration manuell über das Dialogfeld Volumes hinzufügen/bearbeiten fest (im nächsten Schritt verfügbar).

Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie die Option **Volumes für einen vorhandenen Workload erstellen** aus, und wählen Sie den Workload aus der Dropdown-Liste aus.
   - Wählen Sie die Option **Einen neuen Workload erstellen** aus, um einen neuen Workload für eine unterstützte Anwendung oder für „andere“ Anwendungen zu definieren, und führen Sie die folgenden Schritte aus:

- Wählen Sie in der Dropdown-Liste den Namen der Anwendung aus, für die Sie den neuen Workload erstellen möchten. Wählen Sie einen der „anderen“ Einträge aus, wenn die Anwendung, die Sie für dieses Speicher-Array verwenden möchten, nicht aufgeführt ist.
- Geben Sie einen Namen für den zu erstellenden Workload ein.

2. Klicken Sie Auf **Weiter**.
3. Wenn Ihr Workload einem unterstützten Applikationstyp zugewiesen ist, geben Sie die angeforderten Informationen ein. Andernfalls fahren Sie mit dem nächsten Schritt fort.

Schritt 2c: Volumes hinzufügen oder bearbeiten

Im dritten Schritt definieren Sie die Volume-Konfiguration.

Bevor Sie beginnen

- Die Pools oder Volume-Gruppen müssen über eine ausreichende freie Kapazität verfügen.
- In einer Volume-Gruppe sind maximal 256 Volumes zulässig.
- Die maximale Anzahl an Volumes, die in einem Pool zulässig sind, hängt vom Modell des Storage-Systems ab:
  - 2,048 Volumes (EF600 und E5700 Serie)
  - 1,024 Volumes (EF300)
  - 512 Volumes (E2800 Serie)
- Um ein für Data Assurance (da) fähiges Volume zu erstellen, muss die Host-Verbindung, die Sie verwenden möchten, da unterstützen.
  - Wenn Sie ein DA-fähiges Volume erstellen möchten, wählen Sie einen Pool oder eine Volume-Gruppe aus, die für da geeignet ist (suchen Sie in der Tabelle mit den Kandidaten für Pool- und Volume-Gruppen nach **Ja** neben „da“).
  - DA-Funktionen werden auf Pool- und Volume-Gruppenebene präsentiert. DA der Schutz auf Fehler überprüft und korrigiert, die auftreten können, wenn Daten durch die Controller an die Laufwerke übertragen werden. Durch die Auswahl eines da-fähigen Pools oder einer Volume-Gruppe für das neue Volume wird sichergestellt, dass Fehler erkannt und behoben werden.
  - Wenn eine der Host-Verbindungen auf den Controllern im Speicher-Array keine Unterstützung für da bietet, können die zugeordneten Hosts auf da-fähige Volumes keinen Zugriff auf Daten haben.
- Um ein sicheres Volume zu erstellen, muss für das Storage Array ein Sicherheitsschlüssel erstellt werden.
  - Wenn Sie ein sicheres Volume erstellen möchten, wählen Sie einen Pool oder eine Volume-Gruppe aus, die sicher fähig ist (suchen Sie in der Tabelle mit den Kandidaten für Pool und Volume-Gruppen nach „sicher-fähig“).
  - Die Sicherheitsfunktionen für die Laufwerksicherheit werden auf Pool- und Volume-Gruppenebene präsentiert. Sichere Laufwerke verhindern unbefugten Zugriff auf die Daten auf einem Laufwerk, das physisch vom Storage-Array entfernt wird. Ein sicheres Laufwerk verschlüsselt Daten während des Schreibvorgangs und entschlüsselt Daten beim Lesen mithilfe eines eindeutigen Verschlüsselungsschlüssels.
  - Ein Pool oder eine Volume-Gruppe kann sowohl sichere als auch nicht sichere Laufwerke enthalten. Zur Nutzung der Verschlüsselungsfunktionen müssen jedoch alle Laufwerke sicher sein.
- Um ein Volume mit Ressourcenbereitstellung zu erstellen, müssen alle Laufwerke NVMe-Laufwerke mit der dezugewiesenen oder nicht geschriebenen Option Logical Block Error (DULBE) sein.

Über diese Aufgabe

Sie erstellen Volumes aus geeigneten Pools oder Volume-Gruppen, die im Dialogfeld Volumes hinzufügen/bearbeiten angezeigt werden. Für jeden infrage kommenden Pool und jede Volume-Gruppe wird die Anzahl der verfügbaren Laufwerke und die gesamte freie Kapazität angezeigt.

Für einige applikationsspezifische Workloads zeigt jede qualifizierte Pool- oder Volume-Gruppe die vorgeschlagene Kapazität basierend auf der vorgeschlagenen Volume-Konfiguration und zeigt die verbleibende freie Kapazität in gib an. Für andere Workloads wird die vorgeschlagene Kapazität angezeigt, wenn Sie Volumes zu einem Pool oder einer Volume-Gruppe hinzufügen und die gemeldete Kapazität angeben.

Schritte

1. Wählen Sie eine dieser Aktionen aus, basierend darauf, ob Sie im vorherigen Schritt eine andere oder einen applikationsspezifischen Workload ausgewählt haben:
   - **Other** — Klicken Sie **Neues Volume hinzufügen** in jedem Pool oder Volume-Gruppe, die Sie verwenden möchten, um ein oder mehrere Volumes zu erstellen.

Felddetails

Feld	Beschreibung
Volume-Name	Einem Volume wird während der Volume-Erstellungsreihenfolge ein Standardname zugewiesen. Sie können entweder den Standardnamen akzeptieren oder einen aussagekräftigeren Namen angeben, der die Art der im Volume gespeicherten Daten angibt.
Gemeldete Kapazität	Definieren Sie die Kapazität des neuen Volume und der zu verwendenden Kapazitätseinheiten (MiB, gib oder tib). Bei dicken Volumes beträgt die Mindestkapazität 1 MiB, und die maximale Kapazität wird durch die Anzahl und Kapazität der Laufwerke im Pool oder der Volume-Gruppe bestimmt. Storage-Kapazität ist auch für Copy-Services erforderlich (Snapshot Images, Snapshot Volumes, Volume-Kopien und Remote-Spiegelungen). Weisen Sie Standard-Volumes nicht die gesamte Kapazität zu. Die Kapazität in einem Pool wird in Schritten von 4 gib zugewiesen. Kapazität, die nicht ein Vielfaches von 4 gib beträgt, wird zugewiesen, aber nicht nutzbar. Um sicherzustellen, dass die gesamte Kapazität nutzbar ist, geben Sie die Kapazität in Schritten von 4 gib an. Wenn eine nicht nutzbare Kapazität vorhanden ist, besteht die einzige Möglichkeit zur Wiederherstellung darin, die Kapazität des Volume zu erhöhen.
Volume-Block-Größe (nur EF300 und EF600)	Zeigt die Block-Größen, die für das Volume erstellt werden können: • 512–512 Byte • 4 KB – 4,096 Byte

Feld	Beschreibung
Segmentgröße	Zeigt die Einstellung für die Segmentgrößen, die nur für Volumes in einer Volume-Gruppe angezeigt wird. Sie können die Segmentgröße ändern, um die Leistung zu optimieren. **Zulässige Segmentgrößen-Übergänge** — das System bestimmt die zulässigen Segmentgrößen-Übergänge. Segmentgrößen, bei denen es sich um unangemessene Übergänge aus der aktuellen Segmentgröße handelt, sind in der Dropdown-Liste nicht verfügbar. Zulässige Übergänge sind in der Regel doppelt oder halb so groß wie das aktuelle Segment. Wenn die aktuelle Volume-Segmentgröße beispielsweise 32 KiB beträgt, ist eine neue Volume-Segmentgröße von entweder 16 KiB oder 64 KiB zulässig. **SSD Cache-fähige Volumes** — Sie können eine 4-KiB-Segmentgröße für SSD Cache-fähige Volumes angeben. Vergewissern Sie sich, dass Sie die 4-KiB-Segmentgröße nur für SSD-Cache-fähige Volumes auswählen, die I/O-Vorgänge mit kleinen Blöcken bearbeiten (beispielsweise 16 KiB-I/O-Blockgrößen oder kleiner). Die Performance könnte beeinträchtigt werden, wenn Sie 4 als Segmentgröße für SSD Cache-fähige Volumes auswählen, die sequenzielle Operationen von großen Blöcken bearbeiten. **Zeit zum Ändern der Segmentgröße** — die Zeit, die zur Änderung der Segmentgröße eines Volumes benötigt wird, hängt von diesen Variablen ab: • Die I/O-Last vom Host • Die Änderungspriorität des Volumes • Die Anzahl der Laufwerke in der Volume-Gruppe • Die Anzahl der Laufwerkskanäle • Die Verarbeitungsleistung der Speicher-Array-Controller Wenn Sie die Segmentgröße für ein Volume ändern, wirkt sich die I/O-Performance auf die I/O-Performance aus, doch die Daten bleiben verfügbar.
Sicher	**Ja** erscheint neben „Secure-fähig“ nur dann, wenn die Laufwerke im Pool oder in der Volume-Gruppe sicher sind. Die Laufwerkssicherheit verhindert, dass nicht autorisierter Zugriff auf die Daten auf einem Laufwerk erfolgt, das physisch vom Speicher-Array entfernt wird. Diese Option ist nur verfügbar, wenn die Laufwerksicherheit aktiviert wurde und für das Speicher-Array ein Sicherheitsschlüssel eingerichtet wurde. Ein Pool oder eine Volume-Gruppe kann sowohl sichere als auch nicht sichere Laufwerke enthalten. Zur Nutzung der Verschlüsselungsfunktionen müssen jedoch alle Laufwerke sicher sein.
DA	**Ja** erscheint neben „da“ nur dann, wenn die Laufwerke im Pool oder in der Volume-Gruppe Data Assurance (da) unterstützen. DA erhöht die Datenintegrität im gesamten Storage-System. DA ermöglicht es dem Storage-Array, Fehler zu überprüfen, die auftreten können, wenn Daten durch die Controller an die Laufwerke übertragen werden. Die Verwendung von da für das neue Volume stellt sicher, dass alle Fehler erkannt werden.

Feld	Beschreibung
Bereitgestellte Ressource (nur EF300 und EF600)	**Ja** erscheint neben „Ressourcen bereitgestellt“ nur, wenn die Laufwerke diese Option unterstützen. Resource Provisioning ist eine Funktion, die in den EF300- und EF600-Speicher-Arrays zur Verfügung steht und die es ermöglicht, Volumes ohne Hintergrundinitialisierung sofort in Betrieb zu nehmen.

- **Anwendungsspezifischer Workload** — Klicken Sie entweder auf **Weiter**, um die vom System empfohlenen Volumes und Merkmale für den ausgewählten Workload zu akzeptieren, oder klicken Sie auf **Volumes bearbeiten**, um die vom System empfohlenen Volumes und Merkmale für den ausgewählten Workload zu ändern, hinzuzufügen oder zu löschen.

Felddetails

Feld	Beschreibung
Volume-Name	Einem Volume wird während der Volume-Erstellungsreihenfolge ein Standardname zugewiesen. Sie können entweder den Standardnamen akzeptieren oder einen aussagekräftigeren Namen angeben, der die Art der im Volume gespeicherten Daten angibt.
Gemeldete Kapazität	Definieren Sie die Kapazität des neuen Volume und der zu verwendenden Kapazitätseinheiten (MiB, gib oder tib). Bei dicken Volumes beträgt die Mindestkapazität 1 MiB, und die maximale Kapazität wird durch die Anzahl und Kapazität der Laufwerke im Pool oder der Volume-Gruppe bestimmt. Storage-Kapazität ist auch für Copy-Services erforderlich (Snapshot Images, Snapshot Volumes, Volume-Kopien und Remote-Spiegelungen). Weisen Sie Standard-Volumes nicht die gesamte Kapazität zu. Die Kapazität in einem Pool wird in Schritten von 4 gib zugewiesen. Kapazitäten, die nicht ein Vielfaches von 4 gib beträgt, werden zugewiesen, aber nicht nutzbar. Um sicherzustellen, dass die gesamte Kapazität nutzbar ist, geben Sie die Kapazität in Schritten von 4 gib an. Wenn eine nicht nutzbare Kapazität vorhanden ist, besteht die einzige Möglichkeit zur Wiederherstellung darin, die Kapazität des Volume zu erhöhen.
Volume-Typ	Volume-Typ gibt den Volume-Typ an, der für einen applikationsspezifischen Workload erstellt wurde.
Volume-Block-Größe (nur EF300 und EF600)	Zeigt die Block-Größen, die für das Volume erstellt werden können: • 512 — 512 Byte • 4K — 4,096 Byte

Feld	Beschreibung
Segmentgröße	Zeigt die Einstellung für die Segmentgrößen, die nur für Volumes in einer Volume-Gruppe angezeigt wird. Sie können die Segmentgröße ändern, um die Leistung zu optimieren. **Zulässige Segmentgrößen-Übergänge** — das System bestimmt die zulässigen Segmentgrößen-Übergänge. Segmentgrößen, bei denen es sich um unangemessene Übergänge aus der aktuellen Segmentgröße handelt, sind in der Dropdown-Liste nicht verfügbar. Zulässige Übergänge sind in der Regel doppelt oder halb so groß wie das aktuelle Segment. Wenn die aktuelle Volume-Segmentgröße beispielsweise 32 KiB beträgt, ist eine neue Volume-Segmentgröße von entweder 16 KiB oder 64 KiB zulässig. **SSD Cache-fähige Volumes** — Sie können eine 4-KiB-Segmentgröße für SSD Cache-fähige Volumes angeben. Vergewissern Sie sich, dass Sie die 4-KiB-Segmentgröße nur für SSD-Cache-fähige Volumes auswählen, die I/O-Vorgänge mit kleinen Blöcken bearbeiten (beispielsweise 16 KiB-I/O-Blockgrößen oder kleiner). Die Performance könnte beeinträchtigt werden, wenn Sie 4 als Segmentgröße für SSD Cache-fähige Volumes auswählen, die sequenzielle Operationen von großen Blöcken bearbeiten. **Zeit zum Ändern der Segmentgröße** — die Zeit, die zur Änderung der Segmentgröße eines Volumes benötigt wird, hängt von diesen Variablen ab: • Die I/O-Last vom Host • Die Änderungspriorität des Volumes • Die Anzahl der Laufwerke in der Volume-Gruppe • Die Anzahl der Laufwerkskanäle • Die Verarbeitungsleistung der Speicher-Array-Controller Wenn Sie die Segmentgröße für ein Volume ändern, wirkt sich die I/O-Performance auf die I/O-Performance aus, doch die Daten bleiben verfügbar.
Sicher	**Ja** erscheint neben „Secure-fähig“ nur dann, wenn die Laufwerke im Pool oder in der Volume-Gruppe sicher sind. Die Laufwerkssicherheit verhindert, dass nicht autorisierter Zugriff auf die Daten auf einem Laufwerk erfolgt, das physisch vom Speicher-Array entfernt wird. Diese Option ist nur verfügbar, wenn die Sicherheitsfunktion des Laufwerks aktiviert ist und für das Speicher-Array ein Sicherheitsschlüssel eingerichtet wurde. Ein Pool oder eine Volume-Gruppe kann sowohl sichere als auch nicht sichere Laufwerke enthalten. Zur Nutzung der Verschlüsselungsfunktionen müssen jedoch alle Laufwerke sicher sein.
DA	**Ja** erscheint neben „da“ nur dann, wenn die Laufwerke im Pool oder in der Volume-Gruppe Data Assurance (da) unterstützen. DA erhöht die Datenintegrität im gesamten Storage-System. DA ermöglicht es dem Storage-Array, Fehler zu überprüfen, die auftreten können, wenn Daten durch die Controller an die Laufwerke übertragen werden. Die Verwendung von da für das neue Volume stellt sicher, dass alle Fehler erkannt werden.

Feld	Beschreibung
Bereitgestellte Ressource (nur EF300 und EF600)	**Ja** erscheint neben „Ressourcen bereitgestellt“ nur, wenn die Laufwerke diese Option unterstützen. Resource Provisioning ist eine Funktion, die in den EF300- und EF600-Speicher-Arrays zur Verfügung steht und die es ermöglicht, Volumes ohne Hintergrundinitialisierung sofort in Betrieb zu nehmen.

2. Klicken Sie auf **Weiter**, um mit der Volumenerzeugung für die ausgewählte Anwendung fortzufahren.

Schritt 2d: Volumenkonfiguration prüfen

Im letzten Schritt lesen Sie eine Zusammenfassung der Volumes, die Sie erstellen möchten, und nehmen alle erforderlichen Änderungen vor.

Schritte

1. Prüfen Sie die Volumes, die Sie erstellen möchten. Um Änderungen vorzunehmen, klicken Sie auf **Zurück**.
2. Wenn Sie mit Ihrer Volumenkonfiguration zufrieden sind, klicken Sie auf **Fertig stellen**.

Nachdem Sie fertig sind

- Erstellen Sie im vSphere Client Datastores für die Volumes.
- Führen Sie alle auf dem Applikations-Host erforderlichen Betriebssystemänderungen durch, damit die Applikationen das Volume verwenden können.
- Führen Sie das betriebssystemspezifische Dienstprogramm (verfügbar von einem Drittanbieter) aus, und führen Sie dann den Befehl SMcli aus `-identifyDevices` So korrelieren Sie Volume-Namen mit Host-Storage-Array-Namen

  Die SMcli ist im SANtricity Betriebssystem enthalten und kann über den SANtricity System Manager heruntergeladen werden. Weitere Informationen zum Herunterladen des SMcli über den SANtricity-System-Manager finden Sie im "Laden Sie das Thema Befehlszeilenschnittstelle (CLI) in der Online-Hilfe des SANtricity Systemmanagers herunter".

Steigerung der Kapazität eines Volumes im SANtricity Storage Plug-in für vCenter

Sie können die Größe eines Volumes anpassen, um die gemeldete Kapazität zu erhöhen.

Bevor Sie beginnen

Stellen Sie sicher, dass:

- Im zugewiesenen Pool bzw. der Volume-Gruppe des Volumes steht genügend freie Kapazität zur Verfügung.
- Das Volume ist optimal und nicht in einem Zustand der Änderung.
- Im Volume werden keine Hot-Spare-Laufwerke verwendet. (Gilt nur für Volumes in Volume-Gruppen.)

Über diese Aufgabe

Diese Aufgabe beschreibt, wie Sie die gemeldete Kapazität (die Kapazität, die Hosts gemeldet werden) eines Volumes erhöhen, indem Sie die freie Kapazität nutzen, die in dem Pool oder der Volume-Gruppe verfügbar ist. Denken Sie daran, zukünftige Kapazitätsanforderungen für andere Volumes in diesem Pool oder dieser Volume-Gruppe zu berücksichtigen.

Eine Erhöhung der Kapazität eines Volumens wird nur auf bestimmten Betriebssystemen unterstützt. Wenn Sie die Volume-Kapazität auf einem nicht unterstützten Host-Betriebssystem erhöhen, kann die erweiterte Kapazität nicht verwendet werden, und Sie können die ursprüngliche Volume-Kapazität nicht wiederherstellen.

Schritte

1. Wählen Sie auf der Seite **Verwalten** das Speicher-Array aus, das die Volumes enthält, die Sie ändern möchten.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie das Volumen aus, für das Sie die Kapazität erhöhen möchten, und wählen Sie dann **Kapazität erhöhen**.

   Das Dialogfeld Kapazität erhöhen bestätigen wird angezeigt.

4. Wählen Sie **Ja**, um fortzufahren.

   Das Dialogfeld gemeldete Kapazität erhöhen wird angezeigt. In diesem Dialogfeld wird die aktuell gemeldete Kapazität des Volumes und die freie Kapazität angezeigt, die im zugeordneten Pool oder der Volume-Gruppe verfügbar ist.

5. Verwenden Sie das Feld * gemeldete Kapazität erhöhen, indem Sie…* hinzufügen, um die Kapazität der aktuell verfügbaren gemeldeten Kapazität hinzuzufügen. Sie können den Kapazitätswert ändern, um entweder in Mebibyte (MiB), Gibibyte (gib) oder Tebibyte (tib) anzuzeigen.
6. Klicken Sie Auf **Erhöhen**.

   Die Kapazität des Volumes wird je nach Auswahl erhöht. Dieser Vorgang kann langwierig sein und die System-Performance beeinträchtigen.

Nachdem Sie fertig sind

Nachdem Sie die Volume-Kapazität erweitert haben, müssen Sie die Größe des Dateisystems manuell erhöhen, um sie anzupassen. Wie Sie dies tun, hängt von dem Dateisystem ab, das Sie verwenden. Weitere Informationen finden Sie in der Dokumentation Ihres Host-Betriebssystems.

Ändern Sie die Einstellungen für ein Volume im SANtricity Storage Plug-in für vCenter

Sie können die Einstellungen eines Volume ändern, z. B. Name, Host-Zuweisung, Segmentgröße, Änderungspriorität, Caching, Und so weiter.

Bevor Sie beginnen

Stellen Sie sicher, dass das Volume, das Sie ändern möchten, im optimalen Status ist.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus, das die Volumes enthält, die Sie ändern möchten.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie das gewünschte Volume aus und wählen Sie dann **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld Volume-Einstellungen wird angezeigt. Die Konfigurationseinstellungen für das ausgewählte Volume werden in diesem Dialogfeld angezeigt.

4. Wählen Sie die Registerkarte **Basic** aus, um den Namen des Volumes und die Host-Zuweisung zu ändern.

Felddetails

Einstellung	Beschreibung
Name	Zeigt den Namen des Volumes an. Ändern Sie den Namen eines Volumes, wenn der aktuelle Name nicht mehr aussagekräftig oder anwendbar ist.
Kapazität	Zeigt die gemeldete und zugewiesene Kapazität für das ausgewählte Volume an.
Pool-/Volume-Gruppe	Zeigt den Namen und das RAID-Level der Pool- oder Volume-Gruppe an. Gibt an, ob der Pool oder die Volume-Gruppe sicher-fähig und sicher aktiviert ist.
Host	Zeigt die Volumenzuweisung an. Sie weisen einem Host oder Host-Cluster ein Volume zu, damit I/O-Vorgänge darauf zugreifen können. Diese Zuweisung gewährt einem Host oder Host-Cluster Zugriff auf ein bestimmtes Volume oder auf eine Reihe von Volumes in einem Storage-Array. • **Zugeordnet zu** — identifiziert den Host oder Host-Cluster, der Zugriff auf das ausgewählte Volume hat. • **LUN** — Eine logische Gerätenummer (LUN) ist die Nummer, die dem Adressraum zugewiesen ist, den ein Host für den Zugriff auf ein Volume verwendet. Das Volume wird dem Host als Kapazität in Form einer LUN präsentiert. Jeder Host verfügt über seinen eigenen LUN-Adressraum. Daher kann dieselbe LUN von unterschiedlichen Hosts für den Zugriff auf verschiedene Volumes verwendet werden. Für NVMe-Schnittstellen wird in dieser Spalte die Namespace-ID angezeigt. Ein Namespace ist NVM Storage, der für Blockzugriff formatiert ist. Es gleicht einer logischen Einheit in SCSI, die ein Volume im Storage Array bezieht. Die Namespace-ID ist die eindeutige Kennung des NVMe Controllers für den Namespace und kann auf einen Wert zwischen 1 und 255 gesetzt werden. Sie entspricht einer Logical Unit Number (LUN) in SCSI.
Identifikatoren	Zeigt die Kennungen für das ausgewählte Volume an. • Weltweite Kennung (WWID). Eine eindeutige Hexadezimalkennung für das Volume • Erweiterte eindeutige Kennung (EUI). Eine EUI-64-Kennung für das Volume. • Subsystem Identifier (SSID). Die Speicher-Array-Subsystem-Kennung eines Volumes.

5. Wählen Sie die Registerkarte **Erweitert** aus, um zusätzliche Konfigurationseinstellungen für ein Volume in einem Pool oder in einer Volume-Gruppe zu ändern.

Felddetails

Einstellung	Beschreibung
Applikations- und Workload-Informationen	Während der Volume-Erstellung können applikationsspezifische oder andere Workloads erstellt werden. Falls zutreffend, werden für das ausgewählte Volume der Workload-Name, der Applikationstyp und der Volume-Typ angezeigt. Bei Bedarf können Sie den Workload-Namen ändern.
Quality of Service-Einstellungen	**Data Assurance dauerhaft deaktivieren** — Diese Einstellung wird nur angezeigt, wenn das Volume Data Assurance (da) aktiviert ist. DA überprüft und korrigiert Fehler, die auftreten können, wenn Daten durch die Controller zu den Laufwerken übertragen werden. Verwenden Sie diese Option, um da auf dem ausgewählten Volume dauerhaft zu deaktivieren. Wenn diese Option deaktiviert ist, kann da für dieses Volume nicht erneut aktiviert werden. **VorableseRedundanzprüfung aktivieren** — Diese Einstellung wird nur angezeigt, wenn das Volumen ein dickes Volumen ist. Die vorab gelesene Redundanz prüft, ob die Daten auf einem Volume konsistent sind, jederzeit, wenn ein Lesevorgang durchgeführt wird. Ein Volume, auf dem diese Funktion aktiviert ist, gibt Lesefehler zurück, wenn die Daten von der Controller-Firmware als unvereinbar erkannt werden.
Controller-Eigentum	Definiert den Controller, der als Eigentümer des Volume oder als primärer Controller des Volume bezeichnet wird. Die Eigentümerschaft der Controller ist sehr wichtig und sollte sorgfältig geplant werden. Controller sollten für eine GesamtI/OS so eng wie möglich ausgeglichen werden.

Einstellung	Beschreibung
Segmentgrößen	Zeigt die Einstellung für die Segmentgrößen, die nur für Volumes in einer Volume-Gruppe angezeigt wird. Sie können die Segmentgröße ändern, um die Leistung zu optimieren. **Zulässige Segmentgrößen-Übergänge** — das System bestimmt die zulässigen Segmentgrößen-Übergänge. Segmentgrößen, bei denen es sich um unangemessene Übergänge aus der aktuellen Segmentgröße handelt, sind in der Dropdown-Liste nicht verfügbar. Zulässige Übergänge sind in der Regel doppelt oder halb so groß wie das aktuelle Segment. Wenn die aktuelle Volume-Segmentgröße beispielsweise 32 KiB beträgt, ist eine neue Volume-Segmentgröße von entweder 16 KiB oder 64 KiB zulässig. **SSD Cache-fähige Volumes** — Sie können eine 4-KiB-Segmentgröße für SSD Cache-fähige Volumes angeben. Vergewissern Sie sich, dass Sie die 4-KiB-Segmentgröße nur für SSD-Cache-fähige Volumes auswählen, die I/O-Vorgänge mit kleinen Blöcken bearbeiten (beispielsweise 16 KiB-I/O-Blockgrößen oder kleiner). Die Performance könnte beeinträchtigt werden, wenn Sie 4 als Segmentgröße für SSD Cache-fähige Volumes auswählen, die sequenzielle Operationen von großen Blöcken bearbeiten. **Zeitdauer zum Ändern der Segmentgröße.** die Zeit, die zur Änderung der Segmentgröße eines Volumes erforderlich ist, hängt von diesen Variablen ab: • Die I/O-Last vom Host • Die Änderungspriorität des Volumes • Die Anzahl der Laufwerke in der Volume-Gruppe • Die Anzahl der Laufwerkskanäle • Die Verarbeitungsleistung der Speicher-Array-Controller Wenn Sie die Segmentgröße für ein Volume ändern, wirkt sich die I/O-Performance auf die I/O-Performance aus, doch die Daten bleiben verfügbar.
Priorität für Änderungen	Zeigt die Einstellung für die Änderungspriorität an, die nur für Volumes in einer Volume-Gruppe angezeigt wird. Die Änderungspriorität definiert, wie viel Verarbeitungszeit im Verhältnis zur Systemperformance für Volume-Änderungsprozesse zugewiesen wird. Sie können die Änderungspriorität für das Volume erhöhen, obwohl dies unter Umständen die System-Performance beeinträchtigen kann. Verschieben Sie die Schieberegler, um eine Prioritätsebene auszuwählen. **Modifizierung Prioritätsstufen** — die niedrigste Prioritätsrate profitiert von der Systemleistung, aber der Änderungsvorgang dauert länger. Die höchste Prioritätsstufe führt zu Änderungen, die System-Performance kann jedoch beeinträchtigt werden.
Caching	Zeigt die Caching-Einstellung, die Sie ändern können, um die gesamte I/O-Performance eines Volumes zu beeinträchtigen.

Einstellung	Beschreibung
SSD Cache	(Diese Funktion ist auf dem EF600 oder EF300-Speichersystem nicht verfügbar.) Zeigt die Einstellung für SSD Cache, die Sie auf kompatiblen Volumes aktivieren können, um die schreibgeschützte Performance zu verbessern. Volumes sind kompatibel, wenn sie sich dieselben Laufwerkssicherheitsfunktionen und Data Assurance nutzen. Die SSD Cache Funktion verwendet eine oder mehrere Solid State Disks (SSDs) zur Implementierung eines Lese-Caches. Die Applikations-Performance wird durch die schnelleren Lesezeiten für SSDs verbessert. Da sich der Lese-Cache im Storage Array befindet, wird das Caching von allen Applikationen genutzt, die das Storage Array verwenden. Wählen Sie einfach das Volume aus, das Sie zwischenspeichern möchten. Caching erfolgt dann automatisch und dynamisch.

6. Klicken Sie Auf **Speichern**.

Ergebnis

Die Lautstärkeeinstellungen werden basierend auf Ihrer Auswahl geändert.

Fügen Sie Volumes zum Workload im SANtricity Speicher-Plug-in für vCenter hinzu

Sie können einem vorhandenen oder neuen Workload nicht zugewiesene Volumes hinzufügen.

Über diese Aufgabe

Volumes sind keinem Workload zugeordnet, wenn sie mithilfe der Befehlszeilenschnittstelle (CLI) erstellt wurden oder aus einem anderen Storage-Array migriert (importiert/exportiert) wurden.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus, das die Volumes enthält, die Sie hinzufügen möchten.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie die Registerkarte * Anwendungen & Workloads* aus.

   Die Ansicht Applikationen und Workloads wird angezeigt.

4. Wählen Sie **zu Workload hinzufügen**.

   Das Dialogfeld „Workload auswählen“ wird angezeigt.

5. Führen Sie eine der folgenden Aktionen aus:
   - **Hinzufügen von Volumes zu einem bestehenden Workload** — Wählen Sie diese Option, um einem vorhandenen Workload Volumes hinzuzufügen. Wählen Sie einen Workload aus der Dropdown-Liste aus. Der zugehörige Applikationstyp des Workloads wird den Volumes zugewiesen, die Sie diesem Workload hinzufügen.
   - **Hinzufügen von Volumes zu einem neuen Workload** — Wählen Sie diese Option aus, um einen neuen Workload für einen Anwendungstyp zu definieren und dem neuen Workload Volumes hinzuzufügen.

6. Wählen Sie **Weiter**, um mit der Add to Workload-Sequenz fortzufahren.

   Das Dialogfeld Volumes auswählen wird angezeigt.

7. Wählen Sie die Volumes aus, die Sie dem Workload hinzufügen möchten.
8. Prüfen Sie die Volumes, die Sie dem ausgewählten Workload hinzufügen möchten.
9. Wenn Sie mit Ihrer Workload-Konfiguration zufrieden sind, klicken Sie auf **Fertig stellen**.

Ändern Sie die Workload-Einstellungen im SANtricity Storage Plug-in für vCenter

Sie können den Namen für einen Workload ändern und den zugehörigen Applikationstyp anzeigen.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus, das den Workload enthält, den Sie ändern möchten.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie die Registerkarte * Anwendungen & Workloads* aus.

   Die Ansicht Applikationen und Workloads wird angezeigt.

4. Wählen Sie den Workload aus, den Sie ändern möchten, und wählen Sie dann **Einstellungen anzeigen/bearbeiten** aus.

   Das Dialogfeld „Anwendungen und Workloads-Einstellungen“ wird angezeigt.

5. (Optional) Ändern Sie den vom Benutzer bereitgestellten Namen des Workloads.
6. Klicken Sie Auf **Speichern**.

Initialisieren Sie Volumes im SANtricity Speicher-Plug-in für vCenter

Ein Volume wird beim ersten Erstellen automatisch initialisiert. Möglicherweise empfiehlt der Recovery Guru jedoch, ein Volume manuell zu initialisieren, um eine Wiederherstellung nach bestimmten Fehlerbedingungen durchzuführen.

Verwenden Sie diese Option nur unter Anleitung des technischen Supports. Sie können ein oder mehrere Volumes für die Initialisierung auswählen.

Bevor Sie beginnen

- Alle I/O-Vorgänge wurden angehalten.
- Alle Geräte oder Dateisysteme auf den Volumes, die Sie initialisieren möchten, müssen abgehängt werden.
- Die Lautstärke ist optimal und es werden keine Änderungsvorgänge auf dem Volume ausgeführt.*Achtung: *Nach dem Start kann der Vorgang nicht mehr abgebrochen werden. Alle Volume-Daten werden gelöscht. Versuchen Sie diese Operation nur, wenn der Recovery Guru Sie dazu rät. Wenden Sie sich vor Beginn dieses Verfahrens an den technischen Support.

Über diese Aufgabe

Bei der Initialisierung eines Volume bleiben die WWN, Host-Zuweisungen, zugewiesene Kapazität und reservierte Kapazität des Volume erhalten. Zudem werden dieselben Data Assurance (da)-Einstellungen und

Sicherheitseinstellungen beibehalten.

Die folgenden Volume-Typen können nicht initialisiert werden:

- Basis-Volume eines Snapshot-Volumes
- Primäres Volume in einer Spiegelbeziehung
- Sekundäres Volume in einer Spiegelbeziehung
- Quell-Volume in einer Volume-Kopie
- Ziel-Volume in einer Volume-Kopie
- Volume, für das bereits eine Initialisierung läuft

Dieser Vorgang gilt nur für Standard-Volumes, die aus Pools oder Volume-Gruppen erstellt wurden.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus, das die Volumes enthält, die Sie initialisieren möchten.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie ein beliebiges Volume aus, und wählen Sie dann Menü:Mehr[Initialisieren von Volumes].

   Das Dialogfeld Volumes initialisieren wird angezeigt. In diesem Dialogfeld werden alle Volumes im Speicher-Array angezeigt.

4. Wählen Sie ein oder mehrere Volumes aus, die Sie initialisieren möchten, und bestätigen Sie, dass Sie den Vorgang durchführen möchten.

Ergebnisse

Das System führt die folgenden Aktionen durch:

- Löscht alle Daten aus den Volumes, die initialisiert wurden.
- Löscht die Blockindizes, was dazu führt, dass nicht geschriebene Blöcke gelesen werden, als ob sie null gefüllt sind (das Volume scheint vollständig leer zu sein).

Dieser Vorgang kann langwierig sein und die System-Performance beeinträchtigen.

Verteilen Sie Volumes im SANtricity Speicher-Plug-in für vCenter neu

Sie verteilen Volumes neu, um Volumes zurück zu ihren bevorzugten Controller-Besitzern zu verschieben. In der Regel verschieben Multipath-Treiber Volumes vom bevorzugten Controller-Eigentümer, wenn entlang des Datenpfads zwischen dem Host und dem Storage Array ein Problem auftritt.

Bevor Sie beginnen

- Die Volumes, die neu verteilt werden sollen, werden nicht verwendet, sonst treten I/O-Fehler auf.
- Ein Multipath-Treiber wird auf allen Hosts installiert, die die Volumes verwenden, die Sie neu verteilen möchten, sonst treten I/O-Fehler auf. Wenn Sie Volumes ohne Multipath-Treiber auf den Hosts neu verteilen möchten, müssen alle I/O-Aktivitäten auf die Volumes während der Umverteilung unterbrochen werden, um Applikationsfehler zu vermeiden.

Über diese Aufgabe

Die meisten Host Multipath-Treiber versuchen, auf jedes Volume auf einem Pfad zu seinem bevorzugten Controller-Eigentümer zuzugreifen. Falls dieser bevorzugte Pfad jedoch nicht mehr verfügbar ist, erfolgt ein Failover des Multipath-Treibers auf dem Host zu einem alternativen Pfad. Dieser Failover kann dazu führen, dass sich die Volume-Inhaberschaft auf den alternativen Controller ändert. Nachdem Sie die Bedingung behoben haben, die den Failover verursacht hat, verschieben einige Hosts möglicherweise automatisch die Volume-Eigentümerschaft zurück zu dem bevorzugten Controller-Eigentümer. In einigen Fällen müssen Sie die Volumes jedoch möglicherweise manuell neu verteilen.

Schritte

1. Wählen Sie auf der Seite Verwalten das Storage-Array aus, das die Volumes enthält, die Sie neu verteilen möchten.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie Menü:Mehr[Umverteilung von Volumes].

   Das Dialogfeld Volumes neu verteilen wird angezeigt. Alle Volumes im Storage-Array, deren bevorzugter Controller-Eigentümer nicht mit dem aktuellen Eigentümer übereinstimmt, werden in diesem Dialogfeld angezeigt.

4. Wählen Sie ein oder mehrere Volumes aus, die Sie neu verteilen möchten, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

Ergebnis

Das System verschiebt die ausgewählten Volumes in die bevorzugten Controller-Eigentümer oder ein Dialogfeld zum Neuverteilen von Volumes ist nicht erforderlich.

Ändern Sie die Controller-Eigentümerschaft eines Volumes im SANtricity-Speicher-Plug-in für vCenter

Sie können den bevorzugten Controller-Besitz eines Volumes ändern, sodass die I/O-Vorgänge für Host-Applikationen durch den neuen Pfad geleitet werden.

Bevor Sie beginnen

Falls Sie keinen Multipath-Treiber verwenden, müssen alle Host-Applikationen, die derzeit das Volume verwenden, heruntergefahren werden. Dadurch werden Anwendungsfehler verhindert, wenn sich der I/O-Pfad ändert.

Über diese Aufgabe

Sie können die Controller-Eigentumsrechte für ein oder mehrere Volumes in einem Pool oder einer Volume-Gruppe ändern.

Schritte

1. Wählen Sie auf der Seite Verwalten das Storage-Array aus, das die Volumes enthält, für die Sie den Controller-Besitz ändern möchten.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie ein beliebiges Volume aus, und wählen Sie dann Menü:Mehr[Eigentümerschaft ändern].

   Das Dialogfeld Volume-Eigentümer ändern wird angezeigt. In diesem Dialogfeld werden alle Volumes im Speicher-Array angezeigt.

4. Verwenden Sie die Dropdown-Liste **bevorzugter Eigentümer**, um den bevorzugten Controller für jedes zu ändernden Volume zu ändern, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

Ergebnisse

- Das System ändert den Controller-Eigentümer des Volume. Die I/O-Vorgänge zum Volume werden jetzt durch diesen I/O-Pfad geleitet.
- Auf dem Volume wird möglicherweise der neue I/O-Pfad erst dann verwendet, wenn der Multipath-Treiber den neuen Pfad erkennt.

Diese Aktion dauert in der Regel weniger als fünf Minuten.

Ändern Sie die Cache-Einstellungen für ein Volume im SANtricity Storage Plug-in für vCenter

Sie können die Einstellungen für den Lese-Cache und den Schreib-Cache ändern, um die gesamte I/O-Performance eines Volumes zu beeinträchtigen.

Über diese Aufgabe

Beachten Sie bei der Änderung der Cache-Einstellungen für ein Volume die folgenden Richtlinien:

- Nach dem Öffnen des Dialogfelds Cache-Einstellungen ändern wird möglicherweise ein Symbol neben den ausgewählten Cache-Eigenschaften angezeigt. Dieses Symbol zeigt an, dass der Controller vorübergehend Zwischenspeichervorgänge ausgesetzt hat. Diese Aktion kann auftreten, wenn ein neuer Akku geladen wird, wenn ein Controller entfernt wurde oder wenn vom Controller eine Diskrepanz bei den Cachegrößen festgestellt wurde. Nach dem Löschen der Bedingung werden die im Dialogfeld ausgewählten Cache-Eigenschaften aktiv. Wenn die ausgewählten Cache-Eigenschaften nicht aktiv werden, wenden Sie sich an den technischen Support.
- Sie können die Cache-Einstellungen für ein einzelnes Volume oder für mehrere Volumes in einem Storage-Array ändern. Sie können die Cache-Einstellungen für alle Volumes gleichzeitig ändern.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus, das die Volumes enthält, für die Sie die Cache-Einstellungen ändern möchten.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie ein beliebiges Volume aus, und wählen Sie dann Menü:Mehr[Cache-Einstellungen ändern].

   Das Dialogfeld Cache-Einstellungen ändern wird angezeigt. In diesem Dialogfeld werden alle Volumes im Speicher-Array angezeigt.

4. Wählen Sie die Registerkarte **Basic**, um die Einstellungen für Lese-Cache und Schreib-Caching zu ändern.

Felddetails

Cache-Einstellung	Beschreibung
Lese-Caching	Der Lese-Cache ist ein Puffer, der Daten speichert, die von den Laufwerken gelesen wurden. Die Daten für einen Lesevorgang befinden sich möglicherweise bereits im Cache eines früheren Vorgangs, sodass kein Zugriff auf die Laufwerke erforderlich ist. Die Daten bleiben so lange im Lese-Cache, bis sie entfernt werden.
Schreib-Caching	Der Schreib-Cache ist ein Puffer, der Daten des Hosts speichert, die noch nicht auf die Laufwerke geschrieben wurden. Die Daten bleiben im Schreib-Cache, bis sie auf die Laufwerke geschrieben werden. Caching von Schreibzugriffen kann die I/O-Performance steigern. Der Cache wird automatisch gespült, nachdem das Write Caching für ein Volume deaktiviert wurde.

5. Wählen Sie die Registerkarte **Erweitert** aus, um die erweiterten Einstellungen für Thick Volumes zu ändern. Die erweiterten Cache-Einstellungen sind nur für Thick Volumes verfügbar.

Felddetails

Einstellung	Beschreibung
Vorwort Für Dynamischen Lese-Cache	Mit dem Dynamic Cache Read Prefetch kann der Controller zusätzliche sequenzielle Datenblöcke in den Cache kopieren, während Datenblöcke von einem Laufwerk in den Cache gelesen werden. Dadurch erhöht sich die Wahrscheinlichkeit, dass zukünftige Datenanfragen aus dem Cache gefüllt werden können. Der dynamische Cache-Lese-Prefetch ist für Multimedia-Anwendungen, die sequenzielle I/O verwenden, wichtig Die Rate und die Menge der Daten, die im Cache abgerufen werden, passen sich automatisch an die Rate und die Anfragegröße des Host-Leseens an. Ein wahlfreier Zugriff bewirkt nicht, dass Daten im Cache abgerufen werden. Diese Funktion gilt nicht, wenn das Lese-Caching deaktiviert ist.
Schreiben Sie das Caching ohne Batterien	Die Einstellung Write Caching ohne Batterien ermöglicht die Fortsetzung des Schreib-Cache auch dann, wenn die Batterien fehlen, ausfallen, vollständig entladen oder nicht vollständig geladen sind. Die Wahl des Schreib-Caching ohne Batterien ist in der Regel nicht empfohlen, da die Daten verloren gehen können, wenn die Stromversorgung verloren geht. In der Regel wird das Schreibcache vorübergehend vom Controller deaktiviert, bis die Akkus geladen sind oder eine fehlerhafte Batterie ausgetauscht wird. ACHTUNG: **Möglicher Datenverlust** — Wenn Sie diese Option wählen und keine universelle Stromversorgung zum Schutz haben, könnten Sie Daten verlieren. Darüber hinaus könnten Sie Daten verlieren, wenn Sie keine Controller-Batterien haben und Sie die Write Caching ohne Batterien Option aktivieren.
Schreib-Caching mit Spiegelung	Das Schreib-Caching mit Spiegelung erfolgt, wenn die Daten, die auf den Cache-Speicher eines Controllers geschrieben wurden, auch in den Cache-Speicher des anderen Controllers geschrieben werden. Wenn also ein Controller ausfällt, kann der andere alle ausstehenden Schreibvorgänge ausführen. Write Cache Mirroring ist nur verfügbar, wenn Write Caching aktiviert ist und zwei Controller vorhanden sind. Schreib-Caching mit Spiegelung ist die Standardeinstellung bei der Volume-Erstellung.

6. Klicken Sie auf **Speichern**, um die Cache-Einstellungen zu ändern.

Ändern Sie die Einstellungen für die Medienscan für ein Volume im SANtricity Speicher-Plug-in für vCenter

Ein Medien-Scan ist ein Hintergrundvorgang, der alle Daten und Redundanzinformationen auf dem Volume scannt. Verwenden Sie diese Option, um die Einstellungen für den Medienscan für ein oder mehrere Volumes zu aktivieren oder zu deaktivieren oder die Scandauer zu ändern.

Bevor Sie beginnen

Verstehen Sie Folgendes:

- Die Medien-Scans werden kontinuierlich mit konstanter Geschwindigkeit ausgeführt, basierend auf der zu scannenden Kapazität und der Scandauer. Hintergrundscans können vorübergehend durch eine Hintergrundaufgabe mit höherer Priorität ausgesetzt werden (z. B. Rekonstruktion), werden aber mit

derselben konstanten Geschwindigkeit fortgesetzt.

- Ein Volume wird nur dann gescannt, wenn die Option zum Scannen von Medien für das Storage-Array und für das entsprechende Volume aktiviert ist. Wenn auch die Redundanzprüfung für das Volume aktiviert ist, werden die Redundanzinformationen auf dem Volume auf Konsistenz mit Daten überprüft, sofern das Volume über Redundanz verfügt. Der Medien-Scan mit Redundanzprüfung ist standardmäßig für jedes Volume bei seiner Erstellung aktiviert.
- Wenn während des Scans ein nicht behebbarer Medienfehler auftritt, werden die Daten gegebenenfalls durch Redundanzinformationen repariert.

  So stehen beispielsweise Informationen zur Redundanz in optimalen RAID 5-Volumes oder in RAID 6-Volumes zur Verfügung, die optimal sind oder nur ein Laufwerk ausfällt. Wenn der nicht behebbare Fehler nicht mithilfe von Redundanzinformationen behoben werden kann, wird der Datenblock zum unlesbaren Sektor-Log hinzugefügt. Das Event-Protokoll wird sowohl korrigierbare als auch nicht korrigierbare Medienfehler gemeldet.

- Wenn die Redundanzprüfung eine Inkonsistenz zwischen Daten und den Redundanzinformationen findet, wird sie dem Ereignisprotokoll gemeldet.

Über diese Aufgabe

Medienprüfungen erkennen und reparieren Medienfehler auf Festplattenlaufwerken, die selten von Applikationen gelesen werden. Dadurch wird Datenverlust bei einem Laufwerksausfall verhindert, da die Daten der ausgefallenen Laufwerke durch Redundanzinformationen und die Daten anderer Laufwerke in der Volume-Gruppe oder dem Pool rekonstruiert werden.

Sie können folgende Aktionen ausführen:

- Aktivieren oder Deaktivieren von Medienprüfungen im Hintergrund für das gesamte Storage-Array
- Ändern Sie die Scandauer für das gesamte Storage Array
- Aktivieren oder deaktivieren Sie die Medienüberprüfung für ein oder mehrere Volumes
- Aktivieren oder deaktivieren Sie die Redundanzprüfung auf ein oder mehrere Volumes

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus, das die Volumes enthält, für die Sie die Einstellungen für die Medienüberprüfung ändern möchten.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Wählen Sie eine beliebige Lautstärke aus, und wählen Sie dann Menü:Mehr[Einstellungen für Medienscan ändern].

   Das Dialogfeld Einstellungen für Laufwerkmedienscan ändern wird angezeigt. In diesem Dialogfeld werden alle Volumes im Speicher-Array angezeigt.

4. Um den Medienscan zu aktivieren, aktivieren Sie das Kontrollkästchen **Medien scannen über…**. Wenn Sie das Kontrollkästchen Medien-Scan deaktivieren, werden alle Einstellungen für den Medienscan unterbrochen.
5. Geben Sie die Anzahl der Tage an, über die der Medienscan ausgeführt werden soll.
6. Aktivieren Sie das Kontrollkästchen **Media Scan** für jedes Volume, auf dem Sie einen Medien-Scan durchführen möchten. Das System aktiviert die Option Redundanzprüfung für jedes Volume, auf dem Sie einen Medien-Scan ausführen möchten. Wenn es einzelne Volumes gibt, für die Sie keine Redundanzprüfung durchführen möchten, deaktivieren Sie das Kontrollkästchen **Redundanzprüfung**.
7. Klicken Sie Auf **Speichern**.

Ergebnis

Das System wendet basierend auf Ihrer Auswahl Änderungen an Medien-Scans im Hintergrund an.

Löschen Sie das Volume im SANtricity Speicher-Plug-in für vCenter

Sie können ein oder mehrere Volumes löschen, um die freie Kapazität eines Pools oder einer Volume-Gruppe zu erhöhen.

Bevor Sie beginnen

Stellen Sie bei den zu löschenden Volumes Folgendes sicher:

- Alle Daten werden gesichert.
- Alle Eingänge/Ausgänge (E/A) werden angehalten.
- Alle Geräte und Dateisysteme werden abgehängt.

Über diese Aufgabe

Normalerweise löschen Sie Volumes, wenn die Volumes mit falschen Parametern oder Kapazität erstellt wurden oder die Anforderungen der Storage-Konfiguration nicht mehr erfüllt werden. Durch das Löschen eines Volumes wird die freie Kapazität im Pool oder der Volume-Gruppe erhöht.

Das Löschen eines Volumes verursacht den Verlust aller Daten auf diesen Volumes.

Beachten Sie, dass Sie * ein Volume mit einer der folgenden Bedingungen nicht löschen können:

- Das Volume wird initialisiert.
- Das Volume wird wiederhergestellt.
- Das Volume ist Teil einer Volume-Gruppe, die ein Laufwerk enthält, das einen Copyback-Vorgang durchläuft.
- Das Volume wird in einem Änderungsvorgang wie z. B. einer Änderung der Segmentgröße ausgeführt, sofern sich das Volume jetzt nicht mehr im Status „ausgefallen“ befindet.
- Das Volume hält jede Art von persistenter Reservierung.
- Das Volume ist ein Quell-Volume oder ein Ziel-Volume in einem Copy-Volume mit dem Status „Ausstehend“, „in Bearbeitung“ oder „fehlgeschlagen“.

Wenn ein Volume eine bestimmte Größe überschreitet (derzeit 128 TB), wird der Löschvorgang im Hintergrund durchgeführt, wobei der freigegebene Speicherplatz möglicherweise nicht sofort verfügbar ist.

Schritte

1. Wählen Sie auf der Seite **Verwalten** das Speicher-Array aus, das die Volumes enthält, die Sie löschen möchten.
2. Wählen Sie MENU:Provisioning[Volumes verwalten].
3. Klicken Sie Auf **Löschen**.

   Das Dialogfeld Volumes löschen wird angezeigt.

4. Wählen Sie ein oder mehrere Volumes aus, die Sie löschen möchten, und bestätigen Sie anschließend, dass Sie den Vorgang ausführen möchten.

5. Klicken Sie Auf **Löschen**.

Hosts konfigurieren

Erfahren Sie mehr über die Hosterstellung im SANtricity Speicher-Plug-in für vCenter

Für das Storage-Management mit dem Storage Plug-in für vCenter müssen Sie jeden Host im Netzwerk ermitteln oder definieren. Ein Host ist ein Server, der I/O an ein Volume auf einem Storage-Array sendet.

Manuelle Hosterstellung

Das Erstellen eines Hosts ist einer der Schritte, die erforderlich sind, damit das Storage-Array wissen kann, an welche Hosts angeschlossen sind und um den I/O-Zugriff auf die Volumes zu ermöglichen. Ein Host kann manuell erstellt werden.

- **Manuell** — während der manuellen Hosterstellung verknüpfen Sie Host-Port-IDs, indem Sie sie aus einer Liste auswählen oder manuell eingeben. Nachdem Sie einen Host erstellt haben, können Sie ihm Volumes zuweisen oder einem Host Cluster hinzufügen, wenn Sie den Zugriff auf Volumes freigeben möchten.

Wie Volumes zugewiesen werden

Damit ein Host I/O an ein Volume sendet, müssen Sie das Volume ihm zuweisen. Sie können entweder einen Host oder ein Host-Cluster auswählen, wenn Sie ein Volume erstellen, oder Sie können ein Volume später einem Host oder Host-Cluster zuweisen. Ein Host-Cluster ist eine Gruppe von Hosts. Sie erstellen ein Host-Cluster, damit Sie mehrere Hosts dieselben Volumes ganz einfach zuweisen können.

Das Zuweisen von Volumes zu Hosts ist flexibel und somit an Ihre spezifischen Storage-Anforderungen angepasst.

- **Stand-alone Host, nicht Teil eines Host Clusters** — Sie können ein Volume einem einzelnen Host zuweisen. Auf das Volume kann nur von einem Host zugegriffen werden.
- **Host Cluster** — Sie können ein Volume einem Host-Cluster zuweisen. Auf das Volume kann von allen Hosts im Host-Cluster zugegriffen werden.
- **Host innerhalb eines Host-Clusters** — Sie können ein Volume einem einzelnen Host zuweisen, der Teil eines Host-Clusters ist. Obwohl der Host Teil eines Host Clusters ist, kann das Volume nur vom individuellen Host und nicht von anderen Hosts im Host-Cluster abgerufen werden.

Bei Erstellung von Volumes werden automatisch LUNs (Logical Unit Numbers) zugewiesen. Die LUN dient als Adresse zwischen dem Host und dem Controller während I/O-Vorgängen. Sie können LUNs nach der Erstellung des Volume ändern.

Erstellen Sie den Hostzugriff im SANtricity Speicher-Plug-in für vCenter

Für das Storage-Management mit dem Storage Plug-in für vCenter müssen Sie jeden Host im Netzwerk ermitteln oder definieren.

Über diese Aufgabe

Durch die Erstellung eines Hosts definieren Sie die Hostparameter, um eine Verbindung zum Speicher-Array und I/O-Zugriff auf die Volumes herzustellen.

Wenn Sie einen Host erstellen, beachten Sie folgende Richtlinien:

- Sie müssen die dem Host zugeordneten Host-Identifier-Ports definieren.
- Stellen Sie sicher, dass Sie denselben Namen wie den zugewiesenen Systemnamen des Hosts angeben.
- Dieser Vorgang ist nicht erfolgreich, wenn der gewählte Name bereits verwendet wird.
- Die Länge des Namens darf nicht mehr als 30 Zeichen umfassen.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit der Hostverbindung aus.
2. Wählen Sie Menü:Bereitstellung [Hosts konfigurieren].

   Die Seite Hosts konfigurieren wird geöffnet.

3. Klicken Sie auf Menü:Create[Host].

   Das Dialogfeld Host erstellen wird angezeigt.

4. Wählen Sie die entsprechenden Einstellungen für den Host aus.

Felddetails

Einstellung	Beschreibung
Name	Geben Sie einen Namen für den neuen Host ein.
Host-Betriebssystem-Typ	Wählen Sie aus der Dropdown-Liste das auf dem neuen Host ausgeführte Betriebssystem aus.
Host-Schnittstellentyp	(Optional) Wenn auf Ihrem Speicherarray mehr als eine Host-Schnittstelle unterstützt wird, wählen Sie den Host-Schnittstellentyp aus, den Sie verwenden möchten.
Host-Ports	Führen Sie einen der folgenden Schritte aus: • **I/O-Schnittstelle auswählen** — generell sollten sich die Host-Ports angemeldet haben und über die Dropdown-Liste verfügbar sein. Sie können die Host-Port-IDs aus der Liste auswählen. • **Manuelles Hinzufügen** — Wenn eine Host-Port-ID nicht in der Liste angezeigt wird, bedeutet dies, dass der Host-Port nicht angemeldet ist. Mithilfe eines HBA-Dienstprogramms oder des iSCSI-Initiator-Dienstprogramms können die Host-Port-IDs ermittelt und mit dem Host verknüpft werden. Sie können die Host-Port-IDs manuell eingeben oder sie aus dem Dienstprogramm (nacheinander) in das Feld Host-Ports kopieren/einfügen. Sie müssen eine Host-Port-ID gleichzeitig auswählen, um sie dem Host zuzuordnen. Sie können jedoch weiterhin so viele Kennungen auswählen, die dem Host zugeordnet sind. Jede Kennung wird im Feld Host-Ports angezeigt. Bei Bedarf können Sie auch einen Bezeichner entfernen, indem Sie neben ihm die **X**-Option auswählen.
Legen Sie den CHAP-Initiatorschlüssel fest	(Optional) Wenn Sie einen Host-Port mit einem iSCSI-IQN ausgewählt oder manuell eingegeben haben und wenn Sie einen Host benötigen möchten, der versucht, auf das Speicher-Array zuzugreifen, um sich mit dem Challenge Handshake Authentication Protocol (CHAP) zu authentifizieren, aktivieren Sie das Kontrollkästchen „CHAP Initiator Secret festlegen“. Gehen Sie für jeden ausgewählten oder manuell eingegebenen iSCSI-Host-Port wie folgt vor: • Geben Sie denselben CHAP-Schlüssel ein, der auf jedem iSCSI-Hostinitiator für die CHAP-Authentifizierung festgelegt wurde. Wenn Sie die gegenseitige CHAP-Authentifizierung verwenden (zwei-Wege-Authentifizierung, die es einem Host ermöglicht, sich am Speicher-Array zu validieren, und damit sich ein Speicher-Array am Host validieren kann), müssen Sie auch den CHAP-Schlüssel für das Speicher-Array bei der Ersteinrichtung oder durch Ändern von Einstellungen festlegen. • Wenn Sie keine Host-Authentifizierung benötigen, lassen Sie das Feld leer. Derzeit wird nur CHAP verwendet.

5. Klicken Sie Auf **Erstellen**.
6. Wenn Sie die Hostinformationen aktualisieren müssen, wählen Sie den Host aus der Tabelle aus und klicken Sie auf **Einstellungen anzeigen/bearbeiten**.

Ergebnis

Nachdem der Host erfolgreich erstellt wurde, erstellt das System für jeden Host-Port, der für den Host konfiguriert wurde (Benutzungsbezeichnung) einen Standardnamen. Der Standard-Alias ist `<Hostname_Port Number>`. Der Standard-Alias für den ersten Port, der für das Host-IPT erstellt wurde, ist beispielsweise `IPT_1`.

Nachdem Sie fertig sind

Sie müssen ein Volume einem Host zuweisen, damit es für I/O-Vorgänge verwendet werden kann. Gehen Sie zu "Weisen Sie Hosts Volumes zu".

Erstellen Sie im SANtricity-Speichermodul für vCenter einen Hostcluster

Wenn zwei oder mehr Hosts I/O-Zugriff auf dieselben Volumes benötigen, können Sie ein Host-Cluster erstellen.

Über diese Aufgabe

Beachten Sie beim Erstellen eines Host-Clusters die folgenden Richtlinien:

- Dieser Vorgang startet nicht, wenn zum Erstellen des Clusters zwei oder mehr Hosts zur Verfügung stehen.
- Hosts in Host-Clustern können verschiedene Betriebssysteme (heterogen) haben.
- NVMe-Hosts in Host-Clustern können nicht mit nicht-NVMe-Hosts kombiniert werden.
- Um ein für Data Assurance (da) fähiges Volume zu erstellen, muss die Host-Verbindung, die Sie verwenden möchten, da unterstützen.

  Wenn eine der Host-Verbindungen auf den Controllern im Speicher-Array keine Unterstützung für da bietet, können die zugeordneten Hosts auf da-fähige Volumes keinen Zugriff auf Daten haben.

- Dieser Vorgang ist nicht erfolgreich, wenn der gewählte Name bereits verwendet wird.
- Die Länge des Namens darf nicht mehr als 30 Zeichen umfassen.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit der Hostverbindung aus.
2. Wählen Sie Menü:Bereitstellung [Hosts konfigurieren].

   Die Seite Hosts konfigurieren wird geöffnet.

3. Wählen Sie Menü:Create[Host Cluster].

   Das Dialogfeld Host-Cluster erstellen wird angezeigt.

4. Wählen Sie die entsprechenden Einstellungen für den Host-Cluster aus.

Einstellung	Beschreibung
Name	Geben Sie den Namen für das neue Host-Cluster ein.
Wählen Sie Hosts aus, die den Zugriff auf das Volume gemeinsam nutzen sollen	Wählen Sie zwei oder mehr Hosts aus der Dropdown-Liste aus. In der Liste werden nur die Hosts angezeigt, die nicht bereits Teil eines Host-Clusters sind.

5. Klicken Sie Auf **Erstellen**.

   Wenn die ausgewählten Hosts an Schnittstellentypen mit unterschiedlichen Funktionen zur Data Assurance (da) angeschlossen sind, wird ein Dialogfeld mit der Meldung angezeigt, dass da auf dem Host-Cluster nicht verfügbar ist. Durch diese Nichtverfügbarkeit wird verhindert, dass dem Host-Cluster DA-fähige Volumes hinzugefügt werden. Wählen Sie **Ja**, um fortzufahren, oder **Nein**, um den Vorgang abzubrechen.

   DA erhöht die Datenintegrität im gesamten Storage-System. DA ermöglicht es dem Storage-Array, nach Fehlern zu suchen, die auftreten können, wenn Daten zwischen Hosts und Laufwerken verschoben werden. Die Verwendung von da für das neue Volume stellt sicher, dass alle Fehler erkannt werden.

Ergebnis

Der neue Hostcluster wird in der Tabelle mit den zugewiesenen Hosts in den Zeilen darunter angezeigt.

Nachdem Sie fertig sind

Sie müssen ein Volume einem Host-Cluster zuweisen, damit es für I/O-Vorgänge verwendet werden kann. Gehen Sie zu "Weisen Sie Hosts Volumes zu".

Weisen Sie Hosts im SANtricity Speicher-Plug-in für vCenter Volumes zu

Sie müssen ein Volume einem Host oder Host-Cluster zuweisen, damit es für I/O-Vorgänge verwendet werden kann.

Bevor Sie beginnen

Beachten Sie bei der Zuweisung von Volumes zu Hosts die folgenden Richtlinien:

- Sie können ein Volume gleichzeitig nur einem Host oder Host-Cluster zuweisen.
- Zugewiesene Volumes werden von den Controllern im Storage-Array gemeinsam genutzt.
- Die gleiche Logical Unit Number (LUN) kann nicht zweimal von einem Host oder einem Host-Cluster verwendet werden, um auf ein Volume zuzugreifen. Sie müssen eine eindeutige LUN verwenden.
- Wenn Sie bei neuen Volume-Gruppen warten, bis alle Volumes erstellt und initialisiert wurden, bevor Sie sie einem Host zuweisen, wird die Initialisierungszeit des Volumes verkürzt. Beachten Sie, dass sobald ein mit der Volume-Gruppe assoziiertes Volume zugeordnet ist, alle Volumes auf die langsamere Initialisierung zurückgesetzt werden.

Über diese Aufgabe

Eine Volume-Zuweisung gewährt einem Host oder Host-Cluster Zugriff auf dieses Volume in einem Storage-Array.

Während dieser Aufgabe werden alle nicht zugewiesenen Volumes angezeigt, aber Funktionen für Hosts mit oder ohne Data Assurance (da) gelten wie folgt:

- Für einen da-fähigen Host können Sie Volumes auswählen, die entweder als da aktiviert oder nicht als da-aktiviert aktiviert sind.
- Wenn Sie bei einem Host, der nicht für das da-fähig ist, ein Volume auswählen, das für das da-aktiviert ist, wird in einer Warnung angegeben, dass das System vor der Zuweisung des Volumes automatisch das da-on-Volume ausschalten muss.

  Unter diesen Bedingungen schlägt die Zuweisung eines Volumes fehl:

- Alle Volumes werden zugewiesen.
- Das Volume ist bereits einem anderen Host oder Host-Cluster zugewiesen. Die Möglichkeit, ein Volume zuzuweisen, ist unter folgenden Bedingungen nicht verfügbar:
- Es sind keine gültigen Hosts oder Host Cluster vorhanden.
- Für den Host wurden keine Host-Port-IDs definiert.
- Alle Volume-Zuweisungen wurden definiert.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit der Hostverbindung aus.
2. Wählen Sie Menü:Bereitstellung [Hosts konfigurieren].

   Die Seite Hosts konfigurieren wird geöffnet.

3. Wählen Sie den Host oder Host-Cluster aus, dem Sie Volumes zuweisen möchten, und klicken Sie dann auf **Volumes zuweisen**.

   Es wird ein Dialogfeld angezeigt, in dem alle Volumes aufgelistet werden, die zugewiesen werden können. Sie können jede der Spalten sortieren oder etwas in das Filter-Feld eingeben, um bestimmte Volumes einfacher zu finden.

4. Aktivieren Sie das Kontrollkästchen neben jedem Volume, das Sie zuweisen möchten, oder aktivieren Sie das Kontrollkästchen in der Tabellenüberschrift, um alle Volumes auszuwählen.
5. Klicken Sie auf **Zuweisen**, um den Vorgang abzuschließen.

Ergebnisse

Nachdem ein Volume oder ein Volume erfolgreich einem Host oder Host-Cluster zugewiesen wurde, führt das System folgende Aktionen durch:

- Das zugewiesene Volume erhält die nächste verfügbare LUN-Nummer. Der Host verwendet die LUN-Nummer für den Zugriff auf das Volume.
- Der vom Benutzer bereitgestellte Volume-Name wird in den Volume-Listen angezeigt, die dem Host zugeordnet sind. Falls zutreffend, wird das werkseitig konfigurierte Zugriffsvolume auch in den Volume-Listen angezeigt, die dem Host zugeordnet sind.

Heben Sie die Zuweisung von Volumes im SANtricity Speicher-Plug-in für vCenter auf

Wenn Sie keinen I/O-Zugriff mehr auf ein Volume benötigen, können Sie die Zuweisung vom Host oder Host-Cluster aufheben.

Über diese Aufgabe

Beachten Sie bei der Zuweisung von Volumes die folgenden Richtlinien:

- Wenn Sie das zuletzt zugewiesene Volume aus einem Host-Cluster entfernen und zudem über Hosts mit spezifischen zugewiesenen Volumes verfügen, stellen Sie sicher, dass Sie diese Zuweisungen entfernen oder verschieben, bevor Sie die letzte Zuweisung für den Host-Cluster entfernen.
- Wenn ein Host-Cluster, ein Host oder ein Host-Port einem Volume zugewiesen ist, das beim Betriebssystem registriert ist, müssen Sie diese Registrierung löschen, bevor Sie diese Knoten entfernen können.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit der Hostverbindung aus.
2. Wählen Sie Menü:Bereitstellung [Hosts konfigurieren].

   Die Seite Hosts konfigurieren wird geöffnet.

3. Wählen Sie den Host oder Host-Cluster aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Zuweisen von Volumes**.

   Es wird ein Dialogfeld angezeigt, in dem alle Volumes angezeigt werden, die derzeit zugewiesen sind.

4. Aktivieren Sie das Kontrollkästchen neben jedem Volume, das Sie aufheben möchten, oder aktivieren Sie das Kontrollkästchen in der Tabellenüberschrift, um alle Volumes auszuwählen.
5. Klicken Sie Auf **Zuweisung Aufheben**.

Ergebnisse

- Die nicht zugewiesenen Volumes sind für eine neue Zuweisung verfügbar.
- Bis die Änderungen auf dem Host konfiguriert sind, wird das Volume weiterhin vom Host-Betriebssystem erkannt.

Ändern Sie die Einstellungen für einen Host im SANtricity Speicher-Plug-in für vCenter

Sie können den Namen, den Host-Betriebssystem-Typ und die zugehörigen Host-Cluster für einen Host oder Host-Cluster ändern.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit der Hostverbindung aus.
2. Wählen Sie Menü:Bereitstellung [Hosts konfigurieren].

   Die Seite Hosts konfigurieren wird geöffnet.

3. Wählen Sie den Host aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Es wird ein Dialogfeld angezeigt, in dem die aktuellen Hosteinstellungen angezeigt werden.

4. Um die Host-Eigenschaften zu ändern, stellen Sie sicher, dass die Registerkarte **Eigenschaften** ausgewählt ist, und ändern Sie dann die entsprechenden Einstellungen.

Felddetails

Einstellung	Beschreibung
Name	Sie können den vom Benutzer bereitgestellten Namen des Hosts ändern. Die Angabe eines Namens für den Host ist erforderlich.
Zugehöriger Host-Cluster	Sie können eine der folgenden Optionen auswählen: • **Keine** — der Host bleibt ein eigenständiger Host. Wenn der Host einem Host-Cluster zugewiesen war, wird der Host vom Cluster entfernt. • **<Host Cluster>** — das System ordnet den Host dem ausgewählten Cluster zu.
Host-Betriebssystem-Typ	Sie können den Typ des Betriebssystems ändern, das auf dem von Ihnen definierten Host ausgeführt wird.

5. Um die Porteinstellungen zu ändern, klicken Sie auf die Registerkarte **Host Ports** und ändern Sie dann die entsprechenden Einstellungen.

Felddetails

Einstellung	Beschreibung
Host Port	Sie können eine der folgenden Optionen auswählen: • **Add** — Verwenden Sie Add, um dem Host eine neue Host-Port-ID zuzuordnen. Die Länge des Namens der Host-Port-Kennung wird durch die Host-Schnittstellentechnologie bestimmt. Die Namen der Fibre Channel- und InfiniBand-Host-Port-ID müssen 16 Zeichen lang sein. Die Namen der iSCSI-Host-Port-ID dürfen maximal 223 Zeichen lang sein. Der Port muss eindeutig sein. Eine bereits konfigurierte Portnummer ist nicht zulässig. • **Löschen** — Verwenden Sie Löschen, um eine Host-Port-ID zu entfernen (Zuordnung aufheben). Mit der Option Löschen wird der Host-Port nicht physisch entfernt. Mit dieser Option wird die Zuordnung zwischen dem Host-Port und dem Host entfernt. Sofern Sie den Host Bus Adapter oder den iSCSI-Initiator nicht entfernen, wird der Host-Port noch vom Controller erkannt. Wenn Sie eine Host-Port-ID löschen, ist sie diesem Host nicht mehr zugeordnet. Darüber hinaus verliert der Host über diese Host-Port-Kennung den Zugriff auf jedes seiner zugewiesenen Volumes.
Etikett	Um den Namen der Portbezeichnung zu ändern, klicken Sie auf das Symbol **Bearbeiten** (Bleistift). Der Name des Port-Etiketts muss eindeutig sein. Ein bereits konfigurierter Etikettenname ist nicht zulässig.
CHAP-Schlüssel	Erscheint nur für iSCSI-Hosts. Sie können den CHAP-Schlüssel für die Initiatoren (iSCSI-Hosts) festlegen oder ändern. Das System verwendet die CHAP-Methode (Challenge Handshake Authentication Protocol), mit der die Identität von Zielen und Initiatoren während der ersten Verbindung überprüft wird. Die Authentifizierung basiert auf einem gemeinsamen Sicherheitsschlüssel, dem CHAP-Schlüssel.

6. Klicken Sie Auf **Speichern**.

Löschen Sie einen Host oder einen Host-Cluster im SANtricity-Speicher-Plug-in für vCenter

Sie können einen Host oder Host-Cluster entfernen, sodass Volumes diesem Host nicht mehr zugewiesen sind.

Über diese Aufgabe

Beachten Sie beim Löschen eines Hosts oder Host-Clusters folgende Richtlinien:

- Alle spezifischen Volume-Zuweisungen werden gelöscht, und die zugeordneten Volumes stehen für eine neue Zuweisung zur Verfügung.
- Wenn der Host Teil eines Hostclusters ist, das seine eigenen spezifischen Zuweisungen hat, ist der Host-Cluster nicht betroffen. Wenn der Host jedoch Teil eines Host-Clusters ist, das keine anderen Zuweisungen

besitzt, übernehmen der Host-Cluster und andere zugeordnete Hosts oder Host-Port-IDs die Standardzuweisungen.

- Alle dem Host zugeordneten Host-Port-IDs werden undefiniert.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit der Hostverbindung aus.
2. Wählen Sie Menü:Bereitstellung [Hosts konfigurieren].

   Die Seite Hosts konfigurieren wird geöffnet.

3. Wählen Sie den Host oder Host-Cluster aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.

   Das Bestätigungsdialogfeld wird angezeigt.

4. Bestätigen Sie, dass Sie den Vorgang ausführen möchten, und klicken Sie dann auf **Löschen**.

Ergebnisse

Wenn Sie einen Host gelöscht haben, führt das System die folgenden Aktionen durch:

- Löscht den Host und entfernt ihn ggf. aus dem Host-Cluster.
- Entfernt den Zugriff auf alle zugewiesenen Volumes.
- Gibt die zugeordneten Volumes in einen nicht zugewiesenen Status zurück.
- Gibt alle dem Host zugeordneten Host-Port-IDs in einen nicht zugeordneten Status zurück. Wenn Sie ein Host-Cluster gelöscht haben, führt das System die folgenden Aktionen aus:
  - Löscht das Host-Cluster und die zugehörigen Hosts (falls vorhanden).
  - Entfernt den Zugriff auf alle zugewiesenen Volumes.
  - Gibt die zugeordneten Volumes in einen nicht zugewiesenen Status zurück.
  - Gibt alle Host-Port-IDs zurück, die den Hosts zugeordnet sind, in einen nicht zugeordneten Status.

Konfiguration von Pools und Volume-Gruppen

Informieren Sie sich im SANtricity Storage Plug-in für vCenter über Speicherpools und Volume-Gruppen

Um Speicher im Speicher-Plugin für vCenter bereitzustellen, erstellen Sie entweder einen Pool oder eine Volume-Gruppe, die die Festplatten (HDD) oder Solid State Disk (SSD) Laufwerke enthalten, die Sie in Ihrem Speicher-Array verwenden möchten.

Bereitstellung

Physische Hardware wird in logischen Komponenten bereitgestellt, sodass Daten organisiert und einfach abgerufen werden können. Es werden zwei Arten von Gruppierungen unterstützt:

- Pools
- Volume-Gruppen

Pools und Volume-Gruppen sind die obersten Storage-Einheiten in einem Storage Array: Sie teilen die Kapazität von Laufwerken in einfach zu verwaltende Abteilungen. Innerhalb dieser logischen Unterteilungen sind die einzelnen Volumes oder LUNs, in denen die Daten gespeichert werden.

Wenn ein Storage-System implementiert wird, müssen die verschiedenen Hosts über die verfügbare Laufwerkskapazität verfügen:

- Erstellen von Pools oder Volume-Gruppen mit ausreichender Kapazität
- Fügen Sie die Anzahl der erforderlichen Laufwerke hinzu, um den Performance-Anforderungen des Pools oder der Volume-Gruppe zu entsprechen
- Wählen Sie die gewünschte RAID-Schutzstufe (bei Nutzung der Volume-Gruppen) aus, um den spezifischen geschäftlichen Anforderungen gerecht zu werden

Es können zwar Pools oder Volume-Gruppen auf demselben Speichersystem vorhanden sein, ein Laufwerk kann jedoch nicht mehr als ein Pool oder eine Volume-Gruppe umfassen. Volumes, die Hosts für I/O-Vorgänge zur Verfügung gestellt werden, werden dann unter Verwendung des Speicherplatzes im Pool oder der Volume-Gruppe erstellt.

Pools

Pools wurden entwickelt, um physische Festplatten in einem großen Storage-Bereich zu aggregieren und bieten dafür besseren RAID-Schutz. Ein Pool erstellt viele virtuelle RAID-Sätze von der Gesamtzahl der Laufwerke, die dem Pool zugewiesen sind. Dabei werden die Daten gleichmäßig auf alle teilnehmenden Laufwerke verteilt. Wenn ein Laufwerk verloren geht oder hinzugefügt wird, gleicht das System die Daten dynamisch über alle aktiven Laufwerke aus.

Pools funktionieren als weitere RAID-Ebene und virtualisieren die zugrunde liegende RAID-Architektur, um die Performance und Flexibilität bei Aufgaben wie Neuaufbau, Laufwerkserweiterung und Handhabung von Laufwerksausfällen zu optimieren. Das System legt den RAID-Level in einer 8+2-Konfiguration automatisch auf 6 fest (acht Datenfestplatten plus zwei Paritätslaufwerke).

Abstimmung des Laufwerks

Es besteht die Möglichkeit, entweder HDDs oder SSDs zur Nutzung in Pools zur Verfügung zu stellen. Allerdings müssen wie bei Volume-Gruppen alle Laufwerke im Pool dieselbe Technologie verwenden. Die Controller wählen automatisch aus, welche Laufwerke enthalten sollen. Sie müssen daher sicherstellen, dass Sie über eine ausreichende Anzahl an Laufwerken für die von Ihnen gewählte Technologie verfügen.

Verwalten ausgefallener Laufwerke

Pools haben eine minimale Kapazität von 11 Laufwerken; allerdings ist die Kapazität eines Laufwerks im Wert von einer Ersatzkapazität bei einem Laufwerksausfall reserviert. Diese freie Kapazität wird als „Erhaltungskapazität“ bezeichnet.

Wenn Pools erstellt werden, wird eine bestimmte Menge an Kapazität für den Notfall-Einsatz erhalten. Diese Kapazität wird in Form einer Anzahl von Laufwerken ausgedrückt, die tatsächliche Implementierung wird jedoch über alle Festplatten-Pools hinweg verteilt. Die vorbehaltenen Kapazitätsmengen basieren auf der Anzahl der Laufwerke im Pool.

Nach der Erstellung des Pools können Sie den Wert der Erhaltungskapazität auf mehr oder weniger Kapazität ändern oder sogar auf keine Erhaltungskapazität einstellen (Wert 0 Laufwerk). Die maximale Kapazität, die erhalten bleiben kann (ausgedrückt als Anzahl an Laufwerken), ist 10, die verfügbare Kapazität kann jedoch aufgrund der Gesamtzahl der Laufwerke im Pool kleiner sein.

Volume-Gruppen

Volume-Gruppen definieren, wie Kapazität im Storage-System Volumes zugewiesen wird. Festplattenlaufwerke sind in RAID-Gruppen eingeteilt und Volumes befinden sich über die Laufwerke in einer RAID-Gruppe hinweg.

Aus diesem Grund identifizieren die Konfigurationseinstellungen der Volume-Gruppe, welche Laufwerke Teil der Gruppe sind und welches RAID-Level verwendet wird.

Wenn Sie eine Volume-Gruppe erstellen, wählen Controller automatisch die Laufwerke aus, die in die Gruppe aufgenommen werden sollen. Sie müssen manuell die RAID-Ebene für die Gruppe auswählen. Die Kapazität der Volume-Gruppe entspricht der Gesamtzahl der ausgewählten Laufwerke, multipliziert mit ihrer Kapazität.

Abstimmung des Laufwerks

Für die Größe und Performance müssen die Laufwerke in der Volume-Gruppe übereinstimmen. Wenn in der Volume-Gruppe kleinere und größere Laufwerke vorhanden sind, werden alle Laufwerke als die kleinste Kapazitätsgröße erkannt. Wenn es langsamere und schnellere Laufwerke in der Volume-Gruppe gibt, werden alle Laufwerke mit der langsamsten Geschwindigkeit erkannt. Diese Faktoren wirken sich auf die Performance und die Gesamtkapazität des Storage-Systems aus.

Es ist nicht möglich, unterschiedliche Laufwerktechnologien (HDD- und SSD-Laufwerke) miteinander zu kombinieren. RAID 3, 5 und 6 sind auf maximal 30 Laufwerke begrenzt. RAID 1 und RAID 10 verwenden eine Spiegelung, daher müssen diese Volume-Gruppen eine gleichmäßige Anzahl an Festplatten aufweisen.

Verwalten ausgefallener Laufwerke

Volume-Gruppen verwenden Hot-Spare-Laufwerke als Standby, falls ein Laufwerk in RAID 1/10-, RAID 3-, RAID 5- oder RAID 6-Volumes einer Volume-Gruppe ausfällt. Ein Hot-Spare-Laufwerk enthält keine Daten und fügt Ihrem Speicher-Array eine weitere Ebene von Redundanz hinzu.

Wenn ein Laufwerk im Speicher-Array ausfällt, wird das Hot-Spare-Laufwerk automatisch durch das ausgefallene Laufwerk ersetzt, ohne dass ein physischer Austausch erforderlich ist. Wenn das Hot-Spare-Laufwerk verfügbar ist, wenn ein Laufwerk ausfällt, verwendet der Controller Redundanzdaten, um die Daten von dem ausgefallenen Laufwerk auf dem Hot-Spare-Laufwerk zu rekonstruieren.

Entscheiden Sie, ob Pools oder Volume-Gruppen verwendet werden sollen

Wählen Sie einen Pool aus

- Wenn Sie schnellere Laufwerk-Rebuilds und eine vereinfachte Storage-Administration benötigen, und/oder einen hochzufälligen Workload haben.
- Wenn Sie die Daten für jedes Volume zufällig über eine Gruppe von Laufwerken verteilen möchten, die den Pool umfassen.Sie können das RAID-Level von Pools oder die Volumes in den Pools nicht festlegen oder ändern. Pools verwenden RAID Level 6.

Wählen Sie eine Volume-Gruppe aus

- Wenn Sie die maximale Netzwerkbandbreite des Systems benötigen, die Möglichkeit zur Anpassung von Storage-Einstellungen und einen stark sequenziellen Workload benötigen.
- Wenn Sie die Daten basierend auf RAID-Level über die Laufwerke verteilen möchten. Sie können den RAID-Level beim Erstellen der Volume-Gruppe angeben.
- Wenn Sie die Daten für jedes Volume sequenziell über die Laufwerke schreiben möchten, die die Volume-Gruppe umfassen.

Da Pools mit Volume-Gruppen nebeneinander bestehen können, kann ein Storage-Array sowohl Pools als auch Volume-Gruppen enthalten.

Automatische Erstellung von Pools gegenüber manueller Poolanlage

Je nach Ihrer Storage-Konfiguration können Sie es dem System ermöglichen, automatisch Pools zu erstellen, oder Sie können sie manuell selbst erstellen. Ein Pool ist eine Gruppe von logisch gruppierten Laufwerken.

Bevor Sie Pools erstellen und verwalten, prüfen Sie die folgenden Abschnitte, wie Pools automatisch erstellt werden und wann Sie sie möglicherweise manuell erstellen müssen.

Automatische Erstellung

Wenn das System nicht zugewiesene Kapazitäten im Speicher-Array erkennt, wird die automatische Poolerstellung initiiert, wenn das System nicht zugewiesene Kapazitäten in einem Speicher-Array erkennt. Sie werden automatisch aufgefordert, einen oder mehrere Pools zu erstellen, oder die nicht zugewiesene Kapazität einem vorhandenen oder beiden Pool hinzuzufügen.

Automatische Poolerstellung tritt auf, wenn eine dieser Bedingungen zutrifft:

- Pools sind nicht im Speicher-Array vorhanden, und es gibt genügend ähnliche Laufwerke, um einen neuen Pool zu erstellen.
- Neue Laufwerke werden einem Storage-Array hinzugefügt, das mindestens einen Pool hat.jedes Laufwerk in einem Pool muss vom gleichen Laufwerkstyp (HDD oder SSD) sein und eine ähnliche Kapazität haben. Sie werden vom System aufgefordert, die folgenden Aufgaben auszuführen:
- Erstellen Sie einen einzelnen Pool, wenn eine ausreichende Anzahl von Laufwerken dieser Typen vorhanden ist.
- Erstellen Sie mehrere Pools, wenn die nicht zugewiesene Kapazität aus verschiedenen Laufwerkstypen besteht.
- Fügen Sie die Laufwerke zum vorhandenen Pool hinzu, wenn bereits ein Pool im Speicher-Array definiert ist, und fügen Sie dem Pool neue Laufwerke desselben Laufwerkstyps hinzu.
- Fügen Sie die Laufwerke desselben Laufwerkstyps zum vorhandenen Pool hinzu. Erstellen Sie dann mithilfe der anderen Laufwerktypen verschiedene Pools, wenn die neuen Laufwerke unterschiedliche Laufwerkstypen haben.

Manuelle Erstellung

Sie möchten möglicherweise einen Pool manuell erstellen, wenn die automatische Erstellung die beste Konfiguration nicht bestimmen kann. Diese Situation kann aus einem der folgenden Gründe auftreten:

- Die neuen Laufwerke können potenziell mehr als einem Pool hinzugefügt werden.
- Mindestens eine der neuen Poolkandidaten kann einen Shelf-Verlust-Schutz oder Schubladenschutz verwenden.
- Ein oder mehrere der aktuellen Poolkandidaten können ihren Schutz vor Shelf-Verlust oder den Schutz vor Schubladenverlust nicht beibehalten.möglicherweise möchten Sie auch einen Pool manuell erstellen, wenn Sie mehrere Anwendungen auf Ihrem Speicher-Array haben und nicht möchten, dass sie mit denselben Laufwerkressourcen konkurrieren. In diesem Fall könnten Sie erwägen, manuell einen kleineren Pool für eine oder mehrere Anwendungen zu erstellen. Sie können nur ein oder zwei Volumes zuweisen, statt den Workload einem großen Pool mit vielen Volumes zuzuweisen, über die die Daten verteilt werden sollen. Durch die manuelle Erstellung eines separaten Pools, der dem Workload einer bestimmten Applikation zugewiesen ist, kann die Performance von Storage-Array-Operationen mit weniger Konflikten schneller erfolgen.

Erstellen Sie automatisch einen Pool im SANtricity-Speichermodul für vCenter

Sie können Pools automatisch erstellen, wenn das System mindestens 11 nicht zugewiesene Laufwerke erkennt oder ein nicht zugewiesenes Laufwerk erkennt, das für einen vorhandenen Pool geeignet ist. Ein Pool ist eine Gruppe von logisch gruppierten Laufwerken.

Bevor Sie beginnen

Sie können das Dialogfeld „automatische Konfiguration des Pools“ starten, wenn eine der folgenden Bedingungen zutrifft:

- Es wurde mindestens ein nicht zugewiesenes Laufwerk erkannt, das einem vorhandenen Pool mit ähnlichen Laufwerktypen hinzugefügt werden kann.
- Es wurden elf (11) oder mehr nicht zugewiesene Laufwerke erkannt, die zur Erstellung eines neuen Pools verwendet werden können (wenn sie aufgrund unterschiedlicher Antriebstypen nicht zu einem vorhandenen Pool hinzugefügt werden können).

Über diese Aufgabe

Mithilfe der automatischen Pool-Erstellung können alle nicht zugewiesenen Laufwerke im Speicher-Array in einem Pool konfiguriert und Laufwerke zu vorhandenen Pools hinzugefügt werden.

Beachten Sie Folgendes:

- Wenn Sie einem Speicher-Array Laufwerke hinzufügen, erkennt das System automatisch die Laufwerke und fordert Sie auf, basierend auf dem Laufwerkstyp und der aktuellen Konfiguration einen einzelnen Pool oder mehrere Pools zu erstellen.
- Wenn zuvor Pools definiert wurden, fordert das System Sie automatisch auf, die kompatiblen Laufwerke einem vorhandenen Pool hinzuzufügen. Wenn zu einem vorhandenen Pool neue Laufwerke hinzugefügt werden, verteilt das System die Daten automatisch auf die neue Kapazität, die jetzt die neuen Laufwerke enthält, die Sie hinzugefügt haben.
- Wenn Sie ein EF600 oder EF300 Storage-Array konfigurieren, stellen Sie sicher, dass jeder Controller in den ersten 12 Steckplätzen und in den letzten 12 Steckplätzen Zugriff auf eine gleiche Anzahl von Laufwerken hat. Mit dieser Konfiguration können die Controller beide PCIe-Busse auf der Laufwerkseite effektiver nutzen. Für die Erstellung von Pools sollten Sie alle Laufwerke im Speicher-Array verwenden.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array für den Pool aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Wählen Sie MENU:Mehr[Pool Auto-Configuration starten].

   In der Ergebnistabelle werden neue Pools, vorhandene Pools mit hinzugefügten Laufwerken oder beides aufgeführt. Ein neuer Pool wird standardmäßig mit einer sequenziellen Nummer benannt.

   Beachten Sie, dass das System folgende Schritte vornimmt:

   - Erstellt einen einzelnen Pool, wenn es eine ausreichende Anzahl von Laufwerken mit demselben Laufwerkstyp (HDD oder SSD) und ähnliche Kapazität gibt.
   - Erstellt mehrere Pools, wenn die nicht zugewiesene Kapazität aus verschiedenen Laufwerkstypen besteht.
   - Fügt die Laufwerke einem vorhandenen Pool hinzu, wenn bereits ein Pool im Speicher-Array definiert

ist, und Sie fügen dem Pool neue Laufwerke desselben Laufwerkstyps hinzu.

- Fügt dem vorhandenen Pool die Laufwerke desselben Laufwerkstyps hinzu und erstellt mithilfe der anderen Laufwerktypen verschiedene Pools, wenn die neuen Laufwerke unterschiedliche Laufwerkstypen haben.

4. Um den Namen eines neuen Pools zu ändern, klicken Sie auf das Symbol **Bearbeiten** (der Stift).
5. Um zusätzliche Merkmale des Pools anzuzeigen, positionieren Sie den Cursor über oder berühren Sie das Symbol Details (die Seite).

   Es werden Informationen zum Laufwerkstyp, zur Sicherheitsfunktion, zur Data Assurance (da)-Funktion, zum Schutz vor Shelf-Verlust und zum Schutz vor Schubladenverlust angezeigt.

   Bei EF600 und EF300 Storage-Arrays werden die Einstellungen auch für die Ressourcenbereitstellung und Volume-Blockgrößen angezeigt.

6. Klicken Sie Auf **Akzeptieren**.

Erstellen Sie manuell einen Pool im SANtricity-Speichermodul für vCenter

Sie können einen Pool manuell erstellen, wenn Ihr Setup die Anforderungen für die automatische Poolkonfiguration nicht erfüllt. Ein Pool ist eine Gruppe von logisch gruppierten Laufwerken.

Bevor Sie beginnen

- Sie müssen mindestens 11 Laufwerke desselben Typs (HDD oder SSD) haben.
- Zum Schutz vor Shelf-Schäden müssen sich die Laufwerke aus dem Pool in mindestens sechs verschiedenen Laufwerk-Shelfs befinden und es gibt nicht mehr als zwei Laufwerke in einem einzelnen Laufwerk-Shelf.
- Der Schutz vor Schubladenverlust erfordert, dass sich die Laufwerke aus dem Pool in mindestens fünf verschiedenen Schubladen befinden und der Pool eine gleiche Anzahl von Laufwerk-Shelfs von jedem Fach enthält.
- Wenn Sie ein EF600 oder EF300 Storage-Array konfigurieren, stellen Sie sicher, dass jeder Controller in den ersten 12 Steckplätzen und in den letzten 12 Steckplätzen Zugriff auf eine gleiche Anzahl von Laufwerken hat. Mit dieser Konfiguration können die Controller beide PCIe-Busse auf der Laufwerkseite effektiver nutzen. Für die Erstellung von Pools sollten Sie alle Laufwerke im Speicher-Array verwenden.

Über diese Aufgabe

Bei der Erstellung von Pools legen Sie deren Merkmale fest, z. B. Laufwerkstyp, Sicherheitsfunktionen, Data Assurance (da)-Funktion, Shelf-Verlust-Schutz und Schutz vor Schubladenverlust.

Für EF600 und EF300 Storage-Arrays umfassen die Einstellungen auch die Ressourcen-Bereitstellung und Volume-Blockgrößen.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array für den Pool aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Klicken Sie auf Menü:Create[Pool].

   Das Dialogfeld Pool erstellen wird angezeigt.

4. Geben Sie einen Namen für den Pool ein.

5. (Optional) Wenn Sie mehr als einen Laufwerkstyp im Speicher-Array haben, wählen Sie den Laufwerkstyp aus, den Sie verwenden möchten.

   Die Ergebnistabelle enthält alle möglichen Pools, die Sie erstellen können.

6. Wählen Sie den Pool-Kandidaten aus, den Sie anhand der folgenden Eigenschaften verwenden möchten, und klicken Sie dann auf **Erstellen**.

Felddetails

Charakteristisch	Nutzung
Freie Kapazität	Zeigt die freie Kapazität des Poolkandidaten in gib an. Wählen Sie einen Pool-Kandidaten mit der Kapazität für die Speicheranforderungen Ihrer Anwendung aus. Die Erhaltungskapazität (freie) wird ebenfalls im gesamten Pool verteilt und ist nicht Teil der freien Kapazitätsmenge.
Laufwerke Insgesamt	Zeigt die Anzahl der im Pool-Kandidaten verfügbaren Laufwerke an. Das System reserviert automatisch so viele Laufwerke wie möglich zur Erhaltung der Kapazität (für alle sechs Laufwerke eines Pools reserviert das System ein Laufwerk zur Erhaltung der Kapazität). Bei einem Laufwerksausfall werden die rekonstruierten Daten anhand der Festplattenkapazität gespeichert.
Laufwerksblockgröße (nur EF300 und EF600)	Zeigt die Blockgröße (Sektorgröße) an, die die Laufwerke im Pool schreiben können. Die Werte können Folgendes umfassen: • 512 — 512-Byte-Sektorgröße. • 4K – 4,096 Byte Sektorgröße.
Sicher	Zeigt an, ob dieser Pool-Kandidat vollständig aus sicheren Laufwerken besteht, bei denen es sich entweder um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handeln kann. • Sie können Ihren Pool mit Laufwerkssicherheit schützen, aber alle Laufwerke müssen sicher sein, damit diese Funktion verwendet werden kann. • Wenn Sie einen nur-FDE-Pool erstellen möchten, suchen Sie in der Spalte Secure-fähiger nach **Yes - FDE**. Wenn Sie einen nur-FIPS-Pool erstellen möchten, suchen Sie nach **Ja - FIPS** oder **Ja - FIPS (gemischt)**. „Mixed“ zeigt eine Mischung aus 140-2- und 140-3-Level-Laufwerken an. Wenn Sie eine Mischung dieser Ebenen verwenden, beachten Sie, dass der Pool dann mit der niedrigeren Sicherheitsstufe (140-2) funktioniert. • Sie können einen Pool aus Laufwerken erstellen, die möglicherweise sicher sein können oder nicht, oder die eine Kombination aus Sicherheitsstufen sind. Wenn die Laufwerke im Pool Laufwerke enthalten, die nicht sicher sind, können Sie den Pool nicht sichern.
Sicherheit Aktivieren?	Bietet die Möglichkeit, die Sicherheitsfunktion des Laufwerks mit sicheren Laufwerken zu aktivieren. Wenn der Pool sicher-fähig ist und Sie einen Sicherheitsschlüssel erstellt haben, können Sie die Sicherheit aktivieren, indem Sie das Kontrollkästchen aktivieren. Die einzige Möglichkeit, die Laufwerksicherheit zu entfernen, nachdem sie aktiviert ist, ist, den Pool zu löschen und die Laufwerke zu löschen.

Charakteristisch	Nutzung
DA-fähig	Gibt an, ob Data Assurance (da) für diesen Pool-Kandidaten verfügbar ist. DA überprüft und korrigiert Fehler, die auftreten können, wenn Daten durch die Controller zu den Laufwerken übertragen werden. Wenn Sie da verwenden möchten, wählen Sie einen Pool aus, der für das da-fähig ist. Diese Option ist nur verfügbar, wenn die da-Funktion aktiviert wurde. Ein Pool kann Laufwerke enthalten, die für da-fähig sind oder nicht für da-fähig sind. Alle Laufwerke müssen jedoch für die Verwendung dieser Funktion als da-fähig sein.
Resource Provisioning-fähig (nur EF300 und EF600)	Zeigt an, ob für diesen Pool-Kandidaten Ressourcen-Provisioning verfügbar ist. Resource Provisioning ist eine Funktion, die in den EF300- und EF600-Speicher-Arrays zur Verfügung steht und die es ermöglicht, Volumes ohne Hintergrundinitialisierung sofort in Betrieb zu nehmen.
Schutz Vor Shelf-Verlust	Zeigt an, ob Regalverlustschutz verfügbar ist. Der Schutz vor Shelf-Datenverlusten garantiert den Zugriff auf die Daten auf den Volumes in einem Pool, wenn ein vollständiger Verlust der Kommunikation mit einem einzelnen Festplatten-Shelf auftritt.
Schutz Vor Schubladenverlust	Zeigt an, ob ein Schubladenschutz verfügbar ist, der nur zur Verfügung steht, wenn Sie ein Laufwerk-Shelf mit Schubladen verwenden. Der Schutz vor Schubladenausfall garantiert den Zugriff auf die Daten auf den Volumes in einem Pool, falls ein vollständiger Verlust der Kommunikation mit einer einzelnen Schublade in einem Festplatten-Shelf auftritt.
Unterstützte Volume-Block-Größen (nur EF300 und EF600)	Zeigt die Blockgrößen an, die für die Volumes im Pool erstellt werden können: • 512 n — 512 Bytes nativ. • 512 e — 512 Bytes emuliert. • 4K — 4,096 Byte.

Erstellen Sie im SANtricity Speicher-Plug-in für vCenter eine Volume-Gruppe

Sie können eine Volume-Gruppe für ein oder mehrere Volumes erstellen, auf die der Host zugreifen kann. Eine Volume-Gruppe ist ein Container für Volumes mit gemeinsam genutzten Merkmalen wie RAID-Level und Kapazität.

Bevor Sie beginnen

Lesen Sie sich die folgenden Richtlinien durch:

- Sie benötigen mindestens ein nicht zugewiesenes Laufwerk.
- Einschränkungen gibt es hinsichtlich der Laufwerkskapazität, die Sie in einer einzelnen Volume-Gruppe haben können. Diese Einschränkungen variieren je nach Hosttyp.
- Um einen Verlust von Shelfs/Schubladen zu ermöglichen, müssen Sie eine Volume-Gruppe erstellen, die Laufwerke in mindestens drei Shelfs oder Schubladen verwendet, es sei denn, Sie verwenden RAID 1, wo

mindestens zwei Shelfs/Schubladen verwendet werden.

- Wenn Sie ein EF600 oder EF300 Storage-Array konfigurieren, stellen Sie sicher, dass jeder Controller in den ersten 12 Steckplätzen und in den letzten 12 Steckplätzen Zugriff auf eine gleiche Anzahl von Laufwerken hat. Mit dieser Konfiguration können die Controller beide PCIe-Busse auf der Laufwerkseite effektiver nutzen. Das System ermöglicht derzeit die Laufwerkauswahl unter der Funktion Erweitert, wenn eine Volume-Gruppe erstellt wird.

Überprüfen Sie, wie sich die RAID-Auswahl auf die resultierende Kapazität der Volume-Gruppe auswirkt.

- Wenn Sie RAID 1 auswählen, müssen Sie jeweils zwei Laufwerke hinzufügen, um sicherzustellen, dass ein gespiegeltes Paar ausgewählt ist. Spiegelung und Striping (bekannt als RAID 10 oder RAID 1+0) wird erreicht, wenn vier oder mehr Laufwerke ausgewählt werden.
- Wenn Sie RAID 5 auswählen, müssen Sie mindestens drei Laufwerke hinzufügen, um die Volume-Gruppe zu erstellen.
- Wenn Sie RAID 6 auswählen, müssen Sie mindestens fünf Laufwerke hinzufügen, um die Volume-Gruppe zu erstellen.

Über diese Aufgabe

Bei der Erstellung von Volume-Gruppen bestimmen Sie die Gruppenmerkmale, z. B. die Anzahl an Laufwerken, die Sicherheitsfunktion, die Data Assurance (da)-Funktion, den Schutz vor Shelf-Datenverlusten und den Schutz vor Schubladenverlust.

Für EF600 und EF300 Storage-Arrays umfassen die Einstellungen auch die Ressourcenbereitstellung, die Laufwerksblockgrößen und die Volume-Blockgrößen.

Mit Laufwerken mit größerer Kapazität und der Möglichkeit, Volumes über Controller hinweg zu verteilen, bietet das Erstellen von mehr als einem Volume pro Volume-Gruppe eine gute Möglichkeit, die Storage-Kapazität zu nutzen und die Daten zu sichern.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array für die Volume-Gruppe aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Klicken Sie auf Menü:Erstellen[Volume Group].

   Das Dialogfeld Volume-Gruppe erstellen wird angezeigt.

4. Geben Sie einen Namen für die Volume-Gruppe ein.
5. Wählen Sie das RAID Level aus, das Ihre Anforderungen an Storage und Datensicherheit am besten erfüllt. Die Kandidatentabelle für die Volume-Gruppe wird angezeigt und zeigt nur die Kandidaten an, die die ausgewählte RAID-Ebene unterstützen.
6. (Optional) Wenn Sie mehr als einen Laufwerkstyp im Speicher-Array haben, wählen Sie den Laufwerkstyp aus, den Sie verwenden möchten.

   Die Kandidatentabelle für die Volume-Gruppe wird angezeigt und zeigt nur die Kandidaten an, die den ausgewählten Laufwerkstyp und den ausgewählten RAID-Level unterstützen.

7. (Optional) Sie können entweder die automatische oder die manuelle Methode auswählen, um festzulegen, welche Laufwerke in der Volume-Gruppe verwendet werden sollen. Die automatische Methode ist die Standardauswahl.

Verwenden Sie die manuelle Methode nur, wenn Sie ein Experte sind, der die Redundanz und die optimale Laufwerkskonfiguration versteht.

Um Laufwerke manuell auszuwählen, klicken Sie auf den Link **Manuelle Auswahl von Laufwerken (erweitert)**. Wenn Sie auf diese Schaltfläche klicken, wird die Option **automatisch Laufwerke auswählen (erweitert)**.

Mit der manuellen Methode können Sie auswählen, welche spezifischen Laufwerke die Volume-Gruppe umfassen. Wählen Sie bestimmte nicht zugewiesene Laufwerke aus, um die erforderliche Kapazität abzurufen. Wenn das Speicher-Array Laufwerke mit unterschiedlichen Medientypen oder unterschiedlichen Schnittstellentypen enthält, können Sie nur die nicht konfigurierte Kapazität für einen einzelnen Laufwerkstyp auswählen, um die neue Volume-Gruppe zu erstellen.

8. Wählen Sie basierend auf den angezeigten Laufwerkeigenschaften die Laufwerke aus, die Sie in der Volume-Gruppe verwenden möchten, und klicken Sie dann auf **Erstellen**.

Die angezeigten Laufwerkeigenschaften hängen davon ab, ob Sie die automatische oder die manuelle Methode ausgewählt haben. Weitere Informationen finden Sie in der Dokumentation zum SANtricity System Manager "Erstellen einer Volume-Gruppe".

Fügen Sie Kapazität zu einem Pool oder einer Volume-Gruppe im SANtricity Speicher-Plug-in für vCenter hinzu

Sie können Laufwerke hinzufügen, um die freie Kapazität in einem vorhandenen Pool oder einer vorhandenen Volume-Gruppe zu erweitern.

Bevor Sie beginnen

- Die Laufwerke müssen sich im optimalen Zustand befinden.
- Laufwerke müssen über den gleichen Festplattentyp (HDD oder SSD) verfügen.
- Der Pool oder die Volume-Gruppe muss den Status „optimal“ aufweisen.
- Wenn der Pool oder die Volume-Gruppe alle sicheren Laufwerke enthält, fügen Sie nur Laufwerke hinzu, die sicher sind, damit sie weiterhin die Verschlüsselungsfunktionen der sicheren Laufwerke nutzen können.

Sichere Laufwerke können entweder vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) sein.

Über diese Aufgabe

Bei dieser Aufgabe können Sie die freie Kapazität hinzufügen, die in den Pool bzw. die Volume-Gruppe integriert werden kann. Sie können diese freie Kapazität nutzen, um zusätzliche Volumes zu erstellen. Der Zugriff auf die Daten in den Volumes bleibt während dieses Vorgangs erhalten.

Für Pools können Sie maximal 60 Laufwerke gleichzeitig hinzufügen. Für Volume-Gruppen können Sie maximal zwei Laufwerke gleichzeitig hinzufügen. Wenn Sie mehr als die maximale Anzahl an Laufwerken hinzufügen müssen, wiederholen Sie das Verfahren. (Ein Pool darf nicht mehr Laufwerke enthalten als das Höchstlimit eines Speicher-Arrays.)

Mit zusätzlichen Festplatten muss möglicherweise die Aufbewahrungskapazität erhöht werden. Sie sollten Ihre reservierte Kapazität nach einem Erweiterungsvorgang erhöhen.

Vermeiden Sie die Verwendung von Laufwerken, die Data Assurance (da) sind, die Kapazität zu einem Pool oder einer Volume-Gruppe hinzufügen können, die nicht über da-fähig ist. Der Pool oder die Volume-Gruppe können die Funktionen des da-fähigen Laufwerks nicht nutzen. Ziehen Sie in Betracht, Laufwerke zu verwenden, die in dieser Situation nicht für da geeignet sind.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit dem Pool oder der Volume-Gruppe aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Wählen Sie den Pool oder die Volume-Gruppe aus, dem Sie Laufwerke hinzufügen möchten, und klicken Sie dann auf **Kapazität hinzufügen**.

   Das Dialogfeld Kapazität hinzufügen wird angezeigt. Es werden nur die nicht zugewiesenen Laufwerke angezeigt, die mit dem Pool oder der Volume-Gruppe kompatibel sind.

4. Wählen Sie unter **Wählen Sie Laufwerke aus, um Kapazität hinzuzufügen…** ein oder mehrere Laufwerke aus, die Sie dem vorhandenen Pool oder der Volume-Gruppe hinzufügen möchten.

   Die Controller-Firmware ordnet die nicht zugewiesenen Laufwerke den besten Optionen zu, die oben aufgeführt sind. Die dem Pool oder der Volume-Gruppe hinzugefügte freie Gesamtkapazität wird unterhalb der Liste in **gewählte Gesamtkapazität** angezeigt.

Felddetails

Feld	Beschreibung
Shelf	Zeigt den Shelf-Standort des Laufwerks an.
Bucht	Zeigt die Einschubposition des Laufwerks an
Kapazität (gib)	Zeigt die Laufwerkskapazität an. • Wählen Sie nach Möglichkeit Laufwerke aus, die eine Kapazität haben, die den Kapazitäten der aktuellen Laufwerke im Pool oder der Volume-Gruppe entspricht. • Wenn nicht zugewiesene Laufwerke mit kleinerer Kapazität hinzugefügt werden müssen, müssen Sie beachten, dass die nutzbare Kapazität jedes Laufwerks, das sich derzeit im Pool bzw. der Volume-Gruppe befindet, reduziert wird. Daher ist die Laufwerkskapazität für den Pool oder die Volume-Gruppe gleich. • Wenn nicht zugewiesene Laufwerke mit höherer Kapazität hinzugefügt werden müssen, ist zu beachten, dass die nutzbare Kapazität der nicht zugewiesenen Laufwerke, die hinzugefügt werden, reduziert wird, damit sie den aktuellen Kapazitäten der Laufwerke im Pool bzw. der Volume-Gruppe entsprechen.
Sicher	Zeigt an, ob das Laufwerk sicher ist. • Sie können Ihre Pool- oder Volume-Gruppe mit der Laufwerkssicherheitsfunktion schützen, aber alle Laufwerke müssen sicher sein, um diese Funktion verwenden zu können. • Es ist zwar möglich, einen Pool oder eine Volume-Gruppe mit einer Kombination aus sicheren und nicht sicheren Laufwerken zu erstellen, die Sicherheitsfunktion des Laufwerks kann jedoch nicht aktiviert werden. • Ein Pool oder eine Volume-Gruppe mit allen sicheren Laufwerken kann kein nicht sicheres Laufwerk für Sparing oder Expansion akzeptieren, auch wenn die Verschlüsselungsfunktion nicht verwendet wird. • Sichere Laufwerke können entweder vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) sein. Ein FIPS-Laufwerk kann die Level 140-2 oder 140-3 sein, wobei Level 140-3 als höheres Sicherheitsniveau gilt. Wenn Sie eine Mischung aus 140-2- und 140-3-Laufwerken auswählen, arbeitet die Pool- oder Volume-Gruppe dann auf niedrigerer Sicherheitsstufe (140-2).

Feld	Beschreibung
DA-fähig	Gibt an, ob das Laufwerk Data Assurance (da)-fähig ist. • Es wird nicht empfohlen, Laufwerke zu verwenden, die nicht Data Assurance (da) sind, die Kapazität zu einem da-fähigen Pool oder einer Volume-Gruppe hinzufügen können. Der Pool oder die Volume-Gruppe verfügt nicht mehr über da-Funktionen, und Sie haben nicht mehr die Option, da für neu erstellte Volumes innerhalb des Pools oder der Volume-Gruppe zu aktivieren. • Die Verwendung von Laufwerken, die Data Assurance (da) sind, die Kapazität zu einem Pool oder einer Volume-Gruppe hinzufügen können, die nicht für da geeignet ist, wird nicht empfohlen, da dieser Pool oder die Volume-Gruppe die Funktionen des da-fähigen Laufwerks nicht nutzen kann (die Laufwerkattribute stimmen nicht überein). Ziehen Sie in Betracht, Laufwerke zu verwenden, die in dieser Situation nicht da-fähig sind.
DULBE-fähig	Gibt an, ob das Laufwerk über die Option für dezugewiesene oder nicht geschriebene logische Blockfehler (DULBE) verfügt. DULBE ist eine Option auf NVMe-Laufwerken, mit der das EF300- oder EF600-Storage-Array ressourcenbereitgestellte Volumes unterstützt.

5. Klicken Sie Auf **Hinzufügen**.

   Wenn Sie Laufwerke zu einem Pool oder einer Volume-Gruppe hinzufügen, wird ein Bestätigungsdialogfeld angezeigt, wenn Sie ein Laufwerk ausgewählt haben, das dazu führt, dass der Pool oder die Volume-Gruppe nicht mehr über eines oder mehrere der folgenden Attribute verfügt:

   ◦ Schutz vor Regalverlust
   ◦ Schutz vor Schubladenverlust
   ◦ Vollständige Festplattenverschlüsselung
   ◦ Data Assurance
   ◦ DULBE-Fähigkeit

6. Klicken Sie zum Fortfahren auf **Ja**, oder klicken Sie auf **Abbrechen**.

Ergebnis

Nachdem Sie die nicht zugewiesenen Laufwerke einem Pool oder einer Volume-Gruppe hinzugefügt haben, werden die Daten in jedem Volume des Pools oder der Volume-Gruppe neu verteilt, um auch die zusätzlichen Laufwerke einzubeziehen.

Erstellen Sie ein SSD-Cache im SANtricity-Speicher-Plug-in für vCenter

Zur dynamischen Beschleunigung der System-Performance können Sie die SSD Cache Funktion verwenden, um die am häufigsten abgerufenen Daten („heiße“ Daten) auf Solid State Drives (SSDs) mit niedrigerer Latenz zu zwischenspeichern. SSD Cache wird ausschließlich für Host-Lesevorgänge verwendet.

Bevor Sie beginnen

Ihr Speicher-Array muss einige SSD-Laufwerke enthalten.

SSD-Cache ist auf dem EF600 oder EF300 Storage-System nicht verfügbar.

Über diese Aufgabe

Wenn Sie SSD Cache erstellen, können Sie ein oder mehrere Laufwerke verwenden. Da sich der Lese-Cache im Storage Array befindet, wird das Caching von allen Applikationen genutzt, die das Storage Array verwenden. Sie wählen die Volumes aus, die zwischengespeichert werden sollen. Das Caching erfolgt dann automatisch und dynamisch.

Beachten Sie bei der Erstellung von SSD Cache die folgenden Richtlinien.

- Sie können die Sicherheit im SSD-Cache nur aktivieren, wenn Sie sie erstellen, und nicht später.
- Pro Storage Array wird nur ein SSD-Cache unterstützt.
- Die maximale nutzbare SSD-Cache-Kapazität auf einem Speicher-Array hängt von der primären Cache-Kapazität des Controllers ab.
- SSD Cache wird von Snapshot Images nicht unterstützt.
- Wenn Sie Volumes importieren oder exportieren, die SSD Cache aktiviert oder deaktiviert sind, werden die zwischengespeicherten Daten nicht importiert oder exportiert.
- Jedes Volume, das der Nutzung des SSD-Caches eines Controllers zugewiesen ist, kann keine automatische Lastverteilung durchführen.
- Wenn die zugehörigen Volumes für die Sicherheit aktiviert sind, erstellen Sie einen sicheren SSD-Cache.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array für den Cache aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Klicken Sie auf Menü:Create[SSD Cache].

   Das Dialogfeld SSD-Cache erstellen wird angezeigt.

4. Geben Sie einen Namen für den SSD-Cache ein.
5. Wählen Sie den Kandidaten für den SSD-Cache aus, den Sie basierend auf folgenden Merkmalen verwenden möchten.

Felddetails

Charakteristisch	Nutzung
Kapazität	Zeigt die verfügbare Kapazität in gib an. Wählen Sie die Kapazität für die Speicheranforderungen Ihrer Anwendung aus. Die maximale Kapazität für SSD Cache hängt von der primären Cache-Kapazität des Controllers ab. Wenn Sie SSD-Cache mehr als die maximale Menge zuweisen, ist diese zusätzliche Kapazität nicht nutzbar. Die SSD-Cache-Kapazität wird für die Ihrer gesamten zugewiesenen Kapazität gezählt.
Laufwerke insgesamt	Zeigt die Anzahl der für diesen SSD-Cache verfügbaren Laufwerke an. Wählen Sie den SSD-Kandidaten mit der Anzahl der gewünschten Laufwerke aus
Sicher	Gibt an, ob SSD Cache Kandidaten vollständig aus sicheren Laufwerken bestehen, bei denen es sich entweder um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE)-Laufwerke oder um FIPS-Laufwerke (Federal Information Processing Standard) handeln kann. Wenn Sie einen sicheren aktivierten SSD-Cache erstellen möchten, suchen Sie in der Spalte mit sicherem Zugriff „Ja – FDE“ oder „Ja – FIPS“.
Sicherheit aktivieren?	Bietet die Möglichkeit, die Sicherheitsfunktion des Laufwerks mit sicheren Laufwerken zu aktivieren. Wenn Sie einen sicheren SSD-Cache erstellen möchten, aktivieren Sie das Kontrollkästchen **Sicherheit aktivieren**. HINWEIS: Sobald die Option aktiviert ist, kann die Sicherheit nicht deaktiviert werden. Sie können die Sicherheit im SSD-Cache nur aktivieren, wenn Sie sie erstellen, und nicht später.
DA-fähig	Gibt an, ob Data Assurance (da) für diesen SSD-Cache-Kandidaten verfügbar ist. Data Assurance (da) überprüft und korrigiert Fehler, die auftreten können, wenn Daten durch die Controller zu den Laufwerken übertragen werden. Wenn Sie da verwenden möchten, wählen Sie einen SSD-Cache-Kandidaten aus, der für da geeignet ist. Diese Option ist nur verfügbar, wenn die da-Funktion aktiviert wurde. SSD Cache kann sowohl da-fähige als auch nicht-da-fähige Laufwerke enthalten, aber alle Laufwerke müssen für Sie da-fähig sein, da zu verwenden.

6. Verbinden Sie den SSD-Cache mit den Volumes, für die Sie SSD-Lese-Caching implementieren möchten. Um SSD-Cache auf kompatiblen Volumes sofort zu aktivieren, aktivieren Sie das Kontrollkästchen **SSD-Cache aktivieren auf vorhandenen kompatiblen Volumes, die Hosts zugeordnet sind**.

   Volumes sind kompatibel, wenn sie die gleichen Laufwerksicherheit- und da-Funktionen nutzen.

7. Klicken Sie Auf **Erstellen**.

Ändern Sie die Konfigurationseinstellungen für einen Pool im SANtricity-Speichermodul für vCenter

Sie können die Einstellungen für einen Pool bearbeiten, einschließlich Name, Kapazitätswarnungen, Änderungsprioritäten und Erhaltungskapazität.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie die Konfigurationseinstellungen für einen Pool geändert werden.

Sie können den RAID-Level eines Pools nicht mit der Plugin-Schnittstelle ändern. Das Plugin konfiguriert Pools automatisch als RAID 6.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit dem Pool aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Wählen Sie den Pool aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld Pool-Einstellungen wird angezeigt.

4. Wählen Sie die Registerkarte **Einstellungen** aus, und bearbeiten Sie anschließend die Pooleinstellungen entsprechend.

Felddetails

Einstellung	Beschreibung
Name	Sie können den vom Benutzer bereitgestellten Namen des Pools ändern. Die Angabe eines Namens für einen Pool ist erforderlich.
Kapazitätswarnungen	Sie können Benachrichtigungen senden, wenn die freie Kapazität in einem Pool einen bestimmten Schwellenwert erreicht oder überschreitet. Wenn die im Pool gespeicherten Daten den angegebenen Schwellenwert überschreiten, sendet das Plugin eine Nachricht, sodass Sie mehr Speicherplatz hinzufügen oder unnötige Objekte löschen können. Warnmeldungen werden im Bereich Benachrichtigungen auf dem Dashboard angezeigt und können per E-Mail und SNMP-Trap-Nachrichten vom Server an Administratoren gesendet werden. Sie können die folgenden Kapazitätswarnungen definieren: • **Critical Alert** — Diese kritische Warnmeldung informiert Sie, wenn die freie Kapazität im Pool den angegebenen Schwellenwert erreicht oder überschreitet. Verwenden Sie die Spinner-Regler, um den Schwellenwert in Prozent einzustellen. Aktivieren Sie das Kontrollkästchen, um diese Benachrichtigung zu deaktivieren. • **Frühwarnung** — Diese Frühwarnung informiert Sie, wenn die freie Kapazität in einem Pool einen bestimmten Schwellenwert erreicht. Verwenden Sie die Spinner-Regler, um den Schwellenwert in Prozent einzustellen. Aktivieren Sie das Kontrollkästchen, um diese Benachrichtigung zu deaktivieren.

Einstellung	Beschreibung
Änderungsprioritäten	Sie können die Prioritätsstufen für Änderungsvorgänge in einem Pool relativ zur Systemleistung festlegen. Eine höhere Priorität für Änderungsvorgänge in einem Pool führt dazu, dass ein Vorgang schneller abgeschlossen wird, die Host-I/O-Performance jedoch beeinträchtigt wird. Bei geringerer Priorität dauern Vorgänge länger, bis die I/O-Performance des Hosts weniger beeinträchtigt ist. Sie können aus fünf Prioritätsstufen wählen: Niedrigste, niedrige, mittlere, höchste und höchste. Je höher die Priorität, desto größer ist die Auswirkung auf die Host-I/O und System-Performance. • **Kritische Rekonstruktionspriorität** — dieser Schieberegler bestimmt die Priorität eines Datenrekonstruktionsvorgangs, wenn mehrere Laufwerksausfälle zu einem Zustand führen, in dem einige Daten keine Redundanz aufweisen und ein zusätzlicher Laufwerksausfall zu Datenverlust führen kann. • **Degradierte Rekonstruktionspriorität** — dieser Schieberegler bestimmt die Priorität des Datenrekonstruktionsvorgangs bei einem Laufwerksausfall, aber die Daten haben noch Redundanz und ein zusätzlicher Laufwerksausfall führt nicht zu Datenverlust. • **Background Operation Priority** — dieser Schieberegler bestimmt die Priorität der Pool-Hintergrundoperationen, die auftreten, während sich der Pool in einem optimalen Zustand befindet. Zu diesen Vorgängen gehören dynamische Volume-Erweiterung (DVE), Instant Availability Format (IAF) und die Migration von Daten auf ein ersetztes oder hinzugefügtes Laufwerk.

Einstellung	Beschreibung
Dauerhafte Kapazität („Optimierungskapazität “ für die EF600 oder EF300)	**Preservation Capacity** — Sie können die Anzahl der Laufwerke definieren, um die Kapazität zu bestimmen, die im Pool reserviert ist, um potenzielle Laufwerksausfälle zu unterstützen. Bei einem Laufwerksausfall werden die rekonstruierten Daten anhand der Festplattenkapazität gespeichert. Pools verwenden während der Datenrekonstruktion freie Kapazitäten anstelle von Hot-Spare-Laufwerken, die in Volume-Gruppen verwendet werden. Passen Sie mit den Spinner-Steuerungen die Anzahl der Antriebe an. Je nach Anzahl der Laufwerke wird die Konservierungskapazität im Pool neben der Spinner Box angezeigt. Berücksichtigen Sie die folgenden Hinweise zur Konservierungskapazität. • Da die Konservierungskapazität von der gesamten freien Kapazität eines Pools abgezogen wird, wirkt sich die Menge der reservierten Kapazität darauf aus, wie viel freie Kapazität zur Erstellung von Volumes zur Verfügung steht. Wenn Sie für die Erhaltungskapazität 0 angeben, wird die gesamte freie Kapazität im Pool zur Volume-Erstellung genutzt. • Wenn Sie die Konservierungskapazität verringern, erhöhen Sie die Kapazität, die für Pool Volumes genutzt werden kann. **Zusätzliche Optimierungskapazität (nur EF600 und EF300 Arrays)** — Wenn ein Pool erstellt wird, wird eine empfohlene Optimierungskapazität generiert, die ein ausgewogenes Verhältnis zwischen verfügbarer Kapazität und Performance sowie Laufwerksabnutzung bietet. Sie können diese Balance anpassen, indem Sie den Schieberegler nach rechts bewegen, um eine bessere Performance zu erzielen und den Verschleiß zu erhöhen. Wenn Sie die verfügbare Kapazität in die linke Seite verschieben, können Sie die verfügbare Kapazität auf Kosten einer besseren Performance und eines höheren Verschleißes der Laufwerke erhöhen. SSD-Laufwerke haben eine längere Lebensdauer und eine bessere maximale Schreib-Performance, wenn ein Teil ihrer Kapazität nicht zugewiesen ist. Bei Laufwerken, die einem Pool zugeordnet sind, besteht nicht zugewiesene Kapazität aus der Erhaltungskapazität eines Pools, der freien Kapazität (nicht von Volumes genutzte Kapazität) und einem Teil der nutzbaren Kapazität, der als zusätzliche Optimierungskapazität zur Verfügung steht. Die zusätzliche Optimierungskapazität stellt ein Mindestmaß an Optimierungskapazität zur Verfügung, indem die nutzbare Kapazität reduziert wird. Somit ist für die Volume-Erstellung nicht verfügbar.

5. Klicken Sie Auf **Speichern**.

Ändern Sie die Konfigurationseinstellungen für eine Volume-Gruppe im SANtricity Storage Plug-in für vCenter

Sie können die Einstellungen für eine Volume-Gruppe einschließlich Name und RAID-Level bearbeiten.

Bevor Sie beginnen

Wenn Sie die RAID-Ebene ändern, um die Performance-Anforderungen der Applikationen, die auf die Volume-

Gruppe zugreifen, zu erfüllen, müssen Sie die folgenden Voraussetzungen erfüllen:

- Die Volume-Gruppe muss den optimalen Status haben.
- Sie müssen über genügend Kapazität in der Volume-Gruppe verfügen, um auf das neue RAID-Level zu konvertieren.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit der Volume-Gruppe aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Wählen Sie die Volume-Gruppe aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld Volume Group Settings wird angezeigt.

4. Wählen Sie die Registerkarte **Einstellungen** aus, und bearbeiten Sie anschließend die Einstellungen für die Volume-Gruppe.

Felddetails

Einstellung	Beschreibung
Name	Sie können den vom Benutzer bereitgestellten Namen der Volume-Gruppe ändern. Die Angabe eines Namens für eine Volume-Gruppe ist erforderlich.
RAID-Level	Wählen Sie den neuen RAID-Level aus dem Dropdown-Menü aus. • **RAID 0 Striping** — bietet eine hohe Leistung, aber keine Datenredundanz. Wenn ein einzelnes Laufwerk in der Volume-Gruppe ausfällt, fallen alle zugehörigen Volumes aus und alle Daten gehen verloren. Eine Striping-RAID-Gruppe fasst zwei oder mehr Laufwerke zu einem großen logischen Laufwerk zusammen. • **RAID 1 Mirroring** — bietet eine hohe Leistung und beste Datenverfügbarkeit und eignet sich zur Speicherung sensibler Daten auf Unternehmens- oder Persönlichkeitsebene. Schützt Ihre Daten, indem der Inhalt eines Laufwerks automatisch auf das zweite Laufwerk im gespiegelten Paar gespiegelt wird. Er bietet Schutz bei Ausfall eines einzigen Laufwerks. • **RAID 10 Striping/Spiegelung** — bietet eine Kombination aus RAID 0 (Striping) und RAID 1 (Spiegelung) und wird erreicht, wenn vier oder mehr Laufwerke ausgewählt werden. RAID 10 ist für Transaktionsapplikationen mit hohem Volumen, z. B. für eine Datenbank mit hohen Performance- und Fehlertoleranz, geeignet. • **RAID 5** — optimal für Umgebungen mit mehreren Benutzern (wie Datenbank- oder Dateisystemspeicher), in denen die typische I/O-Größe klein ist und ein hoher Anteil an Leseaktivitäten besteht. • **RAID 6** - optimal für Umgebungen, die einen Redundanzschutz über RAID 5 hinaus benötigen, jedoch keine hohe Schreib-Performance erfordern. RAID 3 kann nur Volume-Gruppen über die Befehlszeilenschnittstelle (CLI) zugewiesen werden. Wenn Sie den RAID-Level ändern, können Sie diesen Vorgang nach seinem Start nicht mehr abbrechen. Während der Änderung bleiben Ihre Daten verfügbar.

Einstellung	Beschreibung
Optimierungskapazität (nur EF600 Arrays)	Wenn eine Volume-Gruppe erstellt wird, wird eine empfohlene Optimierungskapazität generiert, die ein Gleichgewicht zwischen der verfügbaren Kapazität und Performance sowie dem Verschleiß von Laufwerken bietet. Sie können diese Balance anpassen, indem Sie den Schieberegler nach rechts bewegen, um eine bessere Performance zu erzielen und den Verschleiß zu erhöhen. Wenn Sie die verfügbare Kapazität in die linke Seite verschieben, können Sie die verfügbare Kapazität auf Kosten einer besseren Performance und eines höheren Verschleißes der Laufwerke erhöhen. SSD-Laufwerke haben eine längere Lebensdauer und eine bessere maximale Schreib-Performance, wenn ein Teil ihrer Kapazität nicht zugewiesen ist. Bei Laufwerken, die einer Volume-Gruppe zugeordnet sind, besteht die nicht zugewiesene Kapazität aus der freien Kapazität einer Gruppe (nicht von Volumes genutzte Kapazität) und einem Teil der nutzbaren Kapazität, der als zusätzliche Optimierungskapazität zur Verfügung steht. Die zusätzliche Optimierungskapazität stellt ein Mindestmaß an Optimierungskapazität zur Verfügung, indem die nutzbare Kapazität reduziert wird. Somit ist für die Volume-Erstellung nicht verfügbar.

5. Klicken Sie Auf **Speichern**.

Wenn die Kapazität reduziert wird, die Volume-Redundanz verloren geht oder der Schutz vor Shelf-/Schubladenverlust infolge einer Änderung auf RAID-Ebene verloren geht, wird ein Bestätigungsdialogfeld mit dem Kunden angezeigt. Wählen Sie **Ja**, um fortzufahren. Klicken Sie andernfalls auf **Nein**.

Ergebnis

Wenn Sie den RAID-Level für eine Volume-Gruppe ändern, ändert das Plugin die RAID-Level jedes Volumes, das die Volume-Gruppe enthält. Die Leistung kann während des Betriebs leicht beeinträchtigt werden.

Ändern Sie die SSD-Cache-Einstellungen im SANtricity Storage Plug-in für vCenter

Sie können den Namen des SSD-Caches bearbeiten und seinen Status, die maximale und aktuelle Kapazität, den Status der Laufwerksicherheit und Data Assurance sowie die zugehörigen Volumes und Laufwerke anzeigen.

Diese Funktion steht nicht auf dem EF600 oder EF300-Storage-System zur Verfügung.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit SSD-Cache aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Wählen Sie den SSD-Cache aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld SSD-Cache-Einstellungen wird angezeigt.

4. Überprüfen oder bearbeiten Sie die SSD-Cache-Einstellungen nach Bedarf.

Felddetails

Einstellung	Beschreibung
Name	Zeigt den Namen des SSD-Caches an, den Sie ändern können. Ein Name für den SSD-Cache ist erforderlich.
Merkmale	Zeigt den Status des SSD-Caches an. Mögliche Status sind: • Optimal • Unbekannt • Beeinträchtigt • Fehlgeschlagen (ein fehlgeschlagener Zustand führt zu einem kritischen MEL-Ereignis.) • Ausgesetzt
Kapazität	Zeigt die aktuelle Kapazität und die maximale Kapazität, die für den SSD-Cache zulässig ist. Die maximale für den SSD-Cache zulässige Kapazität hängt von der Größe des primären Caches des Controllers ab: • Bis zu 1 gib • 1 gib bis 2 gib • 2 gib bis 4 gib • Mehr als 4 gib
Sicherheit und da	Zeigt den Status der Laufwerksicherheit und Data Assurance für den SSD-Cache an. • **Secure-fähig** --gibt an, ob der SSD Cache vollständig aus sicheren Laufwerken besteht. Bei einem sicheren Laufwerk handelt es sich um ein Self-Encrypting Drive, das seine Daten vor unberechtigtem Zugriff schützt. • **Secure-Enabled** — gibt an, ob die Sicherheit auf dem SSD Cache aktiviert ist. • **Da-fähig** — zeigt an, ob der SSD-Cache vollständig aus da-fähigen Laufwerken besteht. Ein da-fähiges Laufwerk kann auf Fehler überprüfen und beheben, die auftreten können, wenn Daten zwischen dem Host und dem Speicher-Array kommuniziert werden.
Zugeordnete Objekte	Zeigt die Volumes und Laufwerke, die dem SSD-Cache zugeordnet sind.

5. Klicken Sie Auf **Speichern**.

Zeigen Sie die SSD-Cache-Statistiken im SANtricity Speicher-Plug-in für vCenter an

Sie können Statistiken für den SSD-Cache anzeigen, z. B. Lese-, Schreib-, Cache-Treffer,

Cache-Zuweisung in Prozent, Und Cache-Auslastung in Prozent.

Diese Funktion steht nicht auf dem EF600 oder EF300-Storage-System zur Verfügung.

Über diese Aufgabe

Die nominalen Statistiken, bei denen es sich um eine Untergruppe der detaillierten Statistiken handelt, werden im Dialogfeld „View SSD Cache Statistics“ angezeigt. Sie können detaillierte Statistiken für den SSD-Cache nur anzeigen, wenn Sie alle SSD-Statistiken in eine .csv-Datei exportieren.

Während Sie die Statistiken überprüfen und interpretieren, beachten Sie, dass einige Interpretationen durch die Prüfung einer Kombination von Statistiken abgeleitet werden.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit SSD-Cache aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Wählen Sie den SSD-Cache aus, für den Sie Statistiken anzeigen möchten, und klicken Sie dann auf Menü:Mehr Statistik[View SSD Cache].

   Das Dialogfeld SSD-Cache-Statistiken anzeigen wird angezeigt und zeigt die nominalen Statistiken für den ausgewählten SSD-Cache an.

   Felddetails

Einstellung	Beschreibung
Lesezugriffe	Zeigt die Gesamtzahl der Host-Lesevorgänge aus den SSD Volumes mit Cache-Aktivierung an. Je mehr das Verhältnis von Lese- zu Schreibzugriffen ist, desto besser ist der Betrieb des Cache.
Schreibvorgänge	Die Gesamtzahl der Host-Schreibvorgänge auf den SSD-Cache-fähigen Volumes, Je mehr das Verhältnis von Lese- zu Schreibzugriffen ist, desto besser ist der Betrieb des Cache.
Cache-Treffer	Zeigt die Anzahl der Cache-Treffer an.
Cache-Treffer %	Zeigt den Prozentsatz von Cache-Treffern an. Diese Zahl leitet sich aus Cache-Hits / (Lese- + Schreibvorgänge) ab. Der Cache-Trefferprozentsatz sollte im Hinblick auf einen effektiven SSD-Cache-Vorgang größer als 50 Prozent sein.
Cache-Zuweisung %	Zeigt den Prozentsatz des zugewiesenen SSD-Cache-Speichers an, ausgedrückt als Prozentsatz des SSD-Cache-Speichers, der für diesen Controller verfügbar ist und aus zugewiesenen Bytes/verfügbaren Bytes abgeleitet wird.
Cache-Auslastung in %	Zeigt den Prozentsatz von SSD-Cache-Storage, der Daten von aktivierten Volumes enthält, die in Prozent des zugewiesenen SSD-Cache-Storage angegeben sind. Diese Menge stellt die Auslastung oder Dichte des SSD-Cache dar. Abgeleitet von zugewiesenen Bytes/verfügbaren Bytes.
Alle Exportieren	Exportiert alle SSD-Cache-Statistiken in ein CSV-Format. Die exportierte Datei enthält alle verfügbaren Statistiken für den SSD-Cache (nominal und detailliert).

4. Klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen.

Prüfen Sie die Volume-Redundanz im SANtricity Storage Plug-in für vCenter

Mithilfe des technischen Supports oder der Anleitung durch den Recovery Guru können Sie die Redundanz auf einem Volume in einem Pool oder einer Volume-Gruppe überprüfen, um zu ermitteln, ob die Daten auf diesem Volume konsistent sind.

Redundanzdaten dienen der schnellen Rekonstruktion von Informationen über das Ersatzlaufwerk, wenn eines der Laufwerke im Pool oder der Volume-Gruppe ausfällt.

Bevor Sie beginnen

- Der Status des Pools oder der Volume-Gruppe muss optimal sein.
- Der Pool oder die Volume-Gruppe darf keine Änderungsvorgänge für das Volume ausführen.
- Sie können Redundanz auf jeder RAID-Ebene außer RAID 0 prüfen, da RAID 0 keine Datenredundanz hat. (Pools sind nur als RAID 6 konfiguriert.)

> Prüfen Sie die Volume-Redundanz nur dann, wenn Sie vom Recovery Guru zur Verfügung stehen und unter Anleitung des technischen Supports dies tun.

Über diese Aufgabe

Sie können diese Prüfung nur für einen Pool oder eine Volume-Gruppe gleichzeitig durchführen. Bei einer Volume-Redundanzprüfung werden folgende Aktionen durchgeführt:

- Scannt die Datenblöcke in einem RAID 3-Volume, einem RAID 5-Volume oder einem RAID 6-Volume und überprüft die Redundanzinformationen für jeden Block. (RAID 3 kann Volume-Gruppen nur über die Befehlszeilenschnittstelle zugewiesen werden.)
- Vergleicht die Datenblöcke auf gespiegelten RAID 1-Laufwerken.
- Gibt Redundanzfehler zurück, wenn die Controller-Firmware feststellt, dass die Daten inkonsistent sind.

> Eine sofortige Durchführung einer Redundanzprüfung auf demselben Pool oder derselben Volume-Gruppe kann zu einem Fehler führen. Um dieses Problem zu vermeiden, warten Sie ein bis zwei Minuten, bevor Sie eine weitere Redundanzprüfung auf demselben Pool oder derselben Volume-Gruppe durchführen.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit dem Pool oder der Volume-Gruppe aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Menü wählen:Sonstige Aufgaben[Volumenredundanz prüfen].

   Das Dialogfeld Redundanz prüfen wird angezeigt.

4. Wählen Sie die Volumes aus, die Sie prüfen möchten, und geben Sie anschließend Check ein, um zu bestätigen, dass Sie diesen Vorgang ausführen möchten.
5. Klicken Sie Auf **Prüfen**.

   Der Vorgang „Volume-Redundanz prüfen“ wird gestartet. Die Volumes im Pool oder in der Volume-Gruppe werden sequenziell gescannt. Sie beginnen dabei von oben in der Tabelle im Dialogfeld. Diese Aktionen werden beim Scannen der einzelnen Volumes ausgeführt:

- Das Volume wird in der Volume-Tabelle ausgewählt.
- Der Status der Redundanzprüfung wird in der Spalte Status angezeigt.
- Die Prüfung wird bei einem Datenträger- oder Paritätsfehler angehalten und meldet dann den Fehler. Die folgende Tabelle bietet weitere Informationen zum Status der Redundanzprüfung:

Felddetails

Status	Beschreibung
Ausstehend	Dies ist das erste zu scannende Volume, und Sie haben nicht auf Start geklickt, um die Redundanzprüfung zu starten. -Oder- die Redundanzprüfung wird auf anderen Volumes im Pool oder der Volume-Gruppe durchgeführt.
Prüfen	Das Volumen wird durch die Redundanzprüfung geprüft.
Bestanden	Das Volume bestand die Redundanzprüfung. In den Redundanzinformationen wurden keine Inkonsistenzen gefunden.
Fehlgeschlagen	Das Volume hat die Redundanzprüfung nicht bestanden. In den Redundanzinformationen wurden Inkonsistenzen gefunden.
Medienfehler	Das Laufwerkmedium ist defekt und unlesbar. Befolgen Sie die Anweisungen im Recovery Guru.
Paritätsfehler	Die Parität ist nicht, was sie für einen bestimmten Teil der Daten sein sollte. Ein Paritätsfehler ist potenziell schwerwiegend und kann zu permanentem Datenverlust führen.

6. Klicken Sie auf **Fertig**, nachdem das letzte Volume im Pool oder der Volume-Gruppe überprüft wurde.

Löschen Sie einen Pool oder eine Volume-Gruppe im SANtricity Speicher-Plug-in für vCenter

Sie können einen Pool oder eine Volume-Gruppe löschen, um mehr nicht zugewiesene Kapazität zu erstellen. Diese können Sie neu konfigurieren, um die Storage-Anforderungen Ihrer Applikation zu erfüllen.

Bevor Sie beginnen

- Sie müssen die Daten auf allen Volumes im Pool oder in der Volume-Gruppe gesichert haben.
- Sie müssen alle ein-/Ausgänge (E/A) angehalten haben.
- Sie müssen die Bereitstellung von Dateisystemen auf den Volumes aufheben.
- Sie müssen alle Spiegelbeziehungen im Pool oder in der Volume-Gruppe gelöscht haben.
- Sie müssen alle laufenden Volume-Kopiervorgang für den Pool oder die Volume-Gruppe angehalten haben.
- Der Pool oder die Volume-Gruppe darf nicht an einem asynchronen Spiegelungsvorgang teilnehmen.
- Die Laufwerke in der Volume-Gruppe dürfen nicht über eine dauerhafte Reservierung verfügen.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit dem Pool oder der Volume-Gruppe aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].

3. Wählen Sie einen Pool oder eine Volume-Gruppe aus der Liste aus.

   Sie können jeweils nur einen Pool oder eine Volume-Gruppe auswählen. Scrollen Sie in der Liste nach unten, um weitere Pools oder Volume-Gruppen zu sehen.

4. Wählen Sie Menü:Sonstige Aufgaben[Löschen] und bestätigen Sie.

Ergebnisse

Das System führt die folgenden Aktionen durch:

- Löscht alle Daten im Pool oder der Volume-Gruppe.
- Löscht alle Laufwerke, die dem Pool oder der Volume-Gruppe zugeordnet sind.
- Hebt die Zuweisung der zugehörigen Laufwerke auf und ermöglicht die Wiederverwendung in neuen oder vorhandenen Pools oder Volume-Gruppen.

Konsolidierung der freien Kapazität für eine Volume-Gruppe im SANtricity Speicher-Plug-in für vCenter

Verwenden Sie die Option freie Kapazität konsolidieren, um vorhandene freie Erweiterungen auf einer ausgewählten Volume-Gruppe zu konsolidieren. Durch diese Aktion können Sie aus der maximalen freien Kapazität in einer Volume-Gruppe zusätzliche Volumes erstellen.

Bevor Sie beginnen

- Die Volume-Gruppe muss mindestens einen freien Kapazitätsbereich enthalten.
- Alle Volumes in der Volume-Gruppe müssen den Status „Online“ und „optimal“ aufweisen.
- Volume-Änderungsvorgänge dürfen nicht ausgeführt werden, z. B. das Ändern der Segmentgröße eines Volumes.

Über diese Aufgabe

Sie können den Vorgang nach dem Start nicht mehr abbrechen. Der Zugriff auf Ihre Daten bleibt während des Konsolidierungsvorgangs erhalten.

Sie können das Dialogfeld Freie Kapazität konsolidieren mit einer der folgenden Methoden starten:

- Wenn für eine Volume-Gruppe mindestens ein freier Kapazitätsbereich erkannt wird, erscheint die Empfehlung zur Konsolidierung freier Kapazität auf der Startseite im Benachrichtigungsbereich. Klicken Sie auf den Link **freie Kapazität konsolidieren**, um das Dialogfeld zu starten.
- Sie können das Dialogfeld „freie Kapazität konsolidieren“ auch auf der Seite Pools & Volume Groups starten, wie in der folgenden Aufgabe beschrieben.

Mehr über freie Kapazitätsbereiche

Ein freier Kapazitätsbereich stellt die freie Kapazität dar, die zum Löschen eines Volumes oder zum Nichtnutzen der gesamten verfügbaren freien Kapazität während der Volume-Erstellung führen kann. Wenn Sie ein Volume in einer Volume-Gruppe mit einem oder mehreren freien Kapazitätsbereichen erstellen, ist die Kapazität des Volumes auf den größten freien Kapazitätsbereich in dieser Volume-Gruppe beschränkt. Wenn beispielsweise eine Volume-Gruppe insgesamt 15 gib freie Kapazität besitzt und der größte Bereich der freien Kapazität 10 gib beträgt, beträgt das größte Volume, das Sie erstellen können, 10 gib.

Sie konsolidieren freie Kapazitäten auf einer Volume-Gruppe, um die Schreib-Performance zu verbessern. Die freie Kapazität Ihrer Volume-Gruppe wird im Laufe der Zeit fragmentiert, wenn der Host Dateien schreibt, ändert und löscht. Schließlich befindet sich die verfügbare Kapazität nicht in einem einzigen zusammenhängenden Block, sondern wird in kleinen Fragmenten über die Volume-Gruppe verteilt. Dies führt zu einer weiteren Dateifragmentierung, da der Host neue Dateien als Fragmente schreiben muss, um sie in die verfügbaren Bereiche freier Cluster zu passen.

Durch die Konsolidierung der freien Kapazität einer ausgewählten Volume-Gruppe wird eine verbesserte Performance des Filesystems erzielt, wenn der Host neue Dateien schreibt. Der Konsolidierungsvorgang wird auch dazu beitragen, dass neue Dateien in Zukunft nicht fragmentiert werden.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit der Volume-Gruppe aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Wählen Sie die Volume-Gruppe mit freier Kapazität, die Sie konsolidieren möchten, und wählen Sie dann Menü:Sonstige Aufgaben[freie Kapazität der Volume-Gruppe konsolidieren].

   Das Dialogfeld Freie Kapazität konsolidieren wird angezeigt.

4. Typ `consolidate` Um zu bestätigen, dass Sie diesen Vorgang ausführen möchten.
5. Klicken Sie Auf **Konsolidieren**.

Ergebnis

Das System beginnt die Konsolidierung (Defragmentierung) der freien Kapazitätsbereiche der Volume-Gruppe in eine zusammenhängende Menge für nachfolgende Speicherkonfigurationsaufgaben.

Nachdem Sie fertig sind

Wählen Sie in der Navigationsleiste **Operationen** aus, um den Fortschritt des Vorgangs „Freie Kapazität konsolidieren“ anzuzeigen. Dieser Vorgang kann langwierig sein und die System-Performance beeinträchtigen.

Schalten Sie die LED-Anzeigen auf einem Laufwerk im SANtricity-Speichermodul für vCenter ein

Nach Laufwerken können Sie alle Laufwerke physisch identifizieren, die einen ausgewählten Pool, eine Volume-Gruppe oder SSD Cache umfassen. An jedem Laufwerk im ausgewählten Pool, der Volume-Gruppe oder dem SSD-Cache leuchtet eine LED-Anzeige auf.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].

3. Wählen Sie den Pool, die Volume-Gruppe oder den SSD-Cache aus, den Sie suchen möchten, und klicken Sie dann auf MENU:Mehr[Locator Lights einschalten].

   Es wird ein Dialogfeld angezeigt, in dem die Leuchten der Laufwerke angezeigt werden, die den ausgewählten Pool, die Volume-Gruppe oder den SSD-Cache enthalten.

4. Nachdem Sie die Laufwerke erfolgreich gefunden haben, klicken Sie auf **Ausschalten**.

Reduzieren Sie die Kapazität eines vorhandenen Pools oder SSD-Caches im SANtricity Storage Plug-in für vCenter

Sie können Laufwerke entfernen, um die Kapazität eines vorhandenen Pools oder SSD-Caches zu reduzieren.

Nach dem Entfernen von Laufwerken werden die Daten in jedem Volume des Pools oder SSD-Caches auf die übrigen Laufwerke verteilt. Entfernte Laufwerke werden nicht zugewiesen, und ihre Kapazität wird Teil der gesamten freien Kapazität des Speicher-Arrays.

Über diese Aufgabe

Beachten Sie beim Entfernen der Kapazität die folgenden Richtlinien:

- Sie können das letzte Laufwerk in einem SSD-Cache nicht entfernen, ohne zuerst den SSD-Cache zu löschen.
- Sie können die Anzahl der Laufwerke in einem Pool nicht auf weniger als 11 Laufwerke reduzieren.
- Sie können maximal 12 Laufwerke gleichzeitig entfernen. Wenn Sie mehr als 12 Laufwerke entfernen müssen, wiederholen Sie den Vorgang.
- Laufwerke können nicht entfernt werden, wenn nicht genügend freie Kapazität im Pool oder SSD-Cache vorhanden ist, um die Daten zu enthalten, wenn diese Daten auf die übrigen Laufwerke im Pool oder SSD-Cache verteilt werden.

Im Folgenden finden Sie potenzielle Performance-Auswirkungen:

- Das Entfernen von Laufwerken aus einem Pool oder SSD Cache kann zu einer reduzierten Volume-Performance führen.
- Die unveränderte Kapazität wird nicht verbraucht, wenn Sie Kapazität aus einem Pool oder SSD Cache entfernen. Die Konservierungskapazität kann sich jedoch aufgrund der Anzahl der im Pool verbliebenen Laufwerke oder des SSD Cache verringern.

Folgende Auswirkungen haben sichere Laufwerke:

- Wenn Sie das letzte Laufwerk entfernen, das nicht sicher-fähig ist, wird der Pool mit allen sicheren Laufwerken belassen. In dieser Situation haben Sie die Möglichkeit, die Sicherheit für den Pool zu aktivieren.
- Wenn Sie das letzte Laufwerk entfernen, das nicht Data Assurance (da)-fähig ist, bleibt der Pool mit allen da-fähigen Laufwerken.
- Alle neuen Volumes, die Sie auf dem Pool erstellen, sind da-fähig. Wenn vorhandene Volumes als da-fähig sein sollen, müssen Sie das Volume löschen und dann neu erstellen.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array aus.

Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].

2. Wählen Sie den Pool oder SSD Cache aus und klicken Sie dann auf Menü:Mehr[Kapazität entfernen].

   Das Dialogfeld Kapazität entfernen wird angezeigt.

3. Wählen Sie ein oder mehrere Laufwerke in der Liste aus.

   Wenn Sie in der Liste Laufwerke auswählen oder deauswählen, wird das Feld für die ausgewählte Gesamtkapazität aktualisiert. Dieses Feld zeigt die Gesamtkapazität des Pools oder SSD-Caches an, die nach dem Entfernen der ausgewählten Laufwerke Ergebnisse liefert.

4. Klicken Sie auf **Entfernen** und bestätigen Sie, dass Sie die Laufwerke entfernen möchten.

Ergebnis

Die neu reduzierte Kapazität des Pool oder SSD-Cache wird in der Ansicht Pools und Volume-Gruppen dargestellt.

Aktivieren Sie die Sicherheit für einen Pool oder eine Volume-Gruppe im SANtricity Speicher-Plug-in für vCenter

Sie können die Laufwerkssicherheit für einen Pool oder eine Volume-Gruppe aktivieren, um unbefugten Zugriff auf die Daten auf den Laufwerken im Pool oder der Volume-Gruppe zu verhindern.

Lese- und Schreibzugriff auf die Laufwerke ist nur über einen Controller verfügbar, der mit einem Sicherheitsschlüssel konfiguriert ist.

Bevor Sie beginnen

- Die Laufwerkssicherheitsfunktion muss aktiviert sein.
- Ein Sicherheitsschlüssel muss erstellt werden.
- Der Pool oder die Volume-Gruppe muss sich im optimalen Zustand befinden.
- Alle Laufwerke im Pool oder in der Volume-Gruppe müssen sichere Laufwerke sein.

Über diese Aufgabe

Wenn Sie die Laufwerkssicherheit verwenden möchten, wählen Sie einen Pool oder eine Volume-Gruppe aus, der sicher ist. Ein Pool oder eine Volume-Gruppe kann sowohl sichere als auch nicht sichere Laufwerke enthalten. Zur Nutzung der Verschlüsselungsfunktionen müssen jedoch alle Laufwerke sicher sein.

Nach Aktivierung der Sicherheitskontrolle können Sie sie nur entfernen, indem Sie den Pool oder die Volume-Gruppe löschen und dann die Laufwerke löschen.

Schritte

1. Wählen Sie auf der Seite Verwalten das Speicher-Array mit dem Pool oder der Volume-Gruppe aus.
2. Wählen Sie Menü:Provisioning[Pools und Volume-Gruppen konfigurieren].
3. Wählen Sie den Pool oder die Volume-Gruppe aus, auf dem Sie die Sicherheit aktivieren möchten, und klicken Sie dann auf Menü:Mehr[Sicherheit aktivieren].

   Das Dialogfeld Sicherheit bestätigen wird angezeigt.

4. Bestätigen Sie, dass Sie die Sicherheit für den ausgewählten Pool oder die ausgewählte Volume-Gruppe

aktivieren möchten, und klicken Sie dann auf **Aktivieren**.

Entfernen Sie das SANtricity Storage Plug-in für vCenter

Sie können das Plugin von der vCenter Server Appliance entfernen und den Plugin Webserver vom Anwendungs-Host deinstallieren.

Dies sind zwei verschiedene Schritte, die Sie in jeder Reihenfolge durchführen können. Wenn Sie jedoch den Plugin-Webserver vor der Registrierung des Plugins vom Anwendungs-Host entfernen möchten, wird das Registrierungsskript während dieses Prozesses entfernt und Sie können die Registrierung nicht mit Methode 1 aufheben.

Registrieren Sie das Plug-in von einer vCenter Server Appliance

Um das Plugin von einer vCenter Server Appliance zu registrieren, wählen Sie eine der folgenden Methoden aus:

- Methode 1: Führen Sie das Registrierungsskript aus
- Methode 2: Verwenden Sie die vCenter Server Mob Seiten

Methode 1: Führen Sie das Registrierungsskript aus

1. Öffnen Sie eine Eingabeaufforderung über die Befehlszeile, und navigieren Sie zum folgenden Verzeichnis:

   ```
   <install directory>\vcenter-register\bin
   ```

2. Ausführen des `vcenter-register.bat` Datei:

   ```
   vcenter-register.bat ^

   -action unregisterPlugin ^

   -vcenterHostname <vCenter FQDN> ^

   -username <Administrator Username> ^
   ```

3. Vergewissern Sie sich, dass das Skript erfolgreich ist.

   Die Protokolle werden in gespeichert `%install_dir%/working/logs/vc-registration.log`.

Methode 2: Verwenden Sie die vCenter Server Mob Seiten

1. Öffnen Sie einen Webbrowser, und geben Sie die folgende url ein:

   https://<FQDN[] Von vCenter Server>/mob

2. Melden Sie sich unter den Anmeldedaten des Administrators an.
3. Suchen Sie nach dem Eigenschaftsnamen von `extensionManager` Und klicken Sie auf den Link, der dieser Eigenschaft zugeordnet ist.
4. Erweitern Sie die Eigenschaftenliste, indem Sie auf **Mehr**… klicken Link unten in der Liste.
5. Überprüfen Sie, ob die Erweiterung `plugin.netapp.eseries` Befindet sich in der Liste.

6. Wenn sie vorhanden ist, klicken Sie auf die Methode `UnregisterExtension`.
7. Geben Sie den Wert ein `plugin.netapp.eseries` Klicken Sie im Dialogfeld auf **Methode aufrufen**.
8. Schließen Sie das Dialogfeld, und aktualisieren Sie den Webbrowser.
9. Überprüfen Sie das `plugin.netapp.eseries` Erweiterung ist nicht in der Liste.

> Durch dieses Verfahren wird das Plugin von der vCenter Server Appliance registriert; es entfernt jedoch keine Plugin-Paketdateien vom Server. Um Paketdateien zu entfernen, verwenden Sie SSH, um auf die vCenter Server Appliance zuzugreifen und um zum folgenden Verzeichnis zu navigieren: `etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/`. Entfernen Sie dann das mit dem Plugin verknüpfte Verzeichnis.

Entfernen Sie den Plugin-Webserver vom Anwendungs-Host

So entfernen Sie die Plugin-Software vom Anwendungs-Host:

1. Navigieren Sie vom Anwendungsserver zur **Systemsteuerung**.
2. Gehen Sie zu **Apps & Features** und wählen Sie dann **SANtricity Storage Plugin für vCenter**.
3. Klicken Sie Auf **Deinstallieren/Ändern**.

   Ein Bestätigungsdialogfeld wird geöffnet.
4. Klicken Sie Auf **Deinstallieren**.

   Nach Abschluss der Deinstallation wird eine Bestätigungsmeldung angezeigt.
5. Klicken Sie Auf **Fertig**.

FAQ zum SANtricity Storage Plugin für vCenter

Diese FAQ kann Ihnen helfen, wenn Sie nur nach einer schnellen Antwort auf eine Frage suchen.

Welche Einstellungen werden importiert?

Die Funktion „Importeinstellungen“ ist ein Batch-Vorgang, bei dem Konfigurationen von einem Speicher-Array auf mehrere Speicher-Arrays geladen werden.

Die während dieses Vorgangs importierten Einstellungen hängen davon ab, wie das Quell-Speicher-Array in System Manager konfiguriert ist. Die folgenden Einstellungen können in mehrere Speicher-Arrays importiert werden:

- **E-Mail-Alarme** — Einstellungen beinhalten eine E-Mail-Server-Adresse und die E-Mail-Adressen der Warnungsempfänger.
- **Syslog Alerts** — Einstellungen beinhalten eine Syslog-Serveradresse und einen UDP-Port.
- **SNMP Alerts** — Einstellungen beinhalten einen Community-Namen und eine IP-Adresse für den SNMP-Server.
- **AutoSupport** — Einstellungen umfassen die separaten Funktionen (Basic AutoSupport, AutoSupport OnDemand und Remote Diagnostics), das Wartungsfenster, die Bereitstellungsmethode, Und dem Versandplan.

- **Directory Services** — die Konfiguration umfasst den Domänennamen und die URL eines LDAP-Servers (Lightweight Directory Access Protocol) sowie die Zuordnungen für die Benutzergruppen des LDAP-Servers zu den vordefinierten Rollen des Speicher-Arrays.
- **Speicherkonfiguration** — Konfigurationen umfassen Volumes (nur dicke und nur nicht-Repository-Volumes), Volume-Gruppen, Pools und Hot-Spare-Laufwerkszuordnungen.
- **Systemeinstellungen** — Konfigurationen umfassen Medien-Scan-Einstellungen für ein Volume, SSD-Cache für Controller und automatischen Lastausgleich (ohne Berichterstellung über Hostkonnektivität).

Warum sehe ich nicht alle meine Storage Arrays?

Während des Vorgangs „Importeinstellungen“ stehen einige Ihrer Speicherarrays möglicherweise nicht im Dialogfeld „Zielauswahl“ zur Verfügung.

Speicher-Arrays werden möglicherweise aus den folgenden Gründen nicht angezeigt:

- Die Firmware-Version ist unter 8.50.
- Das Speicher-Array ist offline.
- Das System kann nicht mit diesem Array kommunizieren (z. B. verfügt das Array über Zertifikat-, Passwort- oder Netzwerkprobleme).

Warum sind diese Volumes nicht mit einem Workload verbunden?

Volumes sind keinem Workload zugeordnet, wenn sie mithilfe der Befehlszeilenschnittstelle (CLI) erstellt wurden oder aus einem anderen Storage-Array migriert (importiert/exportiert) wurden.

Wie wirkt sich mein ausgewählter Workload auf die Erstellung des Volumes aus?

Während der Volume-Erstellung werden Sie aufgefordert, Informationen über die Verwendung eines Workloads zu erhalten. Das System erstellt anhand dieser Informationen eine optimale Volume-Konfiguration für Sie, die Sie nach Bedarf bearbeiten können. Optional können Sie diesen Schritt in der Sequenz zur Volume-Erstellung überspringen.

Ein Workload ist ein Storage-Objekt, das eine Applikation unterstützt. Sie können einen oder mehrere Workloads oder Instanzen pro Applikation definieren. Bei einigen Applikationen konfiguriert das System den Workload so, dass er Volumes mit ähnlichen zugrunde liegenden Volume-Merkmalen enthält. Diese Volume-Merkmale werden basierend auf dem Applikationstyp optimiert, den der Workload unterstützt. Wenn Sie beispielsweise einen Workload erstellen, der eine Microsoft SQL Server Applikation unterstützt und anschließend Volumes für diesen Workload erstellt, werden die zugrunde liegenden Volume-Merkmale zur Unterstützung von Microsoft SQL Server optimiert.

- **Applikationsspezifisch** — Wenn Sie Volumes mit einem anwendungsspezifischen Workload erstellen, empfiehlt das System möglicherweise eine optimierte Volume-Konfiguration, um Konflikte zwischen Applikations-Workload I/O und anderem Traffic aus Ihrer Anwendungsinstanz zu minimieren. Volume-Merkmale wie I/O-Typ, Segmentgröße, Controller-Besitz und Lese- und Schreib-Cache werden automatisch für Workloads empfohlen und optimiert, die für die folgenden Applikationstypen erstellt wurden.
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Videoüberwachungsapplikationen
  - VMware ESXi (für Volumes, die mit dem Virtual Machine File System verwendet werden sollen)

Sie können die empfohlene Volume-Konfiguration prüfen und die vom System empfohlenen Volumes und Eigenschaften bearbeiten, hinzufügen oder löschen. Verwenden Sie dazu das Dialogfeld Volumes hinzufügen/bearbeiten.

- **Andere (oder Anwendungen ohne spezifische Unterstützung der Volumenerzeugung)** — Bei anderen Workloads wird eine Volume-Konfiguration verwendet, die manuell angegeben werden muss, wann ein Workload erstellt werden soll, der nicht mit einer bestimmten Applikation verknüpft ist, oder ob keine integrierte Optimierung für die Applikation vorhanden ist, die Sie im Storage-Array verwenden möchten. Sie müssen die Volume-Konfiguration manuell über das Dialogfeld Volumes hinzufügen/bearbeiten angeben.

Warum sehe ich nicht alle meine Volumes, Hosts oder Host Cluster?

Snapshot-Volumes mit einem da-fähigen Basis-Volume können nicht einem Host zugewiesen werden, der nicht Data Assurance (da)-fähig ist. Sie müssen das da auf dem Basisvolume deaktivieren, bevor ein Snapshot-Volume einem Host zugewiesen werden kann, der nicht über da-fähig ist.

Beachten Sie die folgenden Richtlinien für den Host, dem Sie das Snapshot-Volume zuweisen:

- Ein Host ist nicht da-fähig, wenn er über eine I/O-Schnittstelle, die nicht über da-fähig ist, mit dem Speicher-Array verbunden ist.
- Ein Host-Cluster ist nicht da-fähig, wenn es mindestens ein Hostmitglied hat, das nicht da-fähig ist.

Sie können da nicht auf einem Volume deaktivieren, das mit Snapshots (Konsistenzgruppen, Snapshot-Gruppen, Snapshot-Images und Snapshot-Volumes), Volume-Kopien, Und Spiegelungen. Alle zugeordneten Kapazitäts- und Snapshot-Objekte müssen gelöscht werden, bevor das da auf dem Basis-Volume deaktiviert werden kann.

Warum kann ich den ausgewählten Workload nicht löschen?

Dieser Workload besteht aus einer Gruppe von Volumes, die mithilfe der Befehlszeilenschnittstelle (CLI) erstellt oder von einem anderen Storage Array migriert (importiert/exportiert) wurden. Daher sind die Volumes in diesem Workload keinem applikationsspezifischen Workload zugeordnet, sodass der Workload nicht gelöscht werden kann.

Wie können mir applikationsspezifische Workloads beim Management meines Storage Arrays helfen?

Die Volume-Merkmale Ihres applikationsspezifischen Workloads diktieren, wie der Workload mit den Komponenten des Storage-Arrays interagiert und die Performance Ihrer Umgebung im Rahmen einer bestimmten Konfiguration bestimmt.

Eine Applikation ist Software wie SQL Server oder Exchange. Sie definieren einen oder mehrere Workloads, um jede Applikation zu unterstützen. Für einige Applikationen empfiehlt das System automatisch eine Volume-Konfiguration zur Optimierung des Storage. Merkmale wie I/O-Typ, Segmentgröße, Controller-Eigentümer und Lese- und Schreib-Cache sind in der Volume-Konfiguration enthalten.

Was muss ich tun, um die erweiterte Kapazität erkennen zu können?

Wenn Sie die Kapazität für ein Volume erhöhen, erkennt der Host möglicherweise nicht sofort den Anstieg der Volume-Kapazität.

Die meisten Betriebssysteme erkennen die erweiterte Volume-Kapazität und werden nach dem Start der Volume-Erweiterung automatisch erweitert. Einige könnten jedoch nicht. Wenn Ihr Betriebssystem die erweiterte Volume-Kapazität nicht automatisch erkennt, müssen Sie möglicherweise eine erneute Festplattenüberprüfung durchführen oder einen Neustart durchführen.

Nachdem Sie die Volume-Kapazität erweitert haben, müssen Sie die Größe des Dateisystems manuell erhöhen, um sie anzupassen. Wie Sie dies tun, hängt von dem Dateisystem ab, das Sie verwenden.

Weitere Informationen finden Sie in der Dokumentation Ihres Host-Betriebssystems.

Wann soll ich die spätere Auswahl Host zuweisen verwenden?

Wenn Sie den Prozess zum Erstellen von Volumes beschleunigen möchten, können Sie den Hostzuordnungsschritt überspringen, damit neu erstellte Volumes offline initialisiert werden.

Die neu erstellten Volumes müssen initialisiert werden. Das System kann sie mit einem von zwei Modi initialisieren – entweder einem sofortigen verfügbaren Format (IAF)-Hintergrundinitialisierungsprozess oder einem Offline-Prozess.

Wenn Sie ein Volume einem Host zuordnen, ist es erforderlich, dass alle Initialisierungsvolumes in dieser Gruppe in eine Hintergrundinitialisierung übergehen. Durch diesen Hintergrundinitialisierungsprozess können gleichzeitige Host-I/O-Vorgänge erfolgen, was manchmal sehr zeitaufwendig sein kann.

Wenn keines der Volumes einer Volume-Gruppe zugeordnet ist, wird die Offline-Initialisierung durchgeführt. Der Offline-Prozess ist viel schneller als der Hintergrundprozess.

Was muss ich über die Anforderungen der Host-Blockgröße wissen?

Bei EF300- und EF600-Systemen kann ein Volume so eingestellt werden, dass es 512 Byte oder 4 KiB-Blockgrößen unterstützt (auch als „Sektorgröße“ bezeichnet). Sie müssen den richtigen Wert während der Volume-Erstellung einstellen. Wenn möglich, schlägt das System den entsprechenden Standardwert vor.

Bevor Sie die Blockgröße des Volumes festlegen, lesen Sie die folgenden Einschränkungen und Richtlinien.

- Einige Betriebssysteme und Virtual Machines (vornehmlich VMware) erfordern derzeit eine 512-Byte-Blockgröße und unterstützen keine 4KiB. Achten Sie also darauf, die Host-Anforderungen zu kennen, bevor Sie ein Volume erstellen. In der Regel können Sie die beste Leistung erreichen, indem Sie ein Volumen setzen, um eine 4KiB Block-Größe zu präsentieren; jedoch sicherstellen, dass Ihr Host für 4KiB (oder "4Kn") Blöcke erlaubt.
- Der für den Pool bzw. die Volume-Gruppe ausgewählte Laufwerkstyp legt außerdem fest, welche Volume-Blockgrößen unterstützt werden:
  - Wenn Sie eine Volume-Gruppe mit Laufwerken erstellen, die in 512-Byte-Blöcke schreiben, dann können Sie nur Volumes mit 512-Byte-Blöcken erstellen.
  - Wenn Sie eine Volume-Gruppe mit Laufwerken erstellen, die in 4KiB-Blöcke schreiben, dann können Sie Volumes entweder mit 512-Byte- oder 4KiB-Blöcken erstellen.
- Wenn das Array über eine iSCSI-Host-Schnittstellenkarte verfügt, sind alle Volumes auf 512-Byte-Blöcke beschränkt (unabhängig von der Blockgröße der Volume-Gruppe). Dies ist auf eine bestimmte Hardware-Implementierung zurückzuführen.
- Sobald die Blockgröße festgelegt ist, können Sie sie nicht ändern. Wenn Sie eine Blockgröße ändern müssen, müssen Sie das Volume löschen und neu erstellen.

Warum sollte ich ein Host-Cluster erstellen?

Sie müssen ein Host-Cluster erstellen, wenn Sie mindestens zwei Hosts über gemeinsamen Zugriff auf dieselbe Gruppe von Volumes verfügen möchten. Normalerweise sind auf den einzelnen Hosts Clustering-Software installiert, um den Volume-Zugriff zu koordinieren.

Wie kann ich feststellen, welches Host-Betriebssystem richtig ist?

Das Feld Host-Betriebssystemtyp enthält das Betriebssystem des Hosts. Sie können den empfohlenen Hosttyp aus der Dropdown-Liste auswählen.

Die Hosttypen, die in der Dropdown-Liste angezeigt werden, hängen vom Speicher-Array-Modell und der Firmware-Version ab. Die neuesten Versionen zeigen zuerst die häufigsten Optionen an, die am wahrscheinlichsten geeignet sind. Die Darstellung in dieser Liste impliziert nicht, dass die Option vollständig unterstützt wird.

Weitere Informationen zur Host-Unterstützung finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Einige der folgenden Host-Typen werden möglicherweise in der Liste angezeigt:

Host-Betriebssystem	Betriebssystem und Multipath-Treiber
Linux DM-MP (Kernel 3.10 oder höher)	Unterstützt Linux-Betriebssysteme mit einer Device Mapper Multipath Failover-Lösung mit einem 3.10 oder höher Kernel.
VMware ESXi	Unterstützung für VMware ESXi Betriebssysteme mit der Nnativen Multipathing Plug-in-Architektur (NMP) mit dem integrierten Storage Array Type Policy-Modul SATP_ALUA von VMware.
Windows (Cluster oder nicht-Cluster)	Unterstützt Konfigurationen mit Windows-Clustern oder nicht-Clustern, die den ATTO-Multipathing-Treiber nicht ausführen.
ATTO Cluster (alle Betriebssysteme)	Unterstützt alle Clusterkonfigurationen unter Verwendung des Multipathing-Treibers ATTO Technology, Inc.
Linux (Veritas DMP)	Unterstützung von Linux Betriebssystemen mit einer Veritas DMP-Multipathing-Lösung.
Linux (ATTO)	Unterstützt Linux-Betriebssysteme unter Verwendung eines ATTO Technology, Inc., Multipathing-Treibers.
Mac OS	Unterstützt Mac-Betriebssystemversionen mit einem Multipathing-Treiber ATTO Technology, Inc.
Windows (ATTO)	Unterstützt Windows-Betriebssysteme mit einem Multipathing-Treiber ATTO Technology, Inc.
IBM SVC	Unterstützt eine IBM SAN Volume Controller-Konfiguration.
Werkseitige Standardeinstellung	Reserviert für den Erststart des Speicher-Arrays. Wenn Ihr Host-Betriebssystem auf Werkseinstellung eingestellt ist, ändern Sie es entsprechend dem Host-Betriebssystem und dem Multipath-Treiber, der auf dem angeschlossenen Host ausgeführt wird.
Linux DM-MP (Kernal 3.9 oder früher)	Unterstützt Linux-Betriebssysteme mit einer Device Mapper Multipath Failover-Lösung mit einem 3.9 oder früheren Kernel.

Host-Betriebssystem	Betriebssystem und Multipath-Treiber
Cluster-Fenster (veraltet)	Wenn Ihr Host-Betriebssystem-Typ auf diesen Wert eingestellt ist, verwenden Sie stattdessen die Windows-Einstellung (Cluster oder nicht-Cluster).

Wie Stelle ich die Host-Ports einem Host gegenüber?

Wenn Sie einen Host manuell erstellen, müssen Sie zuerst das entsprechende HBA-Dienstprogramm (Host Bus Adapter) verwenden, das auf dem Host verfügbar ist, um die Host-Port-IDs zu ermitteln, die mit jedem HBA verknüpft sind, der im Host installiert ist.

Wenn Sie über diese Informationen verfügen, wählen Sie aus der Liste im Dialogfeld „Host erstellen“ die Host-Port-IDs aus, die sich beim Speicher-Array angemeldet haben.

Stellen Sie sicher, dass Sie die entsprechenden Host-Port-IDs für den von Ihnen erstellten Host auswählen. Wenn Sie die falschen Host-Port-IDs zuordnen, können Sie unbeabsichtigten Zugriff von einem anderen Host auf diese Daten verursachen.

Was ist das Standard-Cluster?

Das Standard-Cluster ist eine systemdefinierte Einheit, die jedem nicht zugeordneten Host-Port-Identifier, der beim Speicher-Array angemeldet ist, den Zugriff auf Volumes ermöglicht, die dem Standardcluster zugewiesen sind.

Eine nicht zugeordnete Host-Port-ID ist ein Host-Port, der nicht logisch einem bestimmten Host zugeordnet ist, aber physisch in einem Host installiert und beim Speicher-Array angemeldet ist.

Wenn Hosts spezifischen Zugriff auf bestimmte Volumes im Storage-Array haben sollen, dürfen Sie das Standardcluster nicht verwenden. Stattdessen müssen Sie die Host-Port-IDs den entsprechenden Hosts zuordnen. Diese Aufgabe kann während des Vorgangs „Host erstellen“ manuell ausgeführt werden. Anschließend weisen Sie Volumes einem einzelnen Host oder einem Host-Cluster zu.

Sie sollten das Standardcluster nur in besonderen Situationen verwenden, in denen Ihre externe Speicherumgebung geeignet ist, allen Hosts und allen angemeldeten Host-Port-IDs, die mit dem Speicher-Array verbunden sind, Zugriff auf alle Volumes zu gewähren (All-Access-Modus). Ohne die Hosts dem Storage Array oder der Benutzeroberfläche bekannt zu machen.

Zunächst können Sie Volumes über die Befehlszeilenschnittstelle (CLI) nur dem Standard-Cluster zuweisen. Nachdem Sie dem Standard-Cluster jedoch mindestens ein Volume zugewiesen haben, wird diese Einheit (als Standard-Cluster bezeichnet) in der Benutzeroberfläche angezeigt, in der Sie diese Einheit verwalten können.

Was ist Redundanzprüfung?

Durch eine Redundanzprüfung wird ermittelt, ob die Daten auf einem Volume in einem Pool oder einer Volume-Gruppe konsistent sind. Redundanzdaten dienen der schnellen Rekonstruktion von Informationen über das Ersatzlaufwerk, wenn eines der Laufwerke im Pool oder der Volume-Gruppe ausfällt.

Sie können diese Prüfung nur für einen Pool oder eine Volume-Gruppe gleichzeitig durchführen. Bei einer Volume-Redundanzprüfung werden folgende Aktionen durchgeführt:

- Scannt die Datenblöcke in einem RAID 3-Volume, einem RAID 5-Volume oder einem RAID 6-Volume und

überprüft anschließend die Redundanzinformationen für jeden Block. (RAID 3 kann Volume-Gruppen nur über die Befehlszeilenschnittstelle zugewiesen werden.)

- Vergleicht die Datenblöcke auf gespiegelten RAID 1-Laufwerken.
- Gibt Redundanzfehler zurück, wenn die Daten von der Controller-Firmware uneinheitlich sind.

> Eine sofortige Durchführung einer Redundanzprüfung auf demselben Pool oder derselben Volume-Gruppe kann zu einem Fehler führen. Um dieses Problem zu vermeiden, warten Sie ein bis zwei Minuten, bevor Sie eine weitere Redundanzprüfung auf demselben Pool oder derselben Volume-Gruppe durchführen.

Was ist Erhaltungskapazität?

Bei der Konservierung wird die Kapazität (Anzahl der Laufwerke) verwendet, die in einem Pool reserviert ist, um potenzielle Laufwerksausfälle zu unterstützen.

Wenn ein Pool erstellt wird, reserviert das System abhängig von der Anzahl der Laufwerke im Pool automatisch eine standardmäßige Anlagenkapazität.

Pools nutzen während der Rekonstruktion haltende Kapazitäten, wohingegen Volume-Gruppen Hot-Spare-Festplatten zu demselben Zweck einsetzen. Die Methode zur Erhaltung der Kapazität ist eine Verbesserung gegenüber Hot-Spare-Festplatten, da sie eine schnellere Rekonstruktion ermöglicht. Die Konservierungskapazität wird bei einem Hot-Spare-Laufwerk über eine Anzahl von Laufwerken im Pool verteilt, nicht auf einer Festplatte, sodass die Geschwindigkeit und Verfügbarkeit einer einzelnen Festplatte nicht eingeschränkt ist.

Welches RAID-Level eignet sich am besten für meine Applikation?

Um die Performance einer Volume-Gruppe zu maximieren, müssen Sie den entsprechenden RAID-Level auswählen.

Sie können den entsprechenden RAID-Level ermitteln, indem Sie die Prozentsätze für Lese- und Schreibvorgänge für die Anwendungen kennen, die auf die Volume-Gruppe zugreifen. Verwenden Sie die Seite Performance, um diese Prozentsätze zu erhalten.

RAID-Level und Applikations-Performance

RAID verwendet eine Reihe von Konfigurationen, sogenannte Level, um zu ermitteln, wie Benutzer- und Redundanzdaten von den Laufwerken geschrieben und abgerufen werden. Jedes RAID-Level stellt eigene Performance-Funktionen bereit. Applikationen mit einem hohen Prozentsatz für Lesevorgänge können aufgrund der hervorragenden Lese-Performance der RAID 5- und RAID 6-Konfigurationen auch mit RAID 5-Volumes oder RAID 6-Volumes arbeiten.

Applikationen mit einem niedrigen Read-Prozentsatz (schreibintensiv) erbringen keine gute Performance auf RAID 5 Volumes oder RAID 6 Volumes. Die Performance ist beeinträchtigt, und das Ergebnis ist die Art und Weise, wie ein Controller Daten und Redundanzdaten auf die Laufwerke in einer RAID 5-Volume-Gruppe oder einer RAID 6-Volume-Gruppe schreibt.

Wählen Sie basierend auf den folgenden Informationen einen RAID-Level aus.

RAID 0

Beschreibung:

- Nicht-redundant, Striping-Modus.
- RAID 0 verteilt Daten auf alle Laufwerke der Volume-Gruppe.

Datenschutzfunktionen:

- RAID 0 wird für hohe Verfügbarkeitsanforderungen nicht empfohlen. RAID 0 ist besser für nicht-kritische Daten.
- Wenn ein einzelnes Laufwerk in der Volume-Gruppe ausfällt, fallen alle zugehörigen Volumes aus und alle Daten gehen verloren.

Anzahl der Laufwerke:

- Für RAID-Level 0 ist mindestens ein Laufwerk erforderlich.
- RAID 0-Volume-Gruppen können mehr als 30 Laufwerke haben.
- Sie können eine Volume-Gruppe erstellen, die alle Laufwerke im Speicher-Array umfasst.

RAID 1 oder RAID 10

Beschreibung:

- Striping/Mirror-Modus.

Wie es funktioniert:

- RAID 1 verwendet die Festplattenspiegelung, um Daten auf zwei doppelte Festplatten gleichzeitig zu schreiben.
- RAID 10 nutzt Laufwerk-Striping, um Daten über eine Reihe gespiegelter Laufwerkpaare zu verteilen.

Datenschutzfunktionen:

- RAID 1 und RAID 10 bieten eine hohe Performance und eine beste Datenverfügbarkeit.
- RAID 1 und RAID 10 verwenden die Laufwerkspiegelung, um eine exakte Kopie von einem Laufwerk auf ein anderes Laufwerk zu erstellen.
- Fällt eines der Laufwerke in einem Laufwerkspaar aus, kann das Storage-Array sofort auf ein anderes Laufwerk umschalten, ohne dass Daten oder Service verloren gehen.
- Ein Ausfall eines Laufwerks führt dazu, dass zugehörige Volumes beeinträchtigt werden. Das Spiegellaufwerk ermöglicht den Zugriff auf die Daten.
- Ein Laufwerkausfall in einer Volume-Gruppe führt zu einem Ausfall aller damit verbundenen Volumes und es kann zu einem Datenverlust kommen.

Anzahl der Laufwerke:

- Für RAID 1 sind mindestens zwei Laufwerke erforderlich: Ein Laufwerk für die Benutzerdaten und ein Laufwerk für die gespiegelten Daten.
- Wenn Sie vier oder mehr Laufwerke auswählen, wird RAID 10 automatisch für die gesamte Volume-Gruppe konfiguriert: Zwei Laufwerke für Benutzerdaten und zwei Laufwerke für die gespiegelten Daten.
- Sie müssen eine gerade Anzahl von Laufwerken in der Volume-Gruppe haben. Wenn Sie nicht über eine gerade Anzahl von Laufwerken verfügen und noch einige nicht zugewiesene Laufwerke haben, gehen Sie zu **Pools & Volume Groups**, um der Volume-Gruppe zusätzliche Laufwerke hinzuzufügen, und wiederholen Sie den Vorgang.

- RAID 1- und RAID 10-Volume-Gruppen können mehr als 30 Laufwerke haben. Es kann eine Volume-Gruppe erstellt werden, die alle Laufwerke im Storage-Array umfasst.

RAID 5

Beschreibung:

- Hoher I/O-Modus

Wie es funktioniert:

- Benutzerdaten und redundante Informationen (Parität) werden auf die Laufwerke verteilt.
- Die entsprechende Kapazität eines Laufwerks wird für redundante Informationen verwendet.

Datenschutzfunktionen

- Wenn ein einzelnes Laufwerk in einer RAID 5-Volume-Gruppe ausfällt, werden alle zugehörigen Volumes beeinträchtigt. Durch die redundanten Informationen kann weiterhin auf die Daten zugegriffen werden.
- Wenn zwei oder mehr Laufwerke in einer RAID 5-Volume-Gruppe ausfallen, fallen alle damit verbundenen Volumes aus und alle Daten gehen verloren.

Anzahl der Laufwerke:

- Sie müssen mindestens drei Laufwerke in der Volume-Gruppe haben.
- In der Regel sind Sie auf maximal 30 Laufwerke in der Volume-Gruppe begrenzt.

RAID 6

Beschreibung:

- Hoher I/O-Modus

Wie es funktioniert:

- Benutzerdaten und redundante Informationen (Dual Parity) werden auf die Laufwerke verteilt.
- Die entsprechende Kapazität von zwei Laufwerken wird für redundante Informationen verwendet.

Datenschutzfunktionen:

- Wenn ein oder zwei Laufwerke in einer RAID 6-Volume-Gruppe ausfallen, werden alle zugehörigen Volumes beeinträchtigt, aber aufgrund der redundanten Informationen ist es möglich, weiterhin auf die Daten zuzugreifen.
- Wenn drei oder mehr Laufwerke in einer RAID 6-Volume-Gruppe ausfallen, fallen alle damit verbundenen Volumes aus und alle Daten gehen verloren.

Anzahl der Laufwerke:

- Sie müssen mindestens fünf Laufwerke in der Volume-Gruppe haben.
- In der Regel sind Sie auf maximal 30 Laufwerke in der Volume-Gruppe begrenzt.

Sie können den RAID-Level eines Pools nicht ändern. Die Benutzeroberfläche konfiguriert Pools automatisch als RAID 6.

RAID-Level und Datensicherung

RAID 1-, RAID 5- und RAID 6-Daten für Schreibredundanz auf den Datenträger für Fehlertoleranz. Bei den Redundanzdaten kann es sich um eine Kopie der Daten (gespiegelt) oder um einen aus den Daten abgeleiteten, fehlerkorrigierenden Code handelt. Bei einem Laufwerksausfall können Sie mithilfe der Redundanzdaten schnell Informationen über das Ersatzlaufwerk wiederherstellen.

Sie konfigurieren eine einzelne RAID-Ebene für eine einzelne Volume-Gruppe. Alle Redundanzdaten der Volume-Gruppe werden innerhalb der Volume-Gruppe gespeichert. Die Kapazität der Volume-Gruppe ist die aggregierte Kapazität der Mitgliedslaufwerke abzüglich der für Redundanzdaten reservierten Kapazität. Die Menge der zur Redundanz benötigten Kapazität hängt vom verwendeten RAID-Level ab.

Warum werden einige Laufwerke nicht angezeigt?

Im Dialogfeld Kapazität hinzufügen stehen nicht alle Laufwerke zur Verfügung, um einem vorhandenen Pool oder einer Volume-Gruppe Kapazität hinzuzufügen.

Festplatten können aus den folgenden Gründen nicht genutzt werden:

- Ein Laufwerk muss nicht zugewiesen und nicht sicher aktiviert sein. Laufwerke, die bereits zu einem anderen Pool, einer anderen Volume-Gruppe oder als Hot Spare konfiguriert sind, sind nicht berechtigt. Wenn ein Laufwerk nicht zugewiesen, aber sicher aktiviert ist, müssen Sie dieses Laufwerk manuell löschen, damit es in Frage kommt.
- Ein Laufwerk in einem nicht optimalen Zustand ist nicht berechtigt.
- Wenn die Kapazität eines Laufwerks zu klein ist, ist es nicht förderfähig.
- Der Laufwerkstyp muss innerhalb eines Pools oder einer Volume-Gruppe übereinstimmen. Sie können Folgendes nicht mischen:
  - Festplattenlaufwerke (HDDs) mit Solid State Disks (SSDs)
  - NVMe mit SAS-Laufwerken
  - Laufwerke mit 512 Byte und 4 KiB Volume-Blockgrößen
- Wenn ein Pool oder eine Volume-Gruppe alle sicheren Laufwerke enthält, werden nicht sichere Laufwerke nicht aufgelistet.
- Wenn eine Pool- oder Volume-Gruppe alle FIPS-Laufwerke (Federal Information Processing Standards) enthält, werden Laufwerke außerhalb von FIPS nicht aufgeführt.
- Wenn ein Pool oder eine Volume-Gruppe alle Data Assurance (da)-fähigen Laufwerke enthält und mindestens ein da-fähiges Volume im Pool oder in der Volume-Gruppe vorhanden ist, kann ein Laufwerk, das nicht für da geeignet ist, nicht zugelassen werden, sodass es diesem Pool oder dieser Volume-Gruppe nicht hinzugefügt werden kann. Wenn sich jedoch kein da-fähiges Volume im Pool oder in der Volume-Gruppe befindet, kann ein Laufwerk, das nicht über da-fähig ist, zu diesem Pool oder dieser Volume-Gruppe hinzugefügt werden. Wenn Sie sich für eine Kombination dieser Laufwerke entscheiden, sollten Sie bedenken, dass keine da-fähigen Volumes erstellt werden können.

> Die Kapazität kann im Speicher-Array erhöht werden, indem neue Laufwerke hinzugefügt oder Pools oder Volume-Gruppen gelöscht werden.

Warum kann ich meine Konservierungskapazität nicht erhöhen?

Wenn Sie Volumes auf allen verfügbaren nutzbaren Kapazitäten erstellt haben, können Sie die dauerhafte Kapazität möglicherweise nicht erhöhen.

Bei der Festplattenkapazität wird die in einem Pool reservierte Kapazität zur Unterstützung potenzieller Laufwerksausfälle angegeben. Wenn ein Pool erstellt wird, reserviert das System abhängig von der Anzahl der Laufwerke im Pool automatisch eine standardmäßige Anlagenkapazität. Falls Sie Volumes auf allen verfügbaren nutzbaren Kapazitäten erstellt haben, können Sie die dauerhafte Kapazität auch nicht vergrößern, wenn Sie die Kapazität zum Pool erweitern, indem Sie Laufwerke hinzufügen oder Volumes löschen.

Sie können die Erhaltungskapazität aus Pools & Volume-Gruppen ändern. Wählen Sie den Pool aus, den Sie bearbeiten möchten. Klicken Sie auf **Einstellungen anzeigen/bearbeiten** und wählen Sie dann die Registerkarte **Einstellungen**.

Die dauerhafte Kapazität wird als eine Reihe von Laufwerken festgelegt, auch wenn die tatsächliche Festplattenkapazität auf den Laufwerken im Pool verteilt ist.

Was ist Data Assurance?

Data Assurance (da) implementiert den T10 Protection Information (PI)-Standard. Dies erhöht die Datenintegrität, indem Fehler geprüft und korrigiert werden, die bei der Datenübertragung entlang des I/O-Pfads auftreten können.

Die typische Nutzung der Data Assurance Funktion überprüft den Teil des I/O-Pfads zwischen den Controllern und Laufwerken. DA-Funktionen werden auf Pool- und Volume-Gruppenebene präsentiert.

Wenn diese Funktion aktiviert ist, hängt das Speicherarray die Fehlerprüfungscodes (auch zyklische Redundanzprüfungen oder CRCs genannt) an jeden Datenblock im Volume an. Nach dem Verschieben eines Datenblocks ermittelt das Speicher-Array anhand dieser CRC-Codes, ob während der Übertragung Fehler aufgetreten sind. Potenziell beschädigte Daten werden weder auf Festplatte geschrieben noch an den Host zurückgegeben. Wenn Sie die da-Funktion verwenden möchten, wählen Sie einen Pool oder eine Volume-Gruppe aus, die bei der Erstellung eines neuen Volumes unterstützt wird (suchen Sie in der Tabelle mit den Kandidaten für Pool- und Volume-Gruppen nach **ja** neben **da**).

Stellen Sie sicher, dass Sie diese DA-fähigen Volumes einem Host über eine E/A-Schnittstelle zuweisen, die über eine da-fähige Schnittstelle verfügt. Zu den I/O-Schnittstellen, die da fähig sind, gehören Fibre Channel, SAS, iSCSI über TCP/IP, NVMe/FC, NVMe/IB, NVME/RoCE und iSER over InfiniBand (iSCSI-Erweiterungen für RDMA/IB). DA wird von SRP nicht über InfiniBand unterstützt.

Was ist FDE/FIPS-Sicherheit?

FDE/FIPS-Sicherheit bezieht sich auf sichere Laufwerke, die Daten bei Schreibvorgängen verschlüsseln und während Lesevorgängen mit einem eindeutigen Verschlüsselungsschlüssel entschlüsseln.

Diese sicheren Laufwerke verhindern unbefugten Zugriff auf die Daten auf einem Laufwerk, das physisch vom Storage-Array entfernt wird. Sichere Laufwerke können entweder vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) sein. FIPS-Laufwerke wurden getestet.

Für Volumes, die FIPS-Unterstützung erfordern, verwenden Sie nur FIPS-Laufwerke. Durch das Mischen von FIPS- und FDE-Laufwerken in einer Volume-Gruppe oder einem Pool werden alle Laufwerke als FDE-Laufwerke behandelt. Außerdem kann ein FDE-Laufwerk nicht zu einer Ersatzfestplatte in einer reinen FIPS-Volume-Gruppe oder einem Pool hinzugefügt oder verwendet werden.

Was ist sicher-fähig (Drive Security)?

Drive Security ist eine Funktion, die bei Entfernung aus dem Speicher-Array unberechtigten Zugriff auf Daten auf sicheren Laufwerken verhindert.

Dabei können es sich entweder um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE)-Laufwerke oder um FIPS-Laufwerke (Federal Information Processing Standard) handeln.

Wie kann ich sämtliche SSD Cache Statistiken anzeigen und interpretieren?

Sie können nominale Statistiken und detaillierte Statistiken für SSD Cache anzeigen.

Die Nominalstatistiken sind eine Untergruppe der detaillierten Statistiken. Die detaillierten Statistiken können nur angezeigt werden, wenn Sie alle SSD-Statistiken in eine .csv-Datei exportieren. Während Sie die Statistiken überprüfen und interpretieren, beachten Sie, dass einige Interpretationen durch die Prüfung einer Kombination von Statistiken abgeleitet werden.

Nominale Statistiken

Um SSD Cache Statistiken anzuzeigen, gehen Sie zur Seite **Verwalten**. Wählen Sie Menü:Provisioning[Pools & Volume-Gruppen konfigurieren]. Wählen Sie den SSD-Cache aus, für den Sie Statistiken anzeigen möchten, und wählen Sie dann Menü:Mehr[Statistik anzeigen]. Die nominalen Statistiken werden im Dialogfeld „View SSD Cache Statistics“ angezeigt.

Diese Funktion steht nicht auf dem EF600 oder EF300-Storage-System zur Verfügung.

Die Liste enthält nominale Statistiken, die eine Untermenge der detaillierten Statistiken sind.

Detaillierte Statistiken

Die detaillierten Statistiken bestehen aus den Nominalstatistiken sowie zusätzlichen Statistiken. Diese zusätzlichen Statistiken werden zusammen mit den nominalen Statistiken gespeichert, werden aber im Gegensatz zu den nominalen Statistiken nicht im Dialogfeld „View SSD Cache Statistics“ angezeigt. Sie können die detaillierten Statistiken nur anzeigen, nachdem Sie die Statistiken in eine CSV-Datei exportiert haben.

Die detaillierten Statistiken sind nach den Nominalstatistiken aufgelistet.

Was ist der Schutz vor Regalverlust und der Schutz vor Schubladenverlust?

Shelf-Schutz und Schutz vor Schubladenverlust sind Attribute von Pools und Volume-Gruppen, die es Ihnen ermöglichen, den Datenzugriff bei Ausfall eines einzelnen Shelfs oder einer Schublade aufrechtzuerhalten.

Schutz vor Regalverlust

Ein Shelf ist das Gehäuse, das entweder die Laufwerke oder die Laufwerke und den Controller enthält. Der Shelf-Verlust-Schutz garantiert den Zugriff auf die Daten auf den Volumes in einem Pool oder einer Volume-Gruppe, wenn ein totaler Verlust der Kommunikation mit einem einzelnen Festplatten-Shelf auftritt. Ein Beispiel für einen völligen Verlust der Kommunikation kann ein Verlust an Strom am Festplatten-Shelf oder ein Ausfall beider I/O-Module (IOMs) sein.

Der Schutz vor Shelf-Verlust ist nicht gewährleistet, wenn ein Laufwerk bereits im Pool oder in der Volume-Gruppe ausgefallen ist. In dieser Situation kommt es beim Verlust des Zugriffs auf ein Festplatten-Shelf und folglich auch eines anderen Laufwerks im Pool oder der Volume-Gruppe zu Datenverlusten.

Die Kriterien für den Regalverlustschutz hängen von der Schutzmethode ab, wie in der folgenden Tabelle beschrieben.

Ebene	Kriterien für den Schutz vor Regalverlust	Mindestanzahl der benötigten Shelves
Pool	Der Pool muss Laufwerke von mindestens fünf Shelfs enthalten, und es muss eine gleiche Anzahl von Laufwerken in jedem Shelf vorhanden sein. Der Schutz vor Shelf-Datenverlusten ist nicht auf Shelfs mit hoher Kapazität anwendbar. Wenn das System kapazitätsstarke Shelfs enthält, finden Sie weitere Informationen unter Abflussschutz.	5
RAID 6	Die Volume-Gruppe enthält nicht mehr als zwei Laufwerke in einem einzigen Einschub.	3
RAID 3 oder RAID 5	Jedes Laufwerk in der Volume-Gruppe befindet sich in einem separaten Shelf.	3
RAID 1	Jedes Laufwerk in einem RAID-1-Paar muss sich in einem separaten Shelf befinden.	2
RAID 0	Shelf-Verlustschutz kann nicht erreicht werden.	Keine Angabe

Schutz vor Schubladenverlust

Eine Schublade ist eines der Fächer eines Regals, das Sie herausziehen, um auf die Laufwerke zuzugreifen. Nur die Regale mit hoher Kapazität verfügen über Schubladen. Der Schutz vor Schubladenverlust garantiert den Zugriff auf die Daten auf den Volumes in einem Pool oder einer Volume-Gruppe, wenn ein vollständiger Verlust der Kommunikation mit einem einzelnen Fach auftritt. Ein Beispiel für einen Totalverlust der Kommunikation kann zu einem Stromausfall in der Schublade oder einem Ausfall einer internen Komponente in der Schublade führen.

Der Schutz vor Schubladenverlust ist nicht gewährleistet, wenn ein Laufwerk bereits im Pool oder in der Volume-Gruppe ausgefallen ist. Wenn in dieser Situation der Zugriff auf eine Schublade (und folglich ein anderes Laufwerk im Pool oder der Volume-Gruppe) verloren geht, gehen Daten verloren.

Die Kriterien für den Schubladenschutz sind abhängig von der Schutzmethode, wie in der folgenden Tabelle beschrieben:

Ebene	Kriterien für den Schutz vor Schubladenverlust	Mindestanzahl der benötigten Schubladen
Pool	Poolkandidaten müssen Laufwerke aus allen Schubladen enthalten, und in jedem Fach muss eine gleiche Anzahl von Laufwerken vorhanden sein. Der Pool muss Laufwerke aus mindestens fünf Schubladen enthalten und in jeder Schublade muss eine gleiche Anzahl von Laufwerken vorhanden sein. Ein Shelf mit 60 Laufwerken kann einen Schubladenschutz erreichen, wenn der Pool 15, 20, 25, 30, 35, 40, 45, 50, 55 oder 60 Laufwerke. Nach der ersten Erstellung können Vielfache von 5 dem Pool hinzugefügt werden.	5
RAID 6	Die Volume-Gruppe enthält nicht mehr als zwei Laufwerke in einem einzigen Einschub.	3
RAID 3 oder 5	Jedes Laufwerk in der Volume-Gruppe befindet sich in einem separaten Einschub	3
RAID 1	Jedes Laufwerk in einem gespiegelten Paar muss sich in einem separaten Fach befinden.	2
RAID 0	Der Schutz vor Schubladenverlust kann nicht erreicht werden.	Keine Angabe

Wie kann ich den Schutz vor Schubladenausfall wahren?

Verwenden Sie die in der folgenden Tabelle aufgeführten Kriterien, um den Schutz vor Shelf- und Schubladenverlusten für einen Pool oder eine Volume-Gruppe aufrechtzuerhalten.

Ebene	Kriterien für den Schutz vor Shelf-/Schubladenverlust	Mindestanzahl an Shelves/Schubladen erforderlich
Pool	Bei Shelfs darf der Pool nicht mehr als zwei Laufwerke in einem einzelnen Shelf enthalten. Bei Schubladen muss der Pool eine gleiche Anzahl von Laufwerken von jeder Schublade enthalten.	6 für Regale 5 für Schubladen
RAID 6	Die Volume-Gruppe enthält nicht mehr als zwei Laufwerke in einem einzelnen Shelf oder einer einzelnen Schublade.	3

Ebene	Kriterien für den Schutz vor Shelf-/Schubladenverlust	Mindestanzahl an Shelves/Schubladen erforderlich
RAID 3 oder RAID 5	Jedes Laufwerk in der Volume-Gruppe befindet sich in einem separaten Shelf oder einer separaten Schublade.	3
RAID 1	Jedes Laufwerk in einem gespiegelten Paar muss sich in einem eigenen Shelf oder einer separaten Schublade befinden.	2
RAID 0	Schutz vor Shelf-/Schubladenverlust kann nicht erreicht werden.	Keine Angabe

Der Schutz vor Shelf-/Schubladenverlust bleibt nicht erhalten, wenn ein Laufwerk bereits in dem Pool oder der Volume-Gruppe ausgefallen ist. Geht in dieser Situation der Zugriff auf ein Festplatten-Shelf oder eine Laufwerksschublade verloren und somit ein weiteres Laufwerk im Pool bzw. der Volume-Gruppe, geht es zu Datenverlusten.

Was ist die Optimierungskapazität für Pools?

SSD-Laufwerke haben eine längere Lebensdauer und eine bessere maximale Schreib-Performance, wenn ein Teil ihrer Kapazität nicht zugewiesen ist.

Bei Laufwerken, die einem Pool zugeordnet sind, besteht nicht zugewiesene Kapazität aus der Erhaltungskapazität eines Pools, der freien Kapazität (nicht von Volumes genutzte Kapazität) und einem Teil der nutzbaren Kapazität, der als zusätzliche Optimierungskapazität zur Verfügung steht. Die zusätzliche Optimierungskapazität stellt ein Mindestmaß an Optimierungskapazität zur Verfügung, indem die nutzbare Kapazität reduziert wird. Somit ist für die Volume-Erstellung nicht verfügbar.

Wenn ein Pool erstellt wird, wird eine empfohlene Optimierungskapazität generiert, die ein ausgewogenes Verhältnis zwischen Performance, Laufwerksabnutzung und verfügbarer Kapazität bietet. Der Schieberegler „zusätzliche Optimierung der Kapazität“ im Dialogfeld „Pooleinstellungen“ ermöglicht die Anpassung an die Optimierungskapazität des Pools. Durch das Anpassen des Schiebereglers erhalten Sie eine bessere Performance und längere Lebensdauer der Laufwerke, und zwar auf Kosten der verfügbaren Kapazität oder zusätzlicher verfügbarer Kapazität, und zwar auf Kosten der Leistung und des Verschleißes der Laufwerke.

Der Schieberegler „zusätzliche Optimierung der Kapazität“ ist nur für Speichersysteme EF600 und EF300 verfügbar.

Was ist die Optimierungskapazität für Volume-Gruppen?

SSD-Laufwerke haben eine längere Lebensdauer und eine bessere maximale Schreib-Performance, wenn ein Teil ihrer Kapazität nicht zugewiesen ist.

Bei Laufwerken, die einer Volume-Gruppe zugeordnet sind, besteht nicht zugewiesene Kapazität aus der freien Kapazität einer Volume-Gruppe (nicht von Volumes genutzte Kapazität) und einem Teil der nutzbaren Kapazität, die als Optimierungskapazität zur Verfügung gestellt werden. Die zusätzliche Optimierungskapazität stellt ein Mindestmaß an Optimierungskapazität zur Verfügung, indem die nutzbare Kapazität reduziert wird. Somit ist für die Volume-Erstellung nicht verfügbar.

Wenn eine Volume-Gruppe erstellt wird, wird eine empfohlene Optimierungskapazität generiert, die einen Ausgleich zwischen Performance, Laufwerkverschleiß und verfügbarer Kapazität bietet. Mit dem Schieberegler „zusätzliche Optimierung der Kapazität“ im Dialogfeld „Einstellungen der Volume-Gruppe“ können Sie die Optimierungskapazität einer Volume-Gruppe anpassen. Durch das Anpassen des Schiebereglers erhalten Sie eine bessere Performance und längere Lebensdauer der Laufwerke, und zwar auf Kosten der verfügbaren Kapazität oder zusätzlicher verfügbarer Kapazität, und zwar auf Kosten der Leistung und des Verschleißes der Laufwerke.

Der zusätzliche Schieberegler zur Optimierung der Kapazität ist nur für Speichersysteme EF600 und EF300 verfügbar.

Was ist die Fähigkeit zur Ressourcenbereitstellung?

Resource Provisioning ist eine Funktion, die in den EF300- und EF600-Speicher-Arrays zur Verfügung steht und die es ermöglicht, Volumes ohne Hintergrundinitialisierung sofort in Betrieb zu nehmen.

Ein vom Ressourcen bereitgestelltes Volume ist ein Thick Volume in einer SSD-Volume-Gruppe oder einem Pool. Dabei wird bei der Erstellung des Volume die Laufwerkskapazität zugewiesen (dem Volume zugewiesen), die Laufwerksblöcke jedoch aufgehoben (nicht zugewiesen). In einem herkömmlichen Thick Volume werden im Vergleich dazu alle Laufwerkblöcke während der Initialisierung eines Volume im Hintergrund zugeordnet oder zugewiesen, um die Felder für den Schutz der Data Assurance zu initialisieren und die Daten- und RAID-Parität in jedem RAID Stripe konsistent zu gestalten. Bei einem Volume, das für die Ressource bereitgestellt wird, gibt es keine zeitgebundene Hintergrundinitialisierung. Stattdessen wird jeder RAID-Stripe nach dem ersten Schreibvorgang auf einen Volume-Block im Stripe initialisiert.

Über Ressourcen bereitgestellte Volumes werden nur auf SSD-Volume-Gruppen und -Pools unterstützt, wobei alle Laufwerke in der Gruppe oder dem Pool die nicht zugewiesene oder nicht geschriebene DULBE-Fehlerwiederherstellungsfunktion (Logical Block Error Enable) unterstützen. Bei der Erstellung eines Volume mit Ressourcenbereitstellung werden alle dem Volume zugewiesenen Festplattenblöcke wieder zugewiesen (Zuordnung). Zudem können Hosts mithilfe des NVMe-Datensatzmanagements logische Blöcke im Volume deallokalisieren. Die Deallokung von Blöcken kann die SSD-Abnutzung verbessern und die maximale Schreib-Performance erhöhen. Die Verbesserung variiert je nach Modell und Kapazität der Laufwerke.

Was muss ich über die Funktion der Ressourcen-bereitgestellten Volumes wissen?

Resource Provisioning ist eine Funktion, die in den EF300- und EF600-Speicher-Arrays zur Verfügung steht und die es ermöglicht, Volumes ohne Hintergrundinitialisierung sofort in Betrieb zu nehmen.

Die Ressourcen-Provisioning-Funktion ist derzeit nicht verfügbar. In einigen Ansichten können Komponenten als ressourcenschonende Bereitstellung gemeldet werden, aber die Möglichkeit, mit Ressourcen bereitgestellte Volumes zu erstellen, wurde deaktiviert, bis sie in einem zukünftigen Update erneut aktiviert werden kann.

Volumes mit Ressourcenbereitstellung

Ein vom Ressourcen bereitgestelltes Volume ist ein Thick Volume in einer SSD-Volume-Gruppe oder einem Pool. Dabei wird bei der Erstellung des Volume die Laufwerkskapazität zugewiesen (dem Volume zugewiesen), die Laufwerksblöcke jedoch aufgehoben (nicht zugewiesen). In einem herkömmlichen Thick Volume werden im Vergleich dazu alle Laufwerkblöcke während der Initialisierung eines Volume im Hintergrund zugeordnet oder zugewiesen, um die Felder für den Schutz der Data Assurance zu initialisieren und die Daten- und RAID-Parität in jedem RAID Stripe konsistent zu gestalten. Bei einem Volume, das für die Ressource bereitgestellt wird, gibt es keine zeitgebundene Hintergrundinitialisierung. Stattdessen wird jeder RAID-Stripe nach dem ersten Schreibvorgang auf einen Volume-Block im Stripe initialisiert.

Über Ressourcen bereitgestellte Volumes werden nur auf SSD-Volume-Gruppen und -Pools unterstützt, wobei alle Laufwerke in der Gruppe oder dem Pool die nicht zugewiesene oder nicht geschriebene DULBE-Fehlerwiederherstellungsfunktion (Logical Block Error Enable) unterstützen. Bei der Erstellung eines Volume mit Ressourcenbereitstellung werden alle dem Volume zugewiesenen Festplattenblöcke wieder zugewiesen (Zuordnung). Zudem können Hosts mithilfe des NVMe-Datensatzmanagements logische Blöcke im Volume deallokalisieren. Die Deallokung von Blöcken kann die SSD-Abnutzung verbessern und die maximale Schreib-Performance erhöhen. Die Verbesserung variiert je nach Modell und Kapazität der Laufwerke.

Aktivieren und Deaktivieren der Funktion

Die Ressourcenbereitstellung ist standardmäßig auf Systemen aktiviert, auf denen die Laufwerke DULBE unterstützen. Sie können diese Standardeinstellung in Pools und Volume-Gruppen deaktivieren. Die Deaktivierung der Ressourcen-Bereitstellung ist eine permanente Aktion für vorhandene Volumes und kann nicht rückgängig gemacht werden (d. h. Sie können die Ressourcen-Bereitstellung für diese Volume-Gruppen und -Pools nicht erneut aktivieren).

Wenn Sie die Ressourcenbereitstellung jedoch für alle von Ihnen erstellten neuen Volumes erneut aktivieren möchten, können Sie dies über das Menü:Einstellungen[System] tun. Beachten Sie, dass bei der erneuten Aktivierung der Ressourcenbereitstellung nur neu erstellte Volume-Gruppen und Pools betroffen sind. Alle vorhandenen Volume-Gruppen und -Pools bleiben unverändert. Bei Bedarf können Sie die Ressourcenbereitstellung auch wieder über das Menü:Einstellungen[System] deaktivieren.

Worin besteht der Unterschied zwischen internem Sicherheitsschlüssel und externem Sicherheitsschlüsselmanagement?

Wenn Sie die Laufwerksicherheit-Funktion implementieren, können Sie einen internen Sicherheitsschlüssel oder einen externen Sicherheitsschlüssel verwenden, um Daten zu sperren, wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt wird.

Ein Sicherheitsschlüssel ist eine Zeichenkette, die von den sicheren Laufwerken und Controllern in einem Speicher-Array gemeinsam genutzt wird. Interne Schlüssel befinden sich im persistenten Speicher des Controllers. Externe Schlüssel werden mithilfe eines Key Management Interoperability Protocol (KMIP) auf einem separaten Verschlüsselungsmanagement-Server aufbewahrt.

Was muss ich vor der Erstellung eines Sicherheitsschlüssels wissen?

Ein Sicherheitsschlüssel wird von Controllern und sicheren Laufwerken innerhalb eines Storage-Arrays gemeinsam verwendet. Wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt wird, schützt der Sicherheitsschlüssel die Daten vor unberechtigtem Zugriff.

Sie können Sicherheitsschlüssel mit einer der folgenden Methoden erstellen und verwalten:

- Internes Verschlüsselungsmanagement auf dem persistenten Speicher des Controllers.
- Externes Verschlüsselungskeymanagement auf einem externen Verschlüsselungsmanagement-Server.

Internes Verschlüsselungsmanagement

Interne Schlüssel werden in einem nicht zugänglichen Ort im persistenten Speicher des Controllers gepflegt und „versteckt“. Bevor Sie einen internen Sicherheitsschlüssel erstellen, müssen Sie Folgendes tun:

1. Installieren Sie sichere Laufwerke im Speicher-Array. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
2. Stellen Sie sicher, dass die Laufwerksicherheit aktiviert ist. Wenden Sie sich bei Bedarf an Ihren Storage-

Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.

Sie können dann einen internen Sicherheitsschlüssel erstellen, der die Definition einer Kennung und einer Passphrase beinhaltet. Die Kennung ist eine Zeichenfolge, die dem Sicherheitsschlüssel zugeordnet ist und auf dem Controller und allen Laufwerken gespeichert ist, die mit dem Schlüssel verknüpft sind. Der Passphrase wird verwendet, um den Sicherheitsschlüssel für Sicherungszwecke zu verschlüsseln. Wenn Sie fertig sind, wird der Sicherheitsschlüssel auf dem Controller an einem nicht zugänglichen Ort gespeichert. Anschließend können sichere Volume-Gruppen und -Pools erstellt oder die Sicherheit für vorhandene Volume-Gruppen und -Pools aktiviert werden.

Externes Verschlüsselungskeymanagement

Externe Schlüssel werden mithilfe eines Key Management Interoperability Protocol (KMIP) auf einem separaten Verschlüsselungsmanagement-Server aufbewahrt. Bevor Sie einen externen Sicherheitsschlüssel erstellen, müssen Sie Folgendes tun:

1. Installieren Sie sichere Laufwerke im Speicher-Array. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
2. Stellen Sie sicher, dass die Laufwerksicherheit aktiviert ist. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten
3. Abrufen einer signierten Client-Zertifikatdatei. Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit der Verschlüsselungsmanagement-Server ihren KMIP-Anforderungen vertrauen kann.
   a. Zunächst haben Sie eine Client Certificate Signing Request (CSR) abgeschlossen und heruntergeladen. Wechseln Sie zum Menü:Einstellungen[Zertifikate > Schlüsselverwaltung > CSR abschließen].
   b. Als Nächstes fordern Sie ein signiertes Clientzertifikat von einer Zertifizierungsstelle an, die vom Schlüsselverwaltungsserver vertrauenswürdig ist. (Sie können auch mithilfe der heruntergeladenen CSR-Datei ein Client-Zertifikat vom Schlüsselverwaltungsserver erstellen und herunterladen.)
   c. Sobald Sie über eine Clientzertifikatdatei verfügen, kopieren Sie diese Datei auf den Host, auf dem Sie auf System Manager zugreifen.
4. Rufen Sie eine Zertifikatdatei vom Verschlüsselungsmanagement-Server ab, und kopieren Sie diese Datei dann auf den Host, auf dem Sie auf System Manager zugreifen. Ein Zertifikat für den Schlüsselmanagementserver validiert den Schlüsselmanagementserver, damit das Storage-Array seiner IP-Adresse vertrauen kann. Sie können für den Schlüsselverwaltungsserver ein Root-, Intermediate- oder Serverzertifikat verwenden.

Anschließend können Sie einen externen Schlüssel erstellen, der die IP-Adresse des Verschlüsselungsmanagement-Servers und die für die KMIP Kommunikation verwendete Port-Nummer umfasst. Während dieses Prozesses laden Sie auch Zertifikatdateien. Nach Abschluss des Vorgangs stellt das System eine Verbindung zum Schlüsselverwaltungsserver mit den von Ihnen eingegebenen Anmeldedaten her. Anschließend können sichere Volume-Gruppen und -Pools erstellt oder die Sicherheit für vorhandene Volume-Gruppen und -Pools aktiviert werden.

Warum muss ich eine Passphrase definieren?

Der Passphrase wird verwendet, um die auf dem lokalen Management-Client gespeicherte Sicherheitsschlüsseldatei zu verschlüsseln und zu entschlüsseln. Ohne den Passphrase kann der Sicherheitsschlüssel nicht entschlüsselt und verwendet werden, um Daten von einem sicheren Laufwerk zu entsperren, wenn er in einem anderen Speicher-Array neu installiert wird.

Älteren Lösungen dar

Cloud-Connector

Überblick über den SANtricity® Cloud Connector

SANtricity Cloud Connector ist eine Host-basierte Linux Applikation, die vollständige Block- und dateibasierte Backups und Recoverys von E-Series Volumes auf S3-Reklamationskonten (z. B. Amazon Simple Storage Service und NetApp StorageGRID) sowie eine NetApp AltaVault Appliance ermöglicht.

Der SANtricity Cloud Connector ist für die Installation auf RedHat- und SUSE Linux-Plattformen verfügbar und ist eine Paketlösung (.bin-Datei). Nach der Installation von SANtricity Cloud Connector können Sie die Applikation so konfigurieren, dass Backup- und Restore-Jobs für E-Series Volumes auf einer AltaVault Appliance oder Ihren vorhandenen Amazon S3 oder StorageGRID Konten ausgeführt werden. Alle Jobs, die über den SANtricity-Cloud-Connector ausgeführt werden, verwenden REST-basierte APIs.

Das SANtricity Cloud Connector-Tool ist veraltet und kann nicht mehr heruntergeladen werden.

Überlegungen

Beachten Sie bei der Verwendung dieser Verfahren Folgendes:

- Konfigurations- und Sicherungs-/Wiederherstellungsaufträge, die in diesen Verfahren beschrieben werden, gelten für die grafische Benutzeroberflächenversion des SANtricity Cloud Connectors.
- REST-API-Workflows für die Applikation SANtricity Cloud Connector werden in diesen Verfahren nicht beschrieben. Bei erfahrenen Entwicklern stehen Endpunkte für jeden SANtricity Cloud Connector-Vorgang unter der API-Dokumentation zur Verfügung. Auf die API-Dokumentation kann zugegriffen werden, indem Sie zu navigieren `http://<hostname.domain>:<port>/docs` Über einen Browser öffnen.

Arten von Backups

Der SANtricity Cloud Connector bietet zwei Arten von Backups: Image- und dateibasierte Backups.

- **Image-basiertes Backup**

  Ein Backup auf Image-Basis liest die rohen Datenblöcke von einem Snapshot-Volume und sichert sie in eine Datei, die als Image bezeichnet wird. Alle Datenblöcke auf dem Snapshot-Volume werden gesichert, einschließlich leerer Blöcke, von gelöschten Dateien belegten Blöcken, mit Partitionierung verbundenen Blöcken und Dateisystemmetadaten. Image-Backups haben den Vorteil, alle Informationen mit dem Snapshot-Volumen zu speichern, unabhängig vom Partitionierungsschema oder Dateisystem darauf.

  Das Bild wird nicht als einzelne Datei im Backup Target gespeichert, sondern in eine Reihe von Datenblöcken unterteilt, die 64MB groß sind. Durch die Datenblöcke kann SANtricity Cloud Connector mehrere Verbindungen zum Backup-Ziel verwenden und so die Performance des Backup-Prozesses verbessern.

  Für Backups in StorageGRID und Amazon Web Services (S3) verwendet jeder Datenblock einen separaten Verschlüsselungsschlüssel zur Verschlüsselung des Blocks. Der Schlüssel ist ein SHA256-Hash, der aus der Kombination einer vom Benutzer bereitgestellten Passphrase und dem SHA256-Hash der Benutzerdaten besteht. Bei Backups zu AltaVault verschlüsselt der SANtricity Cloud Connector die Datenblöcke nicht, wenn AltaVault diesen Vorgang durchführt.

- * File-basiertes Backup*

  Ein dateibasiertes Backup liest die mit einer Dateisystempartition enthaltenen Dateien und sichert sie in eine Reihe von Datenblöcken, die 64 MB groß sind. Ein dateibasiertes Backup sichert keine gelöschten Dateien oder Partitionierungen und Dateisystem-Metadaten. Wie bei Image-basierten Backups können auch bei den Daten-Chunks SANtricity Cloud Connector mehrere Verbindungen zum Backup-Ziel verwenden und so die Performance des Backup-Prozesses verbessern.

  Für Backups in StorageGRID und Amazon Web Services verwendet jedes Datenpaket einen separaten Verschlüsselungsschlüssel zur Verschlüsselung des Blocks. Der Schlüssel ist ein SHA256-Hash, der aus der Kombination von benutzerbereitem Passphrase und dem SHA256-Hash der Benutzerdaten besteht. Bei Backups auf AltaVault werden die Datenblöcke nicht durch SANtricity Cloud Connector verschlüsselt, da AltaVault diesen Vorgang durchführt.

Systemanforderungen für SANtricity Cloud Connector

Ihr System muss die Kompatibilitätsanforderungen für den SANtricity Cloud Connector erfüllen.

Anforderungen an die Host-Hardware

Ihre Hardware muss die folgenden Mindestanforderungen erfüllen:

- Mindestens 5 GB Speicher; 4 GB für die maximale konfigurierte Heap-Größe
- Mindestens 5 GB freier Festplattenspeicher sind bei der Softwareinstallation erforderlich

Sie müssen den SANtricity Web Services Proxy installieren, um den SANtricity Cloud Connector verwenden zu können. Sie können den Web Services Proxy lokal installieren oder die Anwendung Remote auf einem anderen Server ausführen. Informationen zum Installieren des SANtricity Web Services Proxy finden Sie unter "Web Services Proxy-Themen".

Unterstützte Browser

Die folgenden Browser werden von SANtricity Cloud Connector unterstützt (Mindestversionen angegeben):

- Firefox v31
- Google Chrome v47
- Microsoft Internet Explorer v11
- Microsoft Edge, EdgeHTML 12
- Safari v9

> Die API-Dokumentation für die SANtricity-Cloud-Connector-Anwendung wird nicht geladen, wenn die Einstellung Kompatibilitätsansicht im Microsoft Internet Explorer v11-Browser verwendet wird. Um sicherzustellen, dass die API-Dokumentation im Microsoft Internet Explorer v11-Browser ordnungsgemäß angezeigt wird, wird empfohlen, dass die Einstellung Kompatibilitätsansicht deaktiviert ist.

Kompatible Storage Arrays und Controller Firmware

Vor der Verwendung der SANtricity Cloud Connector-Applikation sollten Sie die Kompatibilität Ihrer Storage-Arrays und Firmware überprüfen.

Eine vollständige und aktuelle Liste aller kompatiblen Storage-Arrays und Firmware für den SANtricity Cloud Connector finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Kompatible Betriebssysteme

Die Anwendung SANtricity Cloud Connector 4.0 ist mit folgenden Betriebssystemen kompatibel und unterstützt:

Betriebssystem	Version	Der Netapp Architektur Sind
Red hat Enterprise Linux (RHEL)	7.x	64 Bit
SUSE Linux Enterprise Server (SLES)	12.x	64 Bit

Unterstützte Dateisysteme

Sie müssen unterstützte Dateisysteme verwenden, um Backups und Wiederherstellungen über die SANtricity-Cloud-Connector-Anwendung durchzuführen.

Die folgenden Dateisysteme werden für Backup- und Restore-Vorgänge unter SANtricity Cloud Connector unterstützt:

- Erw. 2
- Erw. 3
- Ext4

Installieren Sie den SANtricity Cloud Connector

Die SANtricity Cloud Connector-Paketlösung (.bin-Datei) ist nur für RedHat- und SUSE Linux-Plattformen verfügbar.

Sie können die Anwendung SANtricity Cloud Connector über den Grafikmodus oder den Konsolenmodus auf einem kompatiblen Linux-Betriebssystem installieren. Während der Installation müssen Sie die nicht-SSL- und SSL-Portnummern für den SANtricity-Cloud-Connector angeben. Bei der Installation wird der SANtricity Cloud Connector als Daemon Prozess ausgeführt.

Das SANtricity Cloud Connector-Tool ist veraltet und kann nicht mehr heruntergeladen werden.

Bevor Sie beginnen

Lesen Sie die folgenden Hinweise:

- Wenn SANtricity Webservices Proxy bereits auf demselben Server wie der SANtricity Cloud Connector installiert ist, treten Konflikte zwischen nicht-SSL-Portnummern und Konflikten bei SSL-Port-Nummern auf. Wählen Sie in diesem Fall während der Installation des SANtricity Cloud Connectors die entsprechenden Nummern für den nicht-SSL-Port und den SSL-Port aus.
- Wenn Hardware-Änderungen auf Ihrem Host vorgenommen werden, installieren Sie die SANtricity Cloud Connector-Anwendung erneut, um die Konsistenz der Verschlüsselung zu gewährleisten.
- Backups, die durch die Version 3.1 der SANtricity Cloud Connector Anwendung erstellt wurden, sind nicht kompatibel mit Version 4.0 der SANtricity Cloud Connector Anwendung. Wenn Sie diese Backups

beibehalten möchten, müssen Sie Ihre vorherige Version des SANtricity Cloud Connectors weiterhin verwenden. Um eine erfolgreiche Installation von separaten 3.1- und 4.0-Versionen des SANtricity-Cloud-Connectors zu gewährleisten, müssen für jede Version der Anwendung eindeutige Portnummern zugewiesen werden.

Installation von Device Mapper Multipath (DM-MP)

Auf jedem Host, auf dem der SANtricity Cloud Connector ausgeführt wird, muss auch Linux Device Mapper Multipath (DM-MP) ausgeführt werden und das Multipath-Tools-Paket installiert sein.

Der Erkennungsvorgang für SANtricity Cloud Connector verwendet das Multipath-Tool-Paket zur Erkennung und Erkennung der zu sicherenden Volumes und Dateien. Weitere Informationen zum Einrichten und Konfigurieren der Gerätezuordnung finden Sie im Handbuch für Multipath-Treiber für *SANtricity-Speicher-Manager* für die Version von SANtricity, die Sie unter verwenden "E-Series und SANtricity – Dokumentressourcen".

Installieren Sie Cloud Connector

Sie können SANtricity Cloud Connector entweder im grafischen Modus oder im Konsolenmodus auf Linux-Betriebssystemen installieren.

Grafikmodus

Sie können den SANtricity-Cloud-Connector im grafischen Modus auf einem Linux-Betriebssystem installieren.

Bevor Sie beginnen

Bestimmen Sie einen Host-Standort für die Installation des SANtricity Cloud Connectors.

Schritte

1. Laden Sie die Installationsdatei für den SANtricity Cloud Connector auf den gewünschten Host-Speicherort herunter.
2. Öffnen Sie ein Terminal-Fenster.
3. Navigieren Sie zu der Verzeichnisdatei, die die Installationsdatei für den SANtricity Cloud Connector enthält.
4. Starten Sie den Installationsvorgang für den SANtricity Cloud Connector:

   ```
   ./cloudconnector-xxxx.bin –i gui
   ```

   In diesem Befehl `xxxx` Gibt die Versionsnummer der Anwendung an.

   Das Fenster Installer wird angezeigt.

5. Lesen Sie die Einführung und klicken Sie dann auf **Weiter**.

   Die Lizenzvereinbarung für NetApp, Inc. Software wird innerhalb des Installationsfensters angezeigt.

6. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung, und klicken Sie dann auf **Weiter**.

   Die Backups, die mit vorherigen Versionen der Seite SANtricity Cloud Connector erstellt wurden, werden angezeigt.

7. Um die Backups zu bestätigen, die mit früheren Versionen von SANtricity Cloud Connector erstellt wurden, klicken Sie auf **Weiter**.

   Um die Version 4.0 des SANtricity-Cloud-Connectors unter Beibehaltung einer früheren Version zu installieren, müssen für jede Version der Anwendung eindeutige Portnummern zugewiesen werden.

   Die Seite „Installation auswählen“ wird im Fenster „Installer“ angezeigt. Im Feld wo möchten Sie installieren? Wird der folgende Standardinstallationsordner angezeigt: `opt/netapp/santricity_cloud_connector4/`

8. Wählen Sie eine der folgenden Optionen:
   - Um den Standardspeicherort zu übernehmen, klicken Sie auf **Weiter**.
   - Um den Standardspeicherort zu ändern, geben Sie einen neuen Ordnerspeicherort ein. Es wird die Seite „nicht SSL-Jetty-Portnummer eingeben“ angezeigt. Dem nicht-SSL-Port wird ein Standardwert von 8080 zugewiesen.
9. Wählen Sie eine der folgenden Optionen:
   - Um die Standard-SSL-Portnummer zu akzeptieren, klicken Sie auf **Weiter**.
   - Um die Standard-SSL-Portnummer zu ändern, geben Sie den neuen gewünschten Portnummer-Wert ein.
10. Wählen Sie eine der folgenden Optionen:
    - Klicken Sie auf **Weiter**, um die Standard-nicht-SSL-Portnummer zu akzeptieren.
    - Geben Sie zum Ändern der standardmäßigen nicht-SSL-Portnummer den neuen gewünschten Portnummer ein. Die Seite Übersicht vor der Installation wird angezeigt.
11. Überprüfen Sie die angezeigte Übersicht vor der Installation, und klicken Sie dann auf **Installieren**.

    Die Installation des SANtricity Cloud Connectors beginnt und eine Webserver Daemon-Eingabeaufforderung wird angezeigt.

12. Klicken Sie auf **OK**, um die Eingabeaufforderung Webserver Daemon Setup zu bestätigen.

    Die Meldung Installation abgeschlossen wird angezeigt.

13. Klicken Sie auf **Fertig**, um das Installationsprogramm für SANtricity Cloud Connectter zu beenden.

Konsolenmodus

Im Konsolenmodus können Sie den SANtricity-Cloud-Connector auf einem Linux-Betriebssystem installieren.

Bevor Sie beginnen

Bestimmen Sie einen Host-Standort für die Installation des SANtricity Cloud Connectors.

Schritte

1. Laden Sie die Installationsdatei für den SANtricity Cloud Connector auf den gewünschten IO-Host-Speicherort herunter.
2. Öffnen Sie ein Terminal-Fenster.
3. Navigieren Sie zu der Verzeichnisdatei, die die Installationsdatei für den SANtricity Cloud Connector enthält.

4. Starten Sie den Installationsvorgang für den SANtricity Cloud Connector:

```
./cloudconnector-xxxx.bin –i console
```

   In diesem Befehl `xxxx` Gibt die Versionsnummer der Anwendung an.

   Der Installationsvorgang für den SANtricity-Cloud-Konnektor wird initialisiert.

5. Drücken Sie **Enter**, um mit der Installation fortzufahren.

   Die Endbenutzer-Lizenzvereinbarung für NetApp, Inc. Software wird innerhalb des Installationsfensters angezeigt.

   > Um den Installationsprozess jederzeit abzubrechen, geben Sie ein `quit` Unter dem Fenster „Installer“.

6. Drücken Sie die Eingabetaste*, um die einzelnen Teile der Endbenutzer-Lizenzvereinbarung zu durchlaufen.

   Die Abnahmeerklärung zur Lizenzvereinbarung wird im Installationsfenster angezeigt.

7. Um die Bedingungen der Endbenutzer-Lizenzvereinbarung zu akzeptieren und mit der Installation des SANtricity Cloud Connectors fortzufahren, geben Sie ein `Y` Und drücken Sie * Enter * im Fenster des Installationsprogramms.

   Die Backups, die mit vorherigen Versionen der Seite SANtricity Cloud Connector erstellt wurden, werden angezeigt.

   > Wenn Sie die Bedingungen der Endbenutzervereinbarung nicht akzeptieren, geben Sie ein `N` Und drücken Sie **Enter**, um den Installationsvorgang für den SANtricity Cloud Connector zu beenden.

8. Um die Backups zu bestätigen, die mit früheren Versionen der SANtricity Cloud Connector-Nachricht erstellt wurden, drücken Sie **Enter**.

   > Um die Version 4.0 des SANtricity-Cloud-Connectors unter Beibehaltung einer früheren Version zu installieren, müssen für jede Version der Anwendung eindeutige Portnummern zugewiesen werden.

   Es wird eine Meldung „Installationsordner auswählen“ mit dem folgenden Standardinstallationsordner für den SANtricity Cloud Connector angezeigt:`/opt/netapp/santricity_cloud_connector4/`.

9. Wählen Sie eine der folgenden Optionen:
   - Um den Standard-Installationsort zu akzeptieren, drücken Sie **Enter**.
   - Um den Standardspeicherort für die Installation zu ändern, geben Sie den neuen Ordnerspeicherort ein. Es wird die Meldung „nicht SSL-Jetty-Portnummer eingeben“ angezeigt. Dem Non-SSL-Port wird ein Standardwert von 8080 zugewiesen.
10. Wählen Sie eine der folgenden Optionen:
    - Um die Standard-SSL-Portnummer zu akzeptieren, drücken Sie **Weiter**.

- Um die Standard-SSL-Portnummer zu ändern, geben Sie den neuen gewünschten Portnummer-Wert ein.

11. Wählen Sie eine der folgenden Optionen:
    - Um die Standard-nicht-SSL-Portnummer zu akzeptieren, drücken Sie **Enter**.
    - Geben Sie zum Ändern der standardmäßigen nicht-SSL-Portnummer den neuen Portnummer-Wert ein. Die Übersicht vor der Installation für den SANtricity-Cloud-Konnektor wird angezeigt.
12. Überprüfen Sie die angezeigte Zusammenfassung vor der Installation, und drücken Sie **Enter**.
13. Drücken Sie die Eingabetaste*, um die Eingabeaufforderung Webserver Daemon Setup zu bestätigen.

    Die Meldung Installation abgeschlossen wird angezeigt.

14. Drücken Sie **Enter**, um das Installationsprogramm für SANtricity Cloud Connectter zu beenden.

Fügen Sie Serverzertifikat und CA-Zertifikat in einen Schlüsselspeicher hinzu

Um eine sichere HTTPS-Verbindung vom Browser zum SANtricity Cloud Connector-Host zu verwenden, können Sie das selbstsignierte Zertifikat vom SANtricity Cloud Connector-Host akzeptieren oder ein Zertifikat und eine Vertrauenskette hinzufügen, die sowohl vom Browser als auch von der SANtricity Cloud Connector-Anwendung erkannt wird.

Bevor Sie beginnen

Die SANtricity Cloud Connector-Anwendung muss auf einem Host installiert sein.

Schritte

1. Beenden Sie den Dienst mit dem `systemctl` Befehl.
2. Greifen Sie über das Standardinstallationsverzeichnis auf das Arbeitsverzeichnis zu.

   Der Standard-Installationsort für den SANtricity-Cloud-Konnektor ist `/opt/netapp/santricity_cloud_connector4`.

3. Verwenden der `keytool` Erstellen Sie Ihr Serverzertifikat und die Zertifikatsignierungsanforderung (CSR).

   BEISPIEL

   ```
   keytool -genkey -dname "CN=host.example.com, OU=Engineering, O=Company,
   L=<CITY>, S=<STATE>, C=<COUNTRY>" -alias cloudconnect -keyalg "RSA"
   -sigalg SHA256withRSA -keysize 2048 -validity 365 -keystore
   keystore_cloudconnect.jks -storepass changeit
   keytool -certreq -alias cloudconnect -keystore keystore_cloudconnect.jks
   -storepass changeit -file cloudconnect.csr
   ```

4. Senden Sie die generierte CSR an die Zertifizierungsstelle (CA) Ihrer Wahl.

   Die Zertifizierungsstelle unterschreibt die Zertifikatanforderung und gibt ein signiertes Zertifikat zurück. Zusätzlich erhalten Sie ein Zertifikat von der Zertifizierungsstelle selbst. Dieses CA-Zertifikat muss in den Schlüsselspeicher importiert werden.

5. Importieren Sie das Zertifikat und die CA-Zertifikatskette in den Anwendungs-Schlüsselspeicher:

`/<install Path>/working/keystore`

BEISPIEL

```
keytool -import -alias ca-root -file root-ca.cer -keystore
keystore_cloudconnect.jks -storepass <password> -noprompt
keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore
keystore_cloudconnect.jks -storepass <password> -noprompt
keytool -import -trustcacerts -alias cloudconnect -file certnew.cer
-keystore keystore_cloudconnect.jks -storepass <password>
```

6. Starten Sie den Dienst neu.

Fügen Sie ein StorageGRID-Zertifikat in einen Schlüsselspeicher ein

Wenn Sie StorageGRID als Zieltyp für die SANtricity Cloud Connector-Anwendung konfigurieren, müssen Sie zunächst ein StorageGRID-Zertifikat in den Schlüsselspeicher SANtricity Cloud Connector hinzufügen.

Bevor Sie beginnen

- Sie haben ein signiertes StorageGRID-Zertifikat.
- Sie haben die SANtricity Cloud Connector-Anwendung auf einem Host installiert.

Schritte

1. Beenden Sie den Dienst mit dem `systemctl` Befehl.
2. Greifen Sie über das Standardinstallationsverzeichnis auf das Arbeitsverzeichnis zu.

> Der Standard-Installationsort für den SANtricity-Cloud-Konnektor ist `/opt/netapp/santricity_cloud_connector4`.

3. Importieren Sie das StorageGRID-Zertifikat in den Schlüsselspeicher der Anwendung: `/<install Path>/working/keystore`

BEISPIEL

```
opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import
-trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file
/home/ictlabsg01.cer -keystore
/opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
```

4. Starten Sie den Dienst neu.

Konfigurieren Sie den SANtricity Cloud Connector zum ersten Mal

Nach der erfolgreichen Installation können Sie die SANtricity Cloud Connector-Anwendung über den Konfigurationsassistenten einrichten. Der Konfigurationsassistent wird angezeigt, nachdem Sie sich zum ersten Mal am SANtricity Cloud Connector angemeldet haben.

Melden Sie sich zum ersten Mal am SANtricity-Cloud-Connector an

Wenn Sie den SANtricity-Cloud-Connector zum ersten Mal initialisieren, müssen Sie ein Standardpasswort für den Zugriff auf die Anwendung eingeben.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Zugriff auf einen mit dem Internet verbundenen Browser haben.

Schritte

1. Öffnen Sie einen unterstützten Browser.
2. Stellen Sie eine Verbindung zum konfigurierten SANtricity-Cloud-Connector-Server her (z. `http://localhost:8080/`).

   Die erste Anmeldeseite für die SANtricity-Cloud-Connector-Anwendung wird angezeigt.

3. Geben Sie im Feld Administrator-Kennwort das Standardpasswort von ein `password`.
4. Klicken Sie Auf **Anmelden**.

   Der Konfigurationsassistent für SANtricity Cloud Connector wird angezeigt.

Verwenden des Konfigurationsassistenten

Der Konfigurationsassistent wird angezeigt, wenn die erste Anmeldung beim SANtricity-Cloud-Connector erfolgreich durchgeführt wurde.

Über den Konfigurationsassistenten richten Sie das Administratorpasswort, die Anmeldeinformationen für das Webservices-Proxy-Anmeldemanagement, den gewünschten Backup-Zieltyp und den Verschlüsselungspasssatz für den SANtricity-Cloud-Connector ein.

Schritt 1: Administratorpasswort festlegen

Sie können das für die spätere Anmeldung am SANtricity-Cloud-Connector verwendete Passwort über die Seite Administratorkennwort festlegen anpassen.

Durch das Einrichten eines Passworts auf der Seite „Administratorkennwort festlegen“ wird das bei der ersten Anmeldung für die SANtricity Cloud Connector-Anwendung verwendete Standardpasswort ersetzt.

Schritte

1. Geben Sie auf der Seite Administratorkennwort festlegen das gewünschte Anmeldepasswort für den SANtricity Cloud Connector im Feld **Geben Sie das neue Administratorpasswort** ein.
2. Geben Sie im Feld * das neue Administratorpasswort* erneut ein, und geben Sie das Kennwort aus dem ersten Feld erneut ein.
3. Klicken Sie Auf **Weiter**.

   Die Kennworteinrichtung für den SANtricity-Cloud-Konnektor wird akzeptiert und die Seite Passphrase festlegen wird im Konfigurationsassistenten angezeigt.

   > ⓘ Das benutzerdefinierte Administratorkennwort wird erst eingerichtet, wenn Sie den Konfigurationsassistenten abgeschlossen haben.

Schritt 2: Passphrase einstellen

Auf der Seite Enter the Encryption Pass phrase können Sie einen alphanumerischen Passphrase zwischen 8 und 32 Zeichen angeben.

Im Rahmen der Datenverschlüsselung, die von der SANtricity-Cloud-Connector-Anwendung verwendet wird, ist ein benutzerangegebener Passphrase erforderlich.

Schritte

1. Geben Sie im Feld * Passphrase definieren* den gewünschten Passphrase ein.
2. Geben Sie im Feld * Ihre Passphrase* den Passphrase aus dem ersten Feld erneut ein.
3. Klicken Sie Auf **Weiter**.

   Der eingegebene Passphrase für die SANtricity-Cloud-Konnektor-Anwendung wird akzeptiert, und die Seite Zieltyp auswählen für den Konfigurationsassistenten wird angezeigt.

Schritt 3: Zieltyp auswählen

Backup- und Restore-Funktionen sind für Zieltypen von Amazon S3, AltaVault und StorageGRID über den SANtricity Cloud Connector verfügbar. Sie können den gewünschten Speicherzieltyp für die Anwendung SANtricity Cloud Connector auf der Seite Zieltyp auswählen angeben.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie über eines der folgenden Elemente verfügen: AltaVault Mount Point, Amazon AWS Konto oder StorageGRID Konto.

Schritte

1. Wählen Sie im Dropdown-Menü eine der folgenden Optionen aus:
   - Amazon AWS
   - AltaVault
   - StorageGRID

   Im Konfigurationsassistenten wird eine Seite Zieltyp für die ausgewählte Option angezeigt.
2. Beachten Sie die entsprechenden Konfigurationsanweisungen für AltaVault, Amazon AWS oder StorageGRID.

Konfigurieren der AltaVault-Appliance

Nach Auswahl der Option AltaVault Appliance unter der Seite Zieltyp auswählen werden Konfigurationsoptionen für den AltaVault-Zieltyp angezeigt.

Bevor Sie beginnen

- Sie verfügen über den NFS-Mount-Pfad für eine AltaVault Appliance.
- Sie haben die AltaVault Appliance als Zieltyp angegeben.

Schritte

1. Geben Sie im Feld * NFS Mount Path* den Mount Point für den AltaVault-Zieltyp ein.

   Die Werte im Feld **NFS Mount Path** müssen dem Linux-Pfadformat folgen.

2. Aktivieren Sie das Kontrollkästchen **Sichern der Konfigurationsdatenbank auf diesem Ziel**, um eine Sicherung der Konfigurationsdatenbank auf dem ausgewählten Zieltyp zu erstellen.

   Wenn beim Testen der Verbindung eine vorhandene Datenbankkonfiguration auf dem angegebenen Zieltyp erkannt wird, haben Sie die Möglichkeit, die vorhandenen Datenbankkonfigurationsinformationen auf dem SANtricity-Cloud-Connector-Host durch die im Konfigurationsassistenten eingegebenen neuen Backup-Informationen zu ersetzen.

3. Klicken Sie auf **Verbindung testen**, um die Verbindung für die angegebenen AltaVault-Einstellungen zu testen.
4. Klicken Sie Auf **Weiter**.

   Der angegebene Zieltyp für den SANtricity-Cloud-Konnektor wird akzeptiert, und die Seite Webdienste-Proxy wird im Konfigurationsassistenten angezeigt.

5. Weiter mit „Schritt 4: Verbindung zu Web Services Proxy herstellen“.

Amazon AWS Konto konfigurieren

Nach Auswahl der Option Amazon AWS auf der Seite Zieltyp auswählen werden die Konfigurationsoptionen für den Amazon AWS Zieltyp angezeigt.

Bevor Sie beginnen

- Sie verfügen über ein etabliertes Amazon AWS Konto.
- Sie haben Amazon AWS als Zieltyp angegeben.

Schritte

1. Geben Sie im Feld **Zugriffsschlüssel-ID** die Zugriffs-ID für das Amazon AWS Ziel ein.
2. Geben Sie im Feld * Secret Access Key* den geheimen Zugriffsschlüssel für das Ziel ein.
3. Geben Sie im Feld **Bucket Name** den Bucket-Namen für das Ziel ein.
4. Aktivieren Sie das Kontrollkästchen **Sichern der Konfigurationsdatenbank auf diesem Ziel**, um eine Sicherung der Konfigurationsdatenbank auf dem ausgewählten Zieltyp zu erstellen.

   Es wird empfohlen, diese Einstellung zu aktivieren, um sicherzustellen, dass die Daten aus dem Backup-Ziel wiederhergestellt werden können, wenn die Datenbank verloren geht.

   Wenn beim Testen der Verbindung eine vorhandene Datenbankkonfiguration auf dem angegebenen Zieltyp erkannt wird, haben Sie die Möglichkeit, die vorhandenen Datenbankkonfigurationsinformationen auf dem SANtricity-Cloud-Connector-Host durch die im Konfigurationsassistenten eingegebenen neuen Backup-Informationen zu ersetzen.

5. Klicken Sie auf **Verbindung testen**, um die eingegebenen Amazon AWS Anmeldedaten zu überprüfen.
6. Klicken Sie Auf **Weiter**.

   Der angegebene Zieltyp für den SANtricity-Cloud-Konnektor wird akzeptiert, und die Seite Webdienste-Proxy wird unter dem Konfigurationsassistenten angezeigt.

7. Weiter mit „Schritt 4: Verbindung zu Web Services Proxy herstellen“.

StorageGRID-Konto konfigurieren

Nachdem Sie die Option StorageGRID unter Zieltyp auswählen ausgewählt haben, werden die Konfigurationsoptionen für den StorageGRID-Zieltyp angezeigt.

Bevor Sie beginnen

- Sie verfügen über einen StorageGRID Account.
- Sie haben ein signiertes StorageGRID-Zertifikat im SANtricity Cloud Connector Schlüsselspeicher.
- Sie haben StorageGRID als Zieltyp angegeben.

Schritte

1. Geben Sie im Feld **URL** die URL für den Amazon S3-Cloud-Service ein
2. Geben Sie im Feld **Zugriffsschlüssel-ID** die Zugriffs-ID für das S3-Ziel ein.
3. Geben Sie im Feld **Secret Access Key** den geheimen Zugriffsschlüssel für das S3-Ziel ein.
4. Geben Sie im Feld **Bucket Name** den Bucket-Namen für das S3-Ziel ein.
5. Um den Zugriff auf den Pfadstil zu verwenden, aktivieren Sie das Kontrollkästchen * Zugriff im Pfadstil verwenden*.

   Wenn nicht aktiviert, wird der Zugriff im virtuellen Host-Stil verwendet.

6. Aktivieren Sie das Kontrollkästchen **Sichern der Konfigurationsdatenbank auf diesem Ziel**, um eine Sicherung der Konfigurationsdatenbank auf dem ausgewählten Zieltyp zu erstellen.

   Es wird empfohlen, diese Einstellung zu aktivieren, um sicherzustellen, dass die Daten aus dem Backup-Ziel wiederhergestellt werden können, wenn die Datenbank verloren geht.

   Wenn beim Testen der Verbindung eine vorhandene Datenbankkonfiguration auf dem angegebenen Zieltyp erkannt wird, haben Sie die Möglichkeit, die vorhandenen Datenbankkonfigurationsinformationen auf dem SANtricity-Cloud-Connector-Host durch die im Konfigurationsassistenten eingegebenen neuen Backup-Informationen zu ersetzen.

7. Klicken Sie auf **Verbindung testen**, um die eingegebenen S3-Anmeldeinformationen zu überprüfen.

   Für einige S3-konforme Konten sind möglicherweise sichere HTTP-Verbindungen erforderlich. Informationen zum Platzieren eines StorageGRID-Zertifikats in den Schlüsselspeicher finden Sie unter "Fügen Sie ein StorageGRID-Zertifikat in einen Schlüsselspeicher ein".

8. Klicken Sie Auf **Weiter**.

   Der angegebene Zieltyp für den SANtricity-Cloud-Konnektor wird akzeptiert, und die Seite Webdienste-Proxy wird im Konfigurationsassistenten angezeigt.

9. Weiter mit „Schritt 4: Verbindung zu Web Services Proxy herstellen“.

Schritt 4: Stellen Sie eine Verbindung zum Web Services Proxy her

Die Anmelde- und Verbindungsinformationen für den in Verbindung mit dem SANtricity-Cloud-Connector verwendeten Web-Services-Proxy werden über die Seite Webservices-Proxy-URL und -Anmeldeinformationen eingeben eingegeben.

Bevor Sie beginnen

Stellen Sie sicher, dass eine Verbindung zum SANtricity Webservices Proxy hergestellt ist.

Schritte

1. Geben Sie im Feld **URL** die URL des für den SANtricity-Cloud-Konnektor verwendeten WebdienstproProxy ein.
2. Geben Sie im Feld **Benutzername** den Benutzernamen für die Webdienste-Proxy-Verbindung ein.
3. Geben Sie im Feld **Passwort** das Passwort für die Webservices Proxy-Verbindung ein.
4. Klicken Sie auf **Verbindung testen**, um die Verbindung für die eingegebenen Web Services Proxy-Anmeldedaten zu überprüfen.
5. Nachdem die eingegebenen Web Services Proxy-Anmeldeinformationen über die Testverbindung überprüft wurden.
6. Klicken Sie Auf **Weiter**

   Die Anmeldeinformationen für den SANtricity-Cloud-Konnektor für Webdienste werden akzeptiert, und die Seite Speicherarrays auswählen wird im Konfigurationsassistenten angezeigt.

Schritt 5: Storage Arrays auswählen

Basierend auf den über den Konfigurationsassistenten eingegebenen SANtricity Webservices-Proxy-Anmeldeinformationen wird unter der Seite Speicherarrays auswählen eine Liste der verfügbaren Speicher-Arrays angezeigt. Über diese Seite können Sie auswählen, welche Speicher-Arrays der SANtricity-Cloud-Connector für Backup- und Wiederherstellungsaufträge verwendet.

Bevor Sie beginnen

Stellen Sie sicher, dass die Speicherarrays für Ihre SANtricity Web Services Proxy-Anwendung konfiguriert sind.

> Nicht erreichbare Speicher-Arrays, die von der SANtricity Cloud Connector Anwendung beobachtet werden, führen zu API-Ausnahmen in der Protokolldatei. Dies ist das beabsichtigte Verhalten der SANtricity-Cloud-Konnektor-Anwendung, wenn eine Volume-Liste aus einem nicht erreichbaren Array gezogen wird. Um diese API-Ausnahmen in der Protokolldatei zu vermeiden, können Sie das Root-Problem direkt mit dem Speicher-Array beheben oder das betroffene Speicherarray aus der SANtricity Web Services Proxy-Anwendung entfernen.

Schritte

1. Aktivieren Sie die Kontrollkästchen neben dem Storage-Array, das Sie der SANtricity Cloud Connector-Applikation für Backup- und Restore-Vorgänge zuweisen möchten.
2. Klicken Sie Auf **Weiter**.

   Die ausgewählten Speicher-Arrays werden akzeptiert, und die Seite Hosts auswählen wird im Konfigurationsassistenten angezeigt.

> Sie müssen ein gültiges Kennwort für jedes Speicherarray konfigurieren, das auf der Seite Speicherarrays auswählen ausgewählt wurde. Sie können Passwörter für Speicherarrays über die SANtricity Web Services Proxy-API-Dokumentation konfigurieren.

Schritt 6: Wählen Sie Hosts

Basierend auf den über den Konfigurationsassistenten ausgewählten Proxy-gehosteten Webservices-Speicherarrays können Sie einen verfügbaren Host auswählen, der auf der Seite Hosts auswählen die Backup- und Restore-Kandidaten-Volumes der SANtricity Cloud Connector-Anwendung zuordnen kann.

Bevor Sie beginnen

Stellen Sie sicher, dass über den SANtricity Web Services Proxy ein Host zur Verfügung steht.

Schritte

1. Wählen Sie im Dropdown-Menü für das aufgeführte Speicher-Array den gewünschten Host aus.
2. Wiederholen Sie Schritt 1 für alle zusätzlichen Speicher-Arrays, die auf der Seite Host auswählen aufgelistet sind.
3. Klicken Sie Auf **Weiter**.

   Der ausgewählte Host für den SANtricity-Cloud-Konnektor wird akzeptiert, und die Seite Überprüfung wird im Konfigurationsassistenten angezeigt.

Schritt 7: Prüfen Sie die Erstkonfiguration

Auf der letzten Seite des Konfigurationsassistenten für SANtricity Cloud Connector finden Sie eine Zusammenfassung der eingegebenen Ergebnisse.

Prüfen der Ergebnisse der validierten Konfigurationsdaten

- Wenn alle Konfigurationsdaten erfolgreich validiert und erstellt wurden, klicken Sie auf **Fertig stellen**, um den Konfigurationsprozess abzuschließen.
- Wenn ein Teil der Konfigurationsdaten nicht validiert werden kann, klicken Sie auf **Zurück**, um zur entsprechenden Seite des Konfigurationsassistenten zu navigieren, um die übermittelten Daten zu überarbeiten.

Melden Sie sich beim SANtricity Cloud Connector an

Sie können über den konfigurierten Server in einem unterstützten Browser auf die grafische Benutzeroberfläche der SANtricity-Cloud-Connector-Anwendung zugreifen. Stellen Sie sicher, dass Sie über ein Konto für den SANtricity Cloud Connector verfügen.

Schritte

1. Stellen Sie in einem unterstützten Browser eine Verbindung zum konfigurierten SANtricity-Cloud-Connector-Server her (z. B. `http://localhost:8080/`).

   Die Anmeldeseite für den SANtricity-Cloud-Connector wird angezeigt.

2. Geben Sie Ihr konfiguriertes Administratorkennwort ein.
3. Klicken Sie Auf **Login**.

   Die Landing Page für die SANtricity-Cloud-Connector-Anwendung wird angezeigt.

Verwenden Sie SANtricity Cloud Connector, um E-Series Volume-Backups zu erstellen und zu managen

Sie können die Backup-Option im linken Navigationsbereich der SANtricity Cloud Connector-Anwendung aufrufen. Mit der Option Backups wird die Seite Backups angezeigt, auf der Sie neue abbildbasierte oder dateibasierte Sicherungsaufträge erstellen können.

Verwenden Sie die Seite **Backups** der SANtricity Cloud Connector Applikation zur Erstellung und Verarbeitung von Backups von E-Series Volumes. Sie können Image- oder dateibasierte Backups erstellen und diese anschließend sofort oder zu einem späteren Zeitpunkt ausführen. Außerdem können Sie anhand des letzten vollständigen Backups oder inkrementeller Backups durchführen. Auf Grundlage des letzten vollständigen Backups, die durch die SANtricity Cloud Connector Applikation durchgeführt werden, können maximal sechs inkrementelle Backups durchgeführt werden.

> Alle Zeitstempel für Backup- und Wiederherstellungsjobs, die unter der Anwendung SANtricity Cloud Connector aufgeführt sind, verwenden lokale Zeit.

Erstellen Sie ein neues Image-basiertes Backup

Über die Funktion Erstellen können Sie neue abbilderbasierte Backups auf der Backup-Seite der SANtricity Cloud Connector-Anwendung erstellen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Speicherarrays aus dem Webservices Proxy auf dem SANtricity Cloud Connector registriert haben.

Schritte

1. Klicken Sie auf der Backup-Seite auf **Erstellen**.

   Das Fenster Backup erstellen wird angezeigt.

2. Wählen Sie **Erstellen eines Image-basierten Backups**.
3. Klicken Sie Auf **Weiter**.

   Eine Liste der verfügbaren E-Series Volumes wird im Fenster Backup erstellen angezeigt.

4. Wählen Sie das gewünschte Volumen der E-Serie aus und klicken Sie auf **Weiter**.

   Die Seite **Name der Sicherung und eine Beschreibung** des Fensters Create Backup confirmation wird angezeigt.

5. Um den automatisch generierten Backup-Namen zu ändern, geben Sie den gewünschten Namen in das Feld **Job Name** ein.
6. Fügen Sie bei Bedarf eine Beschreibung für das Backup im Feld **Job Description** hinzu.

   > Sie sollten eine Jobbeschreibung eingeben, mit der Sie den Inhalt des Backups leicht identifizieren können.

7. Klicken Sie Auf **Weiter**.

   Eine Zusammenfassung des ausgewählten bildbasierten Backups wird auf der Seite **Backup-Informationen überprüfen** des Fensters Backup erstellen angezeigt.

8. Überprüfen Sie die ausgewählte Sicherung, und klicken Sie auf **Fertig stellen**.

   Das Fenster Backup erstellen wird auf der Bestätigungsseite angezeigt.

9. Wählen Sie eine der folgenden Optionen:
   - **JA** — initiiert eine vollständige Sicherung für das ausgewählte Backup.
   - **NO** — eine vollständige Sicherung für das ausgewählte Image-basierte Backup wird nicht durchgeführt.

   > Ein vollständiges Backup für das ausgewählte Image-basierte Backup kann zu einem späteren Zeitpunkt über die Funktion Ausführen auf der Backup-Seite durchgeführt werden.

10. Klicken Sie auf **OK**.

    Das Backup für das ausgewählte E-Series Volume wird gestartet, und der Status der Aufgabe wird im Abschnitt Ergebnisliste der Backup-Seite angezeigt.

Erstellen Sie ein neues Ordner-/dateibasiertes Backup

Sie können neue Ordner-/dateibasierte Backups über die Funktion Erstellen auf der Backup-Seite der SANtricity Cloud Connector-Anwendung erstellen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Speicherarrays aus dem Webservices Proxy auf dem SANtricity Cloud Connector registriert haben.

Ein dateibasiertes Backup sichert bedingungslos alle Dateien auf dem von Ihnen angegebenen Dateisystem. Sie können jedoch eine selektive Wiederherstellung von Dateien und Ordnern durchführen.

Schritte

1. Klicken Sie auf der Backup-Seite auf **Erstellen**.

   Das Fenster Backup erstellen wird angezeigt.

2. Wählen Sie **Ordner/Datei-basiertes Backup erstellen** aus.
3. Klicken Sie Auf **Weiter**.

   Im Fenster Backup erstellen wird eine Liste von Volumes mit für Backups verfügbaren Dateisystemen angezeigt.

4. Wählen Sie die gewünschte Lautstärke aus und klicken Sie auf **Weiter**.

   Im Fenster Backup erstellen wird eine Liste der verfügbaren Dateisysteme auf dem ausgewählten Volume angezeigt.

   > Wenn Ihr Dateisystem nicht angezeigt wird, überprüfen Sie, ob Ihr Dateisystem-Typ von der SANtricity-Cloud-Connector-Anwendung unterstützt wird. Weitere Informationen finden Sie unter "Unterstützte Dateisysteme".

5. Wählen Sie das gewünschte Dateisystem aus, das den Ordner oder die zu sicherenden Dateien enthält, und klicken Sie auf **Weiter**.

Die Seite **Name der Sicherung und eine Beschreibung** des Fensters Create Backup confirmation wird angezeigt.

6. Um den automatisch generierten Backup-Namen zu ändern, geben Sie den gewünschten Namen in das Feld **Job Name** ein.
7. Fügen Sie bei Bedarf eine Beschreibung für das Backup im Feld **Job Description** hinzu.

   Sie sollten eine Jobbeschreibung eingeben, mit der Sie den Inhalt des Backups leicht identifizieren können.

8. Klicken Sie Auf **Weiter**.

   Eine Zusammenfassung des ausgewählten Ordners/dateibasierten Backups wird im Fenster Backup erstellen auf der Seite **Backup-Informationen überprüfen** angezeigt.

9. Prüfen Sie den ausgewählten Ordner/das dateibasierte Backup und klicken Sie auf **Fertig stellen**.

   Das Fenster Backup erstellen wird auf der Bestätigungsseite angezeigt.

10. Wählen Sie eine der folgenden Optionen:
    - **JA** — initiiert eine vollständige Sicherung für das ausgewählte Backup.
    - **NEIN** — eine vollständige Sicherung für die ausgewählte Sicherung wird nicht durchgeführt.

      Ein vollständiges Backup für das ausgewählte dateibasierte Backup kann auch zu einem späteren Zeitpunkt über die Funktion Ausführen auf der Backup-Seite durchgeführt werden.

11. Klicken Sie Auf **Schließen**.

    Das Backup für das ausgewählte E-Series-Volume wird gestartet, und der Status der Aufgabe wird im Abschnitt Ergebnisliste der Backup-Seite angezeigt.

Vollständige und inkrementelle Backups ausführen

Sie können über die Funktion Ausführen auf der Seite Backups vollständige und inkrementelle Backups durchführen. Inkrementelle Backups sind nur für dateibasierte Backups verfügbar.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie über den SANtricity Cloud Connector einen Backup-Job erstellt haben.

Schritte

1. Wählen Sie auf der Registerkarte Backups den gewünschten Sicherungsauftrag aus und klicken Sie auf **Ausführen**.

   Ein vollständiges Backup wird automatisch durchgeführt, wenn ein Image-basierter Backup-Job oder ein Backup-Job ohne eine zuvor durchgeführte erste Sicherung ausgewählt wird.

   Das Fenster Sicherung ausführen wird angezeigt.

2. Wählen Sie eine der folgenden Optionen:
   - **Full** — sichert alle Daten für das ausgewählte dateibasierte Backup.

- **Incremental** — sichert die Änderungen nur seit dem letzten Backup.

> Basierend auf dem letzten vollständigen Backup, das durch die SANtricity Cloud Connector Applikation durchgeführt wurde, können maximal sechs inkrementelle Backups durchgeführt werden.

3. Klicken Sie Auf **Ausführen**.

   Die Backup-Anfrage wird gestartet.

Löschen Sie einen Sicherungsauftrag

Mit der Funktion Löschen werden gesicherte Daten am angegebenen Zielspeicherort für die ausgewählte Sicherung zusammen mit dem Backup-Satz gelöscht.

Bevor Sie beginnen

Stellen Sie sicher, dass ein Backup mit dem Status „Abgeschlossen“, „Fehlgeschlagen“ oder „abgebrochen“ vorhanden ist.

Schritte

1. Wählen Sie auf der Seite Backups die gewünschte Sicherung aus und klicken Sie auf **Löschen**.

   > Wenn eine vollständige Basissicherung zum Löschen ausgewählt wird, werden auch alle damit verbundenen inkrementellen Backups gelöscht.

   Das Fenster Löschen bestätigen wird angezeigt.

2. Geben Sie im Feld **Typ delete** ein `DELETE` Um die Löschaktion zu bestätigen.
3. Klicken Sie Auf **Löschen**.

   Die ausgewählte Sicherung wird gelöscht.

Erstellen Sie neue Image- oder dateibasierte Restores in SANtricity Cloud Connector

Sie können die Option Wiederherstellen im linken Navigationsbereich der SANtricity-Cloud-Connector-Anwendung aufrufen. Mit der Option Wiederherstellen wird die Seite Wiederherstellen angezeigt, auf der Sie neue abbilbasierte oder dateibasierte Wiederherstellungsaufträge erstellen können.

Der SANtricity Cloud Connector nutzt das Jobkonzept, um die tatsächliche Wiederherstellung eines E-Series Volume durchzuführen. Bevor Sie eine Wiederherstellung durchführen, müssen Sie angeben, welches E-Series Volume für den Vorgang verwendet wird. Nachdem Sie ein E-Series Volume zur Wiederherstellung zum SANtricity Cloud Connector-Host hinzugefügt haben, können Sie das verwenden `Restore` Seite der SANtricity-Cloud-Connector-Anwendung zum Erstellen und Verarbeiten von Wiederherstellungen.

> Alle Zeitstempel für Backup- und Wiederherstellungsjobs, die unter der Anwendung SANtricity Cloud Connector aufgeführt sind, verwenden lokale Zeit.

Erstellen Sie eine neue Image-basierte Wiederherstellung

Sie können neue bildbasierte Wiederherstellungen über die Funktion Erstellen auf der Seite Wiederherstellen der SANtricity-Cloud-Connector-Anwendung erstellen.

Bevor Sie beginnen

Stellen Sie sicher, dass über den SANtricity Cloud Connector ein Image-basiertes Backup verfügbar ist.

Schritte

1. Klicken Sie auf der Seite Wiederherstellen der Anwendung SANtricity Cloud Connector auf **Erstellen**.

   Das Fenster Wiederherstellen wird angezeigt.

2. Wählen Sie das gewünschte Backup aus.
3. Klicken Sie Auf **Weiter**.

   Die Seite Sicherungspunkt auswählen wird im Fenster Wiederherstellen angezeigt.

4. Wählen Sie die gewünschte vollständige Sicherung aus.
5. Klicken Sie Auf **Weiter**.

   Die Seite Restore Target auswählen wird im Fenster Wiederherstellen angezeigt.

6. Wählen Sie das Wiederherstellungsvolume aus und klicken Sie auf **Weiter**.

   Die Seite „Prüfen“ wird im Fenster „Wiederherstellen“ angezeigt.

7. Überprüfen Sie den ausgewählten Wiederherstellungsvorgang und klicken Sie auf **Fertig stellen**.

   Die Wiederherstellung für das ausgewählte Ziel-Host-Volume wird gestartet, und der Status für die Aufgabe wird im Abschnitt Ergebnisliste der Seite Wiederherstellen angezeigt.

Erstellen Sie eine neue dateibasierte Wiederherstellung

Sie können neue dateibasierte Wiederherstellungen über die Funktion Erstellen auf der Seite Wiederherstellen der Anwendung SANtricity Cloud Connector erstellen.

Bevor Sie beginnen

Stellen Sie sicher, dass über den SANtricity Cloud Connector ein dateibasiertes Backup zur Verfügung steht.

Schritte

1. Klicken Sie auf der Seite Wiederherstellen der Anwendung SANtricity Cloud Connector auf **Erstellen**.

   Das Fenster Wiederherstellen wird angezeigt.

2. Wählen Sie im Fenster Wiederherstellen das gewünschte dateibasierte Backup aus.
3. Klicken Sie Auf **Weiter**.

   Die Seite Sicherungspunkt auswählen wird im Fenster Job erstellen angezeigt.

4. Wählen Sie auf der Seite Sicherungspunkt auswählen die gewünschte vollständige Sicherung aus.
5. Klicken Sie Auf **Weiter**.

Im Fenster Wiederherstellen wird eine Liste der verfügbaren Dateisysteme oder Ordner/Dateien angezeigt.

6. Wählen Sie die gewünschten Ordner oder Dateien, die wiederhergestellt werden sollen, und klicken Sie auf **Weiter**.

   Die Seite Restore Target auswählen wird im Fenster Wiederherstellen angezeigt.

7. Wählen Sie das Wiederherstellungsvolume aus und klicken Sie auf **Weiter**.

   Die Seite „Prüfen“ wird im Fenster „Wiederherstellen“ angezeigt.

8. Überprüfen Sie den ausgewählten Wiederherstellungsvorgang und klicken Sie auf **Fertig stellen**.

   Die Wiederherstellung für das ausgewählte Ziel-Host-Volume wird gestartet, und der Status für die Aufgabe wird im Abschnitt Ergebnisliste der Seite Wiederherstellen angezeigt.

Löschen Sie eine Wiederherstellung

Mit der Funktion Löschen können Sie ein ausgewähltes Wiederherstellungselement aus dem Listenbereich Ergebnis der Seite Wiederherstellen löschen.

Bevor Sie beginnen

Stellen Sie sicher, dass ein Wiederherstellungsauftrag mit dem Status „Abgeschlossen“, „Fehlgeschlagen“ oder „abgebrochen“ vorhanden ist.

Schritte

1. Klicken Sie auf der Seite Wiederherstellen auf **Löschen**.

   Das Fenster Löschen bestätigen wird angezeigt.

2. Geben Sie im Feld **Typ delete** ein `delete` Um die Löschaktion zu bestätigen.
3. Klicken Sie Auf **Löschen**.

   > Sie können eine unterbrochene Wiederherstellung nicht löschen.

   Die ausgewählte Wiederherstellung wird gelöscht.

Ändern Sie die Einstellungen für den SANtricity-Cloud-Konnektor

Mit der Option Einstellungen können Sie die aktuellen Konfigurationen der Anwendung für das S3-Konto, verwaltete Speicher-Arrays und Hosts sowie Web Services Proxy-Anmeldeinformationen ändern. Sie können das Passwort für den SANtricity-Cloud-Konnektor auch über die Option Einstellungen ändern.

Ändern Sie die S3-Kontoeinstellungen

Vorhandene S3-Einstellungen für die Anwendung SANtricity Cloud Connector können Sie im Fenster S3-Kontoeinstellungen ändern.

Bevor Sie beginnen

Beachten Sie beim Ändern der URL- oder S3-Bucket-Label-Einstellungen, dass der Zugriff auf vorhandene Backups, die über den SANtricity Cloud Connector konfiguriert wurden, beeinträchtigt wird.

Schritte

1. Klicken Sie in der linken Symbolleiste auf **Einstellungen > Konfiguration**.

   Die Seite Einstellungen - Konfiguration wird angezeigt.

2. Klicken Sie auf **Einstellungen anzeigen/bearbeiten** für S3-Kontoeinstellungen.

   Die Seite S3-Kontoeinstellungen wird angezeigt.

3. Geben Sie in der URL-Datei die URL für den S3-Cloud-Service ein.
4. Geben Sie im Feld **Zugriffsschlüssel-ID** die Zugriffs-ID für das S3-Ziel ein.
5. Geben Sie im Feld **Secret Access Key** den Zugriffsschlüssel für das S3-Ziel ein.
6. Geben Sie im Feld **S3 Bucket Name** den Bucket-Namen für das S3-Ziel ein.
7. Aktivieren Sie bei Bedarf das Kontrollkästchen * Pfad-Stil-Zugriff verwenden*.
8. Klicken Sie auf **Verbindung testen**, um die Verbindung zu den eingegebenen S3-Anmeldeinformationen zu überprüfen.
9. Klicken Sie auf **Speichern**, um die Änderungen anzuwenden.

   Die geänderten S3-Kontoeinstellungen werden angewendet.

Managen Sie Storage-Arrays

Sie können Speicher-Arrays von dem Web-Services-Proxy hinzufügen oder entfernen, der auf der Seite Speicherarrays managen beim SANtricity-Cloud-Connector-Host registriert ist.

Auf der Seite Speicherarrays managen wird eine Liste der Speicher-Arrays aus dem Web-Services-Proxy angezeigt, der für die Registrierung beim SANtricity-Cloud-Connector-Host verfügbar ist.

Schritte

1. Klicken Sie in der linken Symbolleiste auf **Einstellungen > Speicherarrays**.

   Der Bildschirm Einstellungen - Speicherarrays wird angezeigt.

2. Um dem SANtricity Cloud Connector Speicher-Arrays hinzuzufügen, klicken Sie auf **Hinzufügen**.
   a. Aktivieren Sie im Fenster Speicher-Arrays hinzufügen jedes Kontrollkästchen neben den gewünschten Speicher-Arrays in der Ergebnisliste.
   b. Klicken Sie Auf **Hinzufügen**.

      Das ausgewählte Speicher-Array wird dem SANtricity-Cloud-Konnektor hinzugefügt und im Ergebnislistenbereich des Bildschirms Einstellungen - Speicherarrays angezeigt.

3. Um den Host für ein hinzugefügtes Speicher-Array zu ändern, klicken Sie auf **Bearbeiten** für den Zeileneintrag im Ergebnislistenbereich des Bildschirms Einstellungen - Speicher-Arrays.
   a. Wählen Sie im Dropdown-Menü „Associated Host“ den gewünschten Host für das Speicher-Array aus.
   b. Klicken Sie Auf **Speichern**.

      Der ausgewählte Host wird dem Speicher-Array zugewiesen.

4. Um ein vorhandenes Speicher-Array aus dem SANtricity Cloud Connector-Host zu entfernen, wählen Sie die gewünschten Speicher-Arrays aus der unteren Ergebnisliste aus, und klicken Sie auf **Entfernen**.

a. Geben Sie im Feld Speicher-Array bestätigen die Eingabe ein `REMOVE`.

b. Klicken Sie Auf **Entfernen**.

Das ausgewählte Speicher-Array wird aus dem SANtricity-Cloud-Konnektor-Host entfernt.

Ändern Sie die Proxy-Einstellungen für Web Services

Sie können vorhandene Webdienste-Proxy-Einstellungen für die SANtricity Cloud Connector-Anwendung im Fenster Internetdienste-Proxy-Einstellungen ändern.

Bevor Sie beginnen

Der mit dem SANtricity-Cloud-Connector verwendete Web-Services-Proxy muss die entsprechenden Arrays hinzugefügt und das entsprechende Passwort gesetzt haben.

Schritte

1. Klicken Sie in der linken Symbolleiste auf **Einstellungen › Konfiguration**.

   Der Bildschirm Einstellungen - Konfiguration wird angezeigt.

2. Klicken Sie für Web Services Proxy auf **Einstellungen anzeigen/bearbeiten**.

   Der Bildschirm Web Services Proxy-Einstellungen wird angezeigt.

3. Geben Sie im Feld URL die URL des für den SANtricity-Cloud-Konnektor verwendeten Webservices-Proxys ein.
4. Geben Sie im Feld Benutzername den Benutzernamen für die Webdienste-Proxy-Verbindung ein.
5. Geben Sie im Feld Kennwort das Kennwort für die Web Services Proxy-Verbindung ein.
6. Klicken Sie auf **Verbindung testen**, um die Verbindung für die eingegebenen Web Services Proxy-Anmeldedaten zu überprüfen.
7. Klicken Sie auf **Speichern**, um die Änderungen anzuwenden.

Passwort für den SANtricity Cloud Connector ändern

Sie können das Kennwort für den SANtricity-Cloud-Konnektor im Bildschirm Kennwort ändern ändern.

Schritte

1. Klicken Sie in der linken Symbolleiste auf **Einstellungen › Konfiguration**.

   Der Bildschirm Einstellungen - Konfiguration wird angezeigt.

2. Klicken Sie auf **Passwort ändern** für SANtricity Cloud Connector.

   Der Bildschirm Kennwort ändern wird angezeigt.

3. Geben Sie im Feld Aktuelles Passwort Ihr aktuelles Kennwort für die SANtricity-Cloud-Connector-Anwendung ein.
4. Geben Sie im Feld Neues Kennwort Ihr neues Kennwort für die Anwendung SANtricity Cloud Connector ein.
5. Geben Sie im Feld Neues Kennwort bestätigen das neue Kennwort erneut ein.
6. Klicken Sie auf **Ändern**, um das neue Passwort anzuwenden.

Das geänderte Passwort wird auf die SANtricity Cloud Connector Anwendung angewendet.

Deinstallieren Sie den SANtricity Cloud Connector

Sie können den SANtricity-Cloud-Connector über den grafischen Deinstallationsprogramm oder den Konsolen-Modus deinstallieren.

Deinstallieren Sie im grafischen Modus

Sie können den Grafikmodus verwenden, um den SANtricity-Cloud-Connector auf einem Linux-Betriebssystem zu deinstallieren.

Schritte

1. Navigieren Sie in einem Terminal-Fenster zu dem Verzeichnis, das die Deinstallationsdatei des SANtricity Cloud Connectors enthält.

   Die Deinstallationsdatei für den SANtricity-Cloud-Connector ist im folgenden Standardverzeichnis verfügbar:

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. Führen Sie im Verzeichnis, das die Deinstallationsdatei des SANtricity Cloud Connectors enthält, den folgenden Befehl aus:

   ```
   ./uninstall_cloud_connector4 –i gui
   ```

   Der Deinstallationsprozess für den SANtricity-Cloud-Connector wird initialisiert.

3. Klicken Sie im Deinstallationsfenster auf **Deinstallieren**, um mit der Deinstallation des SANtricity Cloud Connectors fortzufahren.

   Die Deinstallation ist abgeschlossen und die Anwendung SANtricity Cloud Connector wird im Betriebssystem Linux deinstalliert.

Deinstallieren Sie im Konsolenmodus

Sie können den Konsolenmodus verwenden, um den SANtricity-Cloud-Connector auf einem Linux-Betriebssystem zu deinstallieren.

Schritte

1. Navigieren Sie in einem Terminal-Fenster zu dem Verzeichnis, das die Deinstallationsdatei des SANtricity Cloud Connectors enthält.

   Die Deinstallationsdatei für den SANtricity-Cloud-Connector ist im folgenden Standardverzeichnis verfügbar:

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. Führen Sie im Verzeichnis, das die Deinstallationsdatei des SANtricity Cloud Connectors enthält, den folgenden Befehl aus:

```
./uninstall_cloud_connector4 –i console
```

   Der Deinstallationsprozess für den SANtricity-Cloud-Connector wird initialisiert.

3. Drücken Sie im Deinstallationsfenster **Enter**, um mit der Deinstallation des SANtricity Cloud Connectors fortzufahren.

   Die Deinstallation ist abgeschlossen und die Anwendung SANtricity Cloud Connector wird im Betriebssystem Linux deinstalliert.