SANtricity Software 11.9 Dokumentation

SANtricity software

NetApp
April 21, 2025

Inhalt

SANtricity Software 11.9 Dokumentation

Versionshinweise

Neuerungen bei SANtricity OS 11.90

In der folgenden Tabelle werden die neuen Funktionen von SANtricity System Manager 11.9 beschrieben.

Neue Funktionen in Version 11.90R2

Diese Version enthält nur geringfügige Änderungen und keine neuen Funktionen. Weitere Informationen zu den Änderungen in dieser Version finden Sie im "Versionshinweise zu E-Series 11.90".

Neue Funktionen in Version 11.90R1

Neues Feature	Beschreibung
Neue Speichersystemmodelle – EF300C und EF600C	In dieser Version werden die All-Flash-NVMe-Storage-Systeme EF300C und EF600C vorgestellt. Bei den EF300C und EF600C handelt es sich um Flash-Versionen mit hoher Kapazität der vorhandenen EF300 und EF600 Storage-Systeme. NVMe-SSD-Laufwerke mit einer hohen Kapazität von 30 TB oder 60 TB werden von EF300C und EF600C unterstützt. Der EF300C/EF600C ist nur für die Verwendung von Dynamic Disk Pools ohne Legacy-RAID-Unterstützung kompatibel.
Unterstützung von 12-GB-SAS-Schnittstellen auf EF4000	Der E4000 Controller unterstützt jetzt 12 GB SAS-Host-Schnittstellenkarten.

Neue Funktionen in Version 11.90

Neues Feature	Beschreibung
Neues Storage-Systemmodell: E4000	Mit dieser Version wird das kostengünstige Speichersystem E4000 eingeführt. Die E4000 unterstützt 12 und 60 Laufwerke und eine einzelne Host Interface Card (HIC) pro Controller. In der ersten Version werden Host-Schnittstellenkarten wie iSCSI und Fibre Channel unterstützt. E4000 Storage-Systeme und andere E-Series Storage-Systeme können in Unified Manager angezeigt und gemanagt werden.
Höhere Kapazität für Dynamic Disk Pools	Die Kapazität von Dynamic Disk Pools (DDP) wurde auf 12 PB erhöht, wenn die Kapazität jedes einzelnen Laufwerks innerhalb des Pools größer als 23 TB ist. Wenn die einzelne Laufwerkskapazität weniger als 23 TB beträgt, beträgt die DDP-Kapazität 6 PB.
Die Standardeinstellungen für den Medienscan wurden erhöht	Die Standard-Scanrate für Medien wurde auf 120 Tage erhöht.

Neues Feature	Beschreibung
Der private Schlüssel wird jetzt für die externe Schlüsselverwaltung akzeptiert	CSR-Datei (Certificate Signing Request), die extern über private und öffentliche Schlüsselpaare generiert wird, kann jetzt über System Manager importiert werden.
Die Anmeldesperre ist jetzt für Web Services verfügbar	Konfigurierbar nur über die REST-API, eine neue Einstellung für die Anmeldesperre ist jetzt für eingebettete und Proxy-Web-Services verfügbar.

Versionshinweise

Versionshinweise sind außerhalb dieser Site erhältlich. Sie werden aufgefordert, sich mit Ihren Anmeldedaten für die NetApp Support Site anzumelden.

- "11.90 Versionshinweise"
- "11.80 Versionshinweise"
- "11.70 Versionshinweise"
- "11.60 Versionshinweise"
- "11.50 Versionshinweise"

Los geht’s

Übersicht über die SANtricity Software

Systeme der E-Series enthalten SANtricity Software für die Storage-Provisionierung und andere Aufgaben.

Auf dieser Site wird die Verwendung der folgenden SANtricity Management-Schnittstellen beschrieben:

- System Manager – eine webbasierte Schnittstelle zur Verwaltung eines einzelnen Speicher-Arrays in Ihrem Netzwerk.
- Unified Manager – eine webbasierte Schnittstelle zur Anzeige und zum Management aller Storage-Arrays in Ihrem Netzwerk.

EF600/EF600C und EF300/EF300C Storage-Arrays unterstützen weder synchrones Spiegeln noch Thin Volumes.

SANtricity System Manager

System Manager ist eine webbasierte Managementsoftware, die in jeden Controller integriert ist. Um auf die Benutzeroberfläche zuzugreifen, rufen Sie die IP-Adresse des Controllers in einem Browser auf. Ein Setup-Assistent hilft Ihnen beim Einstieg in die Systemkonfiguration.

System Manager verfügt über eine Reihe von Managementfunktionen, darunter:

 **Leistung**
Performance-Daten von bis zu 30 Tagen einsehen, einschl. I/O-Latenz, IOPS, CPU-Auslastung und Durchsatz
 **Speicher**
Stellen Sie Storage mithilfe von Pools oder Volume-Gruppen bereit und erstellen Sie Applikations-Workloads.
 **Datenschutz**
Backup und Disaster Recovery mit Snapshots, Volume-Kopien und Remote-Spiegelung

 **Hardware**
Prüfen Sie den Komponentenstatus und führen Sie einige Funktionen aus, die sich auf diese Komponenten beziehen, z. B. die Zuweisung von Hot-Spare-Laufwerken.
 **Warnungen**
Benachrichtigung der Administratoren über wichtige Ereignisse im Storage-Array Warnmeldungen können per E-Mail, SNMP-Traps und Syslog gesendet werden.
 **Access Management**
Konfigurieren Sie die Benutzerauthentifizierung, bei der sich Benutzer mit zugewiesenen Anmeldedaten am System anmelden müssen.
 **Systemeinstellungen**
Konfigurieren Sie weitere System-Performance-Funktionen wie SSD-Cache und automatischer Lastausgleich.
 **Unterstützung**
Anzeigen von Diagnosedaten, Managen von Upgrades und Konfigurieren von AutoSupport. Diese überwachen den Zustand eines Storage-Arrays und senden automatische Entsendungen von Patches an den technischen Support.

SANtricity Unified Manager

Unified Manager ist eine webbasierte Software, die zur Verwaltung Ihrer gesamten Domain verwendet wird. In einer zentralen Ansicht zeigt sich der Status aller neueren E-Series und EF-Series Arrays wie E4000, E2800, EF280, EF300, E5700, EF570, EF600, EF300C und EF600C. Sie können auch Batch-Operationen auf ausgewählten Storage-Arrays ausführen.

Unified Manager wird auf einem Management-Server und dem Web Services Proxy installiert. Um auf Unified Manager zuzugreifen, öffnen Sie einen Browser und geben die URL ein, die auf den Server zeigt, auf dem der Web Services Proxy installiert ist.

Unified Manager bietet eine Vielzahl an Management-Funktionen, darunter:

 **Speicher-Arrays entdecken**
Suchen Sie die zu verwaltenden Speicher-Arrays im Netzwerk Ihres Unternehmens und fügen Sie sie hinzu. Sie können dann den Status aller Speicher-Arrays von einer einzelnen Seite aus anzeigen.
 **Start**
Öffnen Sie eine Instanz des System Managers, um individuelle Managementvorgänge für ein bestimmtes Storage-Array durchzuführen.
 **Importeinstellungen**
Führen Sie einen Batch-Import von einem Storage-Array zu mehreren Arrays durch, einschließlich Einstellungen für Warnmeldungen, AutoSupport und Verzeichnisdienste.
 **Spiegelung**
Konfigurieren Sie asynchrone oder synchrone gespiegelte Paare zwischen zwei Storage-Arrays.
 **Gruppen Verwalten**
Ordnen Sie Storage-Arrays in Gruppen zu, die das Management erleichtern.

 **Upgrade Center**
Aktualisieren Sie die SANtricity OS Software auf mehreren Storage Arrays.
 **Zertifikate**
Erstellen Sie Zertifikatssignierungsanforderungen (CSRs), importieren Sie Zertifikate und verwalten Sie vorhandene Zertifikate für mehrere Speicher-Arrays.
 **Access Management**
Konfigurieren Sie die Benutzerauthentifizierung, bei der sich Benutzer bei Unified Manager mit zugewiesenen Anmeldedaten anmelden müssen.

Unterstützte Browser und Betriebssysteme

SANtricity unterstützt verschiedene Arten von Browsern und Betriebssystemen.

Browser

Die folgenden Browser und Versionen werden unterstützt.

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

Für Unified Manager muss der Web Services Proxy installiert und dem Browser zur Verfügung stehen. Weitere Informationen finden Sie unter "SANtricity Web Services Proxy: Überblick"

Betriebssysteme

Die folgenden Betriebssysteme und Versionen werden unterstützt.

Betriebssystem	Mindestversion/Architektur
Red hat Enterprise Linux (RHEL)	7.x, 8.x / 64-Bit
SUSE Linux Enterprise Server (SLES)	12.x, 15.x / 64-Bit
Oracle Linux (OL)	7.x, 8.x / 64-Bit
Windows Server	2016, 2019, 2022/64-Bit
Ubuntu	18.04, 20.04/64-Bit

Einrichtung von SANtricity System Manager

Greifen Sie auf SANtricity System Manager zu

Für den Zugriff auf die Benutzeroberfläche von SANtricity System Manager rufen Sie die IP-Adresse des Controllers in einem Browser auf. Ein Setup-Assistent hilft Ihnen beim Einstieg in die Systemkonfiguration.

Bevor Sie beginnen

- Installieren und konfigurieren Sie Ihre Hardware, wie in einer der Express-Konfigurationsanleitungen beschrieben:
  - "Linux Express-Konfiguration"
  - "VMware Express-Konfiguration"
  - "Windows Express-Konfiguration"
- Konfigurieren Sie eine Management Station, die die folgenden Anforderungen erfüllt:
  - Mit einem Netzwerk verbunden, das 1 Gbit/s oder schneller ist.
  - An dasselbe Subnetz wie die Storage-Management-Ports angeschlossen.
  - Wird als separate Station und nicht als Host (angehangene I/O-Verbindung) verwendet, der für das Datenmanagement verwendet wird.
  - Einrichtung für Out-of-Band-Management, bei dem eine Storage-Management-Station Befehle über die Ethernet-Verbindungen zum Controller an das Storage-System sendet
  - Richten Sie die Einrichtung mit einem unterstützten Browser ein. Siehe "Unterstützte Browser und Betriebssysteme".

Schritte

1. Geben Sie in Ihrem Browser die folgende URL ein: `https://<IPAddress>`

   `IPAddress` Ist die Adresse für einen der Storage Array Controller.

   Wenn System Manager zum ersten Mal auf einem Array geöffnet wird, das nicht konfiguriert wurde, wird die Eingabeaufforderung Administratorkennwort festlegen angezeigt.

2. Geben Sie in den Feldern Administratorpasswort festlegen und Passwort bestätigen das Passwort für die

Administratorrolle ein und klicken Sie dann auf **Passwort festlegen**.

Der Setup-Assistent wird bei der ersten Anmeldung gestartet.

3. Mit dem Setup-Assistenten können Sie die folgenden Aufgaben ausführen:
   - **Überprüfung der Hardware (Controller und Laufwerke)** - Überprüfen Sie die Anzahl der Controller und Laufwerke im Speicher-Array. Weisen Sie dem Array einen Namen zu.
   - **Überprüfung der Hosts und Betriebssysteme** - Überprüfen Sie die Host- und Betriebssystemtypen, auf die das Speicherarray zugreifen kann.
   - **Pools akzeptieren** — Akzeptieren Sie die empfohlene Poolkonfiguration für die Express-Installationsmethode. Ein Pool ist eine logische Laufwerksgruppe.
   - **Warnungen konfigurieren** — System Manager kann automatische Benachrichtigungen erhalten, wenn ein Problem mit dem Speicher-Array auftritt.
   - **AutoSupport aktivieren** — überwacht automatisch den Zustand Ihres Speicherarrays und sendet Entsendungen an den technischen Support.

Weitere Informationen zum Setup-Assistenten finden Sie unter "Übersicht über den Setup-Assistenten".

Übersicht über den Setup-Assistenten

Mit dem Setup-Assistenten können Sie Ihr Storage-Array konfigurieren, einschließlich Hardware, Hosts, Applikationen, Workloads Pools, Warnmeldungen und AutoSupport.

Ersteinrichtung

Wenn Sie System Manager zum ersten Mal öffnen, wird der Setup-Assistent gestartet. Der Setup-Assistent fordert Sie auf, grundlegende Konfigurationsaufgaben durchzuführen, z. B. die Benennung Ihres Speicher-Arrays, die Konfiguration Ihrer Hosts, die Auswahl von Anwendungen und die Erstellung von Speicherpools.

> Bevor Sie mit der Ersteinrichtung fortfahren können, gehen Sie zum Upgrade Center (Menü:Support[Upgrade Center]) und stellen Sie sicher, dass Ihre SANtricity OS-Software auf dem neuesten Stand ist. Aktualisieren Sie bei Bedarf auf die neueste Version, und aktualisieren Sie Ihren Browser, um mit der Einrichtung fortzufahren. Weitere Informationen finden Sie unter "Übersicht zum Upgrade Center".

Wenn Sie den Assistenten abbrechen, können Sie ihn nicht manuell neu starten. Der Assistent wird automatisch neu gestartet, wenn Sie den System Manager öffnen oder den Browser aktualisieren, und mindestens eine der folgenden Bedingungen erfüllt ist:

- Es werden keine Pools und Volume-Gruppen erkannt.
- Es werden keine Workloads erkannt.
- Es werden keine Benachrichtigungen konfiguriert.

Terminologie

Der Setup-Assistent verwendet die folgenden Begriffe.

Laufzeit	Beschreibung
Applikation	Eine Applikation ist ein Software-Programm wie Microsoft SQL Server oder Microsoft Exchange.
Alarm	Warnungen benachrichtigen Administratoren über wichtige Ereignisse auf den Storage-Arrays. Warnmeldungen können per E-Mail, SNMP-Traps oder Syslog gesendet werden.
AutoSupport	Die AutoSupport Funktion überwacht den Zustand eines Storage Arrays und sendet automatische Aussendungen an den technischen Support.
Trennt	Die Storage-System-Hardware umfasst Storage Arrays, Controller und Laufwerke.
Host	Ein Host ist ein Server, der I/O an ein Volume auf einem Storage-Array sendet.
Objekt	Ein Objekt besteht aus jeder logischen oder physischen Storage-Komponente. Zu den logischen Objekten gehören Volume-Gruppen, Pools und Volumes. Zu den physischen Objekten gehören das Storage-Array, Array-Controller, Hosts und Laufwerke.
Pool	Ein Pool ist eine Reihe von Laufwerken, die logisch gruppiert sind. Mit einem Pool können Sie ein oder mehrere Volumes erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einem Pool oder einer Volume-Gruppe.)
Datenmenge	Ein Volume ist ein Container, in dem Applikationen, Datenbanken und Filesysteme Daten speichern. Dies ist die logische Komponente, die erstellt wird, damit der Host auf den Speicher des Speicherarrays zugreifen kann. Ein Volume wird auf Basis der Kapazität erstellt, die in einem Pool oder einer Volume-Gruppe verfügbar ist. Ein Volume verfügt über eine definierte Kapazität. Obwohl ein Volume aus mehr als einem Laufwerk bestehen kann, wird ein Volume als eine logische Komponente für den Host angezeigt.
Volume-Gruppe	Eine Volume-Gruppe ist ein Container für Volumes mit gemeinsamen Merkmalen. Eine Volume-Gruppe verfügt über eine definierte Kapazität und einen RAID-Level. Sie können eine Volume-Gruppe verwenden, um ein oder mehrere Volumes zu erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einer Volume-Gruppe oder aus einem Pool.)
Workload	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.

FAQs

Was, wenn ich nicht alle meine Hardware-Komponenten sehen?

Wenn im Dialogfeld Hardware überprüfen nicht alle Hardwarekomponenten angezeigt werden, kann dies bedeuten, dass ein Festplatten-Shelf nicht ordnungsgemäß verbunden ist oder dass ein inkompatibles Shelf im Speicher-Array installiert ist.

Vergewissern Sie sich, dass alle Laufwerk-Shelfs ordnungsgemäß angeschlossen sind. Wenn Sie unsicher sind, welche Laufwerkseinschübe kompatibel sind, wenden Sie sich an den technischen Support.

Was, wenn ich nicht alle meine Gastgeber sehen?

Wenn Sie die verbundenen Hosts nicht sehen, ist die automatische Erkennung fehlgeschlagen, die Hosts sind nicht ordnungsgemäß angeschlossen oder es sind derzeit keine Hosts angeschlossen.

Sie können Hosts später konfigurieren, sobald Sie die Einrichtung durchgeführt haben. Sie können Hosts wie folgt manuell erstellen:

- Sie können Hosts manuell erstellen und die entsprechenden Host-Port-IDs zuordnen, indem Sie zu MENU:Storage[Hosts] wechseln. Hosts, die manuell erstellt wurden, werden auch im Assistenten * Initial Setup* angezeigt.
- Ziel und Host müssen für den Host-Port-Typ (z. B. iSCSI oder NVMe over RoCE) konfiguriert werden und eine Session für den Storage, der eingerichtet wurde, bevor die automatische Erkennung funktioniert.

Wie kann ich anhand der Identifizierung von Applikationen mein Storage-Array managen?

Wenn Sie Applikationen identifizieren, empfiehlt SANtricity System Manager automatisch eine Volume-Konfiguration, die den Storage basierend auf dem Applikationstyp optimiert.

Die Optimierung von Volumes durch Applikation ermöglicht einen effizienteren Storage-Betrieb. Merkmale wie I/O-Typ, Segmentgröße, Controller-Eigentümer und Lese- und Schreib-Cache sind in der Volume-Konfiguration enthalten. Zusätzlich können Sie Performance-Daten nach Applikation und Workload anzeigen, um Latenz, IOPS und MiB/s der Applikationen und der zugehörigen Workloads zu bewerten.

Was ist ein Workload?

Für einige Applikationen im Netzwerk, z. B. SQL Server oder Exchange, können Sie einen Workload definieren, der den Storage für die jeweilige Applikation optimiert.

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 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.

Wie konfiguriere ich die Bereitstellungsmethode für AutoSupport?

Um Konfigurationsaufgaben für AutoSupport-Bereitstellungsmethoden aufzurufen, gehen Sie zu **Support › Support Center** und klicken Sie dann auf die Registerkarte **AutoSupport**.

Die folgenden Protokolle werden unterstützt: HTTPS und SMTP.

Woher weiß ich, ob ich die empfohlene Pool-Konfiguration akzeptieren sollte?

Ob Sie die empfohlene Poolkonfiguration akzeptieren, hängt von einigen Faktoren ab.

Ermitteln Sie den Storage-Typ, der Ihre Anforderungen am besten erfüllt, indem Sie folgende Fragen beantworten:

- Bevorzugen Sie mehrere Pools mit geringerer Kapazität, anstatt die größten Pools möglich?
- Bevorzugen Sie RAID-Volume-Gruppen statt Pools?
- Möchten Sie Ihre Laufwerke lieber manuell bereitstellen, anstatt eine Konfiguration für Sie zu empfehlen?

Wenn Sie eine dieser Fragen mit Ja beantwortet haben, sollten Sie die empfohlene Poolkonfiguration ablehnen.

Der SANtricity System Manager hat keine Hosts erkannt. Was mache ich?

Wenn Sie die verbundenen Hosts nicht sehen, ist die automatische Erkennung fehlgeschlagen, die Hosts sind nicht ordnungsgemäß angeschlossen oder es sind derzeit keine Hosts angeschlossen.

Sie können Hosts später konfigurieren, sobald Sie die Einrichtung durchgeführt haben. Sie können Hosts wie folgt manuell erstellen:

- Sie können Hosts manuell erstellen und die entsprechenden Host-Port-IDs zuordnen, indem Sie zu MENU:Storage[Hosts] wechseln. Hosts, die manuell erstellt wurden, werden auch im Assistenten * Initial Setup* angezeigt.
- Ziel und Host müssen für den Host-Port-Typ (z. B. iSCSI oder NVMe over RoCE) konfiguriert werden und eine Session für den Storage, der eingerichtet wurde, bevor die automatische Erkennung funktioniert.

Einrichtung von SANtricity Unified Manager

Installation von SANtricity Unified Manager

SANtricity Unified Manager ist Bestandteil des Web Services Proxy. Hierbei handelt es sich um einen separat auf einem Host-System installierten RESTful API Server zum Management von NetApp Storage-Systemen der E-Serie.

Informationen zur Installation von Web Services Proxy und Unified Manager finden Sie im Dokumentationszentrum E-Series und SANtricity unter:

1. "Installations- und Upgrade-Anforderungen prüfen"
2. "Laden Sie die Web Services Proxy-Datei herunter und installieren Sie sie"

Zugriff auf SANtricity Unified Manager

Nach der Installation des Webdienstproxys können Sie auf den SANtricity Unified Manager zugreifen, um mehrere Speichersysteme über eine webbasierte Schnittstelle zu verwalten.

Informationen zu unterstützten Browsern finden Sie unter "Unterstützte Browser und Betriebssysteme".

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 über Benutzer und Passwörter finden Sie unter "Funktionsweise von Access Management".

Einheitliches Array Management mit SANtricity System Manager 11.9

Hauptschnittstelle

SANtricity System Manager – Überblick über die Benutzeroberfläche

SANtricity System Manager ist eine webbasierte Schnittstelle, über die Sie Storage Array in einer einzigen Ansicht verwalten können.

Homepage

Die Startseite enthält eine Dashboard-Ansicht für die tägliche Verwaltung Ihres Speicherarrays. Wenn Sie sich bei System Manager anmelden, wird die Startseite der erste Bildschirm angezeigt.

Die Dashboard-Ansicht enthält vier Übersichtsbereiche mit wichtigen Informationen zu Status und Zustand Ihres Storage-Arrays. Weitere Informationen finden Sie im Übersichtsbereich.

Werden	Beschreibung
Benachrichtigungen	Im Bereich Benachrichtigungen werden Problembenachrichtigungen angezeigt, die den Status des Speicher-Arrays und seiner Komponenten anzeigen. In diesem Portlet werden automatisierte Warnungen angezeigt, die Sie bei der Behebung von Problemen unterstützen können, bevor diese sich auf andere Bereiche Ihrer Storage-Umgebung auswirken.
Leistung	Im Bereich Performance können Sie die Ressourcennutzung im Laufe der Zeit vergleichen und gegenüberstellen. Sie können die Performance-Kennzahlen eines Storage-Arrays für Reaktionszeit (IOPS), Übertragungsraten (MiB/s) und die Menge der genutzten Verarbeitungskapazität (CPU) anzeigen.
Kapazität	Im Bereich Kapazität wird eine Diagrammansicht der zugewiesenen Kapazität, der freien Speicherkapazität und der nicht zugewiesenen Speicherkapazität im Speicher-Array angezeigt.
Storage-Hierarchie	Der Bereich Speicherhierarchie bietet eine organisierte Ansicht der verschiedenen Hardwarekomponenten und Speicherobjekte, die von Ihrem Speicher-Array verwaltet werden. Klicken Sie auf den Dropdown-Pfeil, um eine bestimmte Aktion für die Hardwarekomponente oder das Storage-Objekt auszuführen.

Schnittstelleneinstellungen

Sie können die Anzeigeeinstellungen und andere Einstellungen über die Hauptschnittstelle ändern.

Einstellung	Beschreibung
Anzeigeeinstellungen	Ändern Sie Kapazitätswerte und den Zeitrahmen im Dropdown-Menü Einstellungen in der oberen rechten Ecke der Schnittstelle.
Session-Timeouts	Konfigurieren Sie Timeouts, so dass die inaktiven Sitzungen des Benutzers nach einer bestimmten Zeit getrennt werden.
Hilfe	Greifen Sie über das Dropdown-Menü oben rechts auf die Hilfedokumentation und andere Ressourcen zu.

Benutzeranmeldungen und Passwörter

Der aktuelle Benutzer, der am System angemeldet ist, wird oben rechts auf der Schnittstelle angezeigt.

Weitere Informationen zu Benutzern und Kennwörtern finden Sie unter:

- "Legen Sie den Schutz des Admin-Passworts fest"
- "Passwörter ändern"

Anzeigen von Performance-Daten

Performance-Überblick

Auf der Seite Performance können Sie ganz einfach die Performance Ihres Storage-Arrays überwachen.

Was kann ich aus Performance-Daten lernen?

Die Performance-Diagramme und -Tabellen zeigen Performance-Daten nahezu in Echtzeit an. So können Sie ermitteln, ob ein Storage-Array Probleme hat. Sie können auch Performance-Daten speichern, um einen historischen Überblick über ein Storage Array zu erstellen und zu erkennen, wann ein Problem gestartet wurde oder welche Ursache ein Problem verursacht hat.

Weitere Informationen:

- "Performance-Diagramme und Richtlinien"
- "Performance-Bedingungen"

Wie kann ich Performance-Daten anzeigen?

Performancedaten sind auf der Startseite und auf der Speicherseite verfügbar.

Weitere Informationen:

- "Anzeigen grafischer Performance-Daten"
- "Anzeigen und Speichern von Leistungsdaten in Tabellenform"
- "Performance-Daten analysieren"

Performance-Diagramme und Richtlinien

Die Seite Performance enthält Diagramme und Tabellen von Daten, mit denen Sie die Performance des Storage-Arrays in verschiedenen wichtigen Bereichen bewerten können.

Mit Leistungsfunktionen können Sie die folgenden Aufgaben ausführen:

- Zeigen Sie Performance-Daten nahezu in Echtzeit an, um zu ermitteln, ob ein Storage-Array Probleme hat.
- Export von Performance-Daten, um eine historische Ansicht eines Storage-Arrays zu erstellen und zu ermitteln, wann ein Problem gestartet wurde oder welche Ursache ein Problem verursacht hat.
- Wählen Sie die Objekte, Performance-Kennzahlen und den Zeitrahmen aus, die Sie anzeigen möchten.
- Vergleichen von Metriken

Performance-Daten sind in drei Formaten verfügbar:

- **Echtzeit-Grafik** — zeichnet Performancedaten auf einem Diagramm in nahezu Echtzeit.
- **Beinahe Echtzeit-Tabelle** — listet Performancedaten in einer Tabelle in nahezu Echtzeit auf.
- **Exportierte CSV-Datei** — ermöglicht das Speichern tabellarischer Leistungsdaten in einer Datei mit kommagetrennten Werten zur weiteren Anzeige und Analyse.

Merkmale der Performance-Datenformate

Art der Leistungsüberwachung	Probenintervall	Angezeigte Zeitdauer	Maximale Anzahl der angezeigten Objekte	Möglichkeit Daten zu speichern
Echtzeit-Grafik, Live Echtzeit-Grafik, historisch	10 Sek. (Live) 5 Min. (Historisch) Die angezeigten Datenpunkte hängen vom ausgewählten Zeitrahmen ab	Der Standardzeitrahmen beträgt 1 Stunde. Optionen: • 5 Minuten • 1 Stunde • 8 Stunden • 1 Tag • 7 Tage • 30 Tage	5	Nein
Tabelle nahezu in Echtzeit (Tabellenansicht)	10 Sekunden - 1 Std	Der aktuellste Wert	Unbegrenzt	Ja.
CSV-Datei (Comma Separated Values)	Abhängig vom ausgewählten Zeitrahmen	Abhängig vom ausgewählten Zeitrahmen	Unbegrenzt	Ja.

Richtlinien zum Anzeigen von Performance-Daten

- Die Erfassung von Performance-Daten ist jederzeit aktiviert. Es besteht keine Möglichkeit, es auszuschalten.
- Jedes Mal, wenn das Abtastintervall abgelaufen ist, wird das Speicher-Array abgefragt und die Daten aktualisiert.
- Für grafische Daten unterstützt der 5-minütige Zeitrahmen eine Aktualisierung von durchschnittlich 10 Sekunden über 5 Minuten. Alle anderen Zeitrahmen werden alle 5 Minuten aktualisiert, gemittelt über den ausgewählten Zeitrahmen.
- Performancedaten in den grafischen Ansichten werden in Echtzeit aktualisiert. Performance-Daten in der Tabellenansicht werden nahezu in Echtzeit aktualisiert.
- Wenn sich ein überwachtes Objekt während der Datenerfassung ändert, verfügt das Objekt möglicherweise nicht über einen vollständigen Satz von Datenpunkten über den ausgewählten Zeitrahmen. Beispielsweise können Volume-Sätze sich beim Erstellen, Löschen, Zuweisung oder nicht zugewiesenen Volume ändern. Oder Laufwerke können hinzugefügt, entfernt oder fehlgeschlagen werden.

Performante Terminologie

Erfahren Sie, welche Performance-Bedingungen auf Ihr Storage Array angewendet werden.

Laufzeit	Beschreibung
Applikation	Eine Applikation ist ein Software-Programm wie SQL oder Exchange.
CPU	CPU ist kurz für „Zentraleinheit“. CPU gibt den Prozentsatz der genutzten Verarbeitungskapazität des Storage-Arrays an.
Host	Ein Host ist ein Server, der I/O an ein Volume auf einem Storage-Array sendet.
IOPS	IOPS steht für Input/Output Operations per Second.
Latenz	Die Latenz ist das Zeitintervall zwischen einer Anforderung, z. B. für einen Lese- oder Schreibbefehl und der Antwort vom Host oder dem Storage Array.
LUN	Eine Logical Unit Number (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.
MIB	MIB ist eine Abkürzung für Mebibyte (Mega-Binärbyte). Ein MiB ist 220 oder 1,048,576 Byte. Vergleichen Sie mit MB, was einen Basiswert von 10 bedeutet. Ein MB entspricht 1,024 Byte.

Laufzeit	Beschreibung
Objekt	Ein Objekt besteht aus jeder logischen oder physischen Storage-Komponente. Zu den logischen Objekten gehören Volume-Gruppen, Pools und Volumes. Zu den physischen Objekten gehören das Storage-Array, Array-Controller, Hosts und Laufwerke.
Pool	Ein Pool ist eine Reihe von Laufwerken, die logisch gruppiert sind. Mit einem Pool können Sie ein oder mehrere Volumes erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einem Pool oder einer Volume-Gruppe.)
Lesen	Der Lesevorgang ist kurz für den „Lesevorgang“, der auftritt, wenn der Host Daten vom Speicher-Array anfordert.
Datenmenge	Ein Volume ist ein Container, in dem Applikationen, Datenbanken und Filesysteme Daten speichern. Dies ist die logische Komponente, die erstellt wird, damit der Host auf den Speicher des Speicherarrays zugreifen kann. Ein Volume wird auf Basis der Kapazität erstellt, die in einem Pool oder einer Volume-Gruppe verfügbar ist. Ein Volume verfügt über eine definierte Kapazität. Obwohl ein Volume aus mehr als einem Laufwerk bestehen kann, wird ein Volume als eine logische Komponente für den Host angezeigt.
Volume-Name	Ein Volume-Name ist eine Zeichenfolge, die dem Volume beim Erstellen zugewiesen wird. Sie können entweder den Standardnamen akzeptieren oder einen aussagekräftigeren Namen angeben, der den Datentyp angibt, der im Volume gespeichert ist.
Volume-Gruppe	Eine Volume-Gruppe ist ein Container für Volumes mit gemeinsamen Merkmalen. Eine Volume-Gruppe verfügt über eine definierte Kapazität und einen RAID-Level. Sie können eine Volume-Gruppe verwenden, um ein oder mehrere Volumes zu erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einer Volume-Gruppe oder aus einem Pool.)
Workload	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.
Schreiben	Der Schreibvorgang ist für „Schreibvorgang“ kurz, wenn Daten vom Host zum Array zur Speicherung gesendet werden.

Anzeigen grafischer Performance-Daten

Sie können grafische Performance-Daten für logische Objekte, physische Objekte, Applikationen und Workloads anzeigen.

Über diese Aufgabe

Die Performance-Diagramme zeigen historische Daten sowie Live-Daten, die derzeit erfasst werden. Eine vertikale Linie im Diagramm, die mit Live Update gekennzeichnet ist, unterscheidet historische Daten von Live-Daten.

Homepage-Ansicht

Die Startseite enthält ein Diagramm mit der Performance auf Speicherarray-Ebene. In dieser Ansicht können Sie eingeschränkte Metriken auswählen oder auf **Leistungsdetails anzeigen** klicken, um alle verfügbaren Metriken auszuwählen.

Detailansicht

Die in der detaillierten Performance-Ansicht verfügbaren Diagramme sind unter drei Registerkarten angeordnet:

- **Logische Ansicht** — zeigt Performancedaten für logische Objekte an, die nach Volume-Gruppen und Pools gruppiert sind. Zu den logischen Objekten gehören Volume-Gruppen, Pools und Volumes.
- **Physical View** — zeigt Leistungsdaten für den Controller, Host-Kanäle, Laufwerkskanäle und Laufwerke an.
- **Applikationen & Workloads View** — zeigt eine Liste der logischen Objekte (Volumes) an, die nach den von Ihnen definierten Anwendungstypen und Workloads gruppiert sind.

Schritte

1. Wählen Sie **Home**.
2. Um eine Ansicht auf Array-Ebene auszuwählen, klicken Sie auf die Schaltfläche IOPS, MiB/s oder CPU.
3. Klicken Sie für weitere Details auf **Performance-Details anzeigen**.
4. Wählen Sie die Registerkarte **logische Ansicht**, die Registerkarte **physische Ansicht** oder die Registerkarte **Anwendungen & Workloads Ansicht** aus.

   Je nach Objekttyp werden auf jeder Registerkarte unterschiedliche Diagramme angezeigt.

Registerkarten anzeigen	Für jeden Objekttyp werden Performance-Daten angezeigt
Logische Ansicht	• **Storage-Array**: IOPS, MiB/s • **Pools**: Latenz, IOPS, MiB/s • **Volume-Gruppen**: Latenz, IOPS, MiB/s • **Volumes**: Latenz, IOPS, MiB/s

Registerkarten anzeigen	Für jeden Objekttyp werden Performance-Daten angezeigt
Physische Ansicht	• * Controller*: IOPS, MiB/s, CPU, Reserve • **Host-Kanäle**: Latenz, IOPS, MiB/s, Reserve • **Drive-Channels**: Latenz, IOPS, MiB/s • **Laufwerke**: Latenz, IOPS, MiB/s
Anzeige Von Applikationen Und Workloads	• **Storage-Array**: IOPS, MiB/s • **Applikationen**: Latenz, IOPS, MiB/s • * Workloads*: Latenz, IOPS, MiB/s • **Volumes**: Latenz, IOPS, MiB/s

5. Verwenden Sie die Optionen, um die gewünschten Objekte und Informationen anzuzeigen.

Optionen

Optionen für die Anzeige von Objekten	Beschreibung
Erweitern Sie ein Fach, um die Liste der Objekte anzuzeigen.	*Navigationsklassen* enthalten Speicherobjekte wie Pools, Volume-Gruppen und Laufwerke. Klicken Sie auf das Fach, um die Liste der Objekte in der Schublade anzuzeigen.
Wählen Sie Objekte aus, die angezeigt werden sollen.	Aktivieren Sie das Kontrollkästchen links neben jedem Objekt, um die Performance-Daten auszuwählen, die Sie anzeigen möchten.
Verwenden Sie Filter, um Objektnamen oder Teilnamen zu suchen.	Geben Sie im Feld Filter den Namen oder einen Teilnamen von Objekten ein, um nur die Objekte in der Schublade aufzulisten.
Klicken Sie nach der Auswahl von Objekten auf **Grafiken aktualisieren**.	Nachdem Sie Objekte aus den Schubladen ausgewählt haben, wählen Sie **Grafiken aktualisieren**, um die grafischen Daten für die ausgewählten Objekte anzuzeigen.
Diagramm ausblenden oder anzeigen	Wählen Sie den Diagrammtitel aus, um das Diagramm auszublenden oder anzuzeigen.

6. Verwenden Sie bei Bedarf die zusätzlichen Optionen zum Anzeigen von Performance-Daten.

Weitere Optionen

Option	Beschreibung
Zeitrahmen	Wählen Sie die gewünschte Zeitspanne aus (5 Minuten, 1 Stunde, 8 Stunden, 1 Tag, 7 Tage, Oder 30 Tage). Der Standardwert ist 1 Stunde. Das Laden der Performance-Daten für einen 30-Tage-Zeitrahmen kann mehrere Minuten dauern. Navigieren Sie nicht von der Webseite weg, aktualisieren Sie die Webseite, oder schließen Sie den Browser während der Daten geladen werden.
Datenpunktdetails	Halten Sie den Mauszeiger über das Diagramm, um Kennzahlen für einen bestimmten Datenpunkt anzuzeigen.
Bildlaufleiste	Verwenden Sie die Bildlaufleiste unter dem Diagramm, um einen früheren oder späteren Zeitraum anzuzeigen.
Zoomleiste	Ziehen Sie unter dem Diagramm die Zoom-Griffe, um einen Zeitbereich zu verkleinern. Je größer der Zoom-Balken, desto weniger granular sind die Details des Diagramms. Um das Diagramm zurückzusetzen, wählen Sie eine der Zeitrahmenoptionen aus.
Drag-and-Drop	Ziehen Sie im Diagramm den Cursor von einem Zeitpunkt zum anderen, um einen Zeitbereich zu vergrößern. Um das Diagramm zurückzusetzen, wählen Sie eine der Zeitrahmenoptionen aus.

Anzeigen und Speichern von Leistungsdaten in Tabellenform

Sie können Performance-Diagrammdaten im Tabellenformat anzeigen und speichern. So können Sie die anzuzeigenden Daten filtern.

Schritte

1. Klicken Sie in einem beliebigen Leistungsdatendiagramm auf **Tabellenansicht starten**.

   Es wird eine Tabelle angezeigt, in der alle Performancedaten für die ausgewählten Objekte aufgelistet sind.

2. Verwenden Sie bei Bedarf die Dropdown-Liste Objektauswahl und den Filter.
3. Klicken Sie auf die Schaltfläche **Spalten einblenden/ausblenden**, um die Spalten auszuwählen, die in die Tabelle eingefügt werden sollen.

   Sie können auf die einzelnen Kontrollkästchen klicken, um ein Element auszuwählen oder die Auswahl aufzuheben.

4. Wählen Sie unten im Bildschirm **Exportieren** aus, um die tabellarische Ansicht in einer Datei mit kommagetrennten Werten (CSV) zu speichern.

   Das Dialogfeld Tabelle exportieren wird angezeigt, in dem die Anzahl der zu exportierenden Zeilen und das Dateiformat des Exports (kommagetrennte Werte oder CSV-Format) angezeigt werden.

5. Klicken Sie auf **Exportieren**, um mit dem Download fortzufahren, oder klicken Sie auf **Abbrechen**.

   Abhängig von den Browsereinstellungen wird die Datei entweder gespeichert oder Sie werden aufgefordert, einen Namen und einen Speicherort für die Datei auszuwählen.

   Das Standardformat für den Dateinamen ist `performanceStatistics-yyyy-mm-dd_hh-mm-ss.csv`, Die das Datum und die Uhrzeit des Exports der Datei enthält.

Performance-Daten analysieren

Performance-Daten können Sie dabei unterstützen, die Performance Ihres Storage-Arrays zu optimieren.

Beachten Sie bei der Interpretation der Performance-Daten, dass mehrere Faktoren die Performance des Storage-Arrays beeinträchtigen. Die folgende Tabelle beschreibt die wichtigsten zu berücksichtigende Bereiche.

Performance-Daten	Auswirkungen auf das Performance-Tuning
Latenz (Millisekunden oder ms)	Überwachen Sie die E/A-Aktivität eines bestimmten Objekts. Identifizierung von Objekten, die Engpässe sind: • Wenn eine Volume-Gruppe von mehreren Volumes gemeinsam genutzt wird, benötigen die einzelnen Volumes möglicherweise ihre eigenen Volume-Gruppen, um die sequenzielle Performance der Laufwerke zu verbessern und die Latenz zu verringern. • Bei Pools kommen größere Latenzen zum Einsatz und zwischen den Laufwerken können ungleichmäßige Workloads vorhanden sein, so dass die Latenzwerte weniger sinnvoll und im Allgemeinen auch höher sind. • Laufwerkstypen und Geschwindigkeit beeinflussen die Latenz. Mit zufälligen I/O-Operationen verbringen schnellere rotierende Laufwerke weniger Zeit damit, von und zu verschiedenen Speicherorten auf der Festplatte zu wechseln. • Zu wenige Laufwerke führen zu mehr Befehlen in Warteschlange und länger zur Verarbeitung des Befehls durch das Laufwerk, was die allgemeine Latenz des Systems erhöht. • Aufgrund der zusätzlichen Zeit, die mit der Datenübertragung verbunden ist, weisen größere I/OS eine höhere Latenz auf. • Eine höhere Latenz kann darauf hindeuten, dass das I/O-Muster von Natur aus zufällig ist. Laufwerke mit zufälligen I/O weisen eine größere Latenz als Laufwerke mit sequenziellem Streaming auf. • Ein Ungleichgewicht in der Latenz bei Laufwerken oder Volumes einer gemeinsamen Volume-Gruppe kann auf ein langsames Laufwerk hinweisen.

Performance-Daten	Auswirkungen auf das Performance-Tuning
IOPS	Faktoren, die Input/Output Operations per Second (IOPS oder iOS/s) beeinflussen, sind folgende Faktoren: • Zugriffsmuster (zufällig oder sequenziell) • I/O-Größe • RAID-Level • Cache-Blockgröße • Gibt an, ob die Lese-Cache-Speicherung aktiviert ist • Gibt an, ob das Schreib-Caching aktiviert ist • Dynamischer Cache-Lese-Prefetch • Segmentgröße • Die Anzahl der Laufwerke in den Volume- oder Speicher-Arrays Je höher die Cache-Trefferrate ist, desto höher sind die I/O-Raten. Im Vergleich zu deaktiviertem Schreib-Caching können höhere I/O-Raten erzielt werden. Bei der Entscheidung, ob das Schreib-Caching für ein einzelnes Volume aktiviert werden soll, müssen die aktuellen IOPS und die maximalen IOPS geprüft werden. Bei sequenziellen I/O-Mustern sollten Sie höhere Raten feststellen als bei zufälligen I/O-Mustern. Aktivieren Sie unabhängig vom I/O-Muster das Caching von Schreibvorgängen, um die I/O-Rate zu maximieren und die Reaktionszeit der Applikationen zu verkürzen. Sie sehen Performance-Verbesserungen, die durch das Ändern der Segmentgröße in den IOPS-Statistiken für ein Volume verursacht wurden. Versuchen Sie, die optimale Segmentgröße zu bestimmen, oder verwenden Sie die Größe des Dateisystems oder die Datenbankblockgröße.
MIB/s	Die Übertragungsraten oder Durchsatzraten werden von der I/O-Größe der Applikation und der I/O-Rate festgelegt. Im Allgemeinen resultieren I/O-Anfragen kleiner Applikationen in einer geringeren Übertragungsrate, bieten aber schnellere I/O-Raten und kürzere Reaktionszeiten. Bei größeren Applikations-I/O-Anfragen sind höhere Durchsatzraten möglich. Wenn Sie die typischen I/O-Muster Ihrer Applikationen kennen, können Sie die maximale I/O-Übertragungsrate für ein bestimmtes Storage-Array ermitteln.

Performance-Daten	Auswirkungen auf das Performance-Tuning
CPU	Dieser Wert ist ein Prozentsatz der genutzten Verarbeitungskapazität. Sie können feststellen, dass die CPU-Nutzung der gleichen Objekttypen eine Ungleichheit hat. Beispielsweise ist die CPU-Auslastung eines Controllers stark oder nimmt im Laufe der Zeit zu, während der des anderen Controllers leichter oder stabiler ist. In diesem Fall möchten Sie möglicherweise den Controller-Besitz von einem oder mehreren Volumes zu dem Controller mit dem niedrigeren CPU-Prozentsatz ändern. Möglicherweise möchten Sie die CPU über das Storage-Array hinweg überwachen. Wenn die CPU mit der Zeit zunimmt und gleichzeitig die Applikations-Performance abnimmt, müssen Sie möglicherweise Storage-Arrays hinzufügen. Durch Hinzufügen von Storage-Arrays zum Unternehmen werden die Applikationsanforderungen weiterhin auf einem akzeptablen Performance-Niveau erfüllt.
Reserve	„Reserve“ bezieht sich auf die verbleibende Performance-Fähigkeit der Controller, der Host-Kanäle des Controllers und der Laufwerkskanäle des Controllers. Dieser Wert wird in Prozent angegeben und stellt die Lücke zwischen der maximalen Performance dar, die diese Objekte liefern können, und dem aktuellen Performance-Level. • Für die Controller beträgt die Reserve einen Prozentsatz der maximal möglichen IOPS. • Für die Kanäle ist „Reserve“ ein Prozentsatz des maximalen Durchsatzes oder „MiB/s“ Der Lesedurchsatz, der Schreibdurchsatz und der bidirektionale Durchsatz sind in der Berechnung enthalten.

Speicherhierarchie anzeigen

Die Speicherhierarchie auf der Hauptschnittstelle bietet eine organisierte Ansicht der verschiedenen Hardwarekomponenten und Speicherobjekte, die von Ihrem Speicher-Array verwaltet werden.

Um die Storage-Hierarchie anzuzeigen, wechseln Sie zur Startseite und klicken Sie auf den Dropdown-Pfeil für eine Storage-Array-Komponente oder ein Storage-Objekt. Ein Storage Array besteht aus einer Sammlung sowohl physischer als auch logischer Komponenten.

Physische Komponenten

Die physischen Komponenten eines Storage-Arrays werden in dieser Tabelle beschrieben.

Komponente	Beschreibung
Controller	Ein Controller besteht aus einer Hauptplatine, Firmware und Software. Sie steuert die Laufwerke und implementiert die Funktionen von System Manager.

Komponente	Beschreibung
Shelf	Ein Shelf ist ein Gehäuse, das in einem Schrank oder Rack installiert ist. Er enthält die Hardwarekomponenten für das Storage-Array. Es gibt zwei Typen von Shelfs: Ein Controller-Shelf und ein Festplatten-Shelf. Ein Controller Shelf enthält Controller und Laufwerke. Ein Festplatten-Shelf enthält ein-/Ausgabemodule (IOMs) und Laufwerke. Wenn Ihr Storage-Array unterschiedliche Medientypen oder Schnittstellentypen enthält, wird für jeden Laufwerkstyp ein Festplatten-Shelf angezeigt.
Laufwerk	Ein Laufwerk ist ein elektromagnetisches mechanisches Gerät oder ein Solid State-Speichergerät, das die physischen Speichermedien für Daten bereitstellt.
Host	Ein Host ist ein Server, der I/O an ein Volume auf einem Storage-Array sendet.
Host Bus Adapter (HBA)	Ein Host Bus Adapter (HBA) ist eine Platine, die sich auf einem Host befindet und einen oder mehrere Host-Ports enthält.
Host-Port	Ein Host Port ist ein Port an einem Host Bus Adapter (HBA), der die physische Verbindung zu einem Controller bereitstellt und für I/O-Vorgänge genutzt wird.
Management- Client	Ein Management-Client ist der Computer, auf dem ein Browser zum Zugriff auf System Manager installiert ist.

Logische Komponenten

Die Laufwerke im Speicher-Array stellen die physische Speicherkapazität für Daten bereit. Mit System Manager lässt sich die physische Kapazität in logischen Komponenten wie Pools, Volume-Gruppen und Volumes konfigurieren. Diese Komponenten sind die Tools, mit denen Sie Daten im Storage Array konfigurieren, speichern, warten und erhalten. In dieser Tabelle werden die logischen Komponenten eines Speicherarrays beschrieben.

Komponente	Beschreibung
Pool	Ein Pool ist eine Reihe von Laufwerken, die logisch gruppiert sind. Mit einem Pool können Sie ein oder mehrere Volumes erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einem Pool oder einer Volume-Gruppe.)
Volume-Gruppe	Eine Volume-Gruppe ist ein Container für Volumes mit gemeinsamen Merkmalen. Eine Volume-Gruppe verfügt über eine definierte Kapazität und einen RAID-Level. Sie können eine Volume-Gruppe verwenden, um ein oder mehrere Volumes zu erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einer Volume-Gruppe oder aus einem Pool.)
Datenmenge	Ein Volume ist ein Container, in dem Applikationen, Datenbanken und Filesysteme Daten speichern. Dies ist die logische Komponente, die erstellt wird, damit der Host auf den Speicher des Speicherarrays zugreifen kann.

Komponente	Beschreibung
Logical Unit Number (LUN)	Eine Logical Unit Number (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.

Verwalten von Schnittstelleneinstellungen

Passwortschutz verwalten

Sie müssen das Speicher-Array mit Kennwörtern konfigurieren, um es vor unbefugtem Zugriff zu schützen.

Kennwörter festlegen und ändern

Wenn Sie System Manager zum ersten Mal starten, werden Sie aufgefordert, ein Administratorpasswort festzulegen. Jeder Benutzer mit dem Admin-Passwort kann Konfigurationsänderungen am Speicher-Array vornehmen, z. B. Objekte oder Einstellungen hinzufügen, ändern oder entfernen. Informationen zum Festlegen des Admin-Passworts während des ersten Startvorgangs finden Sie unter "Greifen Sie Auf System Manager Zu".

Aus Sicherheitsgründen können Sie nur fünf Mal versuchen, ein Passwort einzugeben, bevor das Speicherarray den Status „Sperre“ eingibt. In diesem Zustand weist das Speicherarray nachfolgende Passwortversuche zurück. Sie müssen 10 Minuten warten, bis das Speicherarray auf einen „normalen“ Zustand zurückgesetzt wird, bevor Sie erneut versuchen, ein Passwort einzugeben.

Zusätzlich zum Admin-Passwort enthält das Speicher-Array vordefinierte Benutzerprofile mit einer oder mehreren Rollen, die ihnen zugeordnet sind. Weitere Informationen finden Sie unter "Berechtigungen für zugeordnete Rollen". Die Benutzerprofile und Zuordnungen können nicht geändert werden. Es können nur Passwörter geändert werden. Wenn Sie das Admin-Passwort oder andere Benutzerpasswörter ändern möchten, finden Sie weitere Informationen unter "Passwörter ändern".

Geben Sie Passwörter nach Sitzungszeitungen erneut ein

Das System fordert Sie zur Eingabe des Passworts nur einmal während einer einzigen Verwaltungssitzung auf. Eine Sitzung läuft jedoch nach 30 Minuten Inaktivität ab. Zu diesem Zeitpunkt müssen Sie das Passwort erneut eingeben. Wenn ein anderer Benutzer, der dasselbe Speicher-Array von einem anderen Management-Client aus verwaltet, das Passwort während der Sitzung ändert, werden Sie beim nächsten Versuch eines Konfigurationsvorgangs oder einer Ansicht aufgefordert, ein Passwort einzugeben.

Sie können das Sitzungszeitlimit ändern oder Sitzungszeitüberschreitungen komplett deaktivieren. Siehe "Verwalten von Sitzungszeitungen".

Entfernen Sie Laufwerke oder Kennwortschutz

Wenn Sie passwortgeschützte Laufwerke entfernen oder den Kennwortschutz deaktivieren möchten, beachten Sie Folgendes:

- **Wenn Sie Laufwerke mit Kennwortschutz entfernen** — wird das Passwort auf einem reservierten

Bereich jedes Laufwerks im Speicher-Array gespeichert. Wenn Sie alle Laufwerke aus einem Speicher-Array entfernen, funktioniert das Kennwort nicht mehr. Um diese Bedingung zu beheben, installieren Sie eines der Originallaufwerke erneut in das Speicher-Array.

- **Wenn Sie den Passwortschutz entfernen möchten** — Wenn Sie keine Befehle mehr passwortgeschützt haben möchten, geben Sie das aktuelle Administratorpasswort ein und lassen Sie die neuen Passwortfelder leer.

> Wenn Konfigurationsbefehle auf einem Storage-Array ausgeführt werden, kann dies zu ernsthaften Schäden und Datenverlusten führen. Aus diesem Grund sollten Sie immer ein Administratorkennwort für Ihr Speicherarray festlegen. Verwenden Sie ein langes Administratorkennwort mit mindestens 15 alphanumerischen Zeichen, um die Sicherheit zu erhöhen.

Standardeinheiten für Kapazitätswerte festlegen

SANtricity System Manager kann Kapazitätswerte entweder in Gibibyte (gib) oder Tebibyte (tib) anzeigen.

Einstellungen werden im lokalen Speicher des Browsers gespeichert, so dass alle Benutzer ihre eigenen Einstellungen haben können.

Schritte

1. Wählen Sie Menü:Einstellungen[Voreinstellungen festlegen].
2. Klicken Sie entweder auf das Optionsfeld für **Gibibyte** oder **Tebibyte** und bestätigen Sie, dass Sie den Vorgang durchführen möchten.

   Abkürzungen und Werte finden Sie in der folgenden Tabelle.

Abkürzung	Wert
Gib	$1{,}024^3$ Byte
TIB	$1{,}024^4$ Byte

Legen Sie den Standardzeitrahmen für Performance-Diagramme fest

Sie können den Standardzeitrahmen ändern, der von den Performance-Diagrammen angezeigt wird.

Über diese Aufgabe

Performance-Diagramme, die auf der Startseite und auf der Seite Performance angezeigt werden, zeigen zunächst einen Zeitrahmen von 1 Stunde an. Einstellungen werden im lokalen Speicher des Browsers gespeichert, so dass alle Benutzer ihre eigenen Einstellungen haben können.

Schritte

1. Wählen Sie Menü:Einstellungen[Voreinstellungen festlegen].
2. Wählen Sie in der Dropdown-Liste entweder **5 Minuten**, **1 Stunde**, **8 Stunden**, **1 Tag** oder **7 Tage**, Und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

Anmeldebanner konfigurieren

Sie können ein Login-Banner erstellen, das Benutzern angezeigt wird, bevor sie Sitzungen in SANtricity System Manager einrichten. Das Banner kann einen Hinweishinweisen und eine Einwilligungsmeldung enthalten.

Über diese Aufgabe

Wenn Sie ein Banner erstellen, wird es vor dem Anmeldebildschirm in einem Dialogfeld angezeigt.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie im Abschnitt Allgemein die Option **Anmelde-Banner konfigurieren** aus.

   Das Dialogfeld Anmelde-Banner konfigurieren wird geöffnet.

3. Geben Sie den Text ein, der im Anmeldebanner angezeigt werden soll.

   Verwenden Sie keine HTML- oder andere Markup-Tags zum Formatieren.

4. Klicken Sie Auf **Speichern**.

Ergebnisse

Wenn sich Benutzer beim nächsten Mal bei System Manager anmelden, wird der Text in einem Dialogfeld geöffnet. Benutzer müssen auf **OK** klicken, um mit dem Anmeldebildschirm fortzufahren.

Verwalten von Sitzungszeitungen

Sie können Timeouts in SANtricity System Manager konfigurieren, so dass die inaktiven Sitzungen der Benutzer nach einer bestimmten Zeit getrennt werden.

Über diese Aufgabe

Standardmäßig beträgt die Session-Zeitüberschreitung für System Manager 30 Minuten. Sie können diese Zeit anpassen oder Sitzungszeitausfälle ganz deaktivieren.

Wenn Access Management mit den in das Array integrierten SAML-Funktionen (Security Assertion Markup Language) konfiguriert ist, kann es zu einer Sitzungszeitüberschreitung kommen, wenn die SSO-Sitzung des Benutzers ihre maximale Grenze erreicht. Dies kann vor dem Timeout der System Manager-Sitzung auftreten.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie im Abschnitt Allgemein die Option **Session-Timeout aktivieren/deaktivieren**.

   Das Dialogfeld „Session-Timeout aktivieren/deaktivieren“ wird geöffnet.

3. Verwenden Sie die Spinner-Regler, um die Zeit in Minuten zu erhöhen oder zu verringern.

   Die für System Manager festgelegte minimale Zeitüberschreitung beträgt 15 Minuten.

Deaktivieren Sie zum Deaktivieren von Sitzungszeitzeitaktivits das Kontrollkästchen **Dauer festlegen…**.

4. Klicken Sie Auf **Speichern**.

Benachrichtigungen verwalten

Problembenachrichtigungen – Übersicht

SANtricity System Manager verwendet Symbole und verschiedene andere Methoden, um Sie über Probleme mit dem Speicher-Array zu informieren.

Symbole

System Manager verwendet diese Symbole, um den Status des Speicher-Arrays und seiner Komponenten anzuzeigen.

Symbol	Beschreibung
	Optimal
	Nicht optimal oder fehlgeschlagen
	Muss aufpassen oder korrigieren
	Achtung

System Manager zeigt diese Symbole an verschiedenen Orten an.

- Im Bereich Benachrichtigungen auf der Startseite werden das Fehlersymbol und eine Meldung angezeigt.
- Das Symbol Startseite im Navigationsbereich zeigt das Fehlersymbol an.
- Auf der Seite Komponenten wird in der Grafik für Laufwerke und Controller das Fehlersymbol angezeigt.

Meldungen und LEDs

Zudem wird von System Manager über Probleme in anderer Weise benachrichtigt.

- System Manager sendet SNMP-Benachrichtigungen oder E-Mail-Fehlermeldungen.
- Die LEDs für die Serviceaktion, die für die Hardware erforderlich sind, leuchten auf.

Wenn Sie eine Benachrichtigung über ein Problem erhalten, können Sie es mithilfe des Recovery Guru beheben. Verwenden Sie bei Bedarf die Hardware-Dokumentation mit den Wiederherstellungsschritten, um fehlerhafte Komponenten zu ersetzen.

Vorgänge in Bearbeitung anzeigen und umsetzen

Verwenden Sie die Seite „Vorgänge in Bearbeitung“, um bei lang laufenden Vorgängen Aktionen anzuzeigen und Maßnahmen zu ergreifen.

Über diese Aufgabe

Für jeden Vorgang, der auf der Seite „Vorgänge in Bearbeitung“ aufgeführt ist, werden ein Prozentsatz der Fertigstellung 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. Sie können einen abgeschlossenen Kopiervorgang auch aus der Liste löschen.

Schritte

1. Wählen Sie auf der Startseite die Option **Vorgänge in Bearbeitung anzeigen**.

   Die Seite „Vorgänge in Bearbeitung“ wird angezeigt.

2. 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.

   Sie können den Vorgang einer Volume-Kopie anhalten oder deren Priorität ändern.

3. Sobald ein Vorgang zur Volume-Kopie abgeschlossen ist, können Sie **Löschen** wählen, um es aus der Liste zu entfernen.

   Oben auf der Startseite werden eine Informationsmeldung und ein gelbes Schraubenschlüsselsymbol angezeigt, wenn ein Vorgang abgeschlossen ist. Diese Meldung enthält einen Link, mit dem Sie den Vorgang auf der Seite „Vorgänge in Bearbeitung“ löschen können.

Die Vorgänge, die auf der Seite „Vorgänge in Bearbeitung“ angezeigt werden, umfassen Folgendes:

Betrieb	Möglicher Status des Vorgangs	Maßnahmen, die Sie ergreifen können
Volume-Kopien	Abgeschlossen	Löschen
Volume-Kopien	In Bearbeitung	• Priorität ändern • Hör Auf
Volume-Kopien	Ausstehend	Löschen
Volume-Kopien	Fehlgeschlagen	• Löschen • Erneut kopieren
Volume-Kopien	Angehalten	• Löschen • Erneut kopieren
Volume-Erstellung (nur Thick Pool Volumes über 64 tib)	In Bearbeitung	*None*
Volume-Löschen (nur Thick Pool Volumes über 64 tib)	In Bearbeitung	*None*

Betrieb	Möglicher Status des Vorgangs	Maßnahmen, die Sie ergreifen können
Erste Synchronisierung der asynchronen Spiegelgruppe	In Bearbeitung	Aussetzen
Erste Synchronisierung der asynchronen Spiegelgruppe	Ausgesetzt	Fortsetzen
Synchrones Spiegeln	In Bearbeitung	Aussetzen
Synchrones Spiegeln	Ausgesetzt	Fortsetzen
Rollback von Snapshot Images	In Bearbeitung	Abbrechen
Rollback von Snapshot Images	Ausstehend	Abbrechen
Rollback von Snapshot Images	Angehalten	• Abbrechen • Fortsetzen
Evakuierung der Laufwerke	In Bearbeitung	Abbrechen (abhängig vom Evakuierungstyp der Antriebe)
Hinzufügen von Kapazitäten für den Pool oder die Volume-Gruppe	In Bearbeitung	*None*
Ändern Sie einen RAID-Level für ein Volume	In Bearbeitung	*None*
Reduktion der Kapazität für einen Pool	In Bearbeitung	*None*
Thin Volume-Rückgewinnung	In Bearbeitung	*None*
Prüfen Sie die verbleibende Zeit für einen IAF-Betrieb (Instant Availability Format) für Pool Volumes	In Bearbeitung	*None*
Prüfen Sie die Datenredundanz einer Volume-Gruppe	In Bearbeitung	*None*
Defragmentieren einer Volume-Gruppe	In Bearbeitung	*None*
Initialisieren Sie ein Volume	In Bearbeitung	*None*

Betrieb	Möglicher Status des Vorgangs	Maßnahmen, die Sie ergreifen können
Höhere Kapazität für ein Volume	In Bearbeitung	*None*
Ändern Sie die Segmentgröße für ein Volume	In Bearbeitung	*None*
Laufwerkskopie	In Bearbeitung	*None*
Datenrekonstruktion	In Bearbeitung	*None*
Copyback	In Bearbeitung	*None*
Laufwerk Löschen	In Bearbeitung	*None*
Remote Storage-Import	In Bearbeitung	• Priorität ändern • Hör Auf
Remote Storage-Import	Angehalten	• Fortsetzen • Trennen Sie Die Verbindung
Remote Storage-Import	Fehlgeschlagen	• Fortsetzen • Trennen Sie Die Verbindung
Remote Storage-Import	Abgeschlossen	Trennen Sie Die Verbindung

Mit Recovery Guru können Sie Probleme beheben

Der Recovery Guru ist eine Komponente des SANtricity System Managers, der die Probleme der Storage Arrays diagnostiziert und Recovery-Verfahren empfiehlt, mit denen die Probleme behoben werden können.

Schritte

1. Wählen Sie **Home**.
2. Klicken Sie in der Mitte des Fensters auf den Link **Recover from *n* Problems**.

   Das Dialogfeld Recovery Guru wird angezeigt.

3. Wählen Sie das erste Problem aus der Zusammenfassungsliste aus, und befolgen Sie die Anweisungen im Wiederherstellungsverfahren, um das Problem zu beheben. Verwenden Sie bei Bedarf die Austauschanweisungen, um fehlerhafte Komponenten auszutauschen. Wiederholen Sie diesen Schritt für jedes aufgelistete Problem.

   Innerhalb eines Storage-Arrays können mehrere Probleme auftreten. In diesem Fall kann die Reihenfolge, in der die Probleme korrigiert werden, das Ergebnis beeinflussen. Wählen und korrigieren Sie die Probleme in der Reihenfolge, in der sie in der Zusammenfassungsliste aufgeführt sind.

Mehrere Ausfälle für einen Netzteilbehälter werden gruppiert und als ein Problem in der Zusammenfassungsliste aufgeführt. Mehrere Ausfälle für einen Lüfterbehälter werden ebenfalls als ein Problem aufgeführt.

4. Um sicherzustellen, dass der Wiederherstellungsvorgang erfolgreich war, klicken Sie auf **recheck**.

   Wenn Sie ein Problem für eine asynchrone Spiegelgruppe oder ein Mitglied einer asynchronen Spiegelgruppe ausgewählt haben, klicken Sie zuerst auf **Löschen**, um den Fehler vom Controller zu löschen, und klicken Sie dann auf **recheck**, um das Ereignis aus dem Recovery Guru zu entfernen.

   Wenn alle Probleme behoben wurden, wechselt das Speicherarray-Symbol schließlich von der erforderlichen Aufmerksamkeit zum optimalen. Bei einigen Problemen wird während eines Vorgangs, z. B. der Rekonstruktion, ein Symbol zur Fehlerbehebung angezeigt.

5. **Optional:** um die Recovery Guru-Informationen in einer Datei zu speichern, klicken Sie auf das Symbol **Speichern**.

   Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `recovery-guru-failure-yyyy-mm-dd-hh-mm-ss-mmm.html`.

6. Um die Recovery Guru-Informationen auszudrucken, klicken Sie auf das Symbol **Drucken**.

FAQs

Welche Browser werden unterstützt?

SANtricity System Manager unterstützt die folgenden Browser-Versionen.

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

Was sind die Tastenkombinationen?

Sie können in SANtricity System Manager nur über die Tastatur navigieren.

Gesamtnavigation

Aktion	Tastenkombination
Zum nächsten Element wechseln.	Registerkarte
Zum vorherigen Element wechseln.	Umschalt + Tab

Aktion	Tastenkombination
Wählen Sie ein Element aus.	Eingabe
Dropdown-Liste: Zum nächsten oder vorherigen Element verschieben.	Pfeil nach unten oder nach oben
Kontrollkästchen - Wählen Sie ein Element aus.	Leertaste
Optionsfelder: Wechseln zwischen den Elementen.	Pfeil nach unten oder nach oben
Erweiterbarer Text – Erweiterung oder Vertragselement.	Eingabe

Tabellennavigation

Aktion	Tastenkombination
Wählen Sie eine Zeile aus.	Um eine Zeile auszuwählen, drücken Sie die Eingabetaste
Blättern Sie nach oben oder unten.	Pfeil nach unten/Pfeil nach oben oder Bild nach unten/Bild nach oben
Ändern Sie die Sortierreihenfolge einer Spalte.	Um eine Spaltenüberschrift auszuwählen, drücken Sie die Eingabetaste

Kalendernavigation

Aktion	Tastenkombination
Zum vorherigen Monat wechseln.	Bild Nach Oben
Zum nächsten Monat wechseln.	Bild Nach Unten
Wechseln Sie zum Vorjahr.	Strg + Bild Nach Oben
Gehen Sie zum nächsten Jahr.	Strg + Bild Nach Unten
Öffnen Sie die Datumauswahl, falls sie geschlossen ist.	Control + Home
Wechseln Sie zum aktuellen Monat.	Steuerung / Befehl + Home
Zum vorherigen Tag wechseln.	Steuerung / Befehl + Links

Aktion	Tastenkombination
Gehen Sie zum nächsten Tag.	Steuerung / Befehl + Rechts
Wechseln Sie zur vorherigen Woche.	Steuerung / Befehl + Nach Oben
Gehen Sie zur nächsten Woche.	Steuerung / Befehl + Nach Unten
Wählen Sie das fokussierte Datum aus.	Eingabe
Schließen Sie die Datumsauswahl, und löschen Sie das Datum.	Steuerung / Befehl + Ende
Schließen Sie die Datumsauswahl ohne Auswahl.	Flucht

Wie verhält sich Performance-Statistiken zu einzelnen Volumes mit dem Gesamt?

Die Statistiken für Pools und Volume-Gruppen werden durch Aggregation aller Volumes einschließlich reservierter Kapazitäts-Volumes berechnet.

Die reservierte Kapazität wird intern vom Storage-System zur Unterstützung von Thin Volumes, Snapshots und asynchroner Spiegelung genutzt und ist für I/O-Hosts nicht sichtbar. Aus diesem Grund werden die Statistiken für Pool, Controller und Speicher-Array möglicherweise nicht als Summe der sichtbaren Volumes angezeigt.

Für Applikations- und Workload-Statistiken werden jedoch nur die sichtbaren Volumes aggregiert.

Warum werden Daten in den Diagrammen und in der Tabelle als Null angezeigt?

Wenn für einen Datenpunkt in den Diagrammen und in der Tabelle eine Null angezeigt wird, bedeutet dies, dass für diesen Zeitpunkt keine I/O-Aktivität für das Objekt vorhanden ist. Dies kann passieren, weil der Host keine I/O-Vorgänge an dieses Objekt einleitet oder es ein Problem mit dem Objekt selbst sein kann.

Die historischen Daten für das Objekt können weiterhin angezeigt werden. Die Diagramme und die Tabelle zeigen nicht Null-Daten, sobald die I/O-Aktivität für das Objekt beginnt.

In der folgenden Tabelle sind die häufigsten Gründe aufgeführt, warum ein Datenpunktwert für ein bestimmtes Objekt Null sein könnte.

Objekttyp auf Array-Ebene	Ursachendaten werden als Null angezeigt
Datenmenge	• Das Volume hatte keine Host-Zuweisung.
Volume-Gruppe	• Volume-Gruppe wird importiert. • Volume-Gruppe enthält kein Volume, das einem Host zugewiesen ist. ***und*** Volume-Gruppe enthält keine reservierte Kapazität.

Objekttyp auf Array-Ebene	Ursachendaten werden als Null angezeigt
Laufwerk	• Laufwerk ist ausgefallen. • Laufwerk wurde entfernt. • Das Laufwerk befindet sich in einem unbekannten Zustand.
Controller	• Der Controller ist offline. • Controller ist ausgefallen. • Controller wurde entfernt. • Der Controller befindet sich in einem unbekannten Status.
Storage Array erledigen	• Das Storage-Array enthält keine Volumes.

Was zeigt das Latenzdiagramm?

Das Latenzdiagramm bietet Latenzstatistiken in Millisekunden (ms) für Volumes, Volume-Gruppen, Pools Applikationen und Workloads. Dieses Diagramm wird auf den Registerkarten logische Ansicht, physische Ansicht und Applikationen & Workloads angezeigt.

Bei der Latenz handelt es sich um jegliche Verzögerung, die beim Lesen oder Schreiben von Daten auftritt. Halten Sie den Mauszeiger über einen Punkt im Diagramm, um die folgenden Werte in Millisekunden (ms) für diesen Zeitpunkt anzuzeigen:

- Lesezeit.
- Schreibzeit.
- Durchschnittliche I/O-Größe

Was zeigt das IOPS-Diagramm?

Im IOPS-Diagramm werden Statistiken für die ein-/Ausgabe-Vorgänge pro Sekunde angezeigt. Auf der Startseite werden in diesem Diagramm Statistiken für das Speicher-Array angezeigt. In der logischen Ansicht, der physischen Ansicht und den Registerkarten Applikationen und Workloads der Performance-Ansicht werden in diesem Diagramm Statistiken für das Storage Array, die Volumes, Volume-Gruppen, Pools, Applikationen Und Workloads.

IOPS ist eine Abkürzung für *Input/Output (I/O) Operations per Second*. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um die folgenden Werte für diesen Zeitpunkt anzuzeigen:

- Anzahl der Lesevorgänge.
- Anzahl der Schreibvorgänge.
- Lese- und Schreibvorgänge insgesamt kombiniert.

Was wird im MiB/s-Diagramm angezeigt?

Das MiB/s-Diagramm zeigt Statistiken zur Übertragungsgeschwindigkeit in Mebibyte pro Sekunde an. Auf der Startseite werden in diesem Diagramm Statistiken für das Speicher-Array angezeigt. In der logischen Ansicht, der physischen Ansicht und den Registerkarten Applikationen und Workloads der Performance-Ansicht werden in diesem Diagramm Statistiken für das Storage Array, die Volumes, Volume-Gruppen, Pools, Applikationen Und Workloads.

MIB/s ist eine Abkürzung für *Mebibyte pro Sekunde*, bzw. 1,048,576 Byte pro Sekunde. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um die folgenden Werte für diesen Zeitpunkt anzuzeigen:

- Die Menge der Daten, die gelesen werden.
- Die Menge der geschriebenen Daten.
- Die kombinierte Gesamtdatenmenge, die gelesen und geschrieben wurde.

Was zeigt das CPU Diagramm?

Das CPU-Diagramm zeigt die Statistiken zur Verarbeitungskapazität für jeden Controller (Controller A und Controller B) an. CPU ist eine Abkürzung für *Central Processing Unit*. Auf der Startseite werden in diesem Diagramm Statistiken für das Speicher-Array angezeigt. Auf der Registerkarte „Physical View“ der Kachel „Performance“ werden in diesem Diagramm Statistiken für das Storage Array und die Laufwerke angezeigt.

Das CPU-Diagramm zeigt den Prozentsatz der CPU-Verarbeitungskapazität, die im Vergleich zu Operationen auf dem Array verwendet wird. Selbst wenn keine externe I/O-Vorgänge stattfinden, liegt die CPU-Auslastung in Prozent unter Umständen nicht ganz am Wert des Storage-Betriebssystems. Dies könnte dazu führen, dass Hintergrundvorgänge und das Monitoring durchgeführt werden. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um einen Prozentsatz der Verarbeitungsfähigkeit anzuzeigen, die zu diesem Zeitpunkt verwendet werden.

Was zeigt das Diagramm „Reserve“?

Das Diagramm Reserve bezieht sich auf die verbleibende Performance-Fähigkeit für die Storage Array Controller. Dieses Diagramm ist auf der Startseite und auf der Registerkarte Physical View der Kachel Performance sichtbar.

Das Diagramm Reserve zeigt die verbleibende Performance-Fähigkeit der physischen Objekte im Storage-System. Halten Sie den Mauszeiger über einen Punkt im Diagramm, um den Prozentsatz der noch verbleibenden IOPS- und MiB/s-Fähigkeit für Controller A und für Controller B anzuzeigen

Wo finde ich weitere Informationen zu Anzeigeeinstellungen?

So finden Sie Informationen zu den verfügbaren Anzeigeoptionen:

- Weitere Informationen zu den Standardeinheiten zum Anzeigen von Kapazitätswerten finden Sie unter "Standardeinheiten für Kapazitätswerte festlegen".
- Weitere Informationen zum Standardzeitrahmen zum Anzeigen von Performance-Diagrammen finden Sie unter "Legen Sie den Standardzeitrahmen für Performance-Diagramme fest".

Pools und Volume-Gruppen

Pools und Volume-Gruppen im Überblick

Sie können logische Speicherkapazität von einer Untermenge nicht zugewiesener Laufwerke in Ihrem Speicher-Array erstellen. Diese logische Kapazität kann je nach den Anforderungen Ihrer Umgebung in Form eines Pools oder einer Volume-Gruppe erfolgen.

Was sind Pools und Volume-Gruppen?

Ein *Pool* ist ein Satz von logisch gruppierten Laufwerken. Eine *Volume-Gruppe* ist ein Container für Volumes mit gemeinsam genutzten Merkmalen. Sie können entweder einen Pool oder eine Volume-Gruppe verwenden, um Volumes zu erstellen, auf die ein Host zugreifen kann.

Weitere Informationen:

- "Funktionsweise von Pools und Volume-Gruppen"
- "Terminologie der Kapazität"
- "Entscheiden Sie, ob ein Pool oder eine Volume-Gruppe verwendet werden soll"

Wie erstellen Sie Pools?

System Manager kann es erlauben, Pools automatisch zu erstellen, wenn sie nicht zugewiesene Kapazitäten in einem Speicher-Array erkennt. Wenn die automatische Erstellung die beste Konfiguration nicht bestimmen kann, können Sie Pools manuell aus dem Menü:Storage[Pools & Volume Groups] erstellen.

Weitere Informationen:

- "Automatische Erstellung von Pools gegenüber manueller Poolanlage"
- "Pool automatisch erstellen"
- "Pool manuell erstellen"
- "Hinzufügen von Kapazität zu einem Pool oder einer Volume-Gruppe"

Wie erstellen Sie Volume-Gruppen?

Sie können Volume-Gruppen aus dem Menü:Storage[Pools & Volume Groups] erstellen.

Weitere Informationen:

- "Erstellen einer Volume-Gruppe"
- "Hinzufügen von Kapazität zu einem Pool oder einer Volume-Gruppe"

Verwandte Informationen

Erfahren Sie mehr über Konzepte in Zusammenhang mit Pools und Volume-Gruppen:

- "Funktionsweise von reservierter Kapazität"
- "Funktionsweise von SSD Cache"

Konzepte

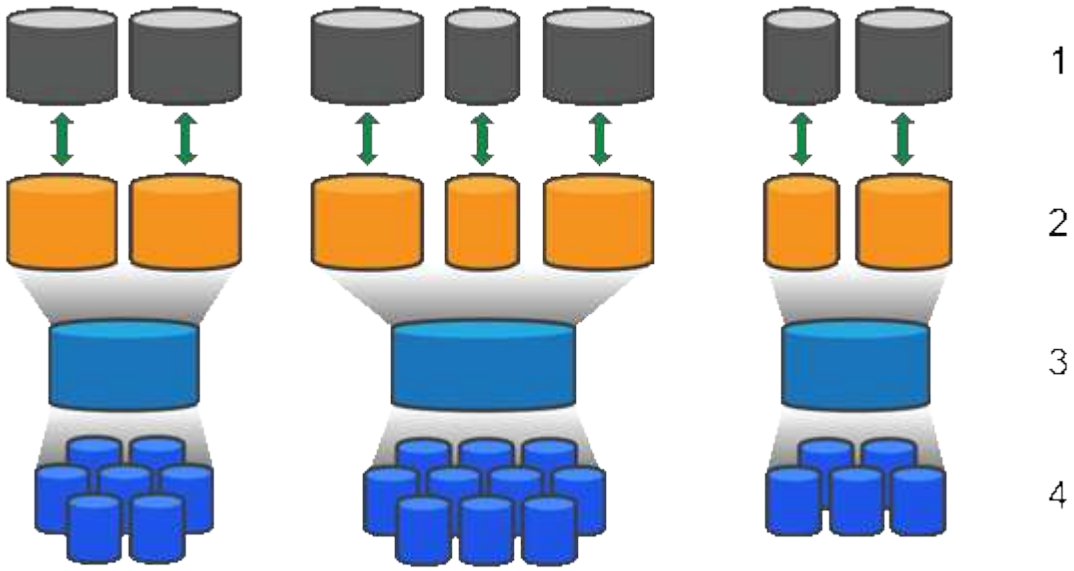
Funktionsweise von Pools und Volume-Gruppen

Um Speicher 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.

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

- Pools
- RAID-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. Dieses Konzept wird in der folgenden Abbildung dargestellt.



[1] Host-LUNs; [2] Volumes; [3] Volume-Gruppen oder Pools; [4] HDD- oder SSD-Laufwerke

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, verteilt System Manager die Daten dynamisch über alle aktiven Laufwerke hinweg.

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. System Manager legt den RAID-Level in einer Konfiguration mit 8+2 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, aber die Kapazität eines Laufwerks ist bei einem Laufwerksausfall für freie Kapazität 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 System Manager mit einer Anzahl von Laufwerken ausgedrückt, die eigentliche Implementierung wird jedoch über alle Laufwerke hinweg verteilt. Die vorbehaltenen Kapazitätsmengen basieren auf der Anzahl der Laufwerke im Pool.

Nach der Erstellung des Pools können Sie den Wert für die unveränderte Kapazität auf mehr oder weniger Kapazität ändern oder sogar auf keine Speicherkapazität einstellen (Wert von 0 Laufwerken). 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.

Terminologie der Kapazität

Erfahren Sie, welche Kapazitätbedingungen sich auf Ihr Storage Array beziehen.

Storage-Objekte

In der folgenden Terminologie werden die verschiedenen Typen von Speicherobjekten beschrieben, die mit Ihrem Speicher-Array interagieren können.

Storage Objekt	Beschreibung
Host	Ein Host ist ein Server, der I/O an ein Volume auf einem Storage-Array sendet.
LUN	Eine Logical Unit Number (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.
Spiegelung der Konsistenzgruppe	Eine gespiegelte Konsistenzgruppe ist ein Container für ein oder mehrere gespiegelte Paare. Für asynchrone Spiegelungsvorgänge müssen Sie eine Konsistenzgruppe erstellen.
Gespiegeltes Volume-Paar	Ein gespiegeltes Paar besteht aus zwei Volumes, einem primären Volume und einem sekundären Volume.
Pool	Ein Pool ist eine Reihe von Laufwerken, die logisch gruppiert sind. Mit einem Pool können Sie ein oder mehrere Volumes erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einem Pool oder einer Volume-Gruppe.)
Snapshot Konsistenzgruppe	Eine Snapshot Konsistenzgruppe ist eine Sammlung von Volumes, die beim Erstellen eines Snapshot Images als eine Einheit behandelt werden. Jedes dieser Volumes verfügt über ein eigenes Snapshot-Image, jedoch werden alle Bilder zum gleichen Zeitpunkt erstellt.

Storage Objekt	Beschreibung
Snapshot-Gruppe	Eine Snapshot-Gruppe ist eine Sammlung von Snapshot Images aus einem einzigen Basis-Volume.
Snapshot Volume	Ein Snapshot-Volume ermöglicht dem Host den Zugriff auf Daten im Snapshot Image. Das Snapshot Volume verfügt über eine eigene reservierte Kapazität, um alle Änderungen am Basis-Volume ohne Beeinträchtigung des ursprünglichen Snapshot Images zu speichern.
Datenmenge	Ein Volume ist ein Container, in dem Applikationen, Datenbanken und Filesysteme Daten speichern. Dies ist die logische Komponente, die erstellt wird, damit der Host auf den Speicher des Speicherarrays zugreifen kann.
Volume-Gruppe	Eine Volume-Gruppe ist ein Container für Volumes mit gemeinsamen Merkmalen. Eine Volume-Gruppe verfügt über eine definierte Kapazität und einen RAID-Level. Sie können eine Volume-Gruppe verwenden, um ein oder mehrere Volumes zu erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einer Volume-Gruppe oder aus einem Pool.)

Storage-Kapazität

In der folgenden Terminologie werden die verschiedenen Kapazitätstypen beschrieben, die auf Ihrem Storage Array verwendet werden.

Kapazitätstyp	Beschreibung
Zugewiesene Kapazität	Zugewiesene Kapazität ist die physische Kapazität, die den Laufwerken in einem Pool bzw. einer Volume-Gruppe zugewiesen ist. Die zugewiesene Kapazität wird zur Erstellung von Volumes und für Kopierdienste genutzt.
Freie Kapazität	Freie Kapazität ist die in einem Pool oder einer Volume-Gruppe verfügbare Kapazität, der der Volume-Erstellung noch nicht zugewiesen wurde.
Pool- oder Volume-Gruppen-Kapazität	Pool-, Volume- oder Volume-Gruppenkapazität ist die Kapazität in einem Speicher-Array, das einem Pool oder einer Volume-Gruppe zugewiesen wurde. Diese Kapazität wird verwendet, um Volumes zu erstellen und die verschiedenen Kapazitätsanforderungen von Services-Vorgängen und Storage-Objekten zu warten.
Pool – nicht nutzbare Kapazität	Die nicht nutzbare Kapazität im Pool ist der Speicherplatz in einem Pool, der aufgrund von nicht übereinstimmenden Laufwerksgrößen nicht verwendet werden kann.
Erhaltungskapazität	Bei der Konservierung wird die Kapazität (Anzahl der Laufwerke) verwendet, die in einem Pool reserviert ist, um potenzielle Laufwerksausfälle zu unterstützen.

Kapazitätstyp	Beschreibung
Gemeldete Kapazität	Die gemeldete Kapazität ist die Kapazität, die dem Host gemeldet wird und vom Host abgerufen werden kann.
Reservierte Kapazität	Reservierte Kapazität ist die zugewiesene physische Kapazität, die für jeden Kopierdienst- und Storage-Objekt verwendet wird. Er ist nicht direkt vom Host lesbar.
SSD Cache	SSD Cache ist eine Gruppe von Solid-State Disk (SSD)-Laufwerken, die Sie logisch in Ihrem Storage-Array zusammenfassen. Die SSD Cache Funktion speichert die am häufigsten verwendeten Daten („heiße“ Daten) im Cache auf SSD-Laufwerken mit niedrigerer Latenz und beschleunigt dadurch Applikations-Workloads dynamisch.
Nicht zugewiesene Kapazität	Nicht zugewiesene Kapazität ist der Speicherplatz in einem Speicher-Array, dem ein Pool oder eine Volume-Gruppe **nicht** zugewiesen wurde.
Geschriebene Kapazität	Die geschriebene Kapazität ist die Menge an Kapazität, die aus der für Thin Volumes zugewiesenen reservierten Kapazität geschrieben wurde.

Entscheiden Sie, ob ein Pool oder eine Volume-Gruppe verwendet werden soll

Sie können Volumes entweder mit einem Pool oder einer Volume-Gruppe erstellen. Die beste Auswahl hängt in erster Linie von den wichtigsten Storage-Anforderungen wie dem erwarteten I/O-Workload, den Performance-Anforderungen und den Datensicherungsanforderungen ab.

Gründe für die Auswahl eines Pools oder einer Volume-Gruppe

Wählen Sie einen Pool

- Wenn Sie schnellere Laufwerk-Rebuilds und eine vereinfachte Storage-Administration benötigen, benötigen Sie Thin Volumes und/oder einen hochzufälligen Workload.
- Wenn Sie die Daten für jedes Volume zufällig über einen Satz von Laufwerken verteilen möchten, die diesen Pool bilden.

  Sie können den RAID-Level von Pools oder Volumes in den Pools nicht festlegen oder ändern. Pools verwenden RAID Level 6.

Wählen Sie eine Volume-Gruppe

- 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.

Funktionsunterschiede zwischen Pools und Volume-Gruppen

Die folgende Tabelle bietet einen Funktionsvergleich zwischen Volume-Gruppen und Pools.

Nutzung	Pool	Volume-Gruppe
Zufälliger Workload	Besser	Gut
Sequenzieller Workload	Gut	Besser
Laufwerks-Rebuild-Zeit	Schneller	Langsamer
Performance (optimaler Modus)	Gut: Am besten für kleine Blöcke, zufällige Workloads.	Gut: Ideal für große Blöcke, sequenzielle Workloads
Performance (Laufwerks-Rebuild-Modus)	Besser: In der Regel besser als RAID 6	Verschlechtert: Bis zu 40 % Leistungsrückgang
Mehrere Laufwerke ausfallen	Höhere Datensicherung: Schnellere, priorisierte Rebuilds	Weniger Datensicherung: Langsame Rebuilds, höheres Risiko von Datenverlust
Hinzufügen von Laufwerken	Schneller: Bei laufendem Betrieb in den Pool aufnehmen	Langsamer: Erfordert dynamische Kapazitätserweiterung
Thin Volumes-Unterstützung	Ja.	Nein
Unterstützung von Solid State Disk (SSD	Ja.	Ja.
Vereinfachte Administration	Ja: Keine Hot Spares oder RAID-Einstellungen zu konfigurieren	Nein: Wir müssen Hot Spares zuweisen, RAID konfigurieren
Abstimmbare Performance	Nein	Ja.

Funktionsvergleich der Pools und Volume-Gruppen

Die Funktion und der Zweck eines Pools und einer Volume-Gruppe sind gleich. Beide Objekte sind eine Gruppe von Laufwerken, die in einem Storage-Array logisch gruppiert sind und dazu verwendet werden, Volumes zu erstellen, auf die ein Host zugreifen kann.

Die folgende Tabelle hilft Ihnen bei der Entscheidung, ob ein Pool oder eine Volume-Gruppe Ihre Storage-Anforderungen am besten erfüllt.

Funktion	Pool	Volume-Gruppe
Unterschiedliche unterstützte RAID-Level	Nein Immer RAID 6 in System Manager.	Ja. RAID 0, 1, 10, 5 und 6 erhältlich.
Unterstützung von Thin Volumes	Ja.	Nein
Unterstützung von vollständiger Festplattenverschlüsselung (Full Disk Encryption, FDE)	Ja.	Ja.
Data Assurance (da) wird unterstützt	Ja.	Ja.
Schutz vor Shelf-Verlust unterstützt	Ja.	Ja.
Schubladenschutz unterstützt	Ja.	Ja.
Unterstützung für gemischte Laufwerksgeschwindigkeiten	Es wird empfohlen, das gleiche zu sein, aber nicht erforderlich. Langsamstes Laufwerk bestimmt die Geschwindigkeit für alle Laufwerke.	Es wird empfohlen, das gleiche zu sein, aber nicht erforderlich. Langsamstes Laufwerk bestimmt die Geschwindigkeit für alle Laufwerke.
Kapazität gemischter Laufwerke wird unterstützt	Es wird empfohlen, das gleiche zu sein, aber nicht erforderlich. Kleinstes Laufwerk bestimmt die Kapazität für alle Laufwerke.	Es wird empfohlen, das gleiche zu sein, aber nicht erforderlich. Kleinstes Laufwerk bestimmt die Kapazität für alle Laufwerke.
Mindestanzahl an Laufwerken	11	Hängt von der RAID-Ebene ab. RAID 0 benötigt 1. RAID 1 oder 10 benötigt 2 (erfordert eine gleichmäßige Zahl). RAID 5 Minimum ist 3. RAID 6 Minimum ist 5.
Maximale Anzahl an Laufwerken	Bis zur Obergrenze für das Storage-Array	RAID 1 und 10 bis zur maximalen Obergrenze für RAID 5- und 6-30-Laufwerke des Speicherarrays
Bei der Erstellung eines Volumes können einzelne Laufwerke ausgewählt werden	Nein	Ja.
Kann die Segmentgröße beim Erstellen eines Volumes festlegen	Ja. 128 KB unterstützt.	Ja.

Funktion	Pool	Volume-Gruppe
Bei der Erstellung eines Volumes können I/O-Merkmale festgelegt werden	Nein	Ja. Dateisystem, Datenbank, Multimedia und benutzerdefinierte Unterstützung.
Schutz vor Laufwerksausfällen	Nutzt die Konservierungskapazität auf jedem Laufwerk im Pool, um die Rekonstruktion zu beschleunigen.	Verwendet ein Hot-Spare-Laufwerk. Die Rekonstruktion wird durch den IOPS des Laufwerks begrenzt.
Warnung beim Erreichen der Kapazitätsgrenze	Ja. Kann eine Meldung festlegen, wenn die genutzte Kapazität einen Prozentsatz der maximalen Kapazität erreicht.	Nein
Migration zu einem anderen unterstützten Storage-Array	Nein Erfordert, dass Sie zuerst zu einer Volume-Gruppe migrieren.	Ja.
Dynamische Segmentgröße (DSS)	Nein	Ja.
Der RAID-Level kann geändert werden	Nein	Ja.
Volume-Erweiterung (zusätzliche Kapazität)	Ja.	Ja.
Kapazitätserweiterung (zusätzliche Kapazität)	Ja.	Ja.
Senkung der Kapazität	Ja.	Nein

Gemischte Laufwerkstypen (HDD, SSD) werden weder für Pools noch für Volume-Gruppen unterstützt.

Automatische Erstellung von Pools gegenüber manueller Poolanlage

Sie erstellen Pools automatisch oder manuell, um eine Gruppierung des physischen Speichers zu ermöglichen und dann dynamisch nach Bedarf zuweisen zu können. Wenn ein Pool erstellt wird, können Sie physische Laufwerke hinzufügen.

Automatische Erstellung

Die automatische Poolerstellung wird initiiert, wenn der System Manager nicht zugewiesene Kapazitäten in einem Speicher-Array erkennt. Wenn nicht zugewiesene Kapazität erkannt wird, fordert System Manager Sie automatisch auf, 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.
- Ein Speicher-Array mit mindestens einem Pool wird mit neuen Laufwerken erweitert.

Jedes Laufwerk in einem Pool muss vom gleichen Laufwerkstyp (HDD oder SSD) sein und eine ähnliche Kapazität haben. Sie werden von System Manager 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.
- Mindestens einer der aktuellen Poolkandidaten kann den Schutz vor Regalverlust oder Schubladenverlust nicht aufrechterhalten.

Möglicherweise möchten Sie auch einen Pool manuell erstellen, wenn Sie mehrere Anwendungen auf Ihrem Speicher-Array haben und nicht möchten, dass sie mit den gleichen 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.

Speicher konfigurieren

Pool automatisch erstellen

Die Poolerstellung wird automatisch gestartet, wenn SANtricity System Manager nicht zugewiesene Laufwerke im Speicher-Array erkennt. Mithilfe der automatischen Pool-Erstellung können alle nicht zugewiesenen Laufwerke im Speicher-Array in einem Pool konfiguriert und Laufwerke zu vorhandenen Pools hinzugefügt werden.

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

Beachten Sie Folgendes:

- Wenn Sie einem Speicher-Array Laufwerke hinzufügen, erkennt System Manager automatisch die Laufwerke und fordert Sie auf, basierend auf dem Laufwerkstyp und der aktuellen Konfiguration einen einzelnen Pool oder mehrere Pools zu erstellen.
- Wenn bereits Pools definiert wurden, fordert Sie System Manager automatisch auf, die kompatiblen Laufwerke einem vorhandenen Pool hinzuzufügen. Wenn zu einem vorhandenen Pool neue Laufwerke hinzugefügt werden, verteilt System Manager 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.

Sie können das Dialogfeld „automatische Konfiguration des Pools“ mit einer der folgenden Methoden starten:

- Wenn nicht zugewiesene Kapazität erkannt wird, wird die Empfehlung für die automatische Konfiguration des Pools auf der Startseite im Bereich Benachrichtigungen angezeigt. Klicken Sie auf **Pool automatisch konfigurieren**, um das Dialogfeld zu starten.
- Sie können das Dialogfeld Automatische Konfiguration des Pools auch auf der Seite Pools und Volume Groups starten, wie in der folgenden Aufgabe beschrieben.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. 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.

   System Manager führt die folgenden Aufgaben aus:

   - 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.
3. Um den Namen eines neuen Pools zu ändern, klicken Sie auf das Symbol **Bearbeiten** (der Stift).
4. 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.

5. Klicken Sie Auf **Akzeptieren**.

Pool manuell erstellen

Sie können einen Pool manuell (aus einer Reihe von Kandidaten) erstellen, wenn die Funktion „Pool Auto Configuration“ keinen Pool bietet, der Ihren Anforderungen entspricht.

Ein Pool bietet die logische Storage-Kapazität, mit der Sie individuelle Volumes erstellen können, die dann zum Hosten Ihrer Applikationen genutzt werden können.

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. Derzeit ermöglicht System Manager die Laufwerkauswahl unter der Funktion Erweitert, wenn eine Volume-Gruppe erstellt wird. Für die Erstellung von Pools wird empfohlen, alle Laufwerke im Speicher-Array zu verwenden.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Klicken Sie auf Menü:Create[Pool].

   Das Dialogfeld Pool erstellen wird angezeigt.

3. Geben Sie einen Namen für den Pool ein.
4. **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.

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

Charakteristisch	Nutzung
Freie Kapazität	Zeigt die freie Kapazität des Poolkandidaten in gib an. Wählen Sie einen Pool-Kandidaten mit der Kapazität für die Storage-Anforderungen Ihrer Applikation 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. System Manager behält automatisch so viele Laufwerke wie möglich zur Erhaltung von Kapazität bei (für alle sechs Laufwerke eines Pools behält der System Manager ein Laufwerk zur Erhaltung der Kapazität vor). 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, dass 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 oder nicht sicher sind oder eine Kombination aus Sicherheitsstufen aufweisen. Wenn die Laufwerke im Pool Laufwerke enthalten, die nicht sicher sind, können Sie den Pool nicht sichern.

Charakteristisch	Nutzung
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.
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. DA ist aktiviert, wenn alle Laufwerke für da-fähig sind. DA kann nach der Erstellung des Volumes durch Auswahl des Menüs:Speicher[Volumes > Einstellungen anzeigen/bearbeiten > Erweitert > Data Assurance dauerhaft deaktivieren] deaktiviert werden. Wenn das da auf einem Volume deaktiviert ist, kann es nicht erneut aktiviert werden.
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 einer Volume-Gruppe

Sie erstellen mithilfe einer Volume-Gruppe ein oder mehrere Volumes, auf die der Host zugreifen kann. Eine Volume-Gruppe ist ein Container für Volumes mit gemeinsam

genutzten Merkmalen wie RAID-Level und Kapazität.

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.

Bevor Sie beginnen

Überprüfen Sie diese Richtlinien, bevor Sie eine Volume-Gruppe erstellen:

- Sie benötigen mindestens ein nicht zugewiesenes Laufwerk.
- Für die Anzahl der Laufwerke, über die Sie in einer einzelnen Volume-Gruppe verfügen können, gibt es Einschränkungen. Diese Einschränkungen variieren je nach RAID-Level.
- 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 über ein EF600- oder EF300-Storage-Array verfügen und Sie eine Volume-Gruppe manuell erstellen möchten, 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. Derzeit ermöglicht System Manager 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.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Klicken Sie auf Menü:Erstellen[Volume Group].

   Das Dialogfeld Volume-Gruppe erstellen wird angezeigt.

3. Geben Sie einen Namen für die Volume-Gruppe ein.
4. 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.

5. **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.

6. **Optional:** Sie können entweder die automatische oder die manuelle Methode wählen, um festzulegen, welche Laufwerke in der Volume-Gruppe verwendet werden sollen. Die automatische Methode ist die

Standardauswahl.

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.

Die manuelle Methode sollte nur von Experten verwendet werden, die die Laufwerkredundanz und die optimale Laufwerkskonfiguration verstehen.

7. 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.

Antriebseigenschaften der automatischen Methode

Charakteristisch	Nutzung
Freie Kapazität	Zeigt die verfügbare Kapazität in gib an. Wählen Sie einen Kandidaten für eine Volume-Gruppe mit der Kapazität für die Storage-Anforderungen Ihrer Applikation aus.
Laufwerke Insgesamt	Zeigt die Anzahl der für diese Volume-Gruppe verfügbaren Laufwerke an. Wählen Sie einen Kandidaten für eine Volume-Gruppe mit der Anzahl der gewünschten Laufwerke aus.
Laufwerksblockgröße (nur EF300 und EF600)	Zeigt die Blockgröße (Sektorgröße) an, die die Laufwerke in der Gruppe schreiben können. Die Werte können Folgendes umfassen: • 512 — 512-Byte-Sektorgröße. • 4K – 4,096 Byte Sektorgröße.
Sicher	Zeigt an, ob dieser Kandidat für diese Volume-Gruppe 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 Ihre Volume-Gruppe mit Drive Security schützen, aber alle Laufwerke müssen sicher für diese Funktion geeignet sein. • Wenn Sie eine nur-FDE-Volume-Gruppe erstellen möchten, suchen Sie in der Spalte Secure-fähiger nach **Ja - FDE**. Wenn Sie eine nur-FIPS-Gruppe 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 die Volume-Gruppe dann auf einer niedrigeren Sicherheitsstufe arbeitet (140-2). • Sie können eine Volume-Gruppe aus Laufwerken erstellen, die möglicherweise sicher sind oder nicht, aber eine Kombination aus Sicherheitsstufen bieten. Wenn die Laufwerke in der Volume-Gruppe Laufwerke enthalten, die nicht sicher sind, können Sie die Volume-Gruppe nicht sichern.
Sicherheit Aktivieren?	Bietet die Möglichkeit, die Sicherheitsfunktion des Laufwerks mit sicheren Laufwerken zu aktivieren. Wenn die Volume-Gruppe sicher ist und Sie einen Sicherheitsschlüssel eingerichtet haben, können Sie die Laufwerksicherheit aktivieren, indem Sie das Kontrollkästchen aktivieren. ⓘ Die einzige Möglichkeit, die Laufwerksicherheit zu entfernen, nachdem sie aktiviert ist, ist, die Volume-Gruppe zu löschen und die Laufwerke zu löschen.

Charakteristisch	Nutzung
DA-fähig	Gibt an, ob Data Assurance (da) für diese Gruppe 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 eine Volume-Gruppe aus, die für das da-fähig ist. (Bei da-fähigen Laufwerken wird da automatisch auf im Pool erstellten Volumes aktiviert.) Eine Volume-Gruppe kann Laufwerke enthalten, die für da-fähig sind oder nicht für da-fähig sind, aber alle Laufwerke müssen für die Verwendung dieser Funktion als da-fähig sein.
Resource Provisioning-fähig (nur EF300 und EF600)	Zeigt an, ob Ressourcen-Provisioning für diese Gruppe 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. Shelf-Schutz garantiert den Zugriff auf die Daten auf den Volumes in einer Volume-Gruppe, wenn ein vollständiger Verlust der Kommunikation zu einem 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 Schubladenverlust garantiert den Zugriff auf die Daten auf den Volumes in einer Volume-Gruppe, wenn 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 in der Gruppe erstellt werden können: • 512 n — 512 Bytes nativ. • 512 e — 512 Bytes emuliert. • 4K — 4,096 Byte.

Eigenschaften des Antriebs mit manueller Methode

Charakteristisch	Nutzung
Medientyp	Gibt den Medientyp an. Folgende Medientypen werden unterstützt: • Festplatte • Solid State-Festplatte (SSD) Alle Laufwerke in einer Volume-Gruppe müssen vom gleichen Medientyp (entweder alle SSDs oder alle Festplatten) sein. Volume-Gruppen können keine Mischung aus Medientypen oder Schnittstellentypen haben.
Laufwerksblockgröße (nur EF300 und EF600)	Zeigt die Blockgröße (Sektorgröße) an, die die Laufwerke in der Gruppe schreiben können. Die Werte können Folgendes umfassen: • 512 — 512-Byte-Sektorgröße. • 4K – 4,096 Byte Sektorgröße.
Laufwerkskapazität	Zeigt die Laufwerkskapazität an. • Wählen Sie nach Möglichkeit Laufwerke aus, die eine Kapazität haben, die den Kapazitäten der aktuellen Laufwerke in 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 in der Volume-Gruppe befindet, reduziert wird. Daher ist die Laufwerkskapazität für die gesamte Volume-Gruppe gleich. • Wenn nicht zugewiesene Laufwerke mit höherer Kapazität hinzugefügt werden müssen, müssen Sie beachten, dass die nutzbare Kapazität der hinzufügenden nicht zugewiesenen Laufwerke reduziert wird, damit sie den aktuellen Kapazitäten der Laufwerke in der Volume-Gruppe entsprechen.
Fach	Zeigt die Position des Fachs des Laufwerks an.
Schlitz	Zeigt die Position des Laufwerksteckplatzes an.
Drehzahl (U/min)	Zeigt die Geschwindigkeit des Laufwerks an.
Größe des logischen Sektors	Gibt die Größe und das Format des Sektors an.

Charakteristisch	Nutzung
Sicher	Zeigt an, ob dieser Kandidat für diese Volume-Gruppe 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 Ihre Volume-Gruppe mit Drive Security schützen, aber alle Laufwerke müssen sicher für diese Funktion geeignet sein. • Wenn Sie eine nur-FDE-Volume-Gruppe erstellen möchten, suchen Sie in der Spalte Secure-fähiger nach **Ja - FDE**. Wenn Sie eine nur-FIPS-Gruppe 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 die Volume-Gruppe dann auf einer niedrigeren Sicherheitsstufe arbeitet (140-2). • Sie können eine Volume-Gruppe aus Laufwerken erstellen, die möglicherweise sicher sind oder nicht, aber eine Kombination aus Sicherheitsstufen bieten. Wenn die Laufwerke in der Volume-Gruppe Laufwerke enthalten, die nicht sicher sind, können Sie die Volume-Gruppe nicht sichern.
DA-fähig	Gibt an, ob Data Assurance (da) für diese Gruppe verfügbar ist. Data Assurance (da) überprüft und korrigiert Fehler, die auftreten können, wenn Daten über die Controller bis zu den Laufwerken übermittelt werden. Wenn Sie da verwenden möchten, wählen Sie eine Volume-Gruppe aus, die für das da-fähig ist. (Bei da-fähigen Laufwerken wird da automatisch auf im Pool erstellten Volumes aktiviert.) Eine Volume-Gruppe kann Laufwerke enthalten, die für da-fähig sind oder nicht für da-fähig sind, aber alle Laufwerke müssen für die Verwendung dieser Funktion als da-fähig sein.
Unterstützte Volume-Block-Größen (nur EF300 und EF600)	Zeigt die Blockgrößen an, die für die Volumes in der Gruppe erstellt werden können: • 512 n — 512 Bytes nativ. • 512 e — 512 Bytes emuliert. • 4K — 4,096 Byte.
Resource Provisioning-fähig (nur EF300 und EF600)	Zeigt an, ob Ressourcen-Provisioning für diese Gruppe 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.

Hinzufügen von Kapazität zu einem Pool oder einer Volume-Gruppe

Sie können Laufwerke hinzufügen, um die freie Kapazität in einem vorhandenen Pool

oder einer vorhandenen Volume-Gruppe zu erweitern.

Mit der Erweiterung wird zusätzliche freie Kapazität in den Pool bzw. die Volume-Gruppe integriert. Sie können diese freie Kapazität nutzen, um zusätzliche Volumes zu erstellen. Der Zugriff auf die Daten in den Volumes bleibt während dieses Vorgangs erhalten.

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.
- 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 (E4000 und E2800 Serie)
- 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

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 Storage-Systems.)

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 Menü:Speicher[Pools & Volume Groups].
2. 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.

3. 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. • Um den Pool oder die Volume-Gruppe mit der Drive Security-Funktion zu schützen, müssen alle Laufwerke sicher sein. • 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. • Als sichere Laufwerke werden entweder vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) gemeldet. • 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.

4. 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:

   - Regalschutz *
   - Schubladenschutz *
   - Vollständige Festplattenverschlüsselung
   - Data Assurance
   - DULBE-Fähigkeit

   * derzeit wird das Bestätigungsdialogfeld nicht angezeigt, wenn Laufwerke zu einem Pool mit Schutz vor Regalverlust oder Schubladenverlust hinzugefügt werden.

1. Klicken Sie zum Fortfahren auf **Ja**, oder klicken Sie auf **Abbrechen**.

Ergebnisse

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.

Storage-Management

Volume-Redundanz prüfen

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.

> 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 Menü:Speicher[Pools & Volume Groups].
2. Menü wählen:Sonstige Aufgaben[Volumenredundanz prüfen].

   Das Dialogfeld Redundanz prüfen wird angezeigt.

3. Wählen Sie die Volumes aus, die Sie prüfen möchten, und geben Sie dann ein `check` Um zu bestätigen, dass Sie diesen Vorgang ausführen möchten.
4. 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.

Mehr zum Status der Redundanzprüfung

Status	Beschreibung
Ausstehend	Dies ist das erste zu scannende Volume, und Sie haben nicht auf Start geklickt, um die Redundanzprüfung zu starten. Oder Der Vorgang der Redundanzprüfung wird auf anderen Volumes im Pool bzw. 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.

5. Klicken Sie auf **Fertig**, nachdem das letzte Volume im Pool oder der Volume-Gruppe überprüft wurde.

Pool oder Volume-Gruppe löschen

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 Menü:Speicher[Pools & Volume Groups].
2. 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.

3. Wählen Sie Menü:Sonstige Aufgaben[Löschen] und bestätigen Sie.

Ergebnisse

System Manager 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.

Konsolidieren Sie freie Kapazitäten für eine Volume-Gruppe

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 „freie Kapazität konsolidieren“ 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 Menü:Speicher[Pools & Volume Groups].
2. 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.

3. Typ `consolidate` Um zu bestätigen, dass Sie diesen Vorgang ausführen möchten.
4. Klicken Sie Auf **Konsolidieren**.

   System Manager beginnt die Konsolidierung (Defragmentierung) der freien Kapazitätsbereiche der Volume-Gruppe in einen zusammenhängenden Betrag für nachfolgende Storage-Konfigurationsaufgaben.

Nachdem Sie fertig sind

Wählen Sie MENU:Home[Vorgänge in Bearbeitung anzeigen], um den Fortschritt des Vorgangs „Freie Kapazität konsolidieren“ anzuzeigen. Dieser Vorgang kann langwierig sein und die System-Performance beeinträchtigen.

Volume-Gruppen exportieren/importieren

Bei der Volume-Gruppenmigration können Sie eine Volume-Gruppe exportieren, sodass Sie die Volume-Gruppe in ein anderes Storage-Array importieren können.

Die Export-/Importfunktion wird in der Benutzeroberfläche von SANtricity System Manager nicht unterstützt. Sie müssen die Befehlszeilenschnittstelle (CLI) verwenden, um eine Volume-Gruppe in ein anderes Storage-Array zu exportieren/zu importieren.

Aktivieren Sie Locator Lights in einem Pool, einer Volume-Gruppe oder einem SSD-Cache

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 Menü:Speicher[Pools & Volume Groups].
2. 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.

3. Nachdem Sie die Laufwerke erfolgreich gefunden haben, klicken Sie auf **Ausschalten**.

Entfernen Sie die Kapazität aus einem Pool oder SSD-Cache

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. Die entfernten Laufwerke werden nicht mehr 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.

Hier erhalten Sie Informationen zu potenziellen Auswirkungen auf die Performance

- 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.

Lesen Sie, welche Auswirkungen sichere Laufwerke haben

- 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 Menü:Speicher[Pools & Volume Groups].
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 **Gesamtkapazität ausgewählt** 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.

   Die neu reduzierte Kapazität des Pool oder SSD-Cache wird in der Ansicht Pools und Volume-Gruppen dargestellt.

Ändern Sie die Pool- und Gruppeneinstellungen

Ändern Sie die Konfigurationseinstellungen für einen Pool

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 die RAID-Ebene eines Pools nicht mit der System Manager Schnittstelle ändern. System Manager konfiguriert Pools automatisch als RAID 6.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Wählen Sie den Pool aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld Pool-Einstellungen wird angezeigt.

3. 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 System Manager eine Meldung, 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.

4. Klicken Sie Auf **Speichern**.

Ändern Sie die Konfigurationseinstellungen für eine Volume-Gruppe

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 Menü:Speicher[Pools & Volume Groups].
2. 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.

3. 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 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 nicht zugewiesene Kapazität aus der freien Kapazität einer Gruppe (nicht von Volumes genutzte Kapazität) und einem Teil der nutzbaren Kapazität, der neben der zusätzlichen Optimierungskapazität 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.

4. 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**.

Ergebnisse

Wenn Sie das RAID-Level für eine Volume-Gruppe ändern, ändert System Manager die RAID-Level jedes Volumes, das die Volume-Gruppe enthält. Die Leistung kann während des Betriebs leicht beeinträchtigt werden.

Aktivieren oder deaktivieren Sie die Ressourcenbereitstellung in vorhandenen Volume-Gruppen und -Pools

Für alle DELBE-fähigen Laufwerke können Sie die Ressourcenbereitstellung auf vorhandenen Volumes in einem Pool oder einer Volume-Gruppe aktivieren oder deaktivieren.

Die Ressourcenbereitstellung ist eine Funktion der EF300- und EF600-Speicher-Arrays, mit der Volumes ohne Hintergrundinitialisierung sofort in Betrieb genommen werden können. Alle dem Volume zugewiesenen Festplattenblöcke werden aufgehoben (ihre Zuordnung wird nicht aufgehoben), was die SSD-Abnutzung verbessert und die maximale Schreib-Performance erhöht.

Standardmäßig ist die Ressourcenbereitstellung auf Systemen aktiviert, auf denen die Laufwerke DULBE unterstützen. Die Ressourcenbereitstellung muss erst aktiviert werden, wenn Sie sie zuvor deaktiviert haben.

Bevor Sie beginnen

- Sie benötigen ein EF300- oder EF600-Storage-Array.

DULBE wird derzeit nicht auf EF300C- oder EF600C-Speicherarrays unterstützt.

- Sie müssen SSD-Volume-Gruppen oder -Pools haben, wobei alle Laufwerke die Funktion zur Wiederherstellung von dezugewiesenen oder nicht geschriebenen logischen Blockfehlern (DULBE) unterstützen. Andernfalls ist die Option zur Ressourcenbereitstellung nicht verfügbar.

Über diese Aufgabe

Wenn Sie die Ressourcenbereitstellung für vorhandene Volume-Gruppen und -Pools aktivieren, werden alle Volumes in der ausgewählten Volume-Gruppe oder dem ausgewählten Pool geändert, damit die Blöcke wieder entzugewiesen werden können. Dieser Prozess kann einen Hintergrundvorgang erfordern, um eine konsistente Zuweisung auf der Granularität zu gewährleisten. Dieser Vorgang zeigt die Zuordnung von Speicherplatz nicht an. Sobald der Hintergrundvorgang abgeschlossen ist, muss das Betriebssystem die Zuordnung ungenutzter Blöcke aufheben, um freien Speicherplatz zu erstellen.

Wenn Sie die Ressourcenbereitstellung für vorhandene Volume-Gruppen oder Pools deaktivieren, schreibt ein Hintergrundvorgang alle logischen Blöcke in jedem Volume neu. Die bestehenden Daten bleiben erhalten. Die Schreibvorgänge zuordnen oder stellen die Blöcke auf den Laufwerken bereit, die der Volume-Gruppe oder dem Pool zugeordnet sind.

Für neue Volume-Gruppen und -Pools können Sie die Ressourcenbereitstellung über Menü:Einstellungen[System > zusätzliche Einstellungen > Aktivieren/Deaktivieren von Volumes mit Ressourcenbereitstellung] aktivieren oder deaktivieren.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. 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.

3. Wählen Sie **Sonstige Aufgaben** und dann entweder **Ressourcenbereitstellung aktivieren** oder **Ressourcenbereitstellung deaktivieren**.
4. Bestätigen Sie im Dialogfeld den Vorgang.

Wenn Sie DULBE erneut aktiviert haben — nach Abschluss des Hintergrundvorgangs müssen Sie möglicherweise den Host neu starten, damit die DULBE-Konfigurationsänderungen erkannt und anschließend alle Dateisysteme neu mounten.

Aktivieren oder Deaktivieren der Ressourcenbereitstellung für neue Volume-Gruppen oder -Pools

Wenn Sie zuvor die Standardfunktion für die Ressourcenbereitstellung deaktiviert haben, können Sie sie für alle neuen von Ihnen erstellten SSD-Volume-Gruppen oder -Pools erneut aktivieren. Sie können die Einstellung auch wieder deaktivieren.

Die Ressourcenbereitstellung ist eine Funktion der EF300- und EF600-Speicher-Arrays, mit der Volumes ohne Hintergrundinitialisierung sofort in Betrieb genommen werden können. Alle dem Volume zugewiesenen Festplattenblöcke werden aufgehoben (ihre Zuordnung wird nicht aufgehoben), was die SSD-Abnutzung verbessert und die maximale Schreib-Performance erhöht.

Standardmäßig ist die Ressourcenbereitstellung auf Systemen aktiviert, auf denen die Laufwerke DULBE unterstützen.

Bevor Sie beginnen

- Sie benötigen ein EF300- oder EF600-Storage-Array.
- Sie müssen SSD-Volume-Gruppen oder -Pools haben, wobei alle Laufwerke die Funktion zur Wiederherstellung von dezugewiesenen oder nicht geschriebenen logischen Blockfehlern (DULBE) unterstützen.

DULBE wird derzeit nicht auf EF300C- oder EF600C-Speicherarrays unterstützt.

Über diese Aufgabe

Wenn Sie die Ressourcen-Bereitstellung für neue Volume-Gruppen oder Pools erneut aktivieren, sind nur neu erstellte Volume-Gruppen und Pools betroffen. Alle vorhandenen Volume-Gruppen und Pools mit aktivierter Ressourcenbereitstellung bleiben unverändert.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Blättern Sie nach unten zu **zusätzliche Einstellungen**, und klicken Sie dann auf **Volumes mit Ressourcenzulauf aktivieren/deaktivieren**.

   Die Einstellungsbeschreibung gibt an, ob die Ressourcenbereitstellung derzeit aktiviert oder deaktiviert ist.
3. Bestätigen Sie im Dialogfeld den Vorgang.

Ergebnisse

Das Aktivieren oder Deaktivieren der Ressourcenbereitstellung betrifft nur neue SSD-Pools oder Volume-Gruppen, die Sie erstellen. Vorhandene Pools oder Volume-Gruppen bleiben unverändert.

Aktivieren Sie die Sicherheit für einen Pool oder eine Volume-Gruppe

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 Menü:Speicher[Pools & Volume Groups].
2. 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.

3. Bestätigen Sie, dass Sie die Sicherheit für den ausgewählten Pool oder die ausgewählte Volume-Gruppe aktivieren möchten, und klicken Sie dann auf **Aktivieren**.

Management des SSD-Caches

Funktionsweise von SSD Cache

Die SSD Cache Funktion ist eine Controller-basierte Lösung, die am häufigsten abgerufene Daten („heiße“ Daten) auf latenzarmen Solid State Drives (SSDs) zwischenspeichert und so die System-Performance dynamisch steigert. SSD Cache wird ausschließlich für Host-Lesevorgänge verwendet.

SSD Cache im Vergleich zum primären Cache

SSD Cache ist ein sekundärer Cache zur Verwendung mit dem primären Cache im dynamischen Random-Access Memory (DRAM) des Controllers.

SSD Cache funktioniert anders als der primäre Cache:

- Im primären Cache muss jeder I/O-Vorgang Daten durch den Cache stacieren, um den Vorgang durchzuführen.

  Im primären Cache werden die Daten nach dem Lesen des Hosts im DRAM gespeichert.

- SSD-Cache wird nur verwendet, wenn es von Vorteil ist, die Daten im Cache zu platzieren, um die Systemperformance insgesamt zu verbessern.

  Im SSD Cache werden die Daten aus Volumes kopiert und auf zwei internen RAID-Volumes (eine pro Controller) gespeichert, die bei der Erstellung eines SSD-Caches automatisch erstellt werden.

Die internen RAID-Volumes werden für die interne Cache-Verarbeitung verwendet. Auf diese Volumes kann nicht zugegriffen oder in der Benutzeroberfläche angezeigt werden. Diese beiden Volumes zählen jedoch die Gesamtanzahl der im Storage Array zulässigen Volumes.

Verwendung von SSD Cache

Mit der intelligenten Cache-Speicherung werden Daten auf einem Laufwerk mit niedrigerer Latenz platziert. So kann schneller auf zukünftige Anfragen nach diesen Daten reagiert werden. Wenn ein Programm Daten anfordert, die sich im Cache befinden (so genannte „`Cache Hit`“), kann diese Transaktion auf der Festplatte mit niedrigerer Latenz verarbeitet werden. Andernfalls tritt ein „`Cache Miss`“ auf, und auf die Daten muss vom ursprünglichen, langsameren Laufwerk zugegriffen werden. Je mehr Cache-Treffer auftreten, desto besser wird die Gesamt-Performance.

Wenn ein Hostprogramm auf die Laufwerke des Storage-Arrays zugreift, werden die Daten im SSD-Cache gespeichert. Wenn das Hostprogramm wieder auf dieselben Daten zugreift, wird es anstelle der Festplatten aus dem SSD-Cache gelesen. Die am häufigsten abgerufenen Daten werden im SSD-Cache gespeichert. Auf

die Festplatten wird nur zugegriffen, wenn die Daten nicht aus dem SSD-Cache gelesen werden können.

SSD Cache wird nur verwendet, wenn es von Vorteil ist, die Daten im Cache zu platzieren, um die Gesamt-Performance des Systems zu verbessern.

Wenn die CPU Lesedaten verarbeiten muss, führt dies wie folgt aus:

1. Überprüfen Sie den DRAM-Cache.
2. Wenn sie nicht im DRAM-Cache gefunden werden, überprüfen Sie den SSD-Cache.
3. Wenn nicht im SSD Cache gefunden, dann von der Festplatte. Wenn Daten für den Cache sinnvoll sind, sollten Sie diese in den SSD Cache kopieren.

Verbesserte Performance

Das Kopieren der am häufigsten aufgerufenen Daten (Hot Spot) in SSD Cache ermöglicht einen effizienteren Festplattenbetrieb, geringere Latenz und eine beschleunigte Lese- und Schreibgeschwindigkeit. Mithilfe hochperformanter SSDs können Daten von HDD-Volumes zwischengespeichert werden, was die I/O-Performance und die Reaktionszeiten verbessert.

Über einfache Volume-I/O-Mechanismen werden Daten in den und aus dem SSD-Cache verschoben. Nachdem Daten im Cache gespeichert und auf den SSDs gespeichert wurden, werden nachfolgende Lesezugriffe auf diese Daten im SSD Cache ausgeführt. Auf das HDD-Volume ist somit kein Zugriff mehr erforderlich.

SSD-Cache und die Laufwerkssicherheitsfunktion

Wenn Sie SSD Cache auf einem Volume verwenden möchten, das auch die Laufwerkssicherheit verwendet (ist sicher aktiviert), müssen die Laufwerksicherheitsfunktionen des Volumes und des SSD-Caches übereinstimmen. Stimmen sie nicht überein, wird das Volume nicht sicher aktiviert.

Implementierung von SSD-Cache

Gehen Sie zum Implementieren von SSD-Cache wie folgt vor:

1. Erstellen Sie den SSD-Cache.
2. Verbinden Sie den SSD-Cache mit den Volumes, für die Sie SSD-Lese-Caching implementieren möchten.

> Jedes Volume, das der Nutzung des SSD-Caches eines Controllers zugewiesen ist, kann keine automatische Lastverteilung durchführen.

Einschränkungen für SSD-Cache

Erfahren Sie mehr über die Einschränkungen bei der Verwendung von SSD Cache in Ihrem Storage Array.

Einschränkungen

- Jedes Volume, das der Nutzung des SSD-Caches eines Controllers zugewiesen ist, kann keine automatische Lastverteilung durchführen.
- Derzeit wird pro Storage-Array nur ein SSD-Cache unterstützt.
- Die maximale nutzbare SSD-Cache-Kapazität auf einem Speicher-Array beträgt 10 TB.

- 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.
- Sie können das letzte Laufwerk in einem SSD-Cache nicht entfernen, ohne zuerst den SSD-Cache zu löschen.

Einschränkungen bei Laufwerkssicherheit

- Sie können die Sicherheit im SSD-Cache nur aktivieren, wenn Sie den SSD-Cache erstellen. Sie können die Sicherheit später nicht wie möglich auf einem Volume aktivieren.
- Wenn Sie Laufwerke kombinieren, die sicher mit Laufwerken verbunden sind, die in SSD Cache nicht sicher-fähig sind, können Sie die Laufwerksicherheit für diese Laufwerke nicht aktivieren.
- Für sichere Volumes muss ein sicherer SSD-Cache aktiviert sein.

Erstellen Sie SSD-Cache

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.

Über diese Aufgabe

Wenn Sie einen neuen SSD-Cache erstellen, können Sie ein einzelnes Laufwerk 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.

Befolgen Sie diese Richtlinien, wenn Sie einen neuen SSD-Cache erstellen.

- 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.
- Wenn nur auf einem Volume der SSD-Cache aktiviert ist, wird der gesamte SSD-Cache dem Controller zugewiesen, der dieses Volume besitzt.
- Die maximale nutzbare SSD-Cache-Kapazität auf einem Storage-Array hängt von der Kapazität des primären Caches 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 Menü:Speicher[Pools & Volume Groups].

2. Klicken Sie auf Menü:Create[SSD Cache].

   Das Dialogfeld SSD-Cache erstellen wird angezeigt.

3. Geben Sie einen Namen für den SSD-Cache ein.
4. Wählen Sie den Kandidaten für den SSD-Cache aus, den Sie basierend auf folgenden Merkmalen verwenden möchten.

Charakteristisch	Nutzung
Kapazität	Zeigt die verfügbare Kapazität in gib an. Wählen Sie die Kapazität für die Storage-Anforderungen Ihrer Applikation 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 SSD-Cache erstellen möchten, suchen Sie in der Spalte Secure-Enabled nach **Yes - FDE** oder **Yes - 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. Nach der Aktivierung 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.

5. 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.

6. Klicken Sie Auf **Erstellen**.

Ändern Sie die SSD-Cache-Einstellungen

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.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. 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.

3. 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** — zeigt 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.

4. Klicken Sie Auf **Speichern**.

Anzeigen von SSD-Cache-Statistiken

Sie können Statistiken für den SSD-Cache anzeigen, z. B. Lese-, Schreib-, Cache-Treffer, Cache-Zuweisung in Prozent, Und Cache-Auslastung in Prozent.

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 zu A exportieren `.csv` Datei:

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 Menü:Speicher[Pools & Volume Groups].
2. Wählen Sie den SSD-Cache aus, für den Sie Statistiken anzeigen möchten, und klicken Sie dann auf Menü:Mehr[View SSD Cache Statistics].

   Das Dialogfeld SSD-Cache-Statistiken anzeigen wird angezeigt und zeigt die nominalen Statistiken für den ausgewählten SSD-Cache an.

Felddetails

Einstellungen	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).

3. Klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen.

Management reservierter Kapazitäten

Funktionsweise von reservierter Kapazität

Reservierte Kapazität wird automatisch erstellt, wenn Kopierservice-Vorgänge wie Snapshots oder asynchrone Spiegelungsvorgänge für Ihre Volumes bereitgestellt werden.

Der Zweck der reservierten Kapazität besteht darin, Datenänderungen auf diesen Volumes zu speichern, sollte etwas schief gehen. Wie Volumes wird auch reservierte Kapazität aus Pools oder Volume-Gruppen erstellt.

Kopieren Sie Serviceobjekte mit reservierter Kapazität

Die reservierte Kapazität ist der zugrunde liegende Storage-Mechanismus, der von diesen Service-Objekten

der Kopie verwendet wird:

- Snapshot Gruppen
- Lese-/Schreib-Snapshot-Volumes
- Volumes für Mitglieder der Konsistenzgruppe
- Gespiegelte Paar-Volumes

Wenn Sie diese Servicepobjekte erstellen oder erweitern, müssen Sie neue reservierte Kapazität entweder aus einem Pool oder einer Volume-Gruppe erstellen. Die reservierte Kapazität beträgt normalerweise 40 % des Basis-Volumes für Snapshot-Vorgänge und 20 % des Basis-Volumes für asynchrone Spiegelungsvorgänge. Die reservierte Kapazität kann jedoch je nach Anzahl der Änderungen an den ursprünglichen Daten variieren.

Thin Volumes und reservierte Kapazität

Wenn bei einem Thin-Volume die maximale gemeldete Kapazität von 256 tib erreicht ist, können Sie seine Kapazität nicht erhöhen. Stellen Sie sicher, dass die reservierte Kapazität des Thin-Volumes auf eine Größe gesetzt ist, die größer als die maximale gemeldete Kapazität ist. (Ein Thin Volume wird immer über Thin Provisioning bereitgestellt. Das bedeutet, dass die Kapazität beim Schreiben der Daten auf das Volume zugewiesen wird.)

Wenn Sie reservierte Kapazität mit einem Thin-Volume in einem Pool erstellen, überprüfen Sie die folgenden Aktionen und Ergebnisse mit der reservierten Kapazität:

- Wenn die reservierte Kapazität eines Thin Volume ausfällt, wechselt das Thin Volume selbst nicht automatisch in den Status „Fehlgeschlagen“. Da jedoch alle I/O-Vorgänge auf einem Thin Volume Zugriff auf das reservierte Kapazitäts-Volume erfordern, werden I/O-Vorgänge immer dazu führen, dass eine Check Condition an den anfordernden Host zurückgegeben wird. Kann das zugrunde liegende Problem mit dem reservierten Kapazitäts-Volume gelöst werden, wird das reservierte Kapazitäts-Volume wieder in einen optimalen Zustand zurückversetzt und das Thin Volume wird wieder in Funktion.
- Wenn Sie ein vorhandenes Thin Volume zum Abschließen eines asynchronen gespiegelten Paares verwenden, wird dieses Thin Volume mit einem neuen reservierten Kapazitäts-Volume neu initialisiert. Bei der ersten Synchronisierung werden nur bereitgestellte Blöcke auf der primären Seite übertragen.

Kapazitätswarnungen

Das Copy-Service-Objekt verfügt über eine konfigurierbare Kapazitätswarnung und Alarmschwelle sowie eine konfigurierbare Antwort, wenn die reservierte Kapazität voll ist.

Wenn sich die reservierte Kapazität eines Volume eines Copy-Service-Objekts dem Füllpunkt nähert, wird dem Benutzer eine Warnmeldung ausgegeben. Standardmäßig wird diese Warnmeldung ausgegeben, wenn das reservierte Kapazitäts-Volume zu 75 % voll ist. Sie können diesen Warnhinweis jedoch nach Bedarf vertikal oder abwärts anpassen. Wenn diese Meldung erhalten wird, können Sie die Kapazität des reservierten Kapazitätsvolumes zu diesem Zeitpunkt erhöhen. Jedes Copy-Service-Objekt kann hier unabhängig konfiguriert werden.

Verwaiste reservierte Kapazitäts-Volumes

Ein verwaiste kapazitätsstarkes Volume ist ein Volume, das keine Daten mehr für Kopierservicevorgänge speichert, da das zugehörige Copy-Service-Objekt gelöscht wurde. Sobald das Copy-Service-Objekt gelöscht wurde, sollte auch das reservierte Kapazitäts-Volume gelöscht werden. Das reservierte Kapazitäts-Volume konnte jedoch nicht gelöscht werden.

Da auf verwaiste reservierte Kapazitäts-Volumes kein Host zugegriffen wird, sind sie Kandidaten für eine

Rückgewinnung. Löschen Sie das verwaiste Volumes mit reservierter Kapazität manuell, sodass Sie dessen Kapazität für andere Vorgänge nutzen können.

System Manager benachrichtigt Sie über verwaiste Kapazitäts-Volumes mit einer Meldung „nicht genutzte Kapazität neu erstellen“ im Bereich „Benachrichtigungen“ auf der Startseite. Sie können auf **ungenutzte Kapazität zurückgewinnen** klicken, um das Dialogfeld „ungenutzte Kapazität neu zuweisen“ anzuzeigen, in dem Sie das verwaiste Volumen der reservierten Kapazität löschen können.

Merkmale der reservierten Kapazität

- Für die reservierte Kapazität muss während der Volume-Erstellung berücksichtigt werden, um ausreichend freie Kapazität zur Verfügung zu haben.
- Die reservierte Kapazität kann kleiner sein als das Basis-Volume (die minimale Größe beträgt 8 MiB).
- Einige Kapazität wird durch Metadaten verbraucht, aber es ist sehr wenig (192 KiB), somit muss man sie nicht bei der Bestimmung der Größe des reservierten Kapazitäts-Volume berücksichtigen.
- Die reservierte Kapazität kann nicht direkt von einem Host gelesen oder geschrieben werden.
- Für jedes Snapshot Volume mit Lese-/Schreibvorgängen, für jede Snapshot Gruppe, für ein Volume für Mitglied der Konsistenzgruppe und für ein gespiegeltes Paar-Volume ist reservierte Kapazität vorhanden.

Reservierte Kapazität wird erhöht

Sie können die reservierte Kapazität erhöhen, die die physisch zugewiesene Kapazität, die für jeden Kopiervorgang auf einem Storage-Objekt genutzt wird.

Bei Snapshot-Vorgängen beträgt dieser Anteil normalerweise 40 % des Basis-Volumes. Bei asynchronen Spiegelungsvorgängen beträgt der Anteil des Basis-Volumes normalerweise 20 %. Normalerweise erhöhen Sie die reservierte Kapazität, wenn Sie eine Warnung erhalten, dass die reservierte Kapazität des Storage-Objekts voll wird.

Bevor Sie beginnen

- Das Volume im Pool oder in der Volume-Gruppe muss den optimalen Status aufweisen und darf sich nicht in einem bestimmten Zustand befinden.
- Freie Kapazität muss im Pool bzw. in der Volume-Gruppe vorhanden sein, mit der die Kapazität erhöht werden soll.

  Wenn auf einem Pool oder Volume-Gruppen keine freie Kapazität vorhanden ist, können Sie einem Pool oder einer Volume-Gruppe nicht zugewiesene Kapazität in Form nicht verwendeter Laufwerke hinzufügen.

Über diese Aufgabe

Sie können die reservierte Kapazität nur in Schritten von 8 gib für die folgenden Storage-Objekte erhöhen:

- Snapshot-Gruppe
- Snapshot Volume
- Mitgliedsvolume der Konsistenzgruppe
- Gespiegeltes Paar-Volume

Verwenden Sie einen hohen Prozentsatz, wenn Sie glauben, dass das primäre Volume viele Änderungen durchlaufen hat oder wenn die Lebensdauer eines bestimmten Kopierdienstes sehr lang ist.

Sie können die reservierte Kapazität für ein schreibgeschütztes Snapshot-Volume nicht erhöhen. Nur Snapshot Volumes mit Lese- und Schreibvorgängen erfordern reservierte Kapazität.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Wählen Sie die Registerkarte **reservierte Kapazität** aus.
3. Wählen Sie das Speicherobjekt aus, für das Sie die reservierte Kapazität erhöhen möchten, und klicken Sie dann auf **Kapazität erhöhen**.

   Das Dialogfeld reservierte Kapazität erhöhen wird angezeigt.

4. Verwenden Sie die Spinner-Box, um den Kapazitätsanteil einzustellen.

   Wenn im Pool oder in der Volume-Gruppe keine freie Kapazität vorhanden ist, die das ausgewählte Speicherobjekt enthält, und das Speicher-Array über nicht zugewiesene Kapazität verfügt, können Sie einen neuen Pool oder eine neue Volume-Gruppe erstellen. Sie können diesen Vorgang dann mit der neuen freien Kapazität in diesem Pool bzw. dieser Volume-Gruppe wiederholen.

5. Klicken Sie Auf **Erhöhen**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Erhöht die reservierte Kapazität für das Storage-Objekt.
- Zeigt die neu hinzugefügte reservierte Kapazität an.

Reservierte Kapazität verringern

Mit der Option Kapazität verkleinern Sie die reservierte Kapazität für die folgenden Speicherobjekte: snapshot-Gruppe, Snapshot-Volume und Mitglied-Volume der Konsistenzgruppe. Die reservierte Kapazität kann nur um den/die Menge(en) verringert werden, den Sie zur Steigerung verwendet haben.

Bevor Sie beginnen

- Das Storage-Objekt muss mehr als ein reserviertes Kapazitäts-Volume enthalten.
- Das Storage-Objekt darf kein gespiegeltes Paar-Volume sein.
- Wenn es sich bei dem Speicherobjekt um ein Snapshot-Volume handelt, muss es ein deaktiviertes Snapshot-Volume sein.
- Wenn es sich bei dem Speicherobjekt um eine Snapshot-Gruppe handelt, darf es keine zugehörigen Snapshot-Images enthalten.

Über diese Aufgabe

Lesen Sie sich die folgenden Richtlinien durch:

- Sie können reservierte Kapazitäts-Volumes nur in der umgekehrten Reihenfolge entfernen, in der sie hinzugefügt wurden.
- Sie können die reservierte Kapazität für ein schreibgeschütztes Snapshot-Volume nicht verringern, da ihm keine zugewiesene Kapazität zur Verfügung steht. Nur Snapshot Volumes mit Lese- und

Schreibvorgängen erfordern reservierte Kapazität.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Klicken Sie auf die Registerkarte **reservierte Kapazität**.
3. Wählen Sie das Speicherobjekt aus, für das die reservierte Kapazität verringert werden soll, und klicken Sie dann auf **Kapazität verringern**.

   Das Dialogfeld reservierte Kapazität verringern wird angezeigt.

4. Wählen Sie den Kapazitätsbetrag aus, um den die reservierte Kapazität verringert werden soll, und klicken Sie dann auf **verringern**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Aktualisiert die Kapazität für das Storage-Objekt.
- Zeigt die neu aktualisierte reservierte Kapazität für das Speicherobjekt an.
- Wenn Sie die Kapazität eines Snapshot-Volume verringern, überträgt System Manager das Snapshot-Volume automatisch in einen deaktivierten Zustand. Deaktiviert bedeutet, dass das Snapshot-Volume derzeit nicht mit einem Snapshot-Image verknüpft ist und daher nicht einem Host für I/O zugewiesen werden kann

Ändern Sie die Einstellungen für die reservierte Kapazität einer Snapshot-Gruppe

Sie können die Einstellungen für eine Snapshot-Gruppe so ändern, dass ihr Name, die Einstellungen für das automatische Löschen, die maximale Anzahl zulässiger Snapshot-Images, der Prozentpunkt, an dem SANtricity System Manager eine Warnmeldung über reservierte Kapazität sendet, oder die Richtlinie, die verwendet wird, wenn die reservierte Kapazität ihren maximal definierten Prozentsatz erreicht.

Während der Erstellung einer Snapshot-Gruppe wird reservierte Kapazität erstellt, um die Daten aller Snapshot-Images der Gruppe zu speichern.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Klicken Sie auf die Registerkarte **reservierte Kapazität**.
3. Wählen Sie die Snapshot-Gruppe aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld Einstellungen für Snapshot-Gruppen wird angezeigt.

4. Ändern Sie ggf. die Einstellungen für die Snapshot-Gruppe.

Felddetails

Einstellung	Beschreibung
Snapshot-Gruppeneinstellungen	Name
Der Name der Snapshot-Gruppe. Die Angabe eines Namens für die Snapshot-Gruppe ist erforderlich.	Automatisches Löschen
Eine Einstellung, bei der die Gesamtanzahl der Snapshot-Bilder in der Gruppe auf einem benutzerdefinierten Maximum oder unter einem festgelegten Wert liegt. Wenn diese Option aktiviert ist, löscht der System Manager bei jeder Erstellung eines neuen Snapshots automatisch das älteste Snapshot-Image in der Gruppe, um der maximalen Anzahl von Snapshot-Images, die für die Gruppe zulässig sind, entsprechen zu können.	Begrenzung des Snapshot Images
Ein konfigurierbarer Wert, der die maximale Anzahl von Snapshot-Images angibt, die für eine Snapshot-Gruppe zulässig sind.	Snapshot Zeitplan
Wenn ja, wird ein Zeitplan für die automatische Erstellung von Snapshots festgelegt.	**Reservierte Kapazitätseinstellungen**

Einstellung	Beschreibung
Benachrichtigen, wenn…	Verwenden Sie das Spinner-Feld, um den Prozentpunkt anzupassen, an dem System Manager eine Warnmeldung sendet, wenn sich die reservierte Kapazität einer Snapshot-Gruppe fast voll befindet. Wenn die reservierte Kapazität der Snapshot-Gruppe den angegebenen Schwellenwert überschreitet, sendet System Manager eine Warnmeldung, sodass Sie die reservierte Kapazität erhöhen oder unnötige Objekte löschen können.
Richtlinie für vollständig reservierte Kapazität	Sie können eine der folgenden Richtlinien auswählen: • **Ältestes Snapshot-Image löschen** — System Manager entfernt automatisch das älteste Snapshot-Image in der Snapshot-Gruppe, welches die reservierte Kapazität des Snapshot-Images zur Wiederverwendung innerhalb der Gruppe freigibt. • **Schreibvorgänge auf Basis-Volume ablehnen** — Wenn die reservierte Kapazität ihren maximalen festgelegten Prozentsatz erreicht, weist der System Manager alle I/O-Schreibanfragen auf das Basis-Volume zurück, das den reservierten Kapazitätszugriff ausgelöst hat.
Assoziierte Objekte	Basis-Volume
Der Name des Basis-Volumes, das für die Gruppe verwendet wird. Ein Basis-Volume ist die Quelle, aus der ein Snapshot Image erstellt wird. Es kann sich um ein Thick- oder Thin-Volume handeln, das in der Regel einem Host zugewiesen ist. Das Basis-Volume kann entweder in einer Volume-Gruppe oder im Laufwerk-Pool gespeichert werden.	Snapshot Images

5. Klicken Sie auf **Speichern**, um Ihre Änderungen auf die Einstellungen der Snapshot-Gruppe anzuwenden.

Ändern Sie die Einstellungen für die reservierte Kapazität eines Snapshot-Volumes

Sie können die Einstellungen für ein Snapshot-Volume ändern, um den Prozentpunkt anzupassen, an dem das System eine Benachrichtigung sendet, wenn die reservierte Kapazität eines Snapshot-Volumes sich der vollen Größe nähert.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Klicken Sie auf die Registerkarte **reservierte Kapazität**.
3. Wählen Sie das Snapshot-Volumen aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld Einstellungen für die reservierte Kapazität des Snapshot-Volumes wird angezeigt.

4. Ändern Sie die Einstellungen für die reservierte Kapazität des Snapshot-Volumes je nach Bedarf.

   Felddetails

Einstellung	Beschreibung
Benachrichtigen, wenn…	Verwenden Sie die Spinner-Box, um den Prozentpunkt anzupassen, an dem das System eine Benachrichtigung sendet, wenn sich die reservierte Kapazität für ein Mitgliedsvolumen fast voll befindet. Wenn die reservierte Kapazität für das Snapshot-Volume den angegebenen Schwellenwert überschreitet, sendet das System eine Warnmeldung, sodass Sie die reservierte Kapazität erhöhen oder unnötige Objekte löschen können.

5. Klicken Sie auf **Speichern**, um Ihre Änderungen auf die Einstellungen für die reservierte Kapazität des Snapshot-Volumes anzuwenden.

Ändern Sie die Einstellungen für die reservierte Kapazität eines Mitglieds der Konsistenzgruppe

Sie können die Einstellungen für ein Mitglied-Volume einer Konsistenzgruppe ändern, um den Prozentpunkt anzupassen, an dem SANtricity System Manager eine Benachrichtigung sendet, wenn die reservierte Kapazität eines Mitglieds-Volumes nahezu voll ist, und um die Richtlinie zu ändern, die verwendet wird, wenn die reservierte Kapazität den maximal definierten Prozentsatz erreicht.

Über diese Aufgabe

Durch Ändern der Einstellungen für die reservierte Kapazität eines einzelnen Member Volumes werden auch die reservierten Kapazitätseinstellungen für alle Mitglied-Volumes geändert, die einer Konsistenzgruppe zugeordnet sind.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Klicken Sie auf die Registerkarte **reservierte Kapazität**.
3. Wählen Sie das Mitgliedsvolume der Konsistenzgruppe aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld Einstellungen für die reservierte Kapazität des Mitgliedvolumes wird angezeigt.

4. Ändern Sie die Einstellungen für die reservierte Kapazität des Mitgliedvolume nach Bedarf.

Felddetails

Einstellung	Beschreibung
Benachrichtigen, wenn…	Verwenden Sie die Spinner-Box, um den Prozentpunkt anzupassen, an dem System Manager eine Benachrichtigung sendet, wenn die reservierte Kapazität für ein Mitglied-Volume sich fast voll befindet. Wenn die reservierte Kapazität für das Mitglied-Volume den angegebenen Schwellenwert überschreitet, sendet System Manager eine Warnmeldung, sodass Sie die reservierte Kapazität erhöhen oder unnötige Objekte löschen können. Wenn Sie die Alarmeinstellung für ein Mitgliedsvolume ändern, wird sie für alle_ Mitgliedvolumes geändert, die zur gleichen Konsistenzgruppe gehören.
Richtlinie für vollständig reservierte Kapazität	Sie können eine der folgenden Richtlinien auswählen: • **Ältestes Snapshot-Image löschen** — System Manager entfernt automatisch das älteste Snapshot-Image in der Consistency Group, das die reservierte Kapazität des Mitglieds zur Wiederverwendung innerhalb der Gruppe freigibt. • **Schreibvorgänge auf Basis-Volume ablehnen** — Wenn die reservierte Kapazität ihren maximalen festgelegten Prozentsatz erreicht, weist der System Manager alle I/O-Schreibanfragen auf das Basis-Volume zurück, das den reservierten Kapazitätszugriff ausgelöst hat.

5. Klicken Sie auf **Speichern**, um Ihre Änderungen anzuwenden.

Ergebnisse

System Manager ändert die Einstellungen für die reservierte Kapazität des Mitglieds-Volumes sowie die Einstellungen für die reservierte Kapazität aller Mitglied-Volumes in der Konsistenzgruppe.

Ändern Sie die Einstellungen für die reservierte Kapazität eines gespiegelten Paar-Volumes

Sie können die Einstellungen für ein Volume mit gespiegelten Paaren ändern, um den Prozentpunkt anzupassen, an dem SANtricity System Manager eine Warnmeldung sendet, wenn die reservierte Kapazität für ein Volume mit gespiegelten Paaren fast voll ist.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Wählen Sie die Registerkarte **reservierte Kapazität** aus.
3. Wählen Sie das zu bearbeitende gespiegelte Paar-Volume aus und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld Einstellungen für die reservierte Kapazität des gespiegelten Paar-Volumes wird angezeigt.

4. Ändern Sie gegebenenfalls die Einstellungen für die reservierte Kapazität des gespiegelten Paar-Volumes.

Felddetails

Einstellung	Beschreibung
Benachrichtigen, wenn…	Verwenden Sie das Spinner-Feld, um den Prozentpunkt anzupassen, an dem System Manager eine Benachrichtigung sendet, wenn die reservierte Kapazität eines gespiegelten Paares sich der vollen Kapazität nähert. Wenn die reservierte Kapazität für das gespiegelte Paar den angegebenen Schwellenwert überschreitet, sendet System Manager eine Warnmeldung, sodass Sie die reservierte Kapazität erweitern können. Durch Ändern der Alarmeinstellung für ein gespiegeltes Paar wird die Alarmeinstellung für alle gespiegelten Paare, die zur gleichen SpiegelungsConsistency Group gehören, geändert.

5. Klicken Sie auf **Speichern**, um Ihre Änderungen anzuwenden.

Abbrechen des ausstehenden Snapshot-Images

Sie können ein ausstehendes Snapshot-Image abbrechen, bevor es abgeschlossen wird. Snapshots werden asynchron ausgeführt und der Status des Snapshots steht bis zum Abschluss des Snapshots aus. Das Snapshot-Image wird abgeschlossen, sobald der Synchronisierungsvorgang abgeschlossen ist.

Über diese Aufgabe

Ein Snapshot-Image befindet sich aufgrund der folgenden gleichzeitigen Bedingungen im Status „Ausstehend“:

- Das Basis-Volume für eine Snapshot-Gruppe oder ein oder mehrere Mitglied-Volumes einer Konsistenzgruppe, die dieses Snapshot-Image enthält, ist Mitglied einer asynchronen Spiegelgruppe.
- Das Volume oder die Volumes befinden sich momentan in einer Synchronisierung mit asynchronem Spiegeln.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Klicken Sie auf die Registerkarte **reservierte Kapazität**.
3. Wählen Sie die Snapshot-Gruppe aus, für die Sie ein ausstehendes Snapshot-Image abbrechen möchten, und klicken Sie dann auf Menü:Sonstige Aufgaben[ausstehende Snapshot-Image abbrechen].
4. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie das ausstehende Snapshot-Image abbrechen möchten.

Snapshot-Gruppe löschen

Sie löschen eine Snapshot-Gruppe, wenn Sie ihre Daten dauerhaft löschen und aus dem System entfernen möchten. Durch das Löschen einer Snapshot-Gruppe wird die reservierte Kapazität zur Wiederverwendung im Pool oder der Volume-Gruppe wieder

beansprucht.

Über diese Aufgabe

Wenn eine Snapshot-Gruppe gelöscht wird, werden auch alle Snapshot-Images in der Gruppe gelöscht.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Klicken Sie auf die Registerkarte **reservierte Kapazität**.
3. Wählen Sie die Snapshot-Gruppe aus, die Sie löschen möchten, und klicken Sie dann auf Menü:Sonstige Aufgaben[Snapshot-Gruppe löschen].

   Das Dialogfeld Snapshot-Gruppe löschen bestätigen wird angezeigt.

4. Typ `delete` Zur Bestätigung.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Löscht alle Snapshot-Images, die der Snapshot-Gruppe zugeordnet sind.
- Deaktiviert alle Snapshot-Volumes, die mit den Bildern der Snapshot-Gruppe verknüpft sind.
- Löscht die reservierte Kapazität, die für die Snapshot-Gruppe vorhanden ist.

FAQs

Was ist eine Volume-Gruppe?

Eine Volume-Gruppe ist ein Container für Volumes mit gemeinsamen Merkmalen. Eine Volume-Gruppe verfügt über eine definierte Kapazität und einen RAID-Level. Sie können eine Volume-Gruppe verwenden, um ein oder mehrere Volumes zu erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einer Volume-Gruppe oder aus einem Pool.)

Was ist ein Pool?

Ein Pool ist eine Reihe von Laufwerken, die logisch gruppiert sind. Mit einem Pool können Sie ein oder mehrere Volumes erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einem Pool oder einer Volume-Gruppe.)

Pools können Administratoren die Auslastung jedes Hosts nicht mehr überwachen und feststellen, wann dieser nicht mehr genügend Speicherplatz hat, und vermeiden, dass herkömmliche Ausfälle aufgrund der Festplattengröße auftreten. Wenn ein Pool knapp wird, können ohne Unterbrechungen zusätzliche Laufwerke zum Pool hinzugefügt werden, und das Kapazitätswachstum ist für den Host transparent.

Mit Pools werden die Daten automatisch neu verteilt, um das Gleichgewicht aufrechtzuerhalten. Durch die Verteilung von Paritätsinformationen und freien Kapazitäten im gesamten Pool kann jedes Laufwerk im Pool zur Neuerstellung eines ausgefallenen Laufwerks verwendet werden. Bei diesem Ansatz werden keine dedizierten Hot Spare-Festplatten verwendet. Stattdessen wird im gesamten Pool die unveränderte (freie) Kapazität reserviert. Beim Laufwerksausfall werden Segmente auf anderen Laufwerken gelesen, um die Daten neu zu erstellen. Anschließend wird ein neues Laufwerk ausgewählt, um jedes Segment, das sich auf einem ausgefallenen Laufwerk befand, zu schreiben, damit die Datenverteilung auf verschiedenen Laufwerken

erhalten bleibt.

Was ist reservierte Kapazität?

Die reservierte Kapazität ist die physisch zugewiesene Kapazität, die Daten für Copy-Service-Objekte wie Snapshot Images, Volumes von Konsistenzgruppen und gespiegelte Paar-Volumes speichert.

Das Volume mit reservierter Kapazität, das einem Kopiervorgang zugeordnet ist, befindet sich in einem Pool oder einer Volume-Gruppe. Sie erstellen reservierte Kapazität entweder aus einem Pool oder einer Volume-Gruppe.

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 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.

Worin bestehen die Unterschiede zwischen Pools und Volume-Gruppen?

Ein Pool ähnelt einer Volume-Gruppe mit den folgenden Unterschieden.

- Die Daten in einem Pool werden zufällig auf allen Laufwerken im Pool gespeichert, im Gegensatz zu Daten in einer Volume-Gruppe, die auf demselben Satz an Laufwerken gespeichert werden.
- Wenn ein Laufwerk ausfällt, weist ein Pool weniger Performance-Einbußen auf und die Rekonstruktionszeit verkürzt sich.
- Ein Pool verfügt über integrierte Konservierungskapazität und benötigt daher keine dedizierten Hot-Spare-Festplatten.
- Ein Pool ermöglicht die Gruppierung einer großen Anzahl von Laufwerken.
- Ein Pool benötigt keine angegebene RAID-Stufe.

Warum sollte ich einen Pool manuell konfigurieren?

Die folgenden Beispiele beschreiben, warum Sie einen Pool manuell konfigurieren möchten.

- Wenn Ihr Storage-Array über mehrere Applikationen verfügt und Sie nicht möchten, dass dieselben Laufwerkressourcen miteinander konkurrieren, sollten Sie möglicherweise manuell einen kleineren Pool für eine oder mehrere Applikationen 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.

  Um einen Pool manuell zu erstellen, wählen Sie **Speicher** und dann **Pools & Volume Groups**. Klicken Sie auf der Registerkarte Alle Kapazitäten auf Menü:Create[Pool].

- Wenn mehrere Pools desselben Laufwerkstyps vorhanden sind, wird eine Meldung angezeigt, dass System Manager die Laufwerke nicht automatisch für einen Pool empfehlen kann. Sie können die Laufwerke jedoch manuell einem vorhandenen Pool hinzufügen.

  So fügen Sie manuell Laufwerke zu einem vorhandenen Pool hinzu: Wählen Sie auf der Seite Pools & Volume Groups den Pool aus und klicken Sie dann auf **Add Capacity**.

Warum sind Kapazitätswarnungen wichtig?

Kapazitätswarnungen geben an, wann Laufwerke zu einem Pool hinzugefügt werden sollen. Ein Pool benötigt ausreichend freie Kapazität, um Storage-Array-Vorgänge erfolgreich durchzuführen. Vermeiden Sie Unterbrechungen dieser Vorgänge, indem Sie SANtricity System Manager so konfigurieren, dass Warnmeldungen gesendet werden, wenn die freie Kapazität eines Pools einen bestimmten Prozentsatz erreicht oder überschreitet.

Sie legen diesen Prozentsatz fest, wenn Sie einen Pool mit der Option **Pool Auto-Configuration** oder mit der Option **Pool erstellen** erstellen. Wenn Sie die Option automatisch wählen, bestimmen die Standardeinstellungen automatisch, wann Sie Benachrichtigungen erhalten. Wenn Sie den Pool manuell erstellen möchten, können Sie die Benachrichtigungseinstellungen festlegen oder die Standardeinstellungen übernehmen. Sie können diese Einstellungen später im Menü:Einstellungen[Warnungen] anpassen.

Wenn die freie Kapazität im Pool den angegebenen Prozentsatz erreicht, wird eine Warnmeldung mit der Methode gesendet, die Sie in der Warnungskonfiguration angegeben haben.

Warum kann ich meine Erhaltungskapazität 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 Groups** 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.

Ist die Anzahl der Laufwerke, die ich aus einem Pool entfernen kann, begrenzt?

SANtricity System Manager legt Grenzwerte für die Anzahl der Laufwerke fest, die aus einem Pool entfernt werden können.

- Sie können die Anzahl der Laufwerke in einem Pool nicht auf weniger als 11 Laufwerke reduzieren.
- Laufwerke können nicht entfernt werden, wenn nicht genügend freie Kapazität im Pool vorhanden ist, um die Daten von den entfernten Laufwerken zu enthalten, wenn diese Daten auf die übrigen Laufwerke im Pool verteilt werden.
- Sie können maximal 60 Laufwerke gleichzeitig entfernen. Wenn Sie mehr als 60 Laufwerke auswählen, ist die Option Laufwerke entfernen deaktiviert. Wenn Sie mehr als 60 Laufwerke entfernen müssen, wiederholen Sie den Vorgang zum Entfernen von Laufwerken.

Welche Medientypen werden für ein Laufwerk unterstützt?

Die folgenden Medientypen werden unterstützt: Festplattenlaufwerk (HDD) und Solid State Disk (SSD).

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 jedoch kein da-fähiges Volume im Pool oder in der Volume-Gruppe vorhanden ist, 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.

Wie kann ich den Schutz vor Shelf-/Schubladenverlust aufrechterhalten?

Verwenden Sie die in der folgenden Tabelle aufgeführten Kriterien, um den Schutz vor Shelf-/Schubladenverlusten für einen Pool oder eine Volume-Gruppe zu erhalten.

Ebene	Kriterien für den Schutz vor Shelf-/Schubladenverlust	Mindestanzahl der benötigten Regale/Schubladen
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 Shelves 5 für Schubladen
RAID 6	Die Volume-Gruppe enthält nicht mehr als zwei Laufwerke in einem einzelnen Shelf oder einer einzelnen Schublade.	3
RAID 3 oder RAID 5	Jedes Laufwerk in der Volume-Gruppe befindet sich in einem separaten Shelf oder einer separaten Schublade.	3

Ebene	Kriterien für den Schutz vor Shelf-/Schubladenverlust	Mindestanzahl der benötigten Regale/Schubladen
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.

Wie sieht die optimale Laufwerkspositionierung von Pools und Volume-Gruppen aus?

Achten Sie beim Erstellen von Pools und Volume-Gruppen darauf, die Laufwerkauswahl zwischen den oberen und unteren Laufwerksschächten auszugleichen.

Bei den EF600- und EF300-Controllern werden die Laufwerksschächte 0-11 mit einer PCI-Bridge verbunden, die Steckplätze 12-23 sind mit einer anderen PCI-Bridge verbunden. Um eine optimale Leistung zu erzielen, sollten Sie die Laufwerksauswahl auf eine ungefähr gleiche Laufwerksanzahl von den oberen und unteren Steckplätzen ausbalancieren. Durch diese Positionierung wird sichergestellt, dass Ihre Volumen nicht früher als nötig auf ein Bandbreitenlimit treffen.

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, die sogenannten *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.
- **Wie es funktioniert**
  - 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.
- **Anforderungen an die Fahrnummer**
  - 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.
- **Anforderungen an die Fahrnummer**
  - 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.
- **Anforderungen an die Fahrnummer**
  - 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.
- **Anforderungen an die Fahrnummer**
  - 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.

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 mit der da-Fähigkeit ausgestattet ist (suchen Sie in der Tabelle „da“ neben „da“ und „Volume-Gruppen-Kandidaten“ nach „Ja“).

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 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.

Was muss ich über die Erhöhung der reservierten Kapazität wissen?

In der Regel sollten Sie die Kapazität erhöhen, wenn Sie die Warnung erhalten, dass die reservierte Kapazität in Gefahr ist, voll zu werden. Sie können die reservierte Kapazität nur in Schritten von 8 gib erhöhen.

- Sie müssen über ausreichende freie Kapazitäten im Pool oder Volume-Gruppe verfügen, damit diese bei Bedarf erweitert werden kann.

  Wenn auf einem Pool oder Volume-Gruppen keine freie Kapazität vorhanden ist, können Sie einem Pool oder einer Volume-Gruppe nicht zugewiesene Kapazität in Form nicht verwendeter Laufwerke hinzufügen.

- Das Volume im Pool oder in der Volume-Gruppe muss den optimalen Status aufweisen und darf sich nicht in einem bestimmten Zustand befinden.
- Freie Kapazität muss im Pool bzw. in der Volume-Gruppe vorhanden sein, mit der die Kapazität erhöht werden soll.

- Sie können die reservierte Kapazität für ein schreibgeschütztes Snapshot-Volume nicht erhöhen. Nur Snapshot Volumes mit Lese- und Schreibvorgängen erfordern reservierte Kapazität.

Für Snapshot-Vorgänge beträgt die reservierte Kapazität normalerweise 40 Prozent des Basis-Volumes. Bei asynchronen Spiegelungsvorgängen beträgt die reservierte Kapazität in der Regel 20 Prozent des Basis-Volumes. Verwenden Sie einen höheren Prozentsatz, wenn Sie glauben, dass das Basis-Volume viele Änderungen durchlaufen wird oder wenn die geschätzte Lebensdauer des Kopierservice eines Storage-Objekts sehr lang sein wird.

Warum kann ich nicht eine andere Menge wählen, um zu verringern?

Sie können die reservierte Kapazität nur um den Betrag reduzieren, den Sie zur Steigerung verwendet haben. Reservierte Kapazität für Mitglieder-Volumes kann nur in umgekehrter Reihenfolge entfernt werden, in der sie hinzugefügt wurden.

Sie können die reservierte Kapazität für ein Speicherobjekt nicht verringern, wenn eine der folgenden Bedingungen vorliegt:

- Wenn es sich bei dem Storage-Objekt um ein gespiegeltes Paar-Volume handelt.
- Wenn das Storage-Objekt nur ein Volume für die reservierte Kapazität enthält. Das Storage-Objekt muss mindestens zwei Volumes für die reservierte Kapazität enthalten.
- Wenn es sich bei dem Speicherobjekt um ein deaktiviertes Snapshot-Volume handelt.
- Wenn das Speicherobjekt mindestens ein Snapshot-Image enthält.

Sie können Volumes für die reservierte Kapazität nur in der umgekehrten Reihenfolge entfernen, in der sie hinzugefügt wurden.

Sie können die reservierte Kapazität für ein schreibgeschütztes Snapshot-Volume nicht verringern, da ihm keine zugewiesene Kapazität zur Verfügung steht. Nur Snapshot Volumes mit Lese- und Schreibvorgängen erfordern reservierte Kapazität.

Warum brauche ich reservierte Kapazität für jedes Member Volume?

Jedes Mitglied-Volume in einer Snapshot-Konsistenzgruppe muss über seine eigene reservierte Kapazität verfügen, um alle Änderungen, die von der Host-Applikation auf dem Basis-Volume vorgenommen wurden, ohne das referenzierte Snapshot-Image der Konsistenzgruppe zu beeinträchtigen. Die reservierte Kapazität ermöglicht der Host-Applikation den Schreibzugriff auf eine Kopie der Daten im Mitglied-Volume, die als Lese- und Schreibzugriff festgelegt ist.

Ein Snapshot-Image für Konsistenzgruppen ist nicht direkt für Hosts zugänglich. Vielmehr wird das Snapshot-Image verwendet, um nur die Daten zu speichern, die vom Basis-Volume erfasst wurden.

Während der Erstellung eines Snapshot Volume für die Konsistenzgruppe, das als Lesen/Schreiben bezeichnet wird, erstellt System Manager für jedes Mitglied-Volume in der Konsistenzgruppe eine reservierte Kapazität. Diese reservierte Kapazität ermöglicht der Host-Applikation den Schreibzugriff auf eine Kopie der Daten im Snapshot Image der Konsistenzgruppe.

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 zu A exportieren `.csv` Datei: 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, wählen Sie Menü:Speicher[Pools & Volume Groups]. 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.

Die folgende Liste enthält nominale Statistiken, die eine Untermenge der detaillierten Statistiken sind.

Nominale Statistik	Beschreibung
Lese-/Schreibvorgänge	Die Gesamtzahl der Host-Lesevorgänge von bzw. Host-Schreibvorgängen auf die SSD Cache-fähigen Volumes. Vergleichen Sie die Lesevorgänge relativ zu den Schreibvorgängen. Für einen effektiven SSD-Cache-Vorgang müssen die Schreibvorgänge größer sein als die Schreibvorgänge. Je mehr das Verhältnis von Lese- zu Schreibzugriffen ist, desto besser der Cache-Betrieb.
Cache-Treffer	Die Anzahl der Cache-Treffer.
Cache-Treffer (%)	Abgeleitet aus Cache-Hits / (Lese- + Schreibvorgänge). Der Cache-Trefferprozentsatz sollte im Hinblick auf einen effektiven SSD-Cache-Vorgang mehr als 50 Prozent betragen. Eine kleine Zahl könnte auf mehrere Dinge hinweisen: • Das Verhältnis von Lese- zu Schreibvorgängen ist zu klein • Lesezugriffe werden nicht wiederholt • Cache-Kapazität ist zu klein
Cache-Zuweisung (%)	Die zugewiesene SSD-Cache-Storage-Menge wird als Prozentsatz des SSD-Cache-Storage ausgedrückt, der für diesen Controller verfügbar ist. Abgeleitet von zugewiesenen Bytes/verfügbaren Bytes. Der Prozentsatz der Cache-Zuweisung wird normalerweise als 100 Prozent angezeigt. Wenn diese Zahl weniger als 100 % beträgt, bedeutet dies, dass entweder der Cache nicht aufgewärmt ist oder die SSD Cache Kapazität größer ist als alle Daten, auf die zugegriffen wird. Im zweiten Fall könnte eine kleinere SSD-Cache-Kapazität das gleiche Performance-Niveau bieten. Beachten Sie, dass dies nicht bedeutet, dass zwischengespeicherte Daten im SSD-Cache gespeichert wurden. Es ist lediglich ein Vorbereitungsschritt, bevor die Daten im SSD-Cache platziert werden können.

Nominale Statistik	Beschreibung
Cache-Auslastung (%)	Die Menge an SSD-Cache-Storage, die Daten von aktivierten Volumes enthält, ausgedrückt als Prozentsatz des zugewiesenen SSD-Cache-Storage. Dieser Wert stellt die Auslastung oder Dichte des SSD-Caches dar, der aus Benutzerdaten-Bytes/zugewiesenen Bytes abgeleitet wird. Die Cache-Auslastung ist in der Regel niedriger als 100 Prozent, vielleicht viel niedriger. Diese Zahl zeigt den Prozentsatz der SSD-Cache-Kapazität an, die mit Cache-Daten gefüllt ist. Diese Zahl ist niedriger als 100 %, da jede Zuweisungseinheit des SSD Cache, der SSD Cache-Block, in kleinere Einheiten unterteilt wird, die als Sub-Blöcke bezeichnet werden und die etwas unabhängig gefüllt werden. Eine höhere Zahl ist im Allgemeinen besser, aber die Leistungssteigerung kann auch bei einer kleineren Zahl signifikant sein.

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 auf A exportiert haben `.csv` Datei:

Beim Anzeigen des `.csv` Beachten Sie, dass die detaillierten Statistiken nach den Nominalstatistiken aufgelistet sind:

Detaillierte Statistiken	Beschreibung
Blöcke Werden Gelesen	Die Anzahl der Blöcke im Host-Lesezugriff.
Schreibblöcke	Die Anzahl der Blöcke im Host-Schreibvorgang.
Full-Hit-Blöcke	Die Anzahl der Blöcke im Cache-Treffer. Die vollständigen Hit-Blöcke geben an, wie viele Blöcke vollständig aus SSD Cache gelesen wurden. Der SSD-Cache bietet nur Vorteile für die Performance bei Vorgängen, die Vollcache-Treffer sind.
Teilweise Treffer	Die Anzahl der Host-Lesezugriffe, bei denen mindestens ein Block, aber nicht alle Blöcke, im SSD Cache waren. Ein partieller Hit ist ein SSD Cache **miss** wo die Reads vom Basis-Volume erfüllt wurden.
Teilweise Treffer - Blöcke	Die Anzahl der Blöcke in Teilbestrahungen. Teilweise Cache-Treffer und partielle Cache-Trefferblöcke resultieren aus einem Vorgang, der nur einen Teil seiner Daten im SSD Cache enthält. In diesem Fall muss der Vorgang die Daten aus dem zwischengespeicherten Festplattenlaufwerk (HDD) abrufen. Der SSD-Cache bietet für diese Art von Hit keine Performance-Vorteile. Wenn die Anzahl der teilweise Cachetreffer-Blöcke höher ist als die der Vollcache-Trefferblöcke, könnte ein anderer I/O-Merkmalstyp (Filesystem, Datenbank oder Web-Server) die Performance verbessern. Es wird erwartet, dass es im Vergleich zu Cache-Hits eine größere Anzahl von Teileinsätzen und -Auslassungen gibt, während sich der SSD Cache wärmt.

Detaillierte Statistiken	Beschreibung
Fehlschläge	Die Anzahl der Host-Lesevorgänge, wo sich keine der Blöcke im SSD Cache befanden. Ein Ausfall des SSD-Caches tritt auf, wenn die Lesevorgänge vom Basis-Volume zufrieden waren. Es wird erwartet, dass es im Vergleich zu Cache-Hits eine größere Anzahl von Teileinsätzen und -Auslassungen gibt, während sich der SSD Cache wärmt.
Fehlschläge - Blöcke	Die Anzahl der Blöcke in Fehlschläge.
Ausfüllen Von Aktionen (Host Reads)	Die Anzahl der Host-Lesevorgänge, auf denen Daten vom Basis-Volume in den SSD Cache kopiert wurden.
Füllen Sie Aktionen (Host-Lesevorgänge) - Blöcke	Die Anzahl der Blöcke in den Befüllen-Aktionen (Host-Lesevorgänge).
Ausfüllen Von Aktionen (Host-Schreibvorgänge)	Die Anzahl der Host-Schreibvorgänge, bei denen Daten vom Basis-Volume in den SSD-Cache kopiert wurden. Die Anzahl der Befüllen-Aktionen (Host-Schreibvorgänge) kann für die Cache-Konfigurationseinstellungen, die den Cache als Folge eines I/O-Vorgangs nicht füllen, Null sein.
Befüllen Von Aktionen (Host Writes) - Blöcken	Die Anzahl der Blöcke in den Befüllen-Aktionen (Host-Schreibvorgänge).
Aktionen Ungültig Machen	Die Anzahl der Mal, dass Daten im SSD-Cache ungültig oder entfernt wurden. Für jeden Host-Schreibanforderung, jede Host-Leseanforderung mit Forced Unit Access (FUA), jede Anforderung zur Überprüfung und unter anderen Umständen wird ein nicht validierter Cache-Vorgang durchgeführt.
Recyclingmaßnahmen	Die Anzahl der Zeiten, in denen der SSD Cache Block für ein anderes Basis-Volume und/oder einen anderen LBA-Bereich (Logical Block Addressing) wiederverwendet wurde. Für einen effektiven Cache-Betrieb muss die Anzahl der Recycles im Vergleich zur kombinierten Anzahl von Lese- und Schreibvorgängen gering sein. Wenn sich die Anzahl der Recycle-Aktionen nahe der kombinierten Anzahl von Lese- und Schreibvorgängen befindet, ist der SSD Cache begeistert. Entweder die Cache-Kapazität muss erhöht werden oder der Workload eignet sich nicht für den Einsatz mit SSD Cache.
Verfügbare Bytes	Die Anzahl der im SSD-Cache zur Verwendung durch diesen Controller verfügbaren Bytes.
Zugewiesene Bytes	Die Anzahl der Bytes, die diesem Controller aus dem SSD-Cache zugewiesen wurden. Aus dem SSD-Cache zugewiesene Bytes können leer sein oder Daten aus Basis-Volumes enthalten.
Benutzerdaten Bytes	Die Anzahl der zugewiesenen Bytes im SSD-Cache, die Daten von Basis-Volumes enthalten. Die verfügbaren Bytes, zugewiesenen Bytes und Benutzerdaten Bytes werden zur Berechnung des prozentualen Cache-Zuordnungsanteils und des Prozentsatzes der Cache-Auslastung verwendet.

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 der 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 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 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 Schieberegler „zusätzliche 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). Zusätzlich können Hosts logische Blöcke im Volume mithilfe des Befehls NVMe Dataset Management oder des Befehls SCSI Unmap ausfindig machen. 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.

DULBE wird derzeit nicht auf EF300C- oder EF600C-Speicherarrays unterstützt.

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.

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). Zusätzlich können Hosts logische Blöcke im Volume mithilfe des Befehls NVMe Dataset Management oder des Befehls SCSI Unmap ausfindig machen. 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.

Die Ressourcenbereitstellung ist standardmäßig auf Systemen aktiviert, auf denen die Laufwerke DULBE unterstützen. Sie können diese Standardeinstellung über **Pools & Volume Groups** deaktivieren.

DULBE wird derzeit nicht auf EF300C- oder EF600C-Speicherarrays unterstützt.

Volumes und Workloads

Volumes und Workloads – Überblick

Sie können ein Volume als Container erstellen, in dem Applikationen, Datenbanken und Filesysteme Daten speichern. Bei der Erstellung eines Volumes wählen Sie auch einen

Workload aus, um die Storage-Array-Konfiguration für eine bestimmte Applikation anzupassen.

Was sind Volumes und Workloads?

Ein *Volume* ist die logische Komponente, die mit spezifischer Kapazität erstellt wurde, auf die der Host zugreifen kann. Obwohl ein Volume aus mehr als einem Laufwerk bestehen kann, wird ein Volume als eine logische Komponente für den Host angezeigt. Sobald ein Volume definiert ist, können Sie es einem Workload hinzufügen. Ein *Workload* ist ein Storage-Objekt, das eine Applikation wie SQL Server oder Exchange unterstützt, mittels dessen Sie den Storage für die jeweilige Applikation optimieren können.

Weitere Informationen:

- "Wie Volumen funktionieren"
- "Funktionsweise von Workloads"
- "Volume-Terminologie"
- "Zuweisung von Kapazität für Volumes"
- "Aktionen, die Sie auf Volumes durchführen können"

Wie erstellen Sie Volumes und Workloads?

Zunächst erstellen Sie einen Workload. Gehen Sie zu **Storage › Volumes** und öffnen Sie einen Assistenten, der Sie durch die Schritte führt. Als Nächstes erstellen Sie ein Volume anhand der Kapazität, die in einem Pool oder einer Volume-Gruppe verfügbar ist, und weisen dann den erstellten Workload zu.

Weitere Informationen:

- "Workflow für die Erstellung von Volumes"
- "Workloads erstellen"
- "Volumes erstellen"
- "Hinzufügen von Volumes zum Workload"

Verwandte Informationen

Erfahren Sie mehr über Konzepte in Bezug auf Volumes:

- "Datenintegrität und Datensicherheit für Volumes"
- "SSD Cache und Volumes"
- "Thin Volume-Monitoring"

Konzepte

Wie Volumen funktionieren

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

Sie erstellen Volumes aus der auf Ihrem Storage Array verfügbaren Storage-Kapazität und erleichtern die Organisation und Nutzung der Systemressourcen. Dieses Konzept ähnelt der Verwendung von

Ordnern/Verzeichnissen auf einem Computer, um Dateien für einen einfachen und schnellen Zugriff zu organisieren.

Volumes sind die einzige Datenebene, die Hosts sichtbar ist. In einer SAN-Umgebung werden Volumes den LUNs (Logical Unit Numbers) zugeordnet, die für Hosts sichtbar sind. 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.

Volume-Typen, die Sie aus Pools und Volume-Gruppen erstellen können, können erstellt werden

Volumes ziehen ihre Kapazität aus Pools oder Volume-Gruppen. Sie können die folgenden Volume-Typen aus den Pools oder Volume-Gruppen auf Ihrem Storage Array erstellen.

- **Aus Pools** — Sie können Volumes aus einem Pool entweder als *Fully-Provisioned (Thick) Volumes* oder als *Thin-Provision (Thin Provisioning) Volumes erstellen.*

> Die Benutzeroberfläche von System Manager bietet keine Option zum Erstellen von Thin Volumes. Wenn Sie Thin Volumes erstellen möchten, verwenden Sie die Befehlszeilenschnittstelle (CLI).

- **Aus Volume-Gruppen** — Sie können Volumes aus einer Volume-Gruppe nur als *voll bereitgestellte (Thick) Volumes* erstellen.

Thick Volumes und Thin Volumes ziehen die Kapazität des Storage-Arrays auf unterschiedliche Weise ein:

- Die Kapazität für ein Thick Volume wird bei der Erstellung des Volume zugewiesen.
- Die Kapazität eines Thin Volume wird beim Schreiben auf das Volume als Daten zugewiesen.

Thin Provisioning vermeidet ungenutzte Kapazität und kann Unternehmen im Vorfeld Kosten für Storage einsparen. Bei Full Provisioning profitieren Sie jedoch von weniger Latenz, da der gesamte Storage gleichzeitig zugewiesen wird, wenn Thick Volumes erstellt werden.

> Die EF600/EF600C und EF300/EF300C Storage-Systeme unterstützen Thin Provisioning nicht.

Eigenschaften der Volumes

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 Einzel-Controller-Array wird der Workload eines Volumes über einen einzelnen Controller gemanagt. Auf einem Dual-Controller-Array verfügt ein Volume über einen bevorzugten Controller (A oder B), der „`besitzt`“ das Volume. In einer Dual-Controller-Konfiguration wird die Eigentümerschaft von Volumes mithilfe der Funktion Automatischer Lastausgleich automatisch angepasst, um eventuelle Probleme beim Lastausgleich zu beheben, wenn Workloads zwischen den Controllern verschoben werden. 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.

- **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.

Funktionsweise von 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 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.

- **Anwendungsspezifisch**. Wenn Sie Volumes mit einem applikationsspezifischen Workload erstellen, empfiehlt das System möglicherweise eine optimierte Volume-Konfiguration, um Konflikte zwischen Applikations-Workload-I/O und anderem Datenverkehr aus Ihrer Applikationsinstanz 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 File System der Virtual Machine 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 für die Erstellung von Volumes). 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 SANtricity 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 **Applikationen & Workloads** in der Kachel Volumes auswählen, um die nach Workload gruppierten Speicher-Array-Volumes und den Applikationstyp anzuzeigen, mit dem der Workload verknüpft ist.
- Im Kachel Performance können Sie auf der Registerkarte **Applikationen & Workloads** Performance Performance 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.

Volume-Terminologie

Erfahren Sie, wie die Volume-Bedingungen auf Ihr Storage Array angewendet werden.

Alle Volume-Typen

Laufzeit	Beschreibung
Zugewiesene Kapazität	Die zugewiesene Kapazität wird zur Erstellung von Volumes und für Kopierdienste genutzt. Die zugewiesene Kapazität und die gemeldete Kapazität sind bei Thick Volumes identisch, unterscheiden sich jedoch bei Thin Volumes. Bei einem dicken Volume entspricht der physisch zugewiesene Speicherplatz dem Speicherplatz, der dem Host gemeldet wird. Bei einem Thin Volume ist die gemeldete Kapazität die den Hosts gemeldete Kapazität, während die zugewiesene Kapazität die Menge an Festplattenspeicher ist, die derzeit zum Schreiben von Daten zugewiesen ist.
Applikation	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.

Laufzeit	Beschreibung
Kapazität	Kapazität ist die Menge an Daten, die Sie in einem Volume speichern können.
Controller-Eigentum	Das Controller-Eigentum definiert den Controller, der als Eigentümer des oder primären Controller des Volume bezeichnet wird. Ein Volume kann einen bevorzugten Controller (A oder B) haben, der „`besitzt`“ des Volume. Die Eigentümerschaft für Volumes wird mithilfe der Funktion Automatischer Lastausgleich automatisch angepasst, um eventuelle Probleme beim Lastenausgleich zu korrigieren, wenn die Workloads sich zwischen den Controllern verschieben. Automatischer Lastausgleich bietet einen automatischen I/O-Workload-Ausgleich und stellt sicher, dass eingehender I/O-Datenverkehr von den Hosts auf beiden Controllern dynamisch gemanagt und ausgeglichen wird.
Dynamischer Cache-Lese-Prefetch	Mit dem dynamischen Lese-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 basierend auf der Geschwindigkeit und der Anfragegröße des Host-Lesevorgängen automatisch an. Ein wahlfreier Zugriff bewirkt nicht, dass Daten im Cache abgerufen werden. Diese Funktion gilt nicht, wenn das Lese-Caching deaktiviert ist. Bei einem Thin Volume ist der dynamische Lese-Prefetch für den Cache immer deaktiviert und kann nicht geändert werden.
Freier Kapazitätsbereich	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. Durch die Konsolidierung der freien Kapazität können Sie zusätzliche Volumes aus der maximalen freien Kapazität in einer Volume-Gruppe erstellen.
Host	Ein Host ist ein Server, der I/O an ein Volume auf einem Storage-Array sendet.
Host-Cluster	Ein Host-Cluster ist eine Gruppe von Hosts. Sie erstellen ein Host-Cluster, damit Sie mehrere Hosts dieselben Volumes ganz einfach zuweisen können.
Hot-Spare-Laufwerk	Hot-Spare-Festplatten werden nur bei Volume-Gruppen unterstützt. Ein Hot-Spare-Laufwerk enthält keine Daten und fungiert als Standby, falls ein Laufwerk in RAID 1-, RAID 3-, RAID 5- oder RAID 6-Volumes einer Volume-Gruppe ausfällt. Das Hot-Spare-Laufwerk sorgt für zusätzliche Redundanz in Ihrem Speicher-Array.

Laufzeit	Beschreibung
LUN	Eine Logical Unit Number (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.
Medien-Scan	Ein Medienscan bietet eine Möglichkeit, Laufwerkfehler zu erkennen, bevor sie während eines normalen Lesevorgangs von oder Schreibvorgangs auf den Laufwerken gefunden werden. Ein Medien-Scan wird als Hintergrundvorgang durchgeführt und scannt alle Daten und Redundanzinformationen in definierten Benutzer-Volumes.
Namespace	Ein Namespace ist NVM Storage, der für Blockzugriff formatiert ist. Es gleicht einer logischen Einheit in SCSI, die ein Volume im Storage Array bezieht.
Pool	Ein Pool ist eine Reihe von Laufwerken, die logisch gruppiert sind. Mit einem Pool können Sie ein oder mehrere Volumes erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einem Pool oder einer Volume-Gruppe.)
Pool- oder Volume-Gruppen-Kapazität	Pool-, Volume- oder Volume-Gruppenkapazität ist die Kapazität in einem Speicher-Array, das einem Pool oder einer Volume-Gruppe zugewiesen wurde. Diese Kapazität wird verwendet, um Volumes zu erstellen und die verschiedenen Kapazitätsanforderungen von Services-Vorgängen und Storage-Objekten zu warten.
Lese-Cache	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.
Gemeldete Kapazität	Die gemeldete Kapazität ist die Kapazität, die dem Host gemeldet wird und vom Host abgerufen werden kann. Gemeldete Kapazität und zugewiesene Kapazität sind für Thick Volumes identisch, unterscheiden sich jedoch bei Thin Volumes. Bei einem dicken Volume entspricht der physisch zugewiesene Speicherplatz dem Speicherplatz, der dem Host gemeldet wird. Bei einem Thin Volume ist die gemeldete Kapazität die den Hosts gemeldete Kapazität, während die zugewiesene Kapazität die Menge an Festplattenspeicher ist, die derzeit zum Schreiben von Daten zugewiesen ist.
Segmentgröße	Ein Segment ist die Datenmenge in Kilobyte (KiB), die auf einem Laufwerk gespeichert ist, bevor das Speicherarray auf das nächste Laufwerk im Stripe (RAID-Gruppe) verschoben wird. Die Segmentgröße ist gleich oder kleiner als die Kapazität der Volume-Gruppe. Die Segmentgröße ist festgelegt und kann für Pools nicht geändert werden.

Laufzeit	Beschreibung
Striping	Durch Striping werden Daten auf dem Speicher-Array gespeichert. Striping teilt den Datenfluss in Blöcke einer bestimmten Größe (sogenannte „Blockgröße“) auf und schreibt diese Blöcke dann nacheinander über die Laufwerke hinweg. Auf diese Weise wird Datenspeicher verwendet, um Daten über mehrere physische Laufwerke zu verteilen und zu speichern. Striping wird für RAID 0 synonym verwendet und verteilt die Daten ohne Parität auf alle Laufwerke einer RAID-Gruppe.
Datenmenge	Ein Volume ist ein Container, in dem Applikationen, Datenbanken und Filesysteme Daten speichern. Dies ist die logische Komponente, die erstellt wird, damit der Host auf den Speicher des Speicherarrays zugreifen kann.
Volume-Zuweisung	Die Volume-Zuweisung ist die Zuweisung von Host-LUNs zu einem Volume.
Volume-Name	Ein Volume-Name ist eine Zeichenfolge, die dem Volume beim Erstellen zugewiesen wird. Sie können entweder den Standardnamen akzeptieren oder einen aussagekräftigeren Namen angeben, der den Datentyp angibt, der im Volume gespeichert ist.
Volume-Gruppe	Eine Volume-Gruppe ist ein Container für Volumes mit gemeinsamen Merkmalen. Eine Volume-Gruppe verfügt über eine definierte Kapazität und einen RAID-Level. Sie können eine Volume-Gruppe verwenden, um ein oder mehrere Volumes zu erstellen, auf die ein Host zugreifen kann. (Sie erstellen Volumes entweder aus einer Volume-Gruppe oder aus einem Pool.)
Workload	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.
Schreib-Cache	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.
Caching von Schreibzugriffen mit Spiegelung	Caching von Schreibzugriffen mit Spiegelung findet statt, wenn die in den Cache-Speicher eines Controllers geschriebenen Daten 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.

Laufzeit	Beschreibung
Schreib-Caching ohne Batterien	Durch die Einstellung Schreib-Cache ohne Batterien wird das Schreib-Caching auch dann fortgesetzt, 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.

Spezifisch für Thin Volumes

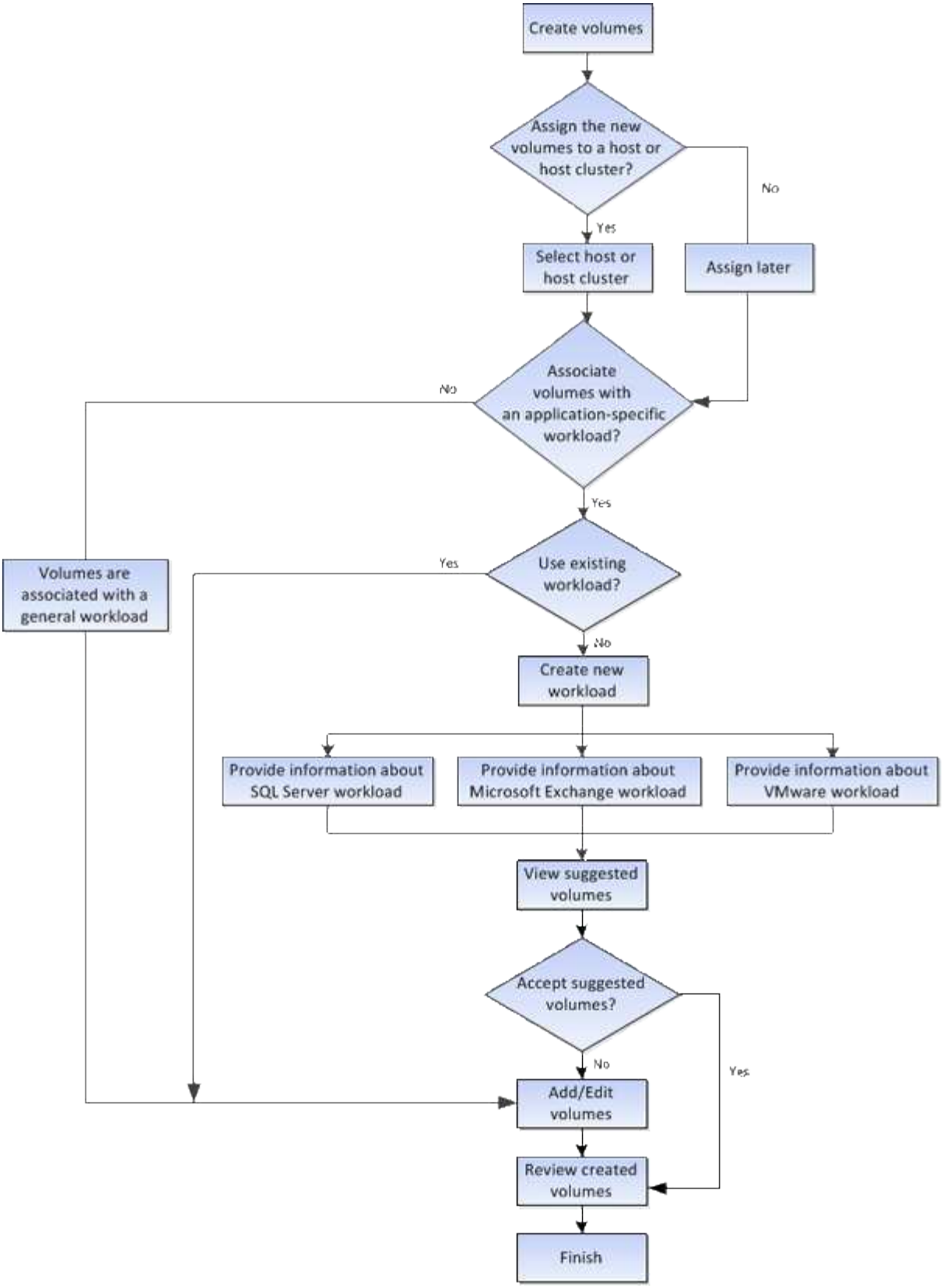
System Manager bietet keine Option zum Erstellen von Thin Volumes. Wenn Sie Thin Volumes erstellen möchten, verwenden Sie die Befehlszeilenschnittstelle (CLI).

Thin Volumes sind für das EF600/EF600C oder EF300/EF300C Storage-System nicht verfügbar.

Laufzeit	Beschreibung
Zugewiesene Kapazitätsgrenze	Die zugewiesene Kapazitätsgrenze ist die Obergrenze für die Größe der zugewiesenen physischen Kapazität für ein Thin Volume.
Geschriebene Kapazität	Die geschriebene Kapazität ist die Menge an Kapazität, die aus der für Thin Volumes zugewiesenen reservierten Kapazität geschrieben wurde.
Warnschwellenwert	Sie können eine Warnung für Warnmeldungen festlegen, die ausgegeben werden soll, wenn die zugewiesene Kapazität für ein Thin-Volume den vollen Prozentsatz erreicht (den Warnungsschwellenwert).

Workflow für die Erstellung von Volumes

In SANtricity System Manager können Sie Volumes erstellen, indem Sie diese Schritte ausführen.



Datenintegrität und Datensicherheit für Volumes

Sie können Volumes für die Verwendung der Data Assurance (da)-Funktion und der Laufwerkssicherheitsfunktion aktivieren. Diese Funktionen werden auf Pool- und Volume-Gruppenebene präsentiert.

Datensicherheit

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 mit der da-Fähigkeit ausgestattet ist (suchen Sie in der Tabelle „da“ neben „da“ und „Volume-Gruppen-Kandidaten“ nach „Ja“).

Laufwerkssicherheit

Drive Security ist eine Funktion, die bei Entfernung aus dem Speicher-Array unberechtigten Zugriff auf Daten auf sicheren Laufwerken verhindert. Diese Laufwerke können entweder vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder Laufwerke sein, die für die Einhaltung von Federal Information Processing Standards 140-2 Level 2 (FIPS-Laufwerke) zertifiziert sind.

Wie Drive Security auf der Laufwerksebene funktioniert

Ein sicheres Laufwerk mit FDE oder FIPS verschlüsselt Daten beim Schreiben und entschlüsselt Daten beim Lesen. Diese Ver- und Entschlüsselung hat keine Auswirkungen auf die Leistung oder den Anwender-Workflow. Jedes Laufwerk verfügt über einen eigenen eindeutigen Verschlüsselungsschlüssel, der nie vom Laufwerk übertragen werden kann.

So arbeitet Drive Security auf Volume-Ebene

Wenn Sie einen Pool oder eine Volume-Gruppe aus sicheren Laufwerken erstellen, können Sie auch die Laufwerksicherheit für diese Pools oder Volume-Gruppen aktivieren. Mit der Option Laufwerkssicherheit können die Laufwerke und damit verbundene Volume-Gruppen und Pools sicher-*enabled* erstellt werden. 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.

So implementieren Sie Drive Security

Um die Laufwerkssicherheit zu implementieren, führen Sie die folgenden Schritte aus.

1. Rüsten Sie Ihr Storage-Array mit sicheren Laufwerken aus – entweder mit FDE- oder mit FIPS-Laufwerken. (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.)
2. Erstellen Sie einen Sicherheitsschlüssel, d. h. eine Zeichenkette, die vom Controller und den Laufwerken für Lese-/Schreibzugriff freigegeben wird. Sie können entweder einen internen Schlüssel aus dem persistenten Speicher des Controllers oder einen externen Schlüssel von einem Schlüsselmanagementserver erstellen. Für das externe Verschlüsselungsmanagement muss eine Authentifizierung mit dem Verschlüsselungsmanagement-Server eingerichtet werden.
3. Aktivieren Sie die Laufwerkssicherheit für Pools und Volume-Gruppen:

- Erstellen Sie einen Pool oder eine Volume-Gruppe (suchen Sie in der Spalte **Secure-able** in der Tabelle Kandidaten nach **Ja**).
- Wählen Sie einen Pool oder eine Volume-Gruppe aus, wenn Sie ein neues Volume erstellen (suchen Sie nach **Ja** neben **sicher-fähig** in der Tabelle für Pool- und Volume-Gruppen Kandidaten).

  Mit der Laufwerkssicherheitsfunktion erstellen Sie einen Sicherheitsschlüssel, der von den sicheren Laufwerken und Controllern in einem Speicher-Array gemeinsam genutzt wird. Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln die sicher-aktivierten Laufwerke in den Status Sicherheitsverriegelt, bis der Controller den Sicherheitsschlüssel anwendet.

SSD Cache und Volumes

Sie können ein Volume zu SSD Cache hinzufügen, um die Leseleistung zu verbessern. SSD-Cache besteht aus einer Reihe von Solid-State Disk-Laufwerken (SSD), die Sie in Ihrem Storage-Array logisch gruppieren.

Volumes

Über einfache Volume-I/O-Mechanismen werden Daten in den und aus dem SSD-Cache verschoben. Nachdem Daten im Cache gespeichert und auf den SSDs gespeichert wurden, werden nachfolgende Lesezugriffe auf diese Daten im SSD Cache ausgeführt. Auf das HDD-Volume ist somit kein Zugriff mehr erforderlich.

SSD Cache ist ein sekundärer Cache zur Verwendung mit dem primären Cache im dynamischen Random-Access Memory (DRAM) des Controllers.

- Im primären Cache werden die Daten nach dem Lesen des Hosts im DRAM gespeichert.
- Im SSD Cache werden die Daten aus Volumes kopiert und auf zwei internen RAID-Volumes (eine pro Controller) gespeichert, die bei der Erstellung eines SSD-Caches automatisch erstellt werden.

Die internen RAID-Volumes werden für die interne Cache-Verarbeitung verwendet. Auf diese Volumes kann nicht zugegriffen oder in der Benutzeroberfläche angezeigt werden. Diese beiden Volumes zählen jedoch die Gesamtanzahl der im Storage Array zulässigen Volumes.

Jedes Volume, das der Nutzung des SSD-Caches eines Controllers zugewiesen ist, kann keine automatische Lastverteilung durchführen.

Laufwerkssicherheit

Wenn Sie SSD Cache auf einem Volume verwenden möchten, das auch die Laufwerkssicherheit verwendet (ist sicher aktiviert), müssen die Laufwerksicherheitsfunktionen des Volumes und des SSD-Caches übereinstimmen. Stimmen sie nicht überein, wird das Volume nicht sicher aktiviert.

Aktionen, die Sie auf Volumes durchführen können

Sie können eine Reihe verschiedener Aktionen auf einem Volume durchführen: Die Kapazität erhöhen, löschen, kopieren, initialisieren, neu verteilen, Ändern der Eigentümerschaft, Ändern der Cache-Einstellungen und Ändern der Einstellungen für die Medienüberprüfung

Erhöhte Kapazität

Es gibt zwei Möglichkeiten, die Kapazität für ein Volume zu erweitern:

- Verwenden Sie die freie Kapazität, die im Pool bzw. der Volume-Gruppe verfügbar ist.

  Sie fügen einem Volume Kapazität hinzu, indem Sie Menü:Speicher[Pools und Volume-Gruppen > Kapazität hinzufügen] auswählen.

- Fügen Sie dem Pool oder der Volume-Gruppe des Volume nicht zugewiesene Kapazität (in Form von nicht verwendeten Laufwerken) hinzu. Verwenden Sie diese Option, wenn im Pool oder in der Volume-Gruppe keine freie Kapazität vorhanden ist.

  Sie fügen dem Pool oder der Volume-Gruppe nicht zugewiesene Kapazität hinzu, indem Sie Menü:Storage[Pools und Volume Groups > Add Capacity] auswählen.

  Wenn im Pool oder in der Volume-Gruppe keine freie Kapazität verfügbar ist, können Sie die Kapazität des Volume nicht erhöhen. Sie müssen zunächst die Größe des Pools oder der Volume-Gruppe erhöhen oder ungenutzte Volumes löschen.

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.

Löschen

Normalerweise löschen Sie Volumes, wenn die Volumes mit falschen Parametern oder Kapazität erstellt wurden, die Storage-Konfigurationsanforderungen nicht mehr erfüllen oder Snapshot Images sind, die nicht mehr für Backup oder Applikationstests erforderlich sind. Durch das Löschen eines Volumes wird die freie Kapazität im Pool oder der Volume-Gruppe erhöht.

Das Löschen von Volumes verursacht den Verlust aller Daten auf diesen Volumes. Wenn Sie ein Volume löschen, werden auch alle zugehörigen Snapshot-Images, Zeitpläne und Snapshot-Volumes gelöscht und alle Spiegelungsbeziehungen entfernt.

Kopieren

Wenn Sie Volumes kopieren, erstellen Sie eine zeitpunktgenaue Kopie von zwei separaten Volumes, dem Quell-Volume und dem Ziel-Volume, auf demselben Storage Array. Sie können Volumes kopieren, indem Sie Menü:Speicher[Volumes > Kopierdienste > Volume kopieren] wählen.

Initialisieren

Durch das Initialisieren eines Volumes werden alle Daten aus dem Volume gelöscht. 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. 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.

Sie können Volumes initialisieren, indem Sie Menü:Speicher[Volumes > Mehr > Volumes initialisieren] auswählen.

Neu Verteilen

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.

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.

Sie können Volumes neu verteilen, indem Sie im Menü:Storage[Volumes > Mehr > Neuverteilung von Volumes] wählen.

Änderung der Volume-Eigentümerschaft

Durch eine Änderung der Eigentümerschaft eines Volumes wird der bevorzugte Controller-Eigentümer des Volumes geändert. Der bevorzugte Controller-Eigentümer eines Volumes wird unter Menü:Storage[Volumes > Einstellungen anzeigen/bearbeiten > Registerkarte Erweitert] aufgelistet.

Sie können das Eigentum eines Volumens ändern, indem Sie Menü:Storage[Volumes > Mehr > Eigentümerschaft ändern] auswählen.

Spiegelung und Volume-Eigentum

Wenn das primäre Volume des gespiegelten Paars Eigentum von Controller A ist, dann befindet sich das sekundäre Volume auch im Besitz von Controller A des Remote Storage Array. Wenn Sie den Eigentümer des primären Volume ändern, wird automatisch der Eigentümer des sekundären Volumes geändert, um sicherzustellen, dass beide Volumes Eigentum des gleichen Controllers sind. Aktuelle Eigentumsänderungen auf der primären Seite werden automatisch an die entsprechenden aktuellen Eigentumsänderungen auf der sekundären Seite übernommen.

Wenn eine Spiegelkonsistent-Gruppe ein lokales sekundäres Volume enthält und die Controller-Eigentümerschaft geändert wird, wird das sekundäre Volume automatisch beim ersten Schreibvorgang wieder an den ursprünglichen Controller-Eigentümer übertragen. Sie können den Controller-Eigentümer eines sekundären Volumes nicht mit der Option **Eigentumsrechte ändern** ändern.

Eigentümerschaft für Kopien und Volumes

Während eines Kopiervorgangs muss derselbe Controller sowohl das Quell-Volume als auch das Ziel-Volume besitzen. Manchmal haben beide Volumen nicht den gleichen bevorzugten Controller, wenn der Kopiervorgang startet. Daher wird das Eigentum des Ziel-Volumes automatisch an den bevorzugten Controller des Quell-Volume übertragen. Wenn die Volume-Kopie abgeschlossen ist oder angehalten wird, wird der Eigentümer des Ziel-Volume auf dem bevorzugten Controller wiederhergestellt.

Wenn sich während des Kopiervorgangs der Besitz des Quell-Volumes ändert, wird auch der Besitz des Zielvolume geändert. Unter bestimmten Betriebssystemumgebungen kann es notwendig sein, den Multipath-Host-Treiber neu zu konfigurieren, bevor ein I/O-Pfad verwendet werden kann. (Einige Multipath-Treiber erfordern eine Bearbeitung, um den I/O-Pfad zu erkennen. Weitere Informationen finden Sie in der Treiberdokumentation.)

Cache-Einstellungen ändern

Cache-Speicher ist ein Bereich von temporär-flüchtigem Speicher (RAM) auf dem Controller, der eine schnellere Zugriffszeit hat als die Datenträger. Wenn Sie Cache-Speicher verwenden, können Sie die gesamte I/O-Performance aus folgenden Gründen erhöhen:

- Die vom Host für einen Lesevorgang angeforderten Daten befinden sich möglicherweise bereits im Cache eines vorherigen Vorgangs, sodass ein Laufwerkzugriff nicht erforderlich ist.
- Schreibdaten werden zunächst in den Cache geschrieben. Dadurch wird die Anwendung wieder freigegeben, anstatt auf das Schreiben der Daten auf das Laufwerk zu warten.

Wählen Sie MENU:Speicher[Volumes > Mehr > Cache-Einstellungen ändern], um die folgenden Cache-Einstellungen zu ändern:

- **Lese- und Schreib-Cache** — 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.

  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.

- **Schreib-Cache mit Spiegelung** — Schreib-Caching mit Spiegelung tritt auf, wenn die in den Cache-Speicher eines Controllers geschriebenen Daten 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.
- **Write Caching ohne Batterien** — das Schreib-Caching ohne Akkueinstellung lässt das Schreib-Caching auch dann fortgesetzt, 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.

  Diese Einstellung ist nur verfügbar, wenn Sie das Schreib-Caching aktiviert haben. Diese Einstellung ist für Thin-Volumes nicht verfügbar.

- **Dynamischer Lese-Cache Prefetch** — der dynamische Cache-Lesevorfetch ermöglicht dem Controller, zusätzliche sequenzielle Datenblöcke in den Cache zu kopieren, während er Datenblöcke von einem Laufwerk in den Cache liest. 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 basierend auf der Geschwindigkeit und der Anfragegröße des Host-Lesevorgängen automatisch an. Ein wahlfreier Zugriff bewirkt nicht, dass Daten im Cache abgerufen werden. Diese Funktion gilt nicht, wenn das Lese-Caching deaktiviert ist.

  Bei einem Thin Volume ist der dynamische Lese-Prefetch für den Cache immer deaktiviert und kann nicht geändert werden.

Ändern Sie die Einstellungen für die Medienüberprüfung

Medienprüfungen erkennen und reparieren Medienfehler auf Festplattenlaufwerken, die selten von

Applikationen gelesen werden. Durch diese Überprüfung kann verhindert werden, dass Datenverluste auftreten, wenn andere Laufwerke im Pool oder in der Volume-Gruppe ausfallen, da Daten für ausgefallene Laufwerke mithilfe von Redundanzinformationen und Daten anderer Laufwerke im Pool bzw. der Volume-Gruppe rekonstruiert werden.

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 jedoch mit derselben konstanten Geschwindigkeit fortgesetzt.

Sie können die Dauer der Medienscan-Ausführung aktivieren und einstellen, indem Sie Menü:Speicher[Volumes > Mehr > Medienscan-Einstellungen ändern] auswählen.

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.

Zuweisung von 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.

Erstellung und Erweiterung von Volumes mithilfe von Kapazität

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 mit 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.

Kapazitätstypen für Thick Volumes und Thin Volumes

Sie können entweder Thick Volumes oder Thin Volumes erstellen. Gemeldete Kapazität und zugewiesene Kapazität sind für Thick Volumes identisch, unterscheiden sich jedoch bei Thin Volumes.

- Bei einem Thick Volume entspricht die gemeldete Kapazität des Volumes der zugewiesenen physischen Storage-Kapazität. 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 Thick Volume so ein, dass die maximale Kapazität sein wird, die Ihrer Meinung nach das Volume vergrößern wird. Thick Volumes bieten eine hohe und vorhersehbare Performance für Ihre Applikationen, vor allem weil sämtliche Benutzerkapazitäten bei der Erstellung reserviert und zugewiesen sind.

- Bei einem Thin Volume ist die gemeldete Kapazität die den Hosts gemeldete Kapazität, während die zugewiesene Kapazität die Menge an Festplattenspeicher ist, die derzeit zum Schreiben von Daten zugewiesen ist.

  Die gemeldete Kapazität kann größer sein als die zugewiesene Kapazität im Speicher-Array. Thin Volumes können angepasst werden, um mit Wachstum Schritt zu halten, ohne die derzeit verfügbaren Ressourcen zu berücksichtigen.

> SANtricity System Manager bietet keine Option zum Erstellen von Thin Volumes. Wenn Sie Thin Volumes erstellen möchten, verwenden Sie die Befehlszeilenschnittstelle (CLI).

Kapazitätsbeschränkungen für Thick Volumes

Die minimale Kapazität für ein dickes Volume beträgt 1 MiB, und die maximale Kapazität wird durch die Anzahl und Kapazität der Laufwerke im Pool oder der Volume-Gruppe bestimmt.

Beachten Sie bei der Erhöhung der gemeldeten Kapazität für ein dickes 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.

Kapazitätsgrenzen für Thin Volumes

Sie können Thin Volumes mit einer gemeldeten Kapazität und einer relativ kleinen zugewiesenen Kapazität erstellen. Dies bietet Vorteile bei der Storage-Auslastung und -Effizienz. Thin Volumes vereinfachen die Storage-Administration, da die zugewiesene Kapazität je nach Applikationsanforderungen erhöht werden kann, ohne Unterbrechung der Applikation zugunsten einer besseren Storage-Auslastung.

Neben der gemeldeten Kapazität und der zugewiesenen Kapazität enthalten Thin Volumes auch die geschriebene Kapazität. Die geschriebene Kapazität ist die Menge an Kapazität, die aus der für Thin Volumes zugewiesenen reservierten Kapazität geschrieben wurde.

In der folgenden Tabelle werden die Kapazitätsgrenzen für ein Thin Volume aufgeführt.

Art der Kapazität	Mindestgröße	Maximale Größe
Berichtet	32 MiB	256 tib
Zugewiesen	4 MiB	64 tib

Wenn bei einem Thin-Volume die maximale gemeldete Kapazität von 256 tib erreicht ist, können Sie seine Kapazität nicht erhöhen. Stellen Sie sicher, dass die reservierte Kapazität des Thin-Volumes auf eine Größe gesetzt ist, die größer als die maximale gemeldete Kapazität ist.

Basierend auf der zugewiesenen Kapazitätsgrenze erweitert das System die zugewiesene Kapazität automatisch. Die zugewiesene Kapazitätsgrenze ermöglicht es Ihnen, das automatische Wachstum des Thin Volumes unter der gemeldeten Kapazität zu begrenzen. Wenn die geschriebene Datenmenge sich in der Nähe der zugewiesenen Kapazität befindet, können Sie das zugewiesene Kapazitätslimit ändern.

Um die zugewiesene Kapazitätsgrenze zu ändern, wählen Sie Menü:Speicher[Volumes > Registerkarte Thin Volume Monitoring > Limit ändern].

Da System Manager beim Erstellen eines Thin Volume nicht die volle Kapazität zuweist, besteht möglicherweise im Pool keine unzureichende freie Kapazität. Nicht genügend Speicherplatz kann Schreibvorgänge in den Pool blockieren, nicht nur für die Thin-Volumes, sondern auch für andere Vorgänge, die Kapazität aus dem Pool benötigen (z. B. Snapshot-Images oder Snapshot-Volumes). Sie können jedoch weiterhin Lesevorgänge aus dem Pool ausführen. Wenn dieser Fall eintritt, erhalten Sie eine Warnung für den Alarmschwellenwert.

Thin Volume-Monitoring

Sie können Thin Volumes auf Speicherplatz überwachen und entsprechende Warnmeldungen generieren, um Kapazitätsüberkapazitäten zu vermeiden.

Thin Provisioning-Umgebungen können mehr logischen Speicherplatz zuweisen, als sie zugrunde liegenden physischen Storage haben. Sie können Menü:Registerkarte „Storage[Volumes > Thin Volume Monitoring]“ auswählen, um das Wachstum Ihrer Thin Volumes zu überwachen, bevor sie die zugewiesene Kapazitätsgrenze erreichen.

Sie können die Ansicht „Thin Monitoring“ verwenden, um die folgenden Aktionen auszuführen:

- Legen Sie die Grenze fest, die die zugewiesene Kapazität einschränkt, auf die sich ein Thin Volume automatisch erweitern kann.
- Legen Sie den Prozentpunkt fest, an dem eine Warnung (Warnungsschwellenwert überschritten) an den Benachrichtigungsbereich auf der Startseite gesendet wird, wenn sich ein Thin-Volume in der Nähe des maximal zugewiesenen Kapazitätslimits befindet.

Um die Kapazität eines Thin-Volumes zu erhöhen, erhöhen Sie dessen gemeldete Kapazität.

System Manager bietet keine Option zum Erstellen von Thin Volumes. Wenn Sie Thin Volumes erstellen möchten, verwenden Sie die Befehlszeilenschnittstelle (CLI).

Thin Volumes sind für das EF600/EF600C oder EF300/EF300C Storage-System nicht verfügbar.

Vergleich von Thick Volumes und Thin Volumes

Ein Thick Volume ist immer vollständig bereitgestellt, was bedeutet, dass bei der Erstellung des Volume alle Kapazitäten zugewiesen werden. Ein Thin Volume wird immer über Thin Provisioning bereitgestellt. Das heißt, die Kapazität wird beim Schreiben der Daten auf das Volume zugewiesen.

System Manager bietet keine Option zum Erstellen von Thin Volumes. Wenn Sie Thin Volumes erstellen möchten, verwenden Sie die Befehlszeilenschnittstelle (CLI).

Volume-Typ	Beschreibung
Thick Volumes	• Thick Volumes werden entweder aus einem Pool oder einer Volume-Gruppe erstellt. • Bei dicken Volumes wird bereits im Vorfeld ein großer Speicherplatz bereitgestellt, damit zukünftige Storage-Anforderungen erfüllt werden können. • Thick Volumes werden mit der gesamten Größe des Volumes erstellt, die bei der Erstellung des Volume vorab über physischen Storage zugewiesen sind. Aufgrund dieser Vorzuweisung verbraucht das Erstellen eines 100 gib Volumes tatsächlich 100 gib der zugewiesenen Kapazität auf Ihren Laufwerken. Der Speicherplatz könnte jedoch nicht genutzt werden, wodurch die Storage-Kapazität zu wenig genutzt wird. • Stellen Sie bei der Erstellung von Thick Volumes sicher, dass Sie die Kapazität eines einzelnen Volume nicht zu hoch zuweisen. Bei der Zuweisung von Kapazität für ein einzelnes Volume kann der gesamte physische Storage in Ihrem System schnell belegt werden. • Beachten Sie, dass auch für Copy-Services (Snapshot Images, Snapshot-Volumes, Volume-Kopien und asynchrone Spiegelung) Storage-Kapazität benötigt wird. Weisen Sie daher nicht alle Kapazitäten Thick Volumes zu. Unzureichender Speicherplatz kann Schreibvorgänge in den Pool oder die Volume-Gruppe blockieren. Im Falle dieses Problems erhalten Sie eine Warnung für den Freikapazitätsschwellenwert.

Volume-Typ	Beschreibung
Thin Volumes	• Thin Volumes werden nur aus einem Pool und nicht aus einer Volume-Gruppe erstellt. • Thin Volumes müssen RAID 6 sein. • Thin Volumes sind für das EF600/EF600C oder EF300/EF300C Storage-System nicht verfügbar. • Sie müssen die CLI zum Erstellen von Thin Volumes verwenden. • Im Gegensatz zu dicken Volumes wird der für das Thin Volume erforderliche Speicherplatz nicht während der Erstellung zugewiesen, sondern zu einem späteren Zeitpunkt nach Bedarf bereitgestellt. • Dank eines Thin Volume können Sie seine Größe überdimensionieren. Das heißt, Sie können eine LUN-Größe zuweisen, die größer ist als das Volume. Sie können das Volume dann nach Bedarf erweitern (falls nötig weitere Laufwerke hinzufügen), ohne die Größe der LUN zu erweitern und müssen daher die Benutzer nicht trennen. • Mithilfe des Thin Provisioning Block Space Reclamation (UNMAP) können Blöcke eines Thin Provisioning Volumes auf dem Storage Array über einen vom Host ausgegebenen SCSI UNMAP-Befehl zurückgewonnen werden. Ein Storage Array, das Thin Provisioning unterstützt, kann den wieder zurückgewonnenen Speicherplatz wiederverwenden, um die Zuweisungsanforderungen für ein anderes Thin Provisioning Volume innerhalb desselben Storage Arrays zu erfüllen. Hierdurch kann der Festplattenplatzverbrauch besser gemeldet und die Ressourcen effizienter genutzt werden.

Thin-Volume-Einschränkungen

Thin Volumes unterstützen alle Vorgänge als Thick Volumes. Die folgenden Ausnahmen gelten:

- Sie können die Segmentgröße eines Thin-Volumes nicht ändern.
- Sie können die vorlesende Redundanzprüfung für ein Thin Volume nicht aktivieren.
- Ein Thin-Volume kann in einem Kopiervorgang nicht als Zielvolume verwendet werden.
- Die zugewiesene Kapazitätsgrenze und der Warnschwellenwert eines Thin Volume können nur auf der primären Seite eines asynchronen gespiegelten Paares geändert werden. Alle Änderungen an diesen Parametern auf der primären Seite werden automatisch auf die sekundäre Seite übertragen.

Speicher konfigurieren

Workloads erstellen

Sie können Workloads für jeden Applikationstyp erstellen.

Über diese Aufgabe

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

Schritte

1. Wählen Sie Menü:Storage[Volumes].
2. Wählen Sie Menü:Erstellen[Workload].

   Das Dialogfeld Anwendungs-Workload erstellen wird angezeigt.

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

Nachdem Sie fertig sind

Sie können dem erstellten Workload Storage-Kapazität hinzufügen. Verwenden Sie die Option **Create Volume**, um ein oder mehrere Volumes für eine Anwendung zu erstellen und jedem Volume bestimmte Mengen an Kapazität zuzuweisen.

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. Darüber hinaus bietet die Erstellung eines Volumes Optionen, mit denen jedem zu erstellenden Volume bestimmte Kapazitätsmengen zugewiesen werden können.

Über diese Aufgabe

Die meisten Applikationstypen sind standardmäßig auf eine benutzerdefinierte Volume-Konfiguration eingestellt. Bei einigen Anwendungstypen wird bei der Volume-Erstellung eine intelligente Konfiguration angewendet. Wenn Sie beispielsweise Volumes für die 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. System Manager verwendet diese Informationen, um eine optimale Volume-Konfiguration für Sie zu erstellen, die Sie nach Bedarf bearbeiten können.

Der Prozess zur Erstellung eines Volumes ist ein mehrstufiges Verfahren.

Schritt 1: Wählen Sie Host für ein Volume

Sie erstellen Volumes, um einem applikationsspezifischen Workload Storage-Kapazität hinzuzufügen und die erstellten Volumes für einen bestimmten Host oder Host-Cluster sichtbar zu machen. Darüber hinaus bietet die Erstellung eines Volumes Optionen, mit denen jedem zu erstellenden Volume bestimmte Kapazitätsmengen zugewiesen werden können.

Bevor Sie beginnen

- Unter dem Feld Hosts sind gültige Hosts oder Host-Cluster vorhanden.
- Für den Host wurden Host-Port-IDs definiert.
- Vor dem Erstellen eines da-fähigen Volumes 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.

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 Menü:Storage[Volumes].
2. Wählen Sie Menü:Erstellen[Volumen].

   Das Dialogfeld Volumes erstellen wird angezeigt.

3. 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.
4. Um die Volume-Erstellungsreihenfolge für den ausgewählten Host oder Host-Cluster fortzusetzen, klicken Sie auf **Weiter** und gehen Sie zu Schritt 2: Wählen Sie einen Workload für ein Volume.

   Das Dialogfeld „Workload auswählen“ wird angezeigt.

Schritt 2: Wählen Sie einen Workload für ein Volume

Wählen Sie einen Workload aus, um die Storage-Array-Konfiguration für eine bestimmte Applikation wie Microsoft SQL Server, Microsoft Exchange, Videoüberwachungsanwendungen oder VMware anzupassen. Sie können „andere Anwendung“ auswählen, wenn die Anwendung, die Sie für dieses Speicher-Array verwenden möchten, nicht aufgeführt ist.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Volumes für einen vorhandenen Workload erstellt werden.

- *Wenn Sie Volumes mit einem applikationsspezifischem Workload* erstellen, empfiehlt das System möglicherweise 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 die vom System empfohlenen Volumes und Merkmale bearbeiten, hinzufügen oder löschen. Verwenden Sie dazu das Dialogfeld Volumes hinzufügen/bearbeiten.
- *Wenn Sie Volumes mit „anderen“* Anwendungen erstellen (oder Anwendungen ohne spezifische Unterstützung der Volume-Erstellung), geben Sie die Volume-Konfiguration manuell über das Dialogfeld Volumes hinzufügen/bearbeiten an.

Schritte

1. Führen Sie einen der folgenden Schritte aus:

- Wählen Sie die Option **Volumes für einen vorhandenen Workload erstellen** aus, um Volumes für einen vorhandenen Workload zu erstellen.
- Wählen Sie die Option **Einen neuen Workload erstellen** aus, um einen neuen Workload für eine unterstützte Anwendung oder für „andere“ Anwendungen zu definieren.
  - 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 fort Schritt 3: Volumes hinzufügen oder bearbeiten.

Schritt 3: Volumes hinzufügen oder bearbeiten

System Manager kann eine Volume-Konfiguration auf Grundlage der von Ihnen ausgewählten Applikation oder Workload vorschlagen. Diese Volume-Konfiguration ist basierend auf dem Applikationstyp optimiert, den der Workload unterstützt. Sie können die empfohlene Volume-Konfiguration akzeptieren oder Sie können sie nach Bedarf bearbeiten. Wenn Sie eine der „anderen“ Anwendungen ausgewählt haben, müssen Sie manuell die Volumes und Merkmale angeben, die Sie erstellen möchten.

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, EF600C und E5700 Series)
  - 1,024 Volumes (EF300 und EF300C)
  - 512 Volumes (E4000 und E2800 Serie)
- Um ein für Data Assurance (da) fähiges Volume zu erstellen, muss die Host-Verbindung, die Sie verwenden möchten, da unterstützen.

  Auswahl eines sicheren Pools oder einer Volume-Gruppe

  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 in System Manager 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.

Auswahl eines sicheren Pools oder einer Volume-Gruppe

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 Laufwerke werden auf Pool- und Volume-Gruppenebene in System Manager dargestellt. 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 während des Lesevorgangs mit einem eindeutigen *Verschlüsselungsschlüssel*.

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 Pools oder Volume-Gruppen. Das Dialogfeld Volumes hinzufügen/bearbeiten zeigt alle berechtigten Pools und Volume-Gruppen im Speicher-Array an. 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, je nachdem, ob Sie 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-Erstellung von System Manager 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 je nach Festplattentyp in Schritten von 4 gib oder 8 gib zugewiesen. Kapazität, die nicht ein Vielfaches von 4- oder 8-gib beträgt, wird zugewiesen, jedoch nicht nutzbar. Um sicherzustellen, dass die gesamte Kapazität nutzbar ist, geben Sie die Kapazität in Schritten von 4 gib oder 8 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 • 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** — System Manager 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.

Feld	Beschreibung
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.
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-Erstellung von System Manager 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 je nach Festplattentyp in Schritten von 4 gib oder 8 gib zugewiesen. Kapazität, die nicht ein Vielfaches von 4- oder 8-gib beträgt, wird zugewiesen, jedoch nicht nutzbar. Um sicherzustellen, dass die gesamte Kapazität nutzbar ist, geben Sie die Kapazität in Schritten von 4 gib oder 8 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** — System Manager 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 Storage-Array-Controller, wenn Sie die Segmentgröße für ein Volume ändern, wirkt sich dies auf die I/O-Performance aus, doch Ihre Daten bleiben verfügbar.

Feld	Beschreibung
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.
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. Um die Sequenz zur Volume-Erstellung für die ausgewählte Anwendung fortzusetzen, klicken Sie auf **Weiter** und gehen Sie zu Schritt 4: Prüfen der Volume-Konfiguration.

Schritt 4: Prüfen der Volume-Konfiguration

Prüfen Sie eine Zusammenfassung der Volumes, die Sie erstellen möchten, und nehmen Sie die erforderlichen Änderungen vor.

Schritte

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

Ergebnisse

System Manager erstellt die neuen Volumes in den ausgewählten Pools und Volume-Gruppen und zeigt dann die neuen Volumes in der Tabelle Alle Volumes an.

Nachdem Sie fertig sind

- 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 direkt über den SANtricity System Manager erhältlich. Diese Version kann von den SMcli heruntergeladen werden und ist für die Controller E4000, EF600, EF600C, EF300, EF300C, E5700, EF570, E2800 und EF280 erhältlich. Um den SMcli im SANtricity System Manager herunterzuladen, wählen Sie **Einstellungen** > **System** und **Add-ons** > **Befehlszeilenschnittstelle**.

Hinzufügen von Volumes zum Workload

Sie können einem vorhandenen oder neuen Workload ein oder mehrere Volumes für Volumes hinzufügen, die derzeit keinem Workload zugewiesen sind.

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 Menü:Storage[Volumes].
2. Wählen Sie die Registerkarte * Anwendungen & Workloads* aus.

   Die Ansicht Applikationen und Workloads wird angezeigt.

3. Wählen Sie **zu Workload hinzufügen**.

   Das Dialogfeld „Workload auswählen“ wird angezeigt.

4. 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.
5. Wählen Sie **Weiter**, um mit der Add to Workload-Sequenz fortzufahren.

   Das Dialogfeld Volumes auswählen wird angezeigt.

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

Volumes managen

Erhöhte Kapazität eines Volumes

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

- 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.
- Die maximale gemeldete Kapazität von 256 tib wurde für Thin-Volumes nicht erreicht.
- Im Volume werden keine Hot-Spare-Laufwerke verwendet. (Gilt nur für Volumes in Volume-Gruppen.)

Sie können die Volume-Kapazität nur auf bis zu 128 tib gleichzeitig erweitern.

Über diese Aufgabe

Bedenken Sie zukünftige Kapazitätsanforderungen für andere Volumes in diesem Pool oder Volume-Gruppe. Stellen Sie sicher, dass ausreichend freie Kapazität zur Erstellung von Snapshot-Images, Snapshot-Volumes oder Remote-Spiegelungen zur Verfügung steht.

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 Menü:Storage[Volumes].
2. 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.

3. 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.

4. 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.

5. Klicken Sie Auf **Erhöhen**.

Ergebnisse

- System Manager erhöht die Kapazität des Volumes basierend auf Ihrer Auswahl.
- Wählen Sie MENU:Home[Vorgänge in Bearbeitung anzeigen], um den Fortschritt des Vorgangs zur Erhöhung der Kapazität anzuzeigen, der derzeit für das ausgewählte Volume ausgeführt wird. 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.

Volumes initialisieren

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.
- Das Volume ist optimal und es werden keine Änderungsvorgänge für das Volume ausgeführt.

> Sie können den Vorgang nach dem Start nicht mehr abbrechen. 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 Typen von Volumes *kann 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

Dieses Thema bezieht sich nur auf Standard-Volumes, die aus Pools oder Volume-Gruppen erstellt wurden.

Schritte

1. Wählen Sie Menü:Storage[Volumes].
2. 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.

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

Ergebnisse

System Manager 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).

Wählen Sie MENU:Home[Vorgänge in Bearbeitung anzeigen], um den Fortschritt des Initialisierungsvorgangs anzuzeigen, der derzeit für das ausgewählte Volume ausgeführt wird. Dieser Vorgang kann langwierig sein und die System-Performance beeinträchtigen.

Neuverteilung von Volumes

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 zu den Volumes *während der Umverteilungsvorgang läuft* muss angehalten 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 Menü:Storage[Volumes].
2. 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.

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

Ergebnisse

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

Ändern Sie den Controller-Eigentum eines Volumes

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 Menü:Storage[Volumes].
2. 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.

3. 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

- System Manager 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.

Volume löschen

Normalerweise löschen Sie Volumes, wenn die Volumes mit falschen Parametern oder Kapazität erstellt wurden, die Storage-Konfigurationsanforderungen nicht mehr erfüllen oder Snapshot Images sind, die nicht mehr für Backup oder Applikationstests erforderlich sind.

Durch das Löschen eines Volumes wird die freie Kapazität im Pool oder der Volume-Gruppe erhöht. Sie können ein oder mehrere zu löschende Volumes auswählen.

Bevor Sie beginnen

Stellen Sie für die Volumes, die Sie löschen möchten, Folgendes sicher:

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

Über diese Aufgabe

Ein Volume mit einer der folgenden Bedingungen kann nicht gelöscht werden:

- 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“.

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

Wenn ein Volume eine bestimmte Größe überschreitet (derzeit 128 TB), wird das Löschen im Hintergrund ausgeführt, sodass der freigegebene Speicherplatz möglicherweise nicht sofort verfügbar ist.

Schritte

1. Wählen Sie Menü:Storage[Volumes].
2. Klicken Sie Auf **Löschen**.

   Das Dialogfeld Volumes löschen wird angezeigt.

3. Wählen Sie ein oder mehrere Volumes aus, die Sie löschen möchten, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.
4. Klicken Sie Auf **Löschen**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Löscht alle zugehörigen Snapshot-Images, Zeitpläne und Snapshot-Volumes.
- Entfernt beliebige Spiegelungsbeziehungen.
- Erhöht die freie Kapazität im Pool bzw. in der Volume-Gruppe.

Ändern Sie die zugewiesene Kapazitätsgrenze für ein Thin Volume

Für Thin Volumes, die Speicherplatz nach Bedarf zuweisen können, können Sie das Limit ändern, das die zugewiesene Kapazität einschränkt, auf der ein Thin Volume automatisch erweitert werden kann.

Sie können auch den Prozentpunkt ändern, an dem eine Warnung (Warnungsschwellenwert überschritten) an

den Benachrichtigungsbereich auf der Startseite gesendet wird, wenn sich ein Thin-Volume in der Nähe der zugewiesenen Kapazitätsgrenze befindet. Sie können diese Benachrichtigung aktivieren oder deaktivieren.

Diese Funktion ist für das Speichersystem EF600/EF600C oder EF300/EF300C nicht verfügbar.

Basierend auf der zugewiesenen Kapazitätsgrenze erweitert das System die zugewiesene Kapazität automatisch. Die zugewiesene Kapazitätsgrenze ermöglicht es Ihnen, das automatische Wachstum des Thin Volumes unter der gemeldeten Kapazität zu begrenzen. Wenn die geschriebene Datenmenge sich in der Nähe der zugewiesenen Kapazität befindet, können Sie das zugewiesene Kapazitätslimit ändern.

Wenn Sie die zugewiesene Kapazitätsgrenze und der Warnschwellenwert eines Thin Volume ändern, müssen Sie den Speicherplatz berücksichtigen, der von den Benutzerdaten des Volumes und den Kopierdienstdaten verbraucht wird.

Schritte

1. Wählen Sie Menü:Storage[Volumes].
2. Wählen Sie die Registerkarte **Thin Volume Monitoring** aus.

   Die Ansicht Thin Volume Monitoring wird angezeigt.

3. Wählen Sie das dünne Volumen aus, das Sie ändern möchten, und wählen Sie dann **Limit ändern**.

   Das Dialogfeld Grenzwert ändern wird angezeigt. Die Einstellung für Kapazitätsgrenze und Warnungsschwellenwert für das ausgewählte Thin-Volume wird in diesem Dialogfeld angezeigt.

4. Ändern Sie die zugewiesene Kapazitätsgrenze und den Warnungsschwellenwert nach Bedarf.

   Felddetails

Einstellung	Beschreibung
Zugewiesene Kapazitätsgrenze ändern in…	Der Schwellenwert, bei dem Schreibzugriffe fehlschlagen, was den Verbrauch zusätzlicher Ressourcen durch Thin Volume verhindert. Dieser Schwellenwert ist ein Prozentsatz der gemeldeten Kapazitätsgröße des Volumes.
Benachrichtigen, wenn… (Warnschwellenwert)	Aktivieren Sie das Kontrollkästchen, wenn das System eine Warnmeldung erstellen soll, wenn sich ein Thin-Volume in der Nähe des zugewiesenen Kapazitätslimits befindet. Die Warnmeldung wird an den Benachrichtigungsbereich auf der Startseite gesendet. Dieser Schwellenwert ist ein Prozentsatz der gemeldeten Kapazitätsgröße des Volumes. Deaktivieren Sie das Kontrollkästchen, um die Benachrichtigung über Warnungsschwellenwert zu deaktivieren.

5. Klicken Sie Auf **Speichern**.

Einstellungen verwalten

Ändern Sie die Einstellungen für ein Volume

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

Bevor Sie beginnen

Das zu änderende Volumen befindet sich im optimalen Status.

Einige Vorgänge sind möglicherweise nicht verfügbar, während Änderungen an den Volume-Einstellungen vorgenommen werden

Schritte

1. Wählen Sie Menü:Storage[Volumes].
2. 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.

3. 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. Gemeldete Kapazität und zugewiesene Kapazität sind für Thick Volumes identisch, unterscheiden sich jedoch bei Thin Volumes. Bei einem dicken Volume entspricht der physisch zugewiesene Speicherplatz dem Speicherplatz, der dem Host gemeldet wird. Bei einem Thin Volume ist die gemeldete Kapazität die den Hosts gemeldete Kapazität, während die zugewiesene Kapazität die Menge an Festplattenspeicher ist, die derzeit zum Schreiben von Daten zugewiesen ist.
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.

Einstellung	Beschreibung
Identifikatoren	Zeigt die Kennungen für das ausgewählte Volume an. • **World-wide Identifier (WWID)** — Ein eindeutiger hexadezimaler Identifier für das Volume. • **Extended Unique Identifier (EUI)** — eine EUI-64 Kennung für das Volumen. • **Subsystem Identifier (SSID)** — die Speicher-Array-Subsystem-Kennung eines Volumes.

4. 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** — System Manager 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 Storage-Array-Controller, wenn Sie die Segmentgröße für ein Volume ändern, wirkt sich dies auf die I/O-Performance aus, doch Ihre 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.

Einstellung	Beschreibung
Caching	Zeigt die Caching-Einstellung, die Sie ändern können, um die gesamte I/O-Performance eines Volumes zu beeinträchtigen.
SSD Cache	Zeigt die Einstellung für SSD Cache, die Sie auf kompatiblen Volumes aktivieren können, um die schreibgeschützte Performance zu verbessern. Die Volumes sind kompatibel, wenn sie dieselben Funktionen für die Laufwerkssicherheit und Datensicherheit nutzen. **Die SSD Cache Funktion verwendet eine oder mehrere Solid State Disks (SSDs), um einen Lese-Cache zu implementieren**. 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.

5. Klicken Sie Auf **Speichern**.

   System Manager ändert die Volume-Einstellungen basierend auf Ihrer Auswahl.

Nachdem Sie fertig sind

Wählen Sie MENU:Startseite[Vorgänge in Bearbeitung anzeigen], um den Fortschritt der derzeit für das ausgewählte Volume ausgeführten Änderungsvorgänge anzuzeigen.

Workload-Einstellungen ändern

Sie können den Namen für einen Workload ändern und den zugehörigen Applikationstyp anzeigen. Ändern Sie den Namen eines Workloads, wenn der aktuelle Name nicht mehr aussagekräftig oder anwendbar ist.

Schritte

1. Wählen Sie Menü:Storage[Volumes].
2. Wählen Sie die Registerkarte * Anwendungen & Workloads* aus.

   Die Ansicht Applikationen und Workloads wird angezeigt.

3. 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.

4. **Optional:** Ändern Sie den vom Benutzer bereitgestellten Namen des Workloads.
5. Klicken Sie Auf **Speichern**.

Ändern Sie die Cache-Einstellungen für ein Volume

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 Standard-Volumes oder alle Thin Volumes gleichzeitig ändern.

Schritte

1. Wählen Sie Menü:Storage[Volumes].
2. 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.

3. 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.

4. 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

Cache-Einstellung	Beschreibung
Vorwort Für Dynamischen Lese-Cache	Mit dem dynamischen Lese-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 basierend auf der Geschwindigkeit und der Anfragegröße des Host-Lesevorgängen automatisch an. Ein wahlfreier Zugriff bewirkt nicht, dass Daten im Cache abgerufen werden. Diese Funktion gilt nicht, wenn das Lese-Caching deaktiviert ist. Bei einem Thin Volume ist der dynamische Lese-Prefetch für den Cache immer deaktiviert und kann nicht geändert werden.
Schreiben Sie das Caching ohne Batterien	Durch die Einstellung Schreib-Cache ohne Batterien wird das Schreib-Caching auch dann fortgesetzt, 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. **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 Option **Write Caching ohne Batterien** aktivieren. Diese Einstellung ist nur verfügbar, wenn Sie das Schreib-Caching aktiviert haben. Diese Einstellung ist für Thin-Volumes nicht verfügbar.
Schreib-Caching mit Spiegelung	Caching von Schreibzugriffen mit Spiegelung findet statt, wenn die in den Cache-Speicher eines Controllers geschriebenen Daten 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. Diese Einstellung ist nur verfügbar, wenn Sie das Schreib-Caching aktiviert haben. Diese Einstellung ist für Thin-Volumes nicht verfügbar.

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

Ändern Sie die Einstellungen für die Mediensuche für ein Volume

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.

Der standardmäßige Medienscan-Zeitraum ist auf 120 Tage festgelegt.

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 Menü:Storage[Volumes].
2. 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.

3. 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.

4. Geben Sie die Anzahl der Tage an, über die der Medienscan ausgeführt werden soll.
5. Aktivieren Sie das Kontrollkästchen **Media Scan** für jedes Volume, auf dem Sie einen Medien-Scan durchführen möchten.

   System Manager 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**.

6. Klicken Sie Auf **Speichern**.

   System Manager wendet basierend auf Ihrer Auswahl Änderungen an Medienprüfungen im Hintergrund an.

Verwenden Sie Kopierdienste

Volume-Übersicht kopieren

Mit der Funktion Copy Volume können Sie eine zeitpunktgenaue Kopie eines Volumes erstellen, indem Sie auf demselben Storage-Array zwei separate Volumes erstellen: Das Quell-Volume und das Ziel-Volume.

Diese Funktion erstellt eine Byte-Weise-Kopie vom Quell-Volume auf das Ziel-Volume, sodass die Daten auf dem Ziel-Volume identisch mit den Daten auf dem Quell-Volume sind.

Kopieren von Daten für besseren Zugriff

Bei Änderungen der Storage-Anforderungen an ein Volume können Sie mithilfe der Funktion Volume kopieren Daten aus Pools oder Volume-Gruppen kopieren, die kleinere Kapazitätslaufwerke in Pools oder Volume-Gruppen verwenden, die größere Kapazitätslaufwerke nutzen. Beispielsweise können Sie mit der Funktion Volume kopieren folgende Aufgaben ausführen:

- Verschieben Sie Daten auf größere Laufwerke.
- Wechseln Sie auf Laufwerke mit einer höheren Datentransferrate.
- Wechseln Sie zu Laufwerken mit neuen Technologien, um eine höhere Performance zu erzielen.
- Ändern Sie ein Thin-Volume in ein Thick Volume.

Quell- und Ziel-Volumes von Kopien müssen dieselben gemeldeten Host-adressierbaren/logischen Blockgrößen (Sektorgröße) aufweisen.

Gemeldete Blockgrößen von Volumes sind:

- **Native Blockgröße** – die Blockgröße des Volumes entspricht der Blockgröße des Laufwerks, entweder 512 oder 4 KB.

- **Emulierte 512 Blockgröße** - Laufwerke sind 4K, aber die gemeldete Blockgröße ist 512.

Ändern Sie ein Thin-Volume in ein Thick Volume

Wenn Sie ein Thin-Volume zu einem Thick Volume ändern möchten, erstellen Sie mithilfe der Operation „Copy Volume“ eine Kopie des Thin-Volume. Ziel eines Kopiervorgangs ist immer ein Thick Volume.

System Manager bietet keine Option zum Erstellen von Thin Volumes. Wenn Sie Thin Volumes erstellen möchten, verwenden Sie die Befehlszeilenschnittstelle (CLI).

Backup-Daten

Mit der Funktion Copy Volume können Sie Backups eines Volumes erstellen, indem Sie Daten von einem Volume auf ein anderes Volume im selben Storage Array kopieren. Sie können das Zielvolume als Backup für das Quell-Volume, für Systemtests oder für ein Backup auf einem anderen Gerät, z. B. als Bandlaufwerk, verwenden.

Stellen Sie Snapshot Volume-Daten auf dem Basis-Volume wieder her

Wenn Sie Daten aus dem zugehörigen Snapshot-Volume in das Basis-Volume wiederherstellen müssen, können Sie die Funktion „Copy Volume“ verwenden, um Daten vom Snapshot-Volume in das Basis-Volume zu kopieren. Sie können eine Volume-Kopie der Daten auf dem Snapshot Volume erstellen und dann die Daten in das Basis-Volume kopieren.

Quell- und Ziel-Volumes

Die folgende Tabelle gibt die Typen von Volumes an, die mit der Funktion „Volume kopieren“ für Quell- und Ziel-Volumes verwendet werden können.

Volume-Typ	Offline Volume Copy Quell-Volume	Online Volume Copy Quell-Volume	Online- und Offline-Ziel-Volume
Thick Volume in einem Pool	Ja.	Ja.	Ja.
Thick Volume in einer Volume-Gruppe	Ja.	Ja.	Ja.
Thin Volume	Ja[1]	Ja.	Nein
Snapshot Volume	Ja[2]	Nein	Nein
Snapshot Basis-Volume	Ja.	Ja.	Nein
Primäres Remote-Spiegel-Volume	Ja[3]	Ja.	Nein

[1] das Ziel-Volume muss eine Kapazität haben, die der gemeldeten Kapazität des Thin-Volumes entspricht oder größer ist.

[2] Sie können die Snapshot-Volume-Kopie erst verwenden, nachdem der Online-Kopiervorgang abgeschlossen ist.

[3] Wenn das Quell-Volume ein primäres Volume ist, muss die Kapazität des Ziel-Volumes gleich oder größer sein als die nutzbare Kapazität des Quell-Volumes.

Typen von Kopiervolumes

Sie können entweder einen Vorgang zum Kopieren von Volumes *offline* oder einen Vorgang zum Kopieren von Volumes *online* ausführen. Ein Offline-Vorgang liest Daten von einem Quell-Volume und kopiert sie auf ein Ziel-Volume. Ein Online-Vorgang verwendet ein Snapshot Volume als Quelle und kopiert seine Daten auf ein Ziel-Volume.

Um die Datenintegrität zu gewährleisten, werden alle I/O-Aktivitäten zum Ziel-Volume während eines Kopiervorgangs ausgesetzt. Diese Aussetzung tritt auf, weil der Zustand der Daten auf dem Zielvolumen uneinheitlich ist, bis das Verfahren abgeschlossen ist.

Im Folgenden werden die Vorgänge „Offline“ und „Online-Copy-Volume“ beschrieben.

Offline Copy Volume Operation

Die Offline-Beziehung des Copy Volume besteht zwischen einem Quell-Volume und einem Ziel-Volume. Eine Offline-Kopie liest Daten vom Quell-Volume und kopiert sie auf ein Ziel-Volume, während gleichzeitig alle Updates für das Quell-Volume unterbrochen werden, während die Kopie gerade läuft. Alle Updates des Quell-Volumes werden ausgesetzt, um zu verhindern, dass chronologische Inkonsistenzen auf dem Ziel-Volume erstellt werden.

Alles, was Sie über Offline-Kopiervorgänge wissen müssen	
Lese- und Schreibanfragen	• Quell-Volumes, die an einer Offline-Kopie teilnehmen, sind für schreibgeschützte E/A-Aktivitäten verfügbar, während ein Kopiervolume den Status „in progress“ oder „Ausstehend“ hat. • Schreibanforderungen sind zulässig, nachdem die Offline-Kopie abgeschlossen ist. • Um Schreibgeschützte Fehlermeldungen zu vermeiden, greifen Sie nicht auf ein Quell-Volume zu, das an einem Kopiervolume-Vorgang beteiligt ist und den Status „wird ausgeführt“ aufweist.
Journaling-Dateisystem	• Wenn das Quell-Volume mit einem Journaling-Dateisystem formatiert wurde, wird möglicherweise jeder Versuch, eine Leseanforderung an das Quell-Volume zu senden, von den Speicher-Array-Controllern abgelehnt, und es wird möglicherweise eine Fehlermeldung angezeigt. • Der Treiber des Journaling-Dateisystems gibt eine Schreibanforderung aus, bevor er versucht, die Leseanforderung auszustellen. Der Controller lehnt die Schreibanforderung ab, und die Leseanforderung kann aufgrund der abgelehnten Schreibanforderung möglicherweise nicht ausgestellt werden. Diese Bedingung kann dazu führen, dass eine Fehlermeldung angezeigt wird, die angibt, dass das Quell-Volume schreibgeschützt ist. • Um dieses Problem zu vermeiden, versuchen Sie nicht, auf ein Quell-Volume zuzugreifen, das an einer Offline-Kopie beteiligt ist, während der Vorgang „Copy Volume“ den Status „in Bearbeitung“ aufweist.

Online-Kopiervolume

Die Online-Beziehung zwischen einem Snapshot-Volume und einem Ziel-Volume besteht. Sie können einen Vorgang zum Kopieren-Volume initiieren, während das Quell-Volume online ist und für Schreibvorgänge verfügbar ist. Diese Funktion wird erreicht, indem ein Snapshot des Volumes erstellt und der Snapshot als tatsächliches Quellvolume für die Kopie verwendet wird.

Wenn Sie einen Vorgang zum Kopieren-Volume für ein Quell-Volume starten, erstellt System Manager ein Snapshot-Image des Basis-Volume und eine Kopierbeziehung zwischen dem Snapshot-Image des Basis-Volumes und einem Ziel-Volume. Wenn das Snapshot-Image als Quell-Volume verwendet wird, kann das Speicher-Array weiterhin auf das Quell-Volume schreiben, während die Kopie gerade läuft.

Während eines Online-Kopiervorgangs wird durch das Copy-on-Write-Verfahren eine Performance-Beeinträchtigung verursacht. Nach Abschluss der Online-Kopie wird die Performance des Basis-Volume wiederhergestellt.

Was Sie über Online-Kopiervorgänge wissen müssen	
Welche Art von Volumes können verwendet werden?	• Das Volume, für das das zeitpunktgenaue Image erstellt wird, wird als Basis-Volume bezeichnet und muss ein Standard-Volume oder ein Thin Volume im Storage Array sein. • Ein Ziel-Volume kann ein Standard-Volume in einer Volume-Gruppe oder ein Standard-Volume in einem Pool sein. Ein Ziel-Volume kann kein Thin-Volume oder ein Basis-Volume in einer Snapshot-Gruppe sein. • Mithilfe der Online-Funktion „Copy Volume“ können Daten von einem Thin Volume in ein Standard-Volume in einem Pool im selben Storage Array kopiert werden. Sie können jedoch die Funktion „Volume kopieren“ nicht verwenden, um Daten von einem Standardvolumen auf ein Thin Volume zu kopieren.
Basis-Volume-Performance	• Wenn das als Quelle der Kopie verwendete Snapshot-Volume aktiv ist, wird die Performance des Basis-Volumes aufgrund von Kopiervorgängen beeinträchtigt. Nach Abschluss der Kopie wird der Snapshot deaktiviert und die Performance des Basis-Volume wiederhergestellt. Obwohl der Snapshot deaktiviert ist, bleiben das reservierte Kapazitäts-Volume und die Kopierbeziehung intakt.
Typen von erstellten Volumes	• Während der Online-Kopie werden ein Snapshot Volume und ein reserviertes Kapazitäts-Volume erstellt. • Das Snapshot Volume ist kein tatsächliches Volume, das Daten enthält, sondern ein Verweis auf die Daten, die zu einem bestimmten Zeitpunkt auf einem Volume enthalten sind. • Für jeden erstellten Snapshot wird ein reserviertes Kapazitäts-Volume erstellt, um die Daten für den Snapshot zu speichern. Das reservierte Kapazitäts-Volume wird nur zum Managen des Snapshot Images verwendet.

Was Sie über Online-Kopiervorgänge wissen müssen	
Reserviertes Kapazitäts-Volume	• Vor der Änderung eines Datenblocks auf dem Quell-Volume werden die Inhalte des zu ändernden Blocks zur Aufbewahrung auf das reservierte Kapazitäts-Volume kopiert. • Da das reservierte Kapazitäts-Volume Kopien der Originaldaten in diesen Datenblöcken speichert, werden weitere Änderungen an diesen Datenblöcken vorgenommen, die nur auf das Quell-Volume schreiben. • Der Vorgang der Online-Kopie belegt weniger Festplattenspeicher als eine vollständige physische Kopie, da die einzigen Datenblöcke, die in dem reservierten Kapazitäts-Volume gespeichert sind, diejenigen sind, die sich seit der Zeit des Snapshots geändert haben.

Volume kopieren

Sie können Daten von einem Volume auf ein anderes im selben Storage Array kopieren und ein physisches, zeitpunktgenaues Duplikat (Klon) eines Quell-Volumes erstellen.

Bevor Sie beginnen

- Alle I/O-Aktivitäten des Quell-Volume und des Ziel-Volume müssen angehalten werden.
- Alle Dateisysteme auf dem Quell-Volume und dem Zielvolume müssen abgehängt werden.
- Wenn Sie das Ziel-Volume zuvor bei einem Kopiervolume-Vorgang verwendet haben, benötigen Sie diese Daten nicht mehr oder haben Sie ein Backup der Daten.

Über diese Aufgabe

Das Quell-Volume ist das Volume, das Host-I/O akzeptiert und Applikationsdaten speichert. Wenn ein Copy Volume gestartet wird, werden Daten aus dem Quell-Volume vollständig in das Ziel-Volume kopiert.

Das Ziel-Volume ist ein Standard-Volume, das eine Kopie der Daten vom Quell-Volume beibehält. Nach Abschluss des Kopiervorgangs ist das Ziel-Volume identisch mit dem Quell-Volume. Das Zielvolume muss die gleiche oder größere Kapazität haben wie das Quell-Volume, es kann jedoch ein anderes RAID-Level aufweisen.

Mehr zu Online- und Offline-Kopien

Online-Kopie

Eine Online-Kopie erstellt eine zeitpunktgenaue Kopie eines beliebigen Volumes innerhalb eines Storage Arrays, während es weiterhin möglich ist, in Bearbeitung der Kopie auf das Volume zu schreiben. Diese Funktion wird erreicht, indem ein Snapshot des Volumes erstellt und der Snapshot als tatsächliches Quellvolume für die Kopie verwendet wird. Das Volume, für das das zeitpunktgenaue Image erstellt wird, wird als Basis-Volume bezeichnet. Es kann sich um ein Standard-Volume oder ein Thin Volume im Storage Array handelt.

Offline-Kopie

Eine Offline-Kopie liest Daten vom Quell-Volume und kopiert sie auf ein Ziel-Volume, während gleichzeitig alle Updates für das Quell-Volume unterbrochen werden, während die Kopie gerade läuft. Alle Updates des Quell-Volumes werden ausgesetzt, um zu verhindern, dass chronologische Inkonsistenzen auf dem Ziel-Volume erstellt werden. Die offline Volume Copy-Beziehung besteht zwischen einem Quell-Volume und einem Ziel-Volume.

Bei einem Vorgang zum Kopieren von Volumes werden die Daten auf dem Ziel-Volume überschrieben und alle dem Ziel-Volume zugeordneten Snapshot-Volumes sind fehlgeschlagen, sofern vorhanden.

Schritte

1. Wählen Sie Menü:Storage[Volumes].
2. Wählen Sie das Volume aus, das Sie als Quelle für den Kopiervolume verwenden möchten, und wählen Sie anschließend Menü:Kopierdienste[Volume kopieren].

   Das Dialogfeld Volume-Select-Ziel kopieren wird angezeigt.

3. Wählen Sie das Ziel-Volume aus, auf das die Daten kopiert werden sollen.

   In der Tabelle dieses Dialogfelds werden alle berechtigten Ziel-Volumes aufgelistet.

4. Verwenden Sie den Schieberegler, um die Kopierpriorität für den Kopiervorgang festzulegen.

   Die Kopierpriorität legt fest, wie viele der Systemressourcen zum Abschluss des Vorgangs „Copy Volume“ im Vergleich zu Service-I/O-Anforderungen verwendet werden.

Mehr zu den Prioritätsraten für Kopien

Es gibt fünf Prioritätsstufen für Kopien:

- Am Niedrigsten
- Niedrig
- Mittel
- Hoch
- Höchste

Wenn die Kopierpriorität auf die niedrigste Rate eingestellt ist, wird die I/O-Aktivität priorisiert und der Vorgang des Kopiervolumens dauert länger. Wenn die Kopierpriorität auf die höchste Rate eingestellt ist, wird der Kopiervolume-Vorgang priorisiert, aber die I/O-Aktivität für das Speicherarray kann davon betroffen sein.

5. Wählen Sie aus, ob Sie eine Online-Kopie oder eine Offline-Kopie erstellen möchten. Um eine Online-Kopie zu erstellen, aktivieren Sie das Kontrollkästchen **Quellvolumen während des Kopiervorgangs online halten**.
6. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie zum Ausführen eines Kopiervorgangs „*Online*“ auf **Weiter**, um mit dem Dialogfeld „Reserve Capacity*“ fortzufahren.
   - Um einen Kopiervorgang *offline* durchzuführen, klicken Sie auf **Fertig stellen**, um die Offline-Kopie zu starten.
7. Wenn Sie eine Online-Kopie erstellen möchten, legen Sie die reservierte Kapazität fest, die zum Speichern von Daten und anderen Informationen für die Online-Kopie benötigt wird, und klicken Sie dann auf **Fertig stellen**, um die Online-Kopie zu starten.

   In der Tabelle für Volume-Kandidaten werden nur die Kandidaten angezeigt, die die angegebene reservierte Kapazität unterstützen. Reservierte Kapazität ist die zugewiesene physische Kapazität, die für jeden Kopierdienst- und Storage-Objekt verwendet wird. Er ist nicht direkt vom Host lesbar.

   Weisen Sie die reservierte Kapazität mithilfe folgender Richtlinien zu:

   - Die Standardeinstellung für die reservierte Kapazität ist 40 % der Kapazität des Basis-Volumes, und in der Regel reicht diese Kapazität aus.
   - Die reservierte Kapazität kann jedoch je nach Anzahl der Änderungen an den ursprünglichen Daten variieren. Je länger ein Storage-Objekt aktiv ist, desto größer sollte die reservierte Kapazität sein.

Ergebnisse

System Manager kopiert alle Daten vom Quell-Volume auf das Ziel-Volume. Nachdem der Vorgang des Copy-Volume abgeschlossen ist, wird das Ziel-Volume automatisch schreibgeschützt für die Hosts.

Nachdem Sie fertig sind

Wählen Sie MENU:Home[Vorgänge in Bearbeitung anzeigen], um den Fortschritt des Vorgangs „Copy Volume“ anzuzeigen. Dieser Vorgang kann langwierig sein und die System-Performance beeinträchtigen.

Führen Sie Maßnahmen bei einem Kopiervolume durch

Sie können einen Kopiervolume-Vorgang in Bearbeitung anzeigen und beenden, Priorität

ändern, neu kopieren oder einen Kopiervorgang löschen.

Schritte

1. Wählen Sie MENU:Startseite[Vorgänge in Bearbeitung anzeigen].

   Das Dialogfeld „laufende Vorgänge“ wird angezeigt.

2. Suchen Sie den Vorgang zum Kopieren von Volumes, auf den Sie eine Aktion ausführen möchten, und klicken Sie dann in der Spalte **Aktionen** auf den Link, um eine der folgenden Aktionen durchzuführen.

   Lesen Sie den gesamten Vorsichtstext in Dialogen, insbesondere beim Beenden einer Operation.

Aktion	Beschreibung
Hör Auf	Sie können einen Kopiervolumenvorgang beenden, während der Vorgang den Status „wird ausgeführt“, „Ausstehend“ oder „Fehlgeschlagen“ hat. Wenn das Copy-Volume angehalten wird, haben alle zugeordneten Hosts Schreibzugriff auf das Quell-Volume. Wenn Daten auf das Quell-Volume geschrieben werden, entsprechen die Daten auf dem Ziel-Volume nicht mehr den Daten auf dem Quell-Volume.
Priorität ändern	Sie können die Priorität eines Kopiervolume-Vorgangs ändern, während der Vorgang den Status „wird ausgeführt“ hat, um die Rate auszuwählen, mit der ein Kopiervolume abgeschlossen wird.
Erneut kopieren	Sie können ein Volume erneut kopieren, wenn Sie einen Kopiervorgang angehalten haben und es erneut starten möchten, oder wenn ein Kopiervorgang fehlgeschlagen oder angehalten wurde. Der Kopiervorgang startet von Anfang an. Die Aktion zum erneuten Kopieren überschreibt vorhandene Daten auf dem Ziel-Volume und schlägt ggf. alle dem Ziel-Volume zugeordneten Snapshot-Volumes fehl.
Löschen	Sie können den Vorgang „Volume kopieren“ entfernen, während der Vorgang den Status „wird ausgeführt“, „Ausstehend“ oder „Fehlgeschlagen“ hat. Achten Sie darauf, dass Sie diese Operation vor der Auswahl von **Löschen** tun möchten. Es gibt kein Bestätigungsdialogfeld.

FAQs

Was ist ein Volume?

Ein Volume ist ein Container, in dem Applikationen, Datenbanken und Filesysteme Daten speichern. Dies ist die logische Komponente, die erstellt wird, damit der Host auf den Speicher des Speicherarrays zugreifen kann.

Ein Volume wird auf Basis der Kapazität erstellt, die in einem Pool oder einer Volume-Gruppe verfügbar ist. Ein

Volume verfügt über eine definierte Kapazität. Obwohl ein Volume aus mehr als einem Laufwerk bestehen kann, wird ein Volume als eine logische Komponente für den Host angezeigt.

Warum sehe ich einen Fehler bei der Überzuweisung, wenn ich genügend freie Kapazität in einer Volume-Gruppe habe, um Volumes zu erstellen?

Die ausgewählte Volume-Gruppe kann einen oder mehrere freie Kapazitätsbereiche haben. 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.

Wenn eine Volume-Gruppe über freie Kapazitätsbereiche verfügt, enthält das Volume-Gruppendiagramm einen Link, der die Anzahl der vorhandenen freien Kapazitätsbereiche angibt. Wählen Sie den Link aus, um ein Popup-Fenster anzuzeigen, in dem die Kapazität der einzelnen Bereiche angezeigt wird.

Durch die Konsolidierung der freien Kapazität können Sie zusätzliche Volumes aus der maximalen freien Kapazität in einer Volume-Gruppe erstellen. Sie können die vorhandene freie Kapazität in einer ausgewählten Volume-Gruppe mit einer der folgenden Methoden konsolidieren:

- Wenn für eine Volume-Gruppe mindestens ein freier Kapazitätsbereich erkannt wird, erscheint die Empfehlung „freie Kapazität konsolidieren“ auf der Startseite im Benachrichtigungsbereich. Klicken Sie auf den Link **freie Kapazität konsolidieren**, um das Dialogfeld zu starten.
- Sie können auch Menü:Pools & Volume Groups [Sonstige Aufgaben > freie Kapazität der Volumengruppe konsolidieren] wählen, um das Dialogfeld zu starten.

Wenn Sie einen bestimmten freien Kapazitätsbereich anstelle des größten Bereichs mit freier Kapazität verwenden möchten, verwenden Sie das Command Line Interface (CLI).

Wie wirkt sich mein ausgewählter Workload auf die Erstellung des Volumes aus?

Während der Erstellung eines Volumes werden Sie aufgefordert, Informationen über die Verwendung eines Workloads einzugeben. 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 File System der Virtual Machine 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 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 sind diese Volumen 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.

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.

Wie können durch die Bereitstellung dieser Informationen Speicher erstellt werden?

Die Workload-Informationen werden verwendet, um die Volume-Merkmale wie I/O-Typ, Segmentgröße und Lese-/Schreib-Cache für den ausgewählten Workload zu optimieren. Diese optimierten Eigenschaften bestimmen, wie Ihr Workload mit den Storage Array-Komponenten interagiert.

Basierend auf den von Ihnen bereitgestellten Workload-Informationen erstellt der System Manager die entsprechenden Volumes und platziert sie in den verfügbaren Pools oder Volume-Gruppen, die derzeit im

System vorhanden sind. Das System erstellt die Volumes und optimiert ihre Eigenschaften auf Grundlage der aktuellen Best Practices für den ausgewählten Workload.

Bevor Sie das Erstellen von Volumes für einen bestimmten Workload abgeschlossen haben, können Sie die empfohlene Volume-Konfiguration prüfen und im Dialogfeld Volumes und -Eigenschaften hinzufügen/bearbeiten, hinzufügen oder löschen, die vom System empfohlen werden.

Informationen zu Best Practices finden Sie in Ihrer anwendungsspezifischen Dokumentation.

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.

Warum sehe ich nicht alle meine Pools und/oder Volume-Gruppen?

Ein Pool oder eine Volume-Gruppe, in die Sie das Volume nicht verschieben können, wird in der Liste nicht angezeigt.

Pools oder Volume-Gruppen können aus folgenden Gründen nicht ausgewählt werden:

- Die Data Assurance (da)-Funktionen eines Pools oder Volume-Gruppen-Pools stimmen nicht überein.
- Ein Pool oder eine Volume-Gruppe befindet sich in einem nicht optimalen Zustand.
- Die Kapazität eines Pools oder einer Volume-Gruppe ist zu klein.

Was ist Segmentgröße?

Ein Segment ist die Datenmenge in Kilobyte (KiB), die auf einem Laufwerk gespeichert ist, bevor das Speicherarray auf das nächste Laufwerk im Stripe (RAID-Gruppe) verschoben wird. Die Segmentgröße gilt nur für Volume-Gruppen, nicht für Pools.

Die Segmentgröße wird durch die Anzahl der enthaltenen Datenblöcke festgelegt. Bei der Bestimmung der Segmentgröße müssen Sie wissen, welche Datentypen in einem Volume gespeichert werden sollen. Wenn eine Applikation typischerweise kleine zufällige Lese- und Schreibvorgänge (IOPS) verwendet, funktioniert ein kleineres Segment in der Regel besser. Wenn die Applikation über umfangreiche sequenzielle Lese- und Schreibvorgänge (Durchsatz) verfügt, sind große Segmente im Allgemeinen besser.

Unabhängig davon, ob eine Applikation kleine zufällige Lese- und Schreibvorgänge oder große sequenzielle Lese- und Schreibvorgänge verwendet, liefert das Storage Array eine bessere Performance, wenn das Segment größer ist als die typische Größe der Datenblöcke. Üblicherweise erfolgen die Laufwerke einfacher und schneller auf die Daten, was für eine bessere Performance des Storage-Arrays wichtig ist.

Umgebungen, in denen die IOPS-Performance wichtig ist

In einer IOPS-Umgebung (I/O Operations per Second) ist das Storage Array besser, wenn Sie eine Segmentgröße verwenden, die größer ist als die typische Blockgröße („`Chunk`"), die auf ein Laufwerk geschrieben wird. So wird sichergestellt, dass jeder Block auf ein einziges Laufwerk geschrieben wird.

Umgebungen, in denen der Durchsatz wichtig ist

In einer Durchsatzumgebung sollte die Segmentgröße einen geraden Bruchteil der gesamten Laufwerke für Daten und eine typische Datenstückgröße (I/O-Größe) betragen. Dies verteilt die Daten als ein einziger Stripe über die Laufwerke der Volume-Gruppe, was zu schnelleren Lese- und Schreibvorgängen führt.

Was ist Ihre bevorzugte Controller-Inhaberschaft?

Der bevorzugte Controller-Besitz definiert den Controller, der als Eigentümer des Volume oder als primärer Controller bestimmt ist.

Die Eigentümerschaft der Controller ist sehr wichtig und sollte sorgfältig geplant werden. Controller sollten für eine GesamtI/OS so eng wie möglich ausgeglichen werden.

Wenn ein Controller beispielsweise in erster Linie große, sequenzielle Datenblöcke liest und der andere Controller kleine Datenblöcke mit häufigen Lese- und Schreibvorgängen hat, unterscheiden sich die Lasten sehr. Wenn Sie wissen, welche Volumes welche Art von Daten enthalten, können Sie I/O-Transfers gleichmäßig über beide Controller verteilen.

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 Performance erreichen, indem Sie ein Volume so einstellen, dass eine 4KiB-Blockgröße vorliegt. Achten Sie jedoch darauf, dass Ihr Host 4KiB-Blöcke (oder „`4Kn`“) zulässt.

- 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.

Hosts und Host-Cluster

Übersicht über Hosts und Host-Cluster

Sie können Hosts und Host-Cluster konfigurieren, die die Verbindungen zwischen dem Speicher-Array und den Datenservern definieren.

Was sind Hosts und Host Cluster?

Ein *Host* ist ein Server, der I/O zu einem Volume auf einem Storage Array sendet. Ein_Host-Cluster_ ist eine Gruppe von Hosts, die Sie erstellen können, um dieselben Volumes mehreren Hosts zuzuweisen.

Weitere Informationen:

- "Hostterminologie"
- "Zugriff auf Volumes"
- "Maximale Anzahl an LUNs"

Wie konfiguriere ich Hosts und Host Cluster?

Um Host-Verbindungen zu definieren, können Sie im Menü Storage[Hosts] den Host manuell konfigurieren. Wenn mindestens zwei Hosts den Zugriff auf dieselbe Gruppe von Volumes gemeinsam nutzen möchten, können Sie dann einen Cluster definieren und die Volumes diesem Cluster zuweisen.

Weitere Informationen:

- "Manuelle Hosterstellung"
- "Wie Volumes Hosts und Host-Clustern zugewiesen werden"
- "Workflow für Host-Erstellung und Volume-Zuweisung"
- "Host manuell erstellen"
- "Erstellen Sie den Host-Cluster"
- "Weisen Sie Hosts Volumes zu"

Verwandte Informationen

Weitere Informationen zu Aufgaben für Hosts:

- "Automatische Lastverteilung festlegen"
- "Legen Sie die Berichterstellung für Host-Konnektivität fest"
- "Ändern des Standard-Hosttyps"

Konzepte

Hostterminologie

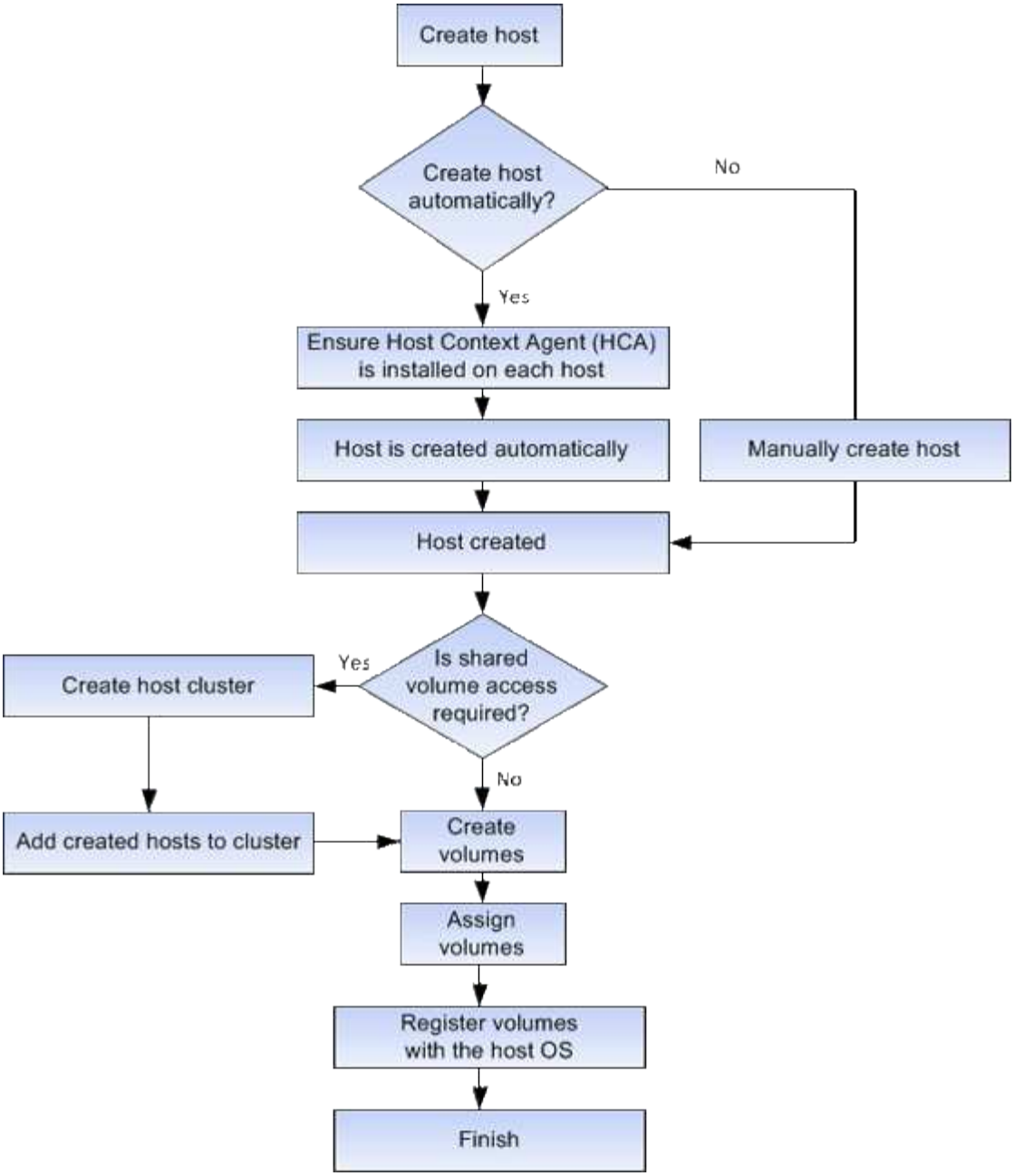
Erfahren Sie, wie die Host-Bedingungen auf Ihr Storage Array zutreffen.

Komponente	Definition
Host	Ein Host ist ein Server, der I/O an ein Volume auf einem Storage-Array sendet.
Host-Name	Der Hostname sollte dem Systemnamen des Hosts entsprechen.
Host-Cluster	Ein Host-Cluster ist eine Gruppe von Hosts. Sie erstellen ein Host-Cluster, damit Sie mehrere Hosts dieselben Volumes ganz einfach zuweisen können.
Host-Schnittstellenprotokoll	Ein Host-Schnittstellenprotokoll ist die Verbindung (wie Fibre Channel, iSCSI usw.) zwischen den Controllern und den Hosts.
HBA oder Netzwerkschnittstellenkarte (NIC)	Ein Host Bus Adapter (HBA) ist eine Platine, die sich auf einem Host befindet und einen oder mehrere Host-Ports enthält.
Host-Port	Ein Host Port ist ein Port an einem Host Bus Adapter (HBA), der die physische Verbindung zu einem Controller bereitstellt und für I/O-Vorgänge genutzt wird.
Host-Port-ID	Eine Host-Port-ID ist ein eindeutiger weltweiter Name, der jedem Host-Port an einem Host Bus Adapter (HBA) zugeordnet ist. • ISCSI-Host-Port-IDs (Internet Small Computer System Interface) müssen 1 bis 233 Zeichen lang sein. ISCSI-Host-Port-IDs werden im Standard-IQN-Format angezeigt (z. B. `iqn.xxx.com.xxx:8b3ad`). • Nicht-iSCSI-Host-Port-IDs wie Fibre Channel und Serial Attached SCSI (SAS) werden nach jeweils zwei Zeichen (z. B. `xx:yy:zz`). Die Fibre-Channel-Host-Port-IDs müssen 16 Zeichen lang sein.
Host-Betriebssystem-Typ	Der Host-Betriebssystemtyp ist eine Konfigurationseinstellung, die definiert, wie die Controller im Speicher-Array auf I/O reagieren, abhängig vom Betriebssystem (oder Variante) des Hosts. Dies wird manchmal auch als *Host type* kurz bezeichnet.

Komponente	Definition
Controller-Host-Port	Ein Controller-Host-Port ist ein Port am Controller, der die physische Verbindung zu einem Host bereitstellt und für I/O-Vorgänge verwendet wird.
LUN	Eine Logical Unit Number (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.

Workflow für Host-Erstellung und Volume-Zuweisung

Die folgende Abbildung zeigt die Konfiguration des Hostzugriffs.



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. Sie können einen Host nur manuell erstellen.

Manuelle Erstellung

Durch die manuelle Hosterstellung können Sie sicherstellen, dass die Host-Port-IDs, die von den Speicher-Array-Controllern erkannt wurden, den Hosts korrekt zugeordnet sind.

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.

Wie Volumes Hosts und Host-Clustern zugewiesen werden

Damit ein Host oder Host-Cluster I/O an ein Volume sendet, müssen Sie das Volume dem Host oder Host-Cluster zuweisen.

Sie können einen Host oder Host-Cluster auswählen, wenn Sie ein Volume erstellen oder 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 während I/O-Vorgängen als „Adresse“ zwischen dem Host und dem Controller. Sie können LUNs nach der Erstellung des Volume ändern.

Zugriff auf Volumes

Ein Zugriffs-Volume ist ein werkseitig konfiguriertes Volume auf dem Storage-Array, das über die Host-I/O-Verbindung für die Kommunikation mit dem Storage-Array und dem Host verwendet wird. Das Zugriffsvolume erfordert eine LUN (Logical Unit Number).

Das Access Volume wird in der folgenden Instanz verwendet:

- **In-Band-Management** — das Zugriffsvolume wird für eine in-Band-Verbindung zur Verwaltung des Speicher-Arrays verwendet. Dies kann nur geschehen, wenn Sie das Storage Array über die Befehlszeilenschnittstelle (CLI) verwalten.

> Für E4000-, EF600-/EF600C- oder EF300/EF300C-Speichersysteme ist das bandinterne Management mit dem Access Volume nicht verfügbar.

Beim ersten Zuweisen eines Volumes zu einem Host wird automatisch ein Zugriffsvolume erstellt. Wenn Sie beispielsweise Volume_1 und Volume_2 einem Host zuweisen, werden beim Anzeigen der Ergebnisse dieser Zuweisung drei Volumes angezeigt (Volume_1, Volume_2 und Access).

Wenn Sie nicht automatisch Hosts erstellen oder ein Speicher-Array in-Band mit der CLI verwalten, brauchen Sie nicht das Zugriffs-Volume, und Sie können die LUN freigeben, indem Sie das Zugriffs-Volume löschen. Durch diese Aktion werden die Zuweisung von Volume zu LUN sowie alle bandinternen Managementverbindungen zum Host entfernt.

Maximale Anzahl an LUNs

Das Speicher-Array verfügt über eine maximale Anzahl an LUNs (Logical Unit Numbers), die für jeden Host verwendet werden können.

Die maximale Anzahl hängt vom Betriebssystem des Hosts ab. Das Speicher-Array verfolgt die Anzahl der verwendeten LUNs. Wenn Sie versuchen, einem Host ein Volume zuzuweisen, der die maximale Anzahl von LUNs überschreitet, kann der Host nicht auf das Volume zugreifen.

Standard-Host-Betriebssystem

Der standardmäßige Hosttyp wird vom Speicher-Array verwendet, wenn Hosts zunächst verbunden sind. Es definiert, wie die Controller im Storage-Array mit dem Betriebssystem des Hosts arbeiten, wenn auf Volumes zugegriffen wird.

Sie können den Host-Typ ändern, wenn Sie den Betrieb des Storage-Arrays relativ zu den mit dem Array verbundenen Hosts ändern müssen. Im Allgemeinen ändern Sie den Standard-Hosttyp, bevor Sie Hosts mit dem Speicher-Array verbinden oder wenn Sie zusätzliche Hosts verbinden.

Beachten Sie folgende Richtlinien:

- Wenn alle Hosts, die Sie eine Verbindung zum Storage Array herstellen möchten, dasselbe Betriebssystem (homogene Host-Umgebung) verwenden möchten, ändern Sie den Host-Typ entsprechend dem Betriebssystem.
- Falls Hosts mit verschiedenen Betriebssystemen vorhanden sind, für die eine Verbindung zum Storage Array (heterogene Host-Umgebung) geplant ist, ändern Sie den Host-Typ so, dass er mit der Mehrheit der Betriebssysteme der Hosts übereinstimmt.

  Wenn Sie beispielsweise acht verschiedene Hosts mit dem Speicher-Array verbinden und sechs dieser Hosts ein Windows-Betriebssystem ausführen, müssen Sie Windows als Standardbetriebssystem auswählen.

- Wenn der Großteil der angeschlossenen Hosts eine Mischung verschiedener Betriebssysteme hat, ändern Sie den Hosttyp auf Werkseinstellung.

  Wenn Sie beispielsweise acht verschiedene Hosts mit dem Storage-Array verbinden und zwei dieser Hosts ein Windows-Betriebssystem ausführen, werden drei unter einem VMware Betriebssystem ausgeführt. Und weitere drei führen ein Linux-Betriebssystem aus. Sie müssen als Standard-Host-Betriebssystem Factory Default auswählen.

Konfigurieren Sie den Hostzugriff

Host manuell erstellen

Für Hosts, die nicht automatisch erkannt werden können, können Sie manuell einen Host erstellen. 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.

Über diese Aufgabe

Beachten Sie beim Erstellen eines Hosts die folgenden 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 Menü:Storage[Hosts].
2. Klicken Sie auf Menü:Create[Host].

   Das Dialogfeld Host erstellen wird angezeigt.

3. 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: • **E/A-Schnittstelle auswählen** Im Allgemeinen sollten sich die Host-Ports angemeldet haben und in der 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.

Einstellung	Beschreibung
CHAP-Initiator	(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**. 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 ist CHAP die einzige in System Manager verwendete iSCSI-Authentifizierungsmethode.

4. Klicken Sie Auf **Erstellen**.

Ergebnisse

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>`. Beispiel: Der Standard-Alias für den ersten Port, für den erstellt wurde `host IPT is IPT_1`.

Erstellen Sie den Host-Cluster

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

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 Menü:Storage[Hosts].
2. Wählen Sie Menü:Erstellen[Host-Cluster].

   Das Dialogfeld Host-Cluster erstellen wird angezeigt.

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

   Felddetails

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.

4. 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.

Ergebnisse

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

Weisen Sie Hosts Volumes zu

Sie müssen ein Volume einem Host oder Host-Cluster zuweisen, damit es für I/O-Vorgänge verwendet werden kann. Diese Zuweisung gewährt einem Host oder Host-Cluster Zugriff auf ein oder mehrere Volumes in einem Storage-Array.

Über diese Aufgabe

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 zur langsameren Initialisierung zurückkehren werden. Sie können den Initialisierungsfortschritt über Menü:Startseite[Operationen in Bearbeitung] überprüfen.

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.

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.

Schritte

1. Wählen Sie Menü:Storage[Hosts].
2. 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 die **Filter** Box geben, um bestimmte Volumen leichter zu finden.

3. Aktivieren Sie das Kontrollkästchen neben jedem Volume, das Sie zuweisen möchten, oder aktivieren Sie das Kontrollkästchen in der Tabellenüberschrift, um alle Volumes auszuwählen.
4. 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.

Management von Hosts und Clustern

Ändern des Standard-Hosttyps

Verwenden Sie die Einstellung Standardbetriebssystem ändern, um den Standardhosttyp auf Speicherarray-Ebene zu ändern. Im Allgemeinen ändern Sie den Standard-Hosttyp, bevor Sie Hosts mit dem Speicher-Array verbinden oder wenn Sie zusätzliche Hosts verbinden.

Über diese Aufgabe

Beachten Sie folgende Richtlinien:

- Wenn alle Hosts, die Sie eine Verbindung zum Storage Array herstellen möchten, dasselbe Betriebssystem (homogene Host-Umgebung) verwenden möchten, ändern Sie den Host-Typ entsprechend dem Betriebssystem.
- Falls Hosts mit verschiedenen Betriebssystemen vorhanden sind, für die eine Verbindung zum Storage Array (heterogene Host-Umgebung) geplant ist, ändern Sie den Host-Typ so, dass er mit der Mehrheit der Betriebssysteme der Hosts übereinstimmt.

  Wenn Sie beispielsweise acht verschiedene Hosts mit dem Speicher-Array verbinden und sechs dieser Hosts ein Windows-Betriebssystem ausführen, müssen Sie Windows als Standardbetriebssystem auswählen.

- Wenn der Großteil der angeschlossenen Hosts eine Mischung verschiedener Betriebssysteme hat, ändern Sie den Hosttyp auf Werkseinstellung.

  Wenn Sie beispielsweise acht verschiedene Hosts mit dem Storage-Array verbinden und zwei dieser Hosts ein Windows-Betriebssystem ausführen, werden drei unter einem VMware Betriebssystem ausgeführt. Und weitere drei führen ein Linux-Betriebssystem aus. Sie müssen als Standard-Host-Betriebssystem Factory Default auswählen.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Blättern Sie nach unten zu **zusätzliche Einstellungen**, und klicken Sie dann auf **Standardbetriebssystemtyp ändern**.
3. Wählen Sie den Host-Betriebssystem-Typ aus, den Sie als Standard verwenden möchten.
4. Klicken Sie Auf **Ändern**.

Zuweisung von Volumes aufheben

Heben Sie die Zuweisung von Volumes von Hosts oder Host Clustern auf, wenn Sie keinen I/O-Zugriff mehr vom Host oder Host-Cluster auf dieses Volume benötigen.

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 Menü:Storage[Hosts].
2. 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.

3. Aktivieren Sie das Kontrollkästchen neben jedem Volume, das Sie aufheben möchten, oder aktivieren Sie das Kontrollkästchen in der Tabellenüberschrift, um alle Volumes auszuwählen.
4. 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.

Host oder Host-Cluster löschen

Sie können einen Host oder Host-Cluster löschen.

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 Menü:Storage[Hosts].
2. Wählen Sie den Host oder Host-Cluster aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.

   Das Bestätigungsdialogfeld wird angezeigt.

3. 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.

Legen Sie die Berichterstellung für Host-Konnektivität fest

Sie können die Berichterstellung für die Host-Konnektivität aktivieren, damit das Storage-Array die Verbindung zwischen den Controllern und den konfigurierten Hosts fortlaufend überwacht. Anschließend werden Sie benachrichtigt, wenn die Verbindung unterbrochen wird. Diese Funktion ist standardmäßig aktiviert.

Über diese Aufgabe

Wenn Sie die Berichterstellung für die Host-Konnektivität deaktivieren, überwacht das System bei einem mit dem Storage-Array verbundenen Host keine Verbindungs- oder Multipath-Treiberprobleme mehr.

> Durch das Deaktivieren der Berichterstellung für Host-Konnektivität wird außerdem der automatische Lastausgleich deaktiviert, der die Ressourcenauslastung des Controllers überwacht und gleichmäßig belastet.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Scrollen Sie nach unten zu **zusätzliche Einstellungen** und klicken Sie dann auf **Host Connectivity Reporting aktivieren/deaktivieren**.

   Der Text unter dieser Option gibt an, ob er derzeit aktiviert oder deaktiviert ist.

   Ein Bestätigungsdialogfeld wird geöffnet.
3. Klicken Sie auf **Ja**, um fortzufahren.

   Wenn Sie diese Option auswählen, schalten Sie die Funktion zwischen aktiviert/deaktiviert ein.

Einstellungen verwalten

Ändern Sie die Einstellungen für einen Host

Sie können den Namen, den Host-Betriebssystemtyp und die zugehörigen Host-Cluster für einen Host ändern.

Schritte

1. Wählen Sie Menü:Storage[Hosts].
2. 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.

3. Wenn er nicht bereits ausgewählt ist, klicken Sie auf die Registerkarte **Eigenschaften**.
4. Ändern Sie die Einstellungen nach Bedarf.

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. Klicken Sie Auf **Speichern**.

Ändern Sie die Einstellungen für ein Host-Cluster

Sie können den Host-Cluster-Namen ändern oder Hosts in einem Host-Cluster hinzufügen oder entfernen.

Schritte

1. Wählen Sie Menü:Storage[Hosts].
2. Wählen Sie den Host-Cluster aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Es wird ein Dialogfeld angezeigt, in dem die aktuellen Host-Cluster-Einstellungen angezeigt werden.

3. Ändern Sie die Einstellungen für das Host-Cluster nach Bedarf.

Felddetails

Einstellung	Beschreibung
Name	Sie können den vom Benutzer bereitgestellten Namen des Host-Clusters angeben. Die Angabe eines Namens für ein Cluster ist erforderlich.
Zugeordnete Hosts	Um einen Host hinzuzufügen, klicken Sie auf das Feld * Associated Hosts* und wählen dann einen Hostnamen aus der Dropdown-Liste aus. Sie können keinen Hostnamen manuell eingeben. Um einen Host zu löschen, klicken Sie neben dem Hostnamen auf **X**.

4. Klicken Sie Auf **Speichern**.

Ändern der Host-Port-IDs für einen Host

Ändern Sie die Host-Port-IDs Wenn Sie die Benutzerbezeichnung auf einer Host-Port-ID ändern möchten, fügen Sie dem Host eine neue Host-Port-ID hinzu oder löschen Sie eine Host-Port-ID vom Host.

Über diese Aufgabe

Beachten Sie beim Ändern der Host-Port-IDs die folgenden Richtlinien:

- **Hinzufügen** — Wenn Sie einen Host-Port hinzufügen, verknüpfen Sie die Host-Port-ID mit dem Host, den Sie für die Verbindung mit Ihrem Speicher-Array erstellt haben. Sie können Portinformationen manuell über ein HBA-Dienstprogramm (Host Bus Adapter) eingeben.
- **Bearbeiten** — Sie können die Host-Ports bearbeiten, um einen Host-Port zu einem anderen Host zu verschieben (zuordnen). Möglicherweise haben Sie den Host Bus Adapter oder iSCSI Initiator auf einen anderen Host verschoben, daher müssen Sie den Host Port zum neuen Host verschieben (zuordnen).
- **Löschen** — Sie können Host-Ports löschen, um Host-Ports von einem Host zu entfernen (unassoziieren).

Schritte

1. Wählen Sie Menü:Storage[Hosts].
2. Wählen Sie den Host aus, dem die Ports zugeordnet werden sollen, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Wenn Sie Ports zu einem Host in einem Host-Cluster hinzufügen möchten, erweitern Sie den Host-Cluster und wählen Sie den gewünschten Host aus. Sie können keine Ports auf Host-Cluster-Ebene hinzufügen.

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

3. Klicken Sie auf die Registerkarte **Host Ports**.

   Im Dialogfeld werden die aktuellen Host-Port-IDs angezeigt.

4. Ändern Sie die Einstellungen für die Host-Port-ID.

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. System Manager 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.

5. Klicken Sie Auf **Speichern**.

FAQs

Was sind Hosts und Host Cluster?

Ein Host ist ein Server, der I/O an ein Volume auf einem Storage-Array sendet. Ein Host-Cluster ist eine Gruppe von Hosts. Sie erstellen ein Host-Cluster, damit Sie mehrere Hosts dieselben Volumes ganz einfach zuweisen können.

Sie definieren einen Host separat. Es kann entweder eine unabhängige Einheit sein oder zu einem Host-Cluster hinzugefügt werden. Sie können Volumes einem individuellen Host zuweisen oder ein Host kann Teil eines Host-Clusters sein, der Zugriff auf ein oder mehrere Volumes für andere Hosts im Host-Cluster freigibt.

Das Host-Cluster ist eine logische Einheit, die Sie in SANtricity System Manager erstellen. Sie müssen Hosts

zum Host-Cluster hinzufügen, bevor Sie Volumes zuweisen können.

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 (ATTO)	Unterstützt Mac-Betriebssystemversionen mit einem Multipathing-Treiber ATTO Technology, Inc.

Host-Betriebssystem	Betriebssystem und Multipath-Treiber
Windows (ATTO)	Unterstützt Windows-Betriebssysteme mit einem Multipathing-Treiber ATTO Technology, Inc.
FlexArray (ALUA)	Unterstützt ein NetApp FlexArray-System mit ALUA für Multipathing.
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 (Kernel 3.9 oder früher)	Unterstützt Linux-Betriebssysteme mit einer Device Mapper Multipath Failover-Lösung mit einem 3.9 oder früheren Kernel.
Cluster-Fenster (veraltet)	Wenn Ihr Host-Betriebssystem-Typ auf diesen Wert eingestellt ist, verwenden Sie stattdessen die Windows-Einstellung (Cluster oder nicht-Cluster).

Was sind HBAs und Adapter-Ports?

Ein Host Bus Adapter (HBA) ist eine Platine, die sich auf einem Host befindet und einen oder mehrere Host-Ports enthält. Ein Host Port ist ein Port an einem Host Bus Adapter (HBA), der die physische Verbindung zu einem Controller bereitstellt und für I/O-Vorgänge genutzt wird.

Die Adapter-Ports auf dem HBA werden Host-Ports genannt. Die meisten HBAs verfügen entweder über einen oder zwei Host-Ports. Der HBA verfügt über eine eindeutige World Wide Identifier (WWID), und jeder HBA-Host-Port hat eine eindeutige WWID. Die Host-Port-IDs werden verwendet, um den entsprechenden HBA mit dem physischen Host zu verknüpfen, wenn Sie den Host manuell über den SANtricity-System-Manager erstellen.

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.

Wie erstelle ich CHAP-Schlüssel?

Wenn Sie die CHAP-Authentifizierung (Challenge Handshake Authentication Protocol) auf einem iSCSI-Host einrichten, der mit dem Speicher-Array verbunden ist, müssen Sie diesen Initiator-CHAP-Schlüssel für jeden iSCSI-Host erneut eingeben.

Dazu können Sie den System Manager entweder im Rahmen der Operation „Host erstellen“ oder über die Option „Einstellungen anzeigen/bearbeiten“ verwenden.

Wenn Sie die gegenseitige CHAP-Authentifizierung verwenden, müssen Sie auf der Seite Einstellungen auch einen CHAP-Zielschlüssel für das Speicherarray definieren und diesen CHAP-Zielschlüssel auf jedem iSCSI-Host erneut eingeben.

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, müssen Sie das Standardcluster *Not* 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 Standard-Cluster 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 die Berichterstellung über Host-Konnektivität?

Wenn die Berichterstellung für die Host-Konnektivität aktiviert ist, überwacht das Storage-Array fortlaufend die Verbindung zwischen den Controllern und den konfigurierten Hosts und warnt anschließend, wenn die Verbindung unterbrochen wird.

Es kann zu Unterbrechungen der Verbindung kommen, wenn ein lockeres, beschädigtes oder fehlendes Kabel oder ein anderes Problem mit dem Host vorliegt. In diesen Situationen öffnet das System möglicherweise eine Recovery Guru Nachricht:

- **Host Redundancy Lost** — wird geöffnet, wenn einer der Controller nicht mit dem Host kommunizieren kann.
- **Host-Typ falsch** — öffnet sich, wenn der Host-Typ auf dem Speicher-Array falsch angegeben ist, was zu Failover-Problemen führen kann.

Möglicherweise möchten Sie die Berichterstellung für die Host-Konnektivität deaktivieren, wenn das Neubooten eines Controllers länger dauern kann als das Verbindungs-Timeout. Wenn Sie diese Funktion deaktivieren, werden Recovery Gurus-Nachrichten unterdrückt.

> Durch das Deaktivieren der Berichterstellung für Hostkonnektivität wird auch der automatische Lastausgleich deaktiviert, der die Nutzung von Controller-Ressourcen überwacht und ausgeglichen. Wenn Sie jedoch die Berichterstellung für Hostkonnektivität erneut aktivieren, wird die automatische Lastausgleichfunktion nicht automatisch wieder aktiviert.

Snapshots

Snapshots – Überblick

Mit der Snapshot Funktion können zeitpunktgenaue Images von Storage Array Volumes erstellt werden, die für Backups und Tests verwendet werden können.

Was sind Snapshot Images?

Ein *Snapshot Image* ist eine logische Kopie von Volume-Daten, die zu einem bestimmten Zeitpunkt erfasst wurde. Wie bei einem Wiederherstellungspunkt können Sie durch Snapshot Images ein Rollback zu einem bekannten fehlerfreien Datensatz durchführen. Obwohl der Host auf das Snapshot-Image zugreifen kann, kann er nicht direkt lesen oder darauf schreiben.

Weitere Informationen:

- "Funktionsweise von Snapshot-Storage"
- "Snapshot Terminologie"
- "Basis-Volumes, reservierte Kapazität und Snapshot-Gruppen"
- "Snapshot Zeitpläne und Konsistenzgruppen"
- "Snapshot Volumes"

Wie erstelle ich Snapshots?

Sie können manuell ein Snapshot-Image aus einem Basis-Volume oder einer Snapshot-Konsistenzgruppe erstellen. Dieser Vorgang ist über das Menü:Speicherung[Snapshots] verfügbar.

Weitere Informationen:

- "Anforderungen und Richtlinien für Snapshots"
- "Workflow für die Erstellung von Snapshot Images und Volumes"
- "Erstellen Sie ein Snapshot-Image"
- "Planen von Snapshot Images"
- "Erstellen einer Snapshot Konsistenzgruppe"
- "Erstellen eines Snapshot Volumes"

Wie lasse ich Daten von einem Snapshot zurückführen?

Ein *Rollback* ist der Vorgang, bei dem Daten in einem Basis-Volume an einen vorherigen Zeitpunkt zurückgegeben werden. Sie können die Snapshot-Daten über das Menü:Speicher[Snapshots] zurückführen.

Weitere Informationen:

- "Snapshot Rollback"
- "Starten Sie ein Rollback eines Snapshot Image für ein Basisvolumen"
- "Starten Sie ein Rollback eines Snapshot Image für ein Mitglied einer Konsistenzgruppe"

Verwandte Informationen

Weitere Informationen zu Aufgaben im Zusammenhang mit Snapshots:

- "Ändern Sie die reservierte Kapazität für ein Snapshot-Volume"
- "Ändern Sie die reservierte Kapazität einer Snapshot-Gruppe"

Konzepte

Funktionsweise von Snapshot-Storage

Die Snapshot Funktion verwendet Copy-on-Write-Technologie zum Speichern von Snapshot Images und zur Nutzung zugewiesener reservierter Kapazitäten.

Verwendung von Snapshot-Images

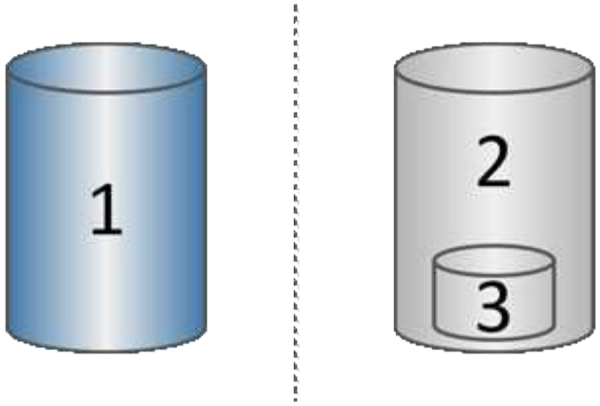
Ein Snapshot-Image ist eine logische, schreibgeschützte Kopie des Volume-Inhalts, die zu einem bestimmten Zeitpunkt erfasst wurde. Sie können Snapshots zum Schutz vor Datenverlust verwenden.

Snapshot Images sind ebenfalls nützlich für Testumgebungen. Es wird eine virtuelle Kopie von Daten erstellt, sodass Daten mithilfe des Snapshots getestet werden können, ohne das eigentliche Volume selbst zu ändern. Darüber hinaus haben Hosts keinen Schreibzugriff auf Snapshot-Images, so dass Ihre Snapshots immer eine sichere Backup-Ressource sind.

Erstellung des Snapshots

Während Snapshots erstellt werden, speichert die Snapshot Funktion Bilddaten wie folgt:

- Ein erstelltes Snapshot Image entspricht genau dem Basis-Volume. Die Snapshot Funktion verwendet Copy-on-Write-Technologie. Nach der Erstellung eines Snapshots werden bei dem ersten Schreibvorgang eines oder mehrere Blöcke in das Basis-Volume die Originaldaten in die reservierte Kapazität kopiert, bevor die neuen Daten in das Basis-Volume geschrieben werden.
- Nachfolgende Snapshots enthalten nur geänderte Datenblöcke. Bevor Daten auf dem Basis-Volume überschrieben werden, verwendet die Snapshot-Funktion ihre Copy-on-Write-Technologie, um die erforderlichen Bilder der betroffenen Sektoren auf die Snapshot-reservierte Kapazität zu speichern.



[1] Basis-Volume (physische Festplattenkapazität); [2] Snapshots (logische Festplattenkapazität); [3] reservierte Kapazität (physische Festplattenkapazität)

- Die reservierte Kapazität speichert die ursprünglichen Datenblöcke für Teile des Basis-Volumes, die nach dem Erstellen des Snapshots geändert wurden, und enthält einen Index zum Nachverfolgen von Änderungen. Im Allgemeinen beträgt die Größe der reservierten Kapazität standardmäßig 40 % des Basis-Volumes. (Wenn Sie mehr reservierte Kapazität benötigen, können Sie den reservierten Speicherplatz erhöhen.)
- Snapshot Images werden basierend auf ihrem Zeitstempel in einer bestimmten Reihenfolge gespeichert. Nur das älteste Snapshot-Image eines Basis-Volumes kann manuell gelöscht werden.

Snapshot Wiederherstellung

Um Daten auf einem Basis-Volume wiederherzustellen, können Sie entweder ein Snapshot-Volume oder ein Snapshot-Image verwenden:

- **Snapshot Volume** — Wenn Sie gelöschte Dateien abrufen müssen, erstellen Sie ein Snapshot-Volume aus einem bekannten guten Snapshot-Image und weisen Sie es dem Host zu.
- **Snapshot Image** — Wenn Sie ein Basis-Volume zu einem bestimmten Zeitpunkt wiederherstellen müssen, verwenden Sie ein vorheriges Snapshot-Image, um ein Rollback der Daten auf das Basis-Volume durchzuführen.

Snapshot Terminologie

Erfahren Sie, wie die Snapshot-Bedingungen auf Ihr Storage Array angewendet werden.

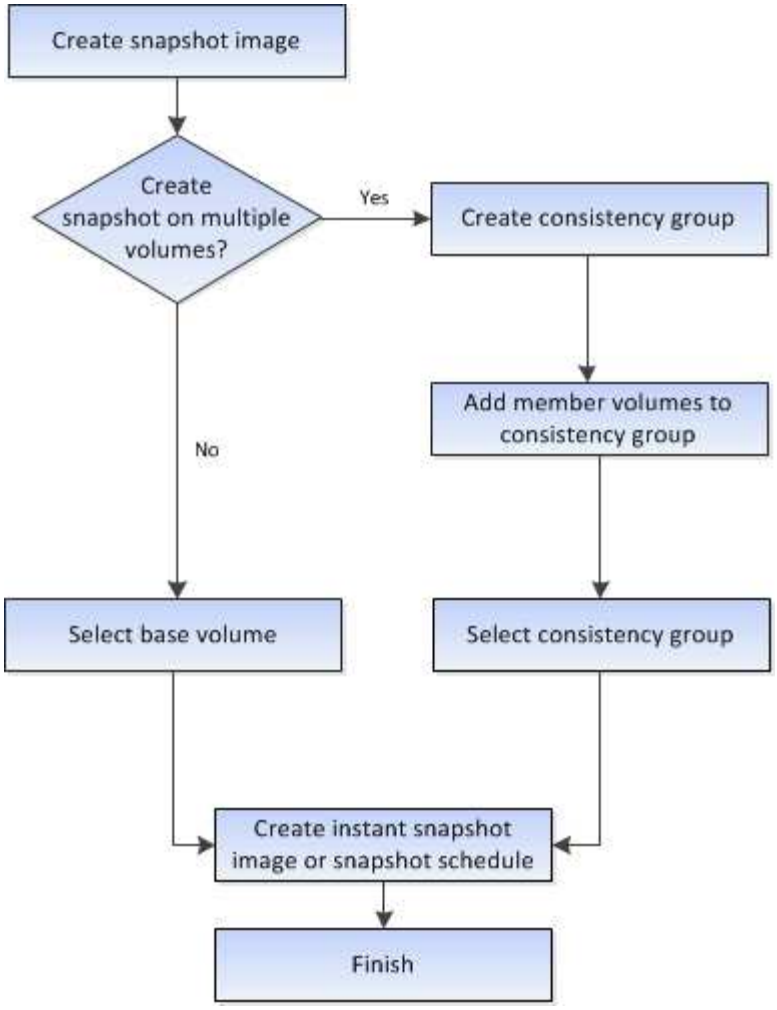
Laufzeit	Beschreibung
Snapshots	Die Snapshot Funktion dient zum Erstellen und Managen von Images von Volumes.
Snapshot Image	Ein Snapshot-Image ist eine logische Kopie der Volume-Daten, die zu einem bestimmten Zeitpunkt erfasst werden. Wie bei einem Wiederherstellungspunkt können Sie durch Snapshot Images ein Rollback zu einem bekannten fehlerfreien Datensatz durchführen. Obwohl der Host auf das Snapshot-Image zugreifen kann, kann er nicht direkt lesen oder darauf schreiben.

Laufzeit	Beschreibung
Basis-Volume	Ein Basis-Volume ist die Quelle, aus der ein Snapshot Image erstellt wird. Es kann sich um ein Thick- oder Thin-Volume handeln, das in der Regel einem Host zugewiesen ist. Das Basis-Volume kann entweder in einer Volume-Gruppe oder im Laufwerk-Pool gespeichert werden.
Snapshot Volume	Ein Snapshot-Volume ermöglicht dem Host den Zugriff auf Daten im Snapshot Image. Das Snapshot Volume verfügt über eine eigene reservierte Kapazität, um alle Änderungen am Basis-Volume ohne Beeinträchtigung des ursprünglichen Snapshot Images zu speichern.
Snapshot-Gruppe	Eine Snapshot-Gruppe ist eine Sammlung von Snapshot Images aus einem einzigen Basis-Volume.
Reserviertes Kapazitäts-Volume	Ein reserviertes Kapazitäts-Volume erfasst, welche Datenblöcke des Basis-Volumes überschrieben werden und welchen Inhalt diese Blöcke erhalten bleiben.
Snapshot Zeitplan	Ein Snapshot-Zeitplan ist ein Zeitplan für das Erstellen von automatischen Snapshot-Images. Über den Zeitplan können Sie die Häufigkeit von Bildkreationen steuern.
Snapshot Konsistenzgruppe	Eine Snapshot Konsistenzgruppe ist eine Sammlung von Volumes, die beim Erstellen eines Snapshot Images als eine Einheit behandelt werden. Jedes dieser Volumes verfügt über ein eigenes Snapshot-Image, jedoch werden alle Bilder zum gleichen Zeitpunkt erstellt.
Mitglied-Volume der Snapshot Konsistenzgruppe	Jedes Volume, das zu einer Snapshot-Konsistenzgruppe gehört, wird als Mitgliedvolume bezeichnet. Wenn Sie einer Snapshot Konsistenzgruppe ein Volume hinzufügen, erstellt System Manager automatisch eine neue Snapshot-Gruppe, die diesem Mitglied-Volume entspricht.
Rollback	Ein Rollback ist der Vorgang, bei dem Daten in einem Basis-Volume an einen vorherigen Zeitpunkt zurückgegeben werden.
Reservierte Kapazität	Reservierte Kapazität ist die zugewiesene physische Kapazität, die für jeden Kopierdienst- und Storage-Objekt verwendet wird. Er ist nicht direkt vom Host lesbar.

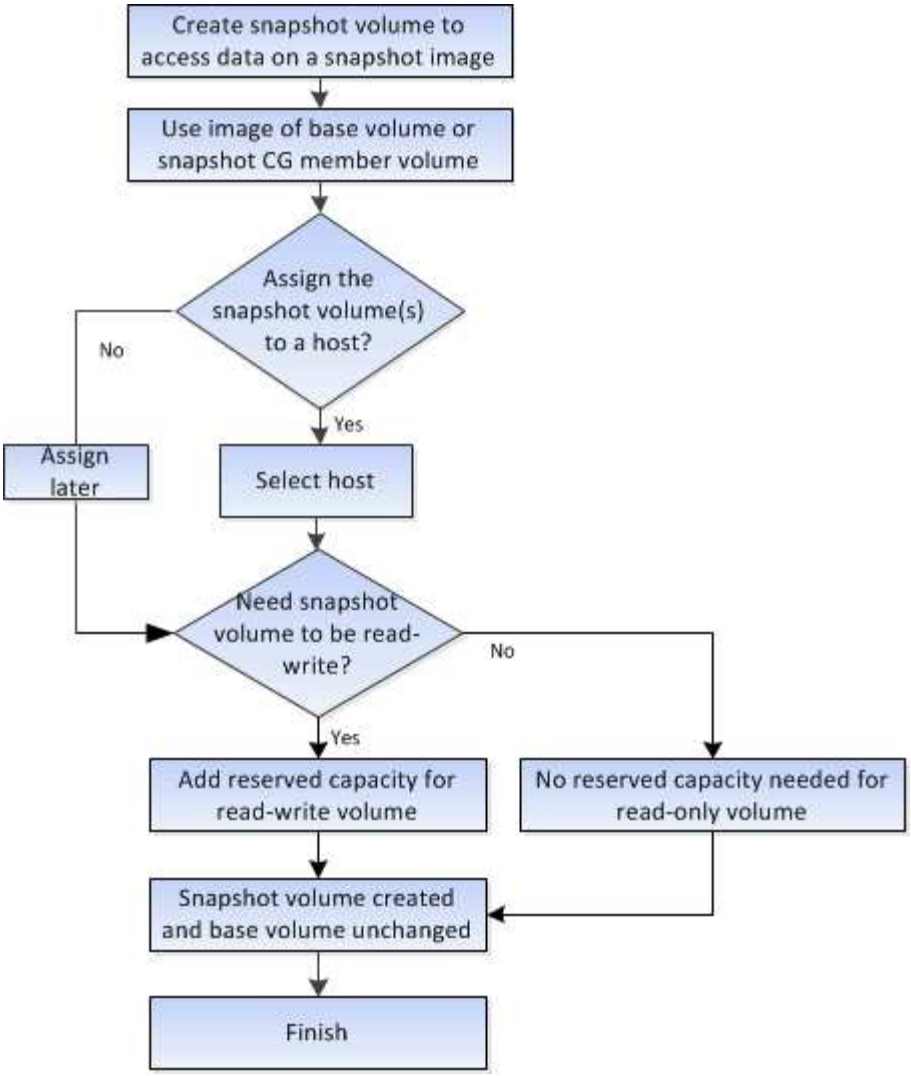
Workflow für die Erstellung von Snapshot Images und Snapshot Volumes

In SANtricity System Manager können Sie Snapshot-Images und Snapshot-Volumes erstellen, indem Sie die folgenden Schritte ausführen.

Workflow zum Erstellen von Snapshot Images



Workflow für die Erstellung von Snapshot Volumes



Anforderungen und Richtlinien für Snapshots

Überprüfen Sie bei der Erstellung und Verwendung von Snapshots die folgenden Anforderungen und Richtlinien.

Snapshot Images und Snapshot Gruppen

- Jedes Snapshot Image ist mit genau einer Snapshot-Gruppe verknüpft.
- Eine Snapshot-Gruppe wird beim ersten Erstellen eines geplanten oder sofortigen Snapshot-Images für ein zugehöriges Objekt erstellt. Dadurch wird reservierte Kapazität erstellt.

  Sie können Snapshot-Gruppen auf der Seite Pools & Volume-Gruppen anzeigen.

- Geplante Snapshot-Images werden nicht ausgeführt, wenn das Speicher-Array offline ist oder ausgeschaltet ist.
- Wenn Sie eine Snapshot-Gruppe mit einem Snapshot-Zeitplan löschen, wird auch der Snapshot-Zeitplan gelöscht.
- Wenn Sie ein Snapshot-Volumen haben, das Sie nicht mehr benötigen, können Sie es zusammen mit beliebiger reservierter Kapazität wiederverwenden, anstatt es zu löschen. Dadurch wird ein anderes Snapshot Volume desselben Basis-Volumes erstellt. Sie können das Snapshot Volume oder das Snapshot Consistency Group Snapshot Volume mit demselben Snapshot Image oder einem anderen Snapshot

Image neu verknüpfen, solange sich das Snapshot Image im selben Basis-Volume befindet.

Snapshot Konsistenzgruppe

- Eine Snapshot Konsistenzgruppe enthält eine Snapshot-Gruppe für jedes Volume, das Mitglied der Snapshot-Konsistenzgruppe ist.
- Sie können eine Snapshot Konsistenzgruppe nur mit einem Zeitplan verknüpfen.
- Wenn Sie eine Snapshot-Konsistenzgruppe löschen, die über einen Snapshot-Zeitplan verfügt, wird auch der Snapshot-Zeitplan gelöscht.
- Sie können eine Snapshot-Gruppe, die einer Snapshot-Konsistenzgruppe zugeordnet ist, nicht einzeln verwalten. Stattdessen müssen Sie die Vorgänge managen (Snapshot Image erstellen, Snapshot Image oder Snapshot-Gruppe löschen und Snapshot-Image zurücksetzen) auf der Ebene der Snapshot-Consistency Group ausführen.

Basis-Volume

- Ein Snapshot-Volume muss dieselben Data Assurance (da) und Sicherheitseinstellungen haben wie das zugehörige Basis-Volume.
- Sie können kein Snapshot-Volume eines ausgefallenen Basis-Volumes erstellen.
- Wenn sich das Basis-Volume auf einer Volume-Gruppe befindet, können sich die Mitglieder-Volumes für eine zugehörige Snapshot-Konsistenzgruppe entweder im Pool oder in der Volume-Gruppe befinden.
- Wenn sich ein Basis-Volume in einem Pool befindet, müssen sich alle Mitglieder-Volumes einer zugehörigen Snapshot-Konsistenzgruppe im selben Pool befinden wie das Basis-Volume.

Reservierte Kapazität

- Die reservierte Kapazität ist nur mit einem Basis-Volume verbunden.
- Die Verwendung eines Zeitplans kann zu einer großen Anzahl von Snapshot Images führen. Stellen Sie sicher, dass Sie über ausreichend reservierte Kapazität für geplante Snapshots verfügen.
- Das für eine Snapshot-Konsistenzgruppe reservierte Kapazitäts-Volume muss dieselben Data Assurance (da) und Sicherheitseinstellungen haben wie das zugehörige Basisvolume für das Mitglied-Volume der Snapshot-Konsistenzgruppe.

Ausstehende Snapshot-Images

Die Erstellung des Snapshot-Images kann unter folgenden Bedingungen im Status „Ausstehend“ verbleiben:

- Das Basis-Volume, das dieses Snapshot Image enthält, ist Mitglied einer asynchronen Spiegelgruppe.
- Das Basisvolume befindet sich derzeit in einem Synchronisierungsvorgang. Die Erstellung des Snapshot-Images ist abgeschlossen, sobald der Synchronisierungsvorgang abgeschlossen ist.

Maximale Anzahl von Snapshot Images

- Wenn ein Volume Mitglied einer Snapshot Konsistenzgruppe ist, erstellt System Manager eine Snapshot Gruppe für das Mitglied-Volume. Diese Snapshot-Gruppe zählt zur maximal zulässigen Anzahl von Snapshot-Gruppen pro Basis-Volume.
- Wenn Sie versuchen, ein Snapshot-Image auf einer Snapshot-Gruppe oder einer Snapshot-Konsistenzgruppe zu erstellen, die zugeordnete Gruppe jedoch die maximale Anzahl an Snapshot-Images erreicht hat, haben Sie zwei Optionen:
  - Aktivieren Sie das automatische Löschen für die Snapshot-Gruppe oder die Snapshot-

Konsistenzgruppe.

- Löschen Sie manuell ein oder mehrere Snapshot Images aus der Snapshot-Gruppe oder der Snapshot-Konsistenzgruppe, und versuchen Sie den Vorgang erneut.

Automatisches Löschen

Wenn die Snapshot-Gruppe oder die Snapshot-Konsistenzgruppe für das automatische Löschen aktiviert ist, löscht System Manager das älteste Snapshot-Image, wenn das System ein neues für die Gruppe erstellt.

Rollback-Vorgang

- Sie können die folgenden Aktionen nicht ausführen, wenn ein Rollback-Vorgang ausgeführt wird:
  - Löschen Sie das Snapshot-Image, das für das Rollback verwendet wird.
  - Erstellen Sie ein neues Snapshot-Image für ein Basis-Volume, das an einem Rollback-Vorgang beteiligt ist.
  - Ändern Sie die Repository-Full-Policy der zugehörigen Snapshot-Gruppe.
- Sie können keinen Rollback-Vorgang starten, wenn einer dieser Vorgänge ausgeführt wird:
  - Kapazitätserweiterung (Hinzufügen von Kapazität zu einem Pool oder einer Volume-Gruppe)
  - Volume-Erweiterung (Erhöhung der Kapazität eines Volumes)
  - Änderung der RAID-Ebene für eine Volume-Gruppe
  - Segmentgröße für ein Volume ändern
- Sie können keinen Rollback-Vorgang starten, wenn das Basisvolume an einer Volume-Kopie beteiligt ist.
- Sie können keinen Rollback-Vorgang starten, wenn das Basisvolume ein sekundäres Volume in einer Remote-Spiegelung ist.
- Ein Rollback-Vorgang schlägt fehl, wenn eine der im zugehörigen Snapshot-Repository-Volume verwendeten Kapazitäten unlesbare Sektoren hat.

Basis-Volumes, reservierte Kapazität und Snapshot-Gruppen

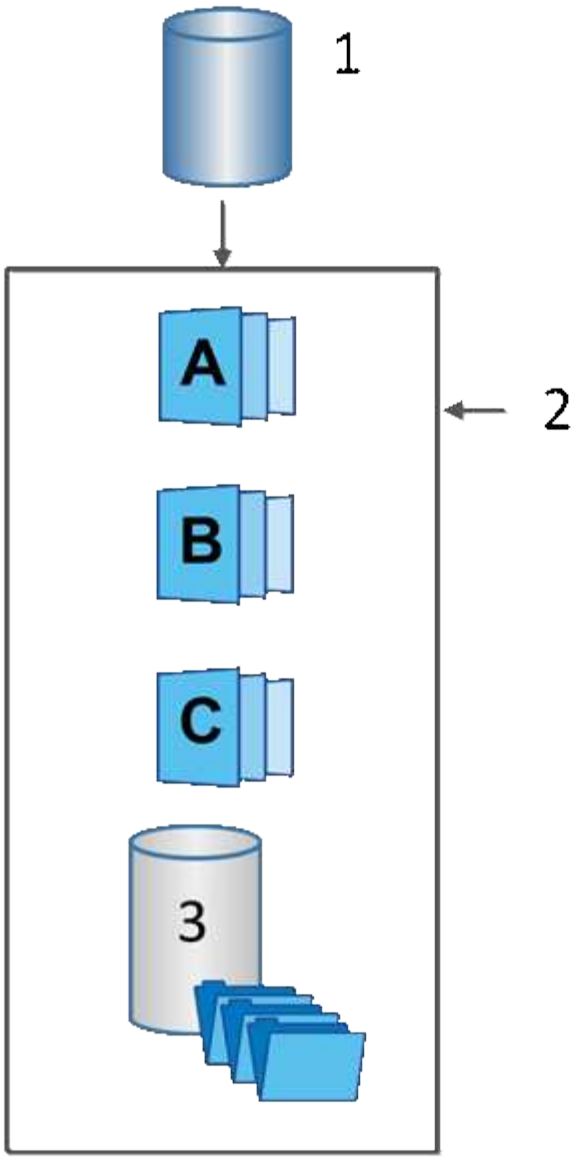
Die Snapshot-Funktion nutzt Basis-Volumes, reservierte Kapazität und Snapshot-Gruppen.

Basis-Volumes

Ein *base Volume* ist das Volume, das als Quelle für ein Snapshot Image verwendet wird. Ein Basis-Volume kann entweder ein Thick Volume oder ein Thin Volume sein und sich entweder in einem Pool oder einer Volume-Gruppe befinden.

Wenn Sie Snapshots des Basis-Volumes erstellen möchten, können Sie jederzeit ein sofortiges Image erstellen oder den Prozess durch die Festlegung eines regelmäßigen Zeitplans für Snapshots automatisieren.

Die folgende Abbildung zeigt die Beziehung zwischen Snapshot Objekten und dem Basis-Volume.



[1] Basis-Volume; [2] Snapshot Objekte in der Gruppe (Images und reservierte Kapazität); [3] reservierte Kapazität für die Snapshot-Gruppe.

Reservierte Kapazität und Snapshot-Gruppen

System Manager organisiert Snapshot Images in *Snapshot Gruppen*. Wenn System Manager die Snapshot-Gruppe erstellt, wird automatisch die zugeordnete *reservierte Kapazität* erstellt, um die Snapshot-Images für die Gruppe aufzubewahren und die nachfolgenden Änderungen an zusätzlichen Snapshots zu verfolgen.

Wenn sich das Basis-Volume in einer Volume-Gruppe befindet, kann die reservierte Kapazität entweder in einem Pool oder in einer Volume-Gruppe gefunden werden. Wenn sich das Basis-Volume in einem Pool befindet, muss sich die reservierte Kapazität im selben Pool wie das Basis-Volume befinden.

Snapshot-Gruppen erfordern keine Benutzeraktion, Sie können jedoch jederzeit die reservierte Kapazität einer Snapshot-Gruppe anpassen. Darüber hinaus werden Sie möglicherweise aufgefordert, eine reservierte Kapazität zu erstellen, wenn die folgenden Bedingungen erfüllt sind:

- Jedes Mal, wenn Sie einen Snapshot eines Basis-Volumes erstellen, das noch keine Snapshot-Gruppe

besitzt, erstellt System Manager automatisch eine Snapshot-Gruppe. Durch diesen Vorgang wird auch die reservierte Kapazität für das Basis-Volume erstellt, mit dem nachfolgende Snapshot Images gespeichert werden.

- Jedes Mal, wenn Sie einen Snapshot-Zeitplan für ein Basis-Volume erstellen, erstellt System Manager automatisch eine Snapshot-Gruppe.

Automatisches Löschen

Verwenden Sie bei der Arbeit mit Snapshots die Standardoption zum automatischen Löschen aktiviert. Durch das automatische Löschen wird automatisch das älteste Snapshot-Image gelöscht, wenn die Snapshot-Gruppe die maximal 32 Bilder der Snapshot-Gruppe erreicht. Wenn Sie die automatische Löschung deaktivieren, werden die Limits für Snapshot-Gruppen schließlich überschritten. Sie müssen manuelle Aktionen durchführen, um die Einstellungen für Snapshot-Gruppen zu konfigurieren und die reservierte Kapazität zu managen.

Snapshot Zeitpläne und Snapshot Konsistenzgruppen

Nutzen Sie Zeitpläne für die Erfassung von Snapshot Images und managen Sie mithilfe von Snapshot Konsistenzgruppen mehrere Basis-Volumes.

Zur einfachen Verwaltung von Snapshot-Vorgängen für Basis-Volumes können Sie folgende Funktionen verwenden:

- **Snapshot Schedule** — automatisierte Snapshots für ein einzelnes Basis-Volume.
- **Snapshot Consistency Group** — Verwalten Sie mehrere Basis-Volumes als eine Einheit.

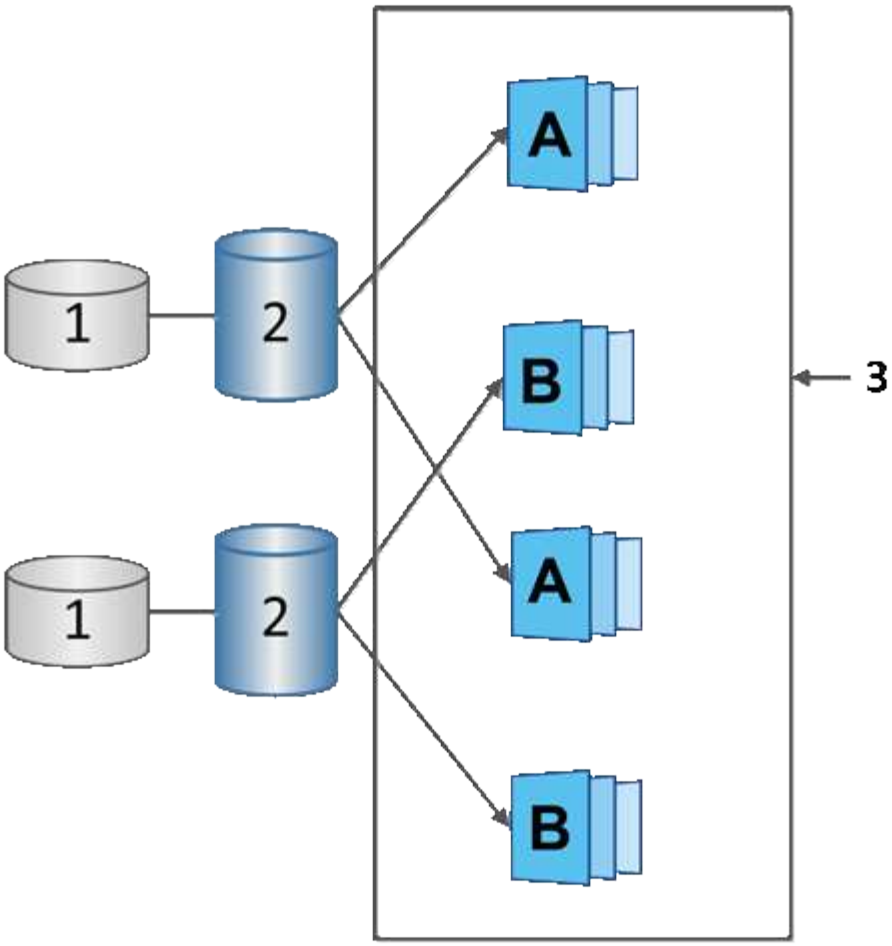
Snapshot Zeitplan

Wenn Sie automatisch Snapshots für ein Basis-Volume erstellen möchten, können Sie einen Zeitplan erstellen. Sie können beispielsweise einen Zeitplan festlegen, der jeden Samstag um Mitternacht, am ersten jeden Monat oder an beliebigen Daten und Uhrzeiten Snapshot-Bilder erstellt. Nachdem die maximale Anzahl von 32 Snapshots für einen einzigen Zeitplan erreicht wurde, können Sie die geplanten Snapshots unterbrechen, mehr reservierte Kapazität erstellen oder Snapshots löschen. Snapshots können manuell oder automatisiert gelöscht werden. Nach dem Löschen eines Snapshot Images steht zusätzliche reservierte Kapazität zur Wiederverwendung zur Verfügung.

Snapshot Konsistenzgruppe

Sie erstellen eine Snapshot-Konsistenzgruppe, wenn Sie sicherstellen möchten, dass Snapshot-Images gleichzeitig auf mehreren Volumes erstellt werden. Aktionen für das Snapshot Image werden auf der gesamten Snapshot-Konsistenzgruppe durchgeführt. Beispielsweise können Sie synchronisierte Snapshots aller Volumes mit dem gleichen Zeitstempel planen. Snapshot-Konsistenzgruppen eignen sich ideal für Applikationen, die mehrere Volumes umfassen, z. B. Datenbankapplikationen, die Protokolle auf einem Volume speichern, und Datenbankdateien auf einem anderen Volume.

Die Volumes, die in einer Snapshot-Konsistenzgruppe enthalten sind, werden als Mitgliedvolumes bezeichnet. Wenn Sie einer Konsistenzgruppe ein Volume hinzufügen, erstellt System Manager automatisch eine neue reservierte Kapazität, die dem entsprechenden Mitglied-Volume entspricht. Sie können einen Zeitplan definieren, in dem automatisch ein Snapshot-Image für jedes Mitgliedsvolume erstellt wird.



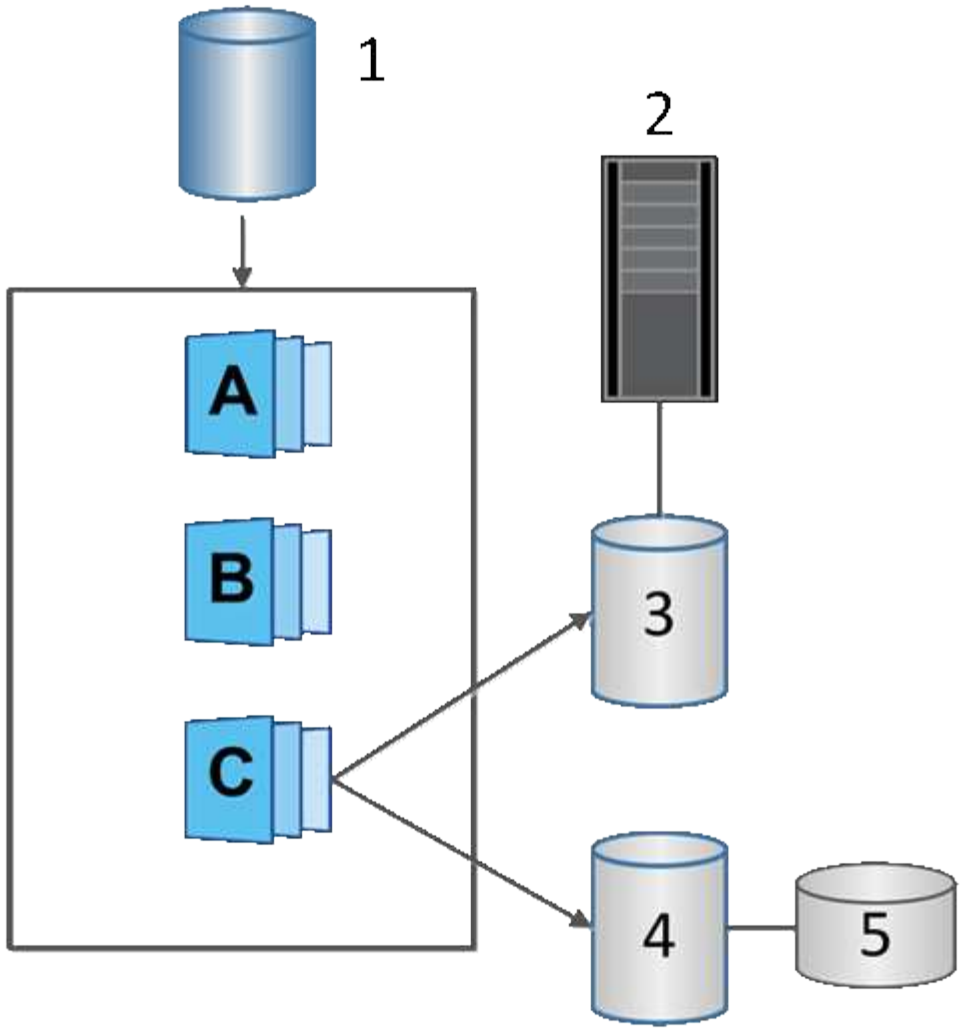
[1] reservierte Kapazität; [2] Member Volume; [3] Snapshot Images der Konsistenzgruppe

Snapshot Volumes

Sie können ein Snapshot-Volume erstellen und einem Host zuweisen, wenn Sie Snapshot-Daten lesen oder schreiben möchten. Das Snapshot Volume verfügt über dieselben Eigenschaften wie das Basis-Volume (RAID-Level, I/O-Eigenschaften usw.).

Wenn Sie ein Snapshot-Volume erstellen, können Sie es als *read-only* oder *read-write Accessible* bezeichnen.

Wenn Sie schreibgeschützte Snapshot Volumes erstellen, müssen Sie keine reservierte Kapazität hinzufügen. Wenn Sie Snapshot-Volumes mit Lese- und Schreibvorgängen erstellen, müssen Sie reservierte Kapazität hinzufügen, um Schreibzugriff zu ermöglichen.



[1] Basis-Volume; [2] Host; [3] schreibgeschütztes Snapshot-Volume; [4] Snapshot-Volume mit Lese- und Schreibzugriff; [5] reservierte Kapazität

Snapshot Rollback

Ein Rollback-Vorgang gibt ein Basisvolumen in einen vorherigen Zustand zurück, der vom ausgewählten Snapshot bestimmt wird.

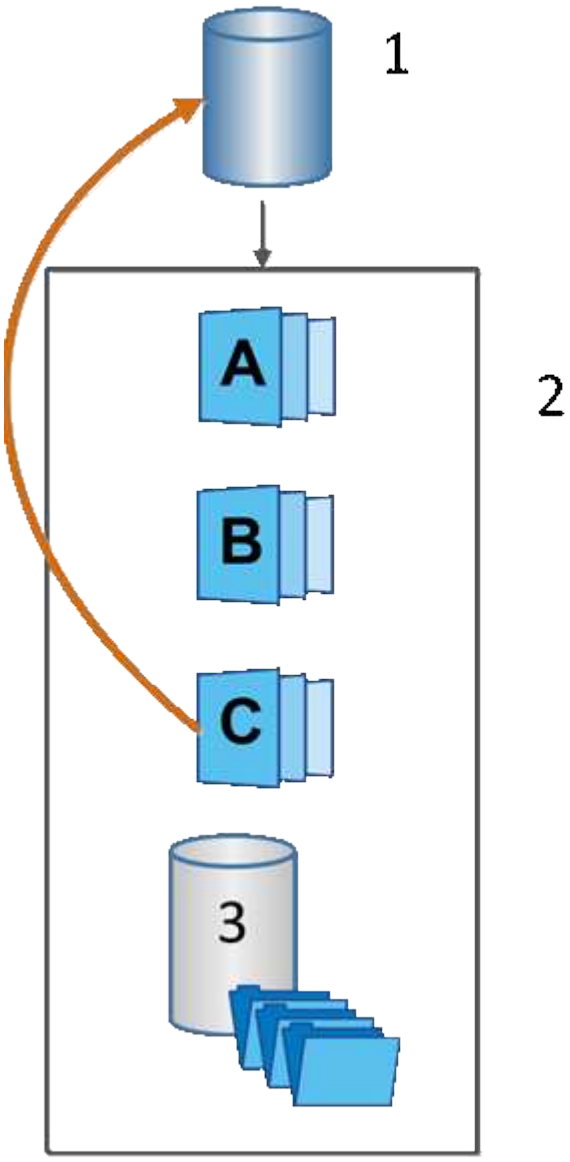
Für das Rollback können Sie ein Snapshot-Bild aus einer der folgenden Quellen auswählen:

- **Snapshot Image Rollback**, für eine vollständige Wiederherstellung eines Basis-Volumes.
- **Snapshot Consistency Group Rollback**, mit dem ein oder mehrere Volumes zurückgesetzt werden können.

Während des Rollback behält die Snapshot-Funktion alle Snapshot-Images in der Gruppe bei. Zudem kann der Host bei diesem Prozess bei Bedarf auf das Basis-Volume zugreifen.

Sobald ein Rollback gestartet wird, wird ein Hintergrundprozess für das Basis-Volume durch die logischen Block-Adressen (LBAs) geleitet und dann werden Copy-on-Write-Daten im Rollback Snapshot Image gefunden, die wiederhergestellt werden sollen. Da auf das Basis-Volume für Lese- und Schreibvorgänge sofort zugegriffen werden kann und alle zuvor geschriebenen Daten sofort zur Verfügung stehen, muss das

reservierte Kapazitäts-Volume so groß sein, dass alle Änderungen bei der Verarbeitung des Rollback berücksichtigt werden. Die Datenübertragung wird im Hintergrund fortgesetzt, bis das Rollback abgeschlossen ist.



[1] Basis-Volume; [2] Snapshot Objekte in einer Gruppe; [3] Snapshot-Gruppe reservierte Kapazität

Erstellen von Snapshots und Snapshot-Objekten

Erstellen von Snapshot Images

Sie können manuell ein Snapshot-Image aus einem Basis-Volume oder einer Snapshot-Konsistenzgruppe erstellen. Dies wird auch als *Instant Snapshot* oder *Instant Image* bezeichnet.

Bevor Sie beginnen

- Das Basis-Volume muss optimal sein.

- Der Antrieb muss optimal sein.
- Die Snapshot-Gruppe kann nicht als „`reserviert.`“ bezeichnet werden.
- Das Volume mit reservierter Kapazität muss über dieselben Data Assurance (da)-Einstellungen wie das zugehörige Basis-Volume für die Snapshot-Gruppe verfügen.

Schritte

1. Führen Sie eine der folgenden Aktionen durch, um ein Snapshot-Image zu erstellen:
   - Wählen Sie Menü:Storage[Volumes]. Wählen Sie das Objekt (Basis-Volume oder Snapshot-Konsistenzgruppe) aus, und wählen Sie dann Menü:Kopierdienste[Instant Snapshot erstellen].
   - Wählen Sie Menü:Storage[Snapshots]. Wählen Sie die Registerkarte **Snapshot Images** und dann Menü:Erstellen[Instant Snapshot].

     Das Dialogfeld Snapshot-Bild erstellen wird angezeigt. Wählen Sie das Objekt aus (Basis-Volume oder Snapshot-Consistency Group) und klicken Sie dann auf **Next**. Wenn ein vorheriges Snapshot Image für die Konsistenzgruppe des Volumes oder Snapshots erstellt wurde, erstellt das System sofort den sofortigen Snapshot. Andernfalls wird das Dialogfeld Snapshot-Bild bestätigen angezeigt, wenn dies das erste Mal ist, wenn ein Snapshot-Image für die Konsistenzgruppe des Volumes oder der Snapshot erstellt wird.

2. Klicken Sie auf **Erstellen**, um die Benachrichtigung zu akzeptieren, dass reservierte Kapazität benötigt wird, und um mit dem Schritt Reserve Kapazität fortzufahren.

   Das Dialogfeld Kapazität reservieren wird angezeigt.

3. Verwenden Sie das Spinner-Feld, um den Kapazitätsprozentsatz anzupassen, und klicken Sie dann auf **Weiter**, um die in der Tabelle hervorgehobene Kandidatenmenge zu akzeptieren.

   Das Dialogfeld Einstellungen bearbeiten wird angezeigt.

4. Wählen Sie die entsprechenden Einstellungen für das Snapshot-Image aus, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

Felddetails

Einstellung	Beschreibung
Snapshot-Bildeinstellungen	Begrenzung des Snapshot Images
Aktivieren Sie das Kontrollkästchen, wenn Snapshot-Bilder nach dem festgelegten Limit automatisch gelöscht werden sollen. Ändern Sie die Begrenzung mit dem Spinner-Feld. Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Erstellung von Snapshot-Bildern nach 32 Bildern angehalten.	**Reservierte Kapazitätseinstellungen**
Benachrichtigen, wenn…	Verwenden Sie die Spinner-Box, um den Prozentpunkt anzupassen, an dem das System eine Warnmeldung sendet, wenn sich die reservierte Kapazität einer Snapshot-Gruppe fast voll befindet. Wenn die reservierte Kapazität der Snapshot-Gruppe den angegebenen Schwellenwert überschreitet, erhöhen Sie mit der Vorankündigung die reservierte Kapazität oder löschen Sie unnötige Objekte, bevor der verbleibende Speicherplatz ausgeht.
Richtlinie für vollständig reservierte Kapazität	Wählen Sie eine der folgenden Richtlinien aus: • **Ältestes Snapshot-Image löschen** — das System entfernt automatisch das älteste Snapshot-Image in der Snapshot-Gruppe, wodurch das Snapshot-Image der reservierten Kapazität zur Wiederverwendung innerhalb der Gruppe freigegeben wird. • **Schreibvorgänge auf Basis-Volume ablehnen** — Wenn die reservierte Kapazität ihren maximalen festgelegten Prozentsatz erreicht, weist das System eine E/A-Schreibanforderung auf das Basis-Volume zurück, das den reservierten Kapazitätszugriff ausgelöst hat.

Ergebnisse

- System Manager zeigt das neue Snapshot-Image in der Tabelle Snapshot Images an. In der Tabelle ist das neue Image nach Zeitstempel und dem zugehörigen Basis-Volume oder der Snapshot Konsistenzgruppe aufgeführt.
- Die Erstellung eines Snapshot kann aufgrund der folgenden Bedingungen in einem Status „Ausstehend“ verbleiben:
  - Das Basis-Volume, das dieses Snapshot Image enthält, ist Mitglied einer asynchronen Spiegelgruppe.

- Das Basisvolume befindet sich derzeit in einem Synchronisierungsvorgang. Die Erstellung des Snapshot-Images ist abgeschlossen, sobald der Synchronisierungsvorgang abgeschlossen ist.

Planen von Snapshot Images

Sie erstellen einen Snapshot-Zeitplan, um die Recovery bei Problemen mit dem Basis-Volume zu ermöglichen und geplante Backups durchzuführen. Snapshots von Basis-Volumes oder Snapshot-Konsistenzgruppen können täglich, wöchentlich oder monatlich erstellt werden, zu jeder Tageszeit.

Bevor Sie beginnen

Das Basis-Volume muss optimal sein.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie ein Snapshot-Zeitplan für eine vorhandene Snapshot-Konsistenzgruppe oder das Basis-Volume erstellt wird.

Sie können auch einen Snapshot-Zeitplan gleichzeitig erstellen, damit Sie ein Snapshot-Image eines Basis-Volumes oder einer Snapshot-Konsistenzgruppe erstellen können.

Schritte

1. Führen Sie eine der folgenden Aktionen aus, um einen Snapshot-Zeitplan zu erstellen:
   - Wählen Sie Menü:Storage[Volumes].

     Wählen Sie das Objekt (Volume oder Snapshot Consistency Group) für diesen Snapshot-Zeitplan aus, und wählen Sie dann Menü:Copy Services[Create Snapshot Schedule].

   - Wählen Sie Menü:Storage[Snapshots].

     Wählen Sie die Registerkarte **Zeitpläne** aus und klicken Sie dann auf **Erstellen**.

2. Wählen Sie das Objekt (Volume oder Snapshot Consistency Group) für diesen Snapshot-Zeitplan aus, und klicken Sie dann auf **Next**.

   Das Dialogfeld Snapshot-Zeitplan erstellen wird angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:
   - **Verwenden Sie einen zuvor definierten Zeitplan aus einem anderen Snapshot-Objekt**.

     Stellen Sie sicher, dass erweiterte Optionen angezeigt werden. Klicken Sie auf **Weitere Optionen anzeigen**. Klicken Sie auf **Zeitplan importieren**, wählen Sie das Objekt mit dem zu importierenden Zeitplan aus und klicken Sie dann auf **Import**.

   - **Ändern Sie die Basis- oder erweiterten Optionen**.

     Klicken Sie im oberen rechten Bereich des Dialogfelds auf **Weitere Optionen anzeigen**, um alle Optionen anzuzeigen, und gehen Sie dann in die folgende Tabelle.

Felddetails

Feld	Beschreibung
Grundeinstellungen	Wählen Sie Tage
Wählen Sie einzelne Wochentage für Snapshot-Bilder aus.	Startzeit
Wählen Sie aus der Dropdown-Liste eine neue Startzeit für die täglichen Snapshots aus (die Auswahl erfolgt in Schritten von einer halben Stunde). Die Startzeit liegt standardmäßig auf eine halbe Stunde vor der aktuellen Zeit.	Zeitzone
Wählen Sie aus der Dropdown-Liste die Zeitzone Ihres Arrays aus.	**Erweiterte Einstellungen**
Tag / Monat	Wählen Sie eine der folgenden Optionen: • **Daily / Weekly** — Wählen Sie einzelne Tage für Synchronisations-Snapshots. Sie können auch das Kontrollkästchen **Alle Tage auswählen** oben rechts auswählen, wenn Sie einen Tagesablauf wünschen. • **Monatlich / jährlich** — Wählen Sie einzelne Monate für Synchronisations-Snapshots aus. Geben Sie im Feld * am Tag(e)* die Tage des Monats ein, an denen Synchronisationen stattfinden sollen. Gültige Eingaben sind **1** bis **31** und **Letzte**. Sie können mehrere Tage durch Komma oder Semikolon voneinander trennen. Verwenden Sie einen Bindestrich für inklusives Datum. Zum Beispiel: 1,3,4,10-15,Last. Sie können auch das Kontrollkästchen **Alle Monate auswählen** oben rechts auswählen, wenn Sie einen monatlichen Zeitplan wünschen.
Startzeit	Wählen Sie aus der Dropdown-Liste eine neue Startzeit für die täglichen Snapshots aus (die Auswahl erfolgt in Schritten von einer halben Stunde). Die Startzeit liegt standardmäßig auf eine halbe Stunde vor der aktuellen Zeit.
Zeitzone	Wählen Sie aus der Dropdown-Liste die Zeitzone Ihres Arrays aus.

Feld	Beschreibung
Snapshots pro Tag/Zeit zwischen Snapshots	Wählen Sie die Anzahl der pro Tag zu erstellenden Snapshot-Bilder aus. Wenn Sie mehrere auswählen, wählen Sie auch die Zeit zwischen Snapshot-Bildern aus. Bei mehreren Snapshot-Images ist darauf zu achten, dass ausreichend Kapazität reserviert ist.
Jetzt Snapshot Image erstellen?	Aktivieren Sie dieses Kontrollkästchen, um zusätzlich zu den von Ihnen erstellten automatischen Bildern ein sofortiges Bild zu erstellen.
Start-/Enddatum oder kein Enddatum	Geben Sie das Startdatum für die Synchronisierung ein. Geben Sie auch ein Enddatum ein oder wählen Sie **kein Enddatum**.

4. Führen Sie eine der folgenden Aktionen aus:
   - Wenn es sich bei dem Objekt um eine Snapshot-Konsistenzgruppe handelt, klicken Sie auf **Erstellen**, um die Einstellungen zu akzeptieren und den Zeitplan zu erstellen.
   - Wenn es sich bei dem Objekt um ein Volume handelt, klicken Sie auf **Weiter**, um die reservierte Kapazität für die Snapshot-Images zuzuweisen.

     In der Tabelle für Volume-Kandidaten werden nur die Kandidaten angezeigt, die die angegebene reservierte Kapazität unterstützen. Reservierte Kapazität ist die zugewiesene physische Kapazität, die für jeden Kopierdienst- und Storage-Objekt verwendet wird. Er ist nicht direkt vom Host lesbar.
5. Verwenden Sie die Spinner-Box, um die reservierte Kapazität für die Snapshot-Bilder zuzuweisen. Führen Sie eine der folgenden Aktionen aus:
   - **Die Standardeinstellungen akzeptieren.**

     Verwenden Sie diese empfohlene Option, um die reservierte Kapazität für die Snapshot-Images mit den Standardeinstellungen zuzuweisen.
   - **Zuweisen Ihrer eigenen reservierten Kapazitätseinstellungen entsprechend Ihren Datenspeicheranforderungen.**

     Wenn Sie die Standardeinstellung für reservierte Kapazität ändern, klicken Sie auf **Kandidaten aktualisieren**, um die Kandidatenliste für die von Ihnen angegebene reservierte Kapazität zu aktualisieren.

     Weisen Sie die reservierte Kapazität mithilfe folgender Richtlinien zu:

     - Die Standardeinstellung für die reservierte Kapazität ist 40 % der Kapazität des Basis-Volume. In der Regel ist diese Kapazität ausreichend.
     - Die benötigte Kapazität ist unterschiedlich, abhängig von der Häufigkeit und Größe der I/O-Schreibvorgänge auf den Volumes sowie von der Menge und Dauer der Snapshot-Image-Erfassung.
6. Klicken Sie Auf **Weiter**.

   Das Dialogfeld Einstellungen bearbeiten wird angezeigt.
7. Bearbeiten Sie die Einstellungen für den Snapshot-Zeitplan nach Bedarf und klicken Sie dann auf **Fertig stellen**.

Felddetails

Einstellung	Beschreibung
Snapshot-Bildlimit	Automatisches Löschen von Snapshot-Images aktivieren, wenn…
Aktivieren Sie das Kontrollkästchen, wenn Snapshot-Bilder nach dem festgelegten Limit automatisch gelöscht werden sollen. Ändern Sie die Begrenzung mit dem Spinner-Feld. Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Erstellung von Snapshot-Bildern nach 32 Bildern angehalten.	**Reservierte Kapazitätseinstellungen**
Benachrichtigen, wenn…	Verwenden Sie das Spinner-Feld, um den Prozentpunkt anzupassen, an dem das System eine Benachrichtigung sendet, wenn sich die reservierte Kapazität eines Zeitplans fast voll befindet. Wenn die reservierte Kapazität für den Zeitplan den angegebenen Schwellenwert überschreitet, verwenden Sie den Vorankündigung, um die reservierte Kapazität zu erhöhen oder um unnötige Objekte zu löschen, bevor der verbleibende Speicherplatz erschöpft ist.
Richtlinie für vollständig reservierte Kapazität	Wählen Sie eine der folgenden Richtlinien aus: • **Ältestes Snapshot-Image löschen** — das System entfernt automatisch das älteste Snapshot-Image, welches die reservierte Kapazität für die Wiederverwendung innerhalb der Snapshot-Gruppe freigibt. • **Schreibvorgänge auf Basis-Volume ablehnen** — Wenn die reservierte Kapazität ihren maximalen festgelegten Prozentsatz erreicht, weist das System eine E/A-Schreibanforderung auf das Basis-Volume zurück, das den reservierten Kapazitätszugriff ausgelöst hat.

Erstellen der Snapshot Konsistenzgruppe

Um sicherzustellen, dass Sie über konsistente Kopien verfügen, können Sie einen Satz von mehreren Volumes erstellen, die als „*Snapshot Consistency Group*“ bezeichnet werden.

Mit dieser Gruppe können Sie zur Wahrung der Konsistenz gleichzeitig Snapshot-Images aller Volumes erstellen. Jedes Volume, das zu einer Snapshot Konsistenzgruppe gehört, wird als „*Member Volume*“ bezeichnet. Wenn Sie einer Snapshot Konsistenzgruppe ein Volume hinzufügen, erstellt das System

automatisch eine neue Snapshot-Gruppe, die diesem Mitglied-Volume entspricht.

Über diese Aufgabe

Mit der Sequenz zur Erstellung von Snapshot-Konsistenzgruppen können Sie Mitglieder-Volumes für die Gruppe auswählen und den Mitglied-Volumes Kapazität zuweisen.

Der Prozess zum Erstellen einer Snapshot-Konsistenzgruppe wird in mehreren Schritten durchgeführt.

Schritt 1: Hinzufügen von Mitgliedern zu der Snapshot-Konsistenzgruppe

Wählen Sie Mitglieder aus, um eine Sammlung von Volumes anzugeben, die die Snapshot-Konsistenzgruppe enthalten. Alle Aktionen, die Sie auf der Snapshot Konsistenzgruppe durchführen, werden gleichmäßig auf ausgewählte Mitglied-Volumes erweitert.

Bevor Sie beginnen

Die Mitgliedvolumes müssen optimal sein.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Klicken Sie auf die Registerkarte **Snapshot Consistency Groups**.
3. Wählen Sie Menü:Erstellen[Snapshot Konsistenzgruppe].

   Das Dialogfeld Snapshot Konsistenzgruppe erstellen wird angezeigt.

4. Wählen Sie die Volumes aus, die der Snapshot-Konsistenzgruppe als Mitgliedvolumes hinzugefügt werden sollen.
5. Klicken Sie auf **Weiter**, und gehen Sie zu Schritt 2: Reservekapazität für Snapshot Konsistenzgruppe.

Schritt 2: Reservekapazität für Snapshot Konsistenzgruppe

Zuweisen der reservierten Kapazität zur Snapshot-Konsistenzgruppe. System Manager legt die Volumes und die Kapazität auf Grundlage der Eigenschaften der Snapshot-Konsistenzgruppe vor. Sie können die empfohlene Konfiguration für reservierte Kapazität akzeptieren oder den zugewiesenen Storage anpassen.

Über diese Aufgabe

Im Dialogfeld „Reserve-Kapazität“ werden in der Tabelle „Volume-Kandidaten“ nur die Kandidaten angezeigt, die die angegebene reservierte Kapazität unterstützen. Reservierte Kapazität ist die zugewiesene physische Kapazität, die für jeden Kopierdienst- und Storage-Objekt verwendet wird. Er ist nicht direkt vom Host lesbar.

Schritte

1. Verwenden Sie die Spinner-Box, um die reservierte Kapazität der Snapshot-Konsistenzgruppe zuzuweisen. Führen Sie eine der folgenden Aktionen aus:
   - **Die Standardeinstellungen akzeptieren**.

     Verwenden Sie diese empfohlene Option, um jedem Mitglied-Volume die reservierte Kapazität mit den Standardeinstellungen zuzuweisen.

   - **Zuweisen Ihrer eigenen reservierten Kapazitätseinstellungen entsprechend Ihren Datenspeicheranforderungen.**

     Weisen Sie die reservierte Kapazität mithilfe der folgenden Richtlinien zu.

- Die Standardeinstellung für die reservierte Kapazität ist 40 % der Kapazität des Basis-Volume. In der Regel ist diese Kapazität ausreichend.
- Die benötigte Kapazität ist unterschiedlich, abhängig von der Häufigkeit und Größe der I/O-Schreibvorgänge auf den Volumes sowie von der Menge und Dauer der Snapshot-Image-Erfassung.

2. **Optional:** Wenn Sie die Einstellung für reservierte Standardkapazität ändern, klicken Sie auf **Kandidaten aktualisieren** um die Kandidatenliste für die von Ihnen angegebene reservierte Kapazität zu aktualisieren.
3. Klicken Sie auf **Weiter**, und gehen Sie zu Schritt 3: Bearbeiten Sie die Einstellungen für die Snapshot Konsistenzgruppe.

Schritt 3: Bearbeiten Sie die Einstellungen für die Snapshot Konsistenzgruppe

Akzeptieren oder wählen Sie die Einstellungen zum automatischen Löschen und die Schwellenwerte für reservierte Kapazitätswarnschwellenwerte für die Snapshot-Konsistenzgruppe aus.

Über diese Aufgabe

Mit der Sequenz zur Erstellung von Snapshot-Konsistenzgruppen können Sie Mitglieder-Volumes für die Gruppe auswählen und den Mitglied-Volumes Kapazität zuweisen.

Schritte

1. Übernehmen Sie die Standardeinstellungen für die Snapshot-Konsistenzgruppe oder ändern Sie diese je nach Bedarf.

Felddetails

Einstellung	Beschreibung
Snapshot Consistency Group Einstellungen	Name
Geben Sie den Namen für die Snapshot Konsistenzgruppe an.	Automatisches Löschen von Snapshot-Images aktivieren, wenn…
Aktivieren Sie das Kontrollkästchen, wenn Snapshot-Bilder nach dem festgelegten Limit automatisch gelöscht werden sollen. Ändern Sie die Begrenzung mit dem Spinner-Feld. Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Erstellung von Snapshot-Bildern nach 32 Bildern angehalten.	**Reservierte Kapazitätseinstellungen**
Benachrichtigen, wenn…	Verwenden Sie die Spinner-Box, um den Prozentpunkt anzupassen, an dem das System eine Warnmeldung sendet, wenn sich die reservierte Kapazität einer Snapshot-Konsistenzgruppe fast voll nähert. Wenn die reservierte Kapazität für die Snapshot Konsistenzgruppe den angegebenen Schwellenwert überschreitet, erhöhen Sie mit der Vorankündigung die reservierte Kapazität oder um unnötige Objekte zu löschen, bevor der verbleibende Speicherplatz erschöpft ist.
Richtlinie für vollständig reservierte Kapazität	Wählen Sie eine der folgenden Richtlinien aus: • **Ältestes Snapshot-Image löschen** — das System entfernt automatisch das älteste Snapshot-Image in der Snapshot-Consistency Group, welches die reservierte Kapazität des Snapshot-Images zur Wiederverwendung innerhalb der Gruppe freigibt. • **Schreibvorgänge auf Basis-Volume ablehnen** — Wenn die reservierte Kapazität ihren maximalen festgelegten Prozentsatz erreicht, weist das System eine E/A-Schreibanforderung auf das Basis-Volume zurück, das den reservierten Kapazitätszugriff ausgelöst hat.

2. Klicken Sie nach der Konfiguration Ihrer Snapshot Consistency Group auf **Finish**.

Erstellen eines Snapshot Volume

Sie erstellen ein Snapshot-Volume, um Host-Zugriff auf ein Snapshot-Image eines Volumes oder einer Snapshot-Konsistenzgruppe zu ermöglichen. Sie können das Snapshot-Volume entweder als schreibgeschützt oder als Lese-/Schreibzugriff festlegen.

Über diese Aufgabe

Mithilfe der Sequenz zur Erstellung von Snapshot Volumes können Sie ein Snapshot Volume aus einem Snapshot Image erstellen und Optionen zur Zuweisung reservierter Kapazität bereitstellen, wenn das Volume gelesen/geschrieben wird. Ein Snapshot Volume kann wie folgt konfiguriert werden:

- Ein schreibgeschütztes Snapshot-Volume ermöglicht einer Host-Anwendung den Lesezugriff auf eine Kopie der im Snapshot-Image enthaltenen Daten, jedoch ohne die Möglichkeit, das Snapshot-Image zu ändern. Einem schreibgeschützten Snapshot-Volume ist keine reservierte Kapazität zugewiesen.
- Ein Lese-Schreib-Snapshot-Volume ermöglicht der Host-Anwendung Schreibzugriff auf eine Kopie der Daten im Snapshot Image. Es verfügt über eine eigene reservierte Kapazität, mit der nachfolgende Änderungen der Host-Applikation auf dem Basis-Volume gespeichert werden, ohne dass das referenzierte Snapshot Image beeinträchtigt wird.

Der Prozess zur Erstellung eines Snapshot-Volumes ist ein mehrstufiges Verfahren.

Schritt 1: Überprüfen Sie die Mitglieder für ein Snapshot-Volumen

Wählen Sie entweder ein Snapshot Image eines Basis-Volumes oder eine Snapshot-Konsistenzgruppe aus. Wenn Sie ein Snapshot-Snapshot-Image für Konsistenzgruppen auswählen, werden die Mitgliedvolumes der Snapshot-Konsistenzgruppe zur Überprüfung angezeigt.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wählen Sie die Registerkarte **Snapshot Volumes** aus.
3. Wählen Sie **Erstellen**.

   Das Dialogfeld Snapshot-Volume erstellen wird angezeigt.

4. Wählen Sie das Snapshot-Image (Volumen oder Snapshot Consistency Group) aus, das Sie in ein Snapshot-Volumen konvertieren möchten, und klicken Sie dann auf **Next**. Verwenden Sie einen Texteintrag im Feld **Filter**, um die Liste einzugrenzen.

   Wenn die Auswahl für ein Snapshot-Snapshot-Snapshot-Image der Konsistenzgruppe war, wird das Dialogfeld Mitglieder überprüfen angezeigt.

   Überprüfen Sie im Dialogfeld Mitglieder überprüfen die Liste der Volumes, die für die Konvertierung in Snapshot-Volumes ausgewählt wurden, und klicken Sie dann auf **Weiter**.

5. Gehen Sie zu Schritt 2: Snapshot-Volume dem Host zuweisen.

Schritt 2: Snapshot-Volume dem Host zuweisen

Wählen Sie einen bestimmten Host oder Host-Cluster aus, um ihn dem Snapshot-Volume zuzuweisen. Diese Zuweisung gewährt einem Host oder Host-Cluster Zugriff auf das Snapshot-Volume. Sie können bei Bedarf später einen Host zuweisen.

Bevor Sie beginnen

- Gültige Hosts oder Host-Cluster sind auf der Seite Hosts vorhanden.
- Host-Port-IDs müssen für den Host definiert worden sein.
- Überprüfen Sie vor der Erstellung eines da-fähigen Volumes, ob Ihre geplante Hostverbindung die Data Assurance (da)-Funktion unterstützt. 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 folgende Richtlinien:

- Das Betriebssystem eines Hosts kann bestimmte Einschränkungen für die Zugriffsmöglichkeiten auf die Anzahl der Volumes haben, auf die der Host zugreifen kann.
- Sie können eine Host-Zuweisung für jedes Snapshot Volume im Speicher-Array definieren.
- Zugewiesene Volumes werden von den Controllern im Storage-Array gemeinsam genutzt.
- Dieselbe Logical Unit Number (LUN) kann nicht zweimal von einem Host oder einem Host-Cluster verwendet werden, um auf ein Snapshot-Volume zuzugreifen. Sie müssen eine eindeutige LUN verwenden.

> Die Zuweisung eines Volumes zu einem Host schlägt fehl, wenn Sie versuchen, einem Hostcluster ein Volume zuzuweisen, das mit einer festgelegten Zuweisung für einen Host im Hostcluster in Konflikt steht.

Schritte

1. Wählen Sie im Dialogfeld **dem Host zuweisen** den Host oder Host-Cluster aus, den Sie dem neuen Volume zuweisen möchten. Wenn Sie das Volume erstellen möchten, ohne einen Host zuzuweisen, wählen Sie in der Dropdown-Liste **später zuweisen** aus.
2. Wählen Sie den Zugriffsmodus aus. Folgenden Optionen wählbar:
   - **Lesen/Schreiben** — Diese Option bietet dem Host Lese-/Schreibzugriff auf das Snapshot-Volumen und benötigt reservierte Kapazität.
   - **Schreibgeschützt** — Diese Option bietet dem Host schreibgeschützten Zugriff auf das Snapshot-Volumen und benötigt keine reservierte Kapazität.
3. Klicken Sie auf **Weiter**, und führen Sie einen der folgenden Schritte aus:
   - Wenn Ihr Snapshot-Volumen Lese-/Schreibzugriff ist, wird das Dialogfeld Kapazität überprüfen angezeigt. Gehen Sie zu Schritt 3: Reservekapazität für ein Snapshot-Volume.
   - Wenn Ihr Snapshot-Volume schreibgeschützt ist, wird das Dialogfeld Priorität bearbeiten angezeigt. Gehen Sie zu Schritt 4: Einstellungen für ein Snapshot-Volume bearbeiten.

Schritt 3: Reservekapazität für ein Snapshot-Volume

Zuweisen der reservierten Kapazität zu einem Lese-/Schreib-Snapshot-Volume System Manager legt die Volumes und die Kapazität basierend auf den Eigenschaften des Basis-Volume oder der Snapshot-Konsistenzgruppe vor. Sie können die empfohlene Konfiguration für reservierte Kapazität akzeptieren oder den zugewiesenen Storage anpassen.

Über diese Aufgabe

Sie können die reservierte Kapazität des Snapshot-Volumes je nach Bedarf erhöhen oder verringern. Wenn Sie feststellen, dass die reservierte Snapshot Kapazität größer ist, als Sie benötigen, können Sie ihre Größe verringern, um Speicherplatz freizugeben, der von anderen logischen Volumes benötigt wird.

Schritte

1. Verwenden Sie die Spinner Box, um die reservierte Kapazität für das Snapshot-Volumen zuzuweisen.

   In der Tabelle Volume Candidate werden nur die Kandidaten angezeigt, die die angegebene reservierte Kapazität unterstützen.

   Führen Sie eine der folgenden Aktionen aus:

   - **Die Standardeinstellungen akzeptieren**.

     Verwenden Sie diese empfohlene Option, um die reservierte Kapazität für das Snapshot-Volume mit den Standardeinstellungen zuzuweisen.

   - **Zuweisen Ihrer eigenen reservierten Kapazitätseinstellungen entsprechend Ihren Datenspeicheranforderungen**.

     Wenn Sie die Standardeinstellung für reservierte Kapazität ändern, klicken Sie auf **Kandidaten aktualisieren**, um die Kandidatenliste für die von Ihnen angegebene reservierte Kapazität zu aktualisieren.

     Weisen Sie die reservierte Kapazität mithilfe der folgenden Richtlinien zu.

     - Die Standardeinstellung für die reservierte Kapazität ist 40 % der Kapazität des Basis-Volumes, und in der Regel reicht diese Kapazität aus.
     - Die benötigte Kapazität ist unterschiedlich, abhängig von der Häufigkeit und Größe der I/O-Schreibvorgänge auf den Volumes sowie von der Menge und Dauer der Snapshot-Image-Erfassung.

2. **Optional:** Wenn Sie das Snapshot-Volume für eine Snapshot-Consistency Group erstellen, wird in der Tabelle Reservierte Kapazitätskandidaten die Option zum Ändern des Kandidaten angezeigt. Klicken Sie auf **Kandidaten ändern**, um einen anderen Kandidaten für reservierte Kapazität auszuwählen.
3. Klicken Sie auf **Weiter**, und gehen Sie zu Schritt 4: Einstellungen für ein Snapshot-Volume bearbeiten.

Schritt 4: Einstellungen für ein Snapshot-Volume bearbeiten

Ändern Sie die Einstellungen für ein Snapshot Volume, z. B. Name, Caching, Warnmeldungen für reservierte Kapazität usw.

Über diese Aufgabe

Sie können das Volume einem SSD-Cache (Solid State Disk) hinzufügen, um die schreibgeschützte Performance zu verbessern. SSD-Cache besteht aus einer Reihe von SSD-Laufwerken, die Sie in Ihrem Storage Array logisch gruppieren.

Schritte

1. Übernehmen oder ändern Sie die Einstellungen für das Snapshot-Volume je nach Bedarf.

Felddetails

Einstellung	Beschreibung
Snapshot-Lautstärkeeinstellungen	Name
Geben Sie den Namen für das Snapshot-Volume an.	Aktivieren Sie SSD-Cache
Wählen Sie diese Option aus, um die schreibgeschützte Cache-Speicherung auf SSDs zu aktivieren.	**Reservierte Kapazitätseinstellungen**
Benachrichtigen, wenn…	**Erscheint nur für ein Lese-/Schreib-Snapshot-Volumen**. Verwenden Sie die Spinner-Box, um den Prozentpunkt anzupassen, an dem das System eine Warnmeldung sendet, wenn sich die reservierte Kapazität einer Snapshot-Gruppe fast voll befindet. Wenn die reservierte Kapazität der Snapshot-Gruppe den angegebenen Schwellenwert überschreitet, erhöhen Sie mit der Vorankündigung die reservierte Kapazität oder löschen Sie unnötige Objekte, bevor der verbleibende Speicherplatz ausgeht.

2. Prüfen Sie die Konfiguration des Snapshot-Volumes. Klicken Sie auf **Zurück**, um Änderungen vorzunehmen.
3. Wenn Sie mit der Konfiguration des Snapshot-Volumens zufrieden sind, klicken Sie auf **Fertig stellen**.

Managen von Snapshot-Zeitplänen

Ändern Sie die Einstellungen für einen Snapshot-Zeitplan

Für einen Snapshot-Zeitplan können Sie die automatische Erfassungszeit oder die Häufigkeit der Erfassung ändern.

Über diese Aufgabe

Sie können Einstellungen aus einem vorhandenen Snapshot-Zeitplan importieren oder Einstellungen nach Bedarf ändern.

Da ein Snapshot Zeitplan einer Snapshot-Gruppe oder einer Snapshot Konsistenzgruppe zugeordnet ist, kann die reservierte Kapazität durch Änderungen an den Zeitplaneinstellungen beeinträchtigt werden.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].

2. Klicken Sie auf die Registerkarte **Zeitpläne**.
3. Wählen Sie den Snapshot-Zeitplan aus, den Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

   Das Dialogfeld Snapshot-Zeitplan bearbeiten wird angezeigt.

4. Führen Sie einen der folgenden Schritte aus:
   - **Verwenden Sie einen zuvor definierten Zeitplan aus einem anderen Snapshot-Objekt** — Klicken Sie auf **Zeitplan importieren**, wählen Sie das Objekt mit dem zu importierenden Zeitplan aus und klicken Sie dann auf **Import**.
   - **Bearbeiten Sie die Zeitplaneinstellungen** — Siehe Felddetails weiter unten.

Felddetails

Einstellung	Beschreibung
Tag / Monat	Wählen Sie eine der folgenden Optionen: • **Daily / Weekly** — Wählen Sie einzelne Tage für Synchronisations-Snapshots. Sie können auch das Kontrollkästchen **Alle Tage auswählen** oben rechts auswählen, wenn Sie einen Tagesablauf wünschen. • **Monatlich / jährlich** — Wählen Sie einzelne Monate für Synchronisations-Snapshots aus. Geben Sie im Feld * am Tag(e)* die Tage des Monats ein, an denen Synchronisationen stattfinden sollen. Gültige Eingaben sind **1** bis **31** und **Letzte**. Sie können mehrere Tage durch Komma oder Semikolon voneinander trennen. Verwenden Sie einen Bindestrich für inklusives Datum. Zum Beispiel: 1,3,4,10-15,Last. Sie können auch das Kontrollkästchen **Alle Monate auswählen** oben rechts auswählen, wenn Sie einen monatlichen Zeitplan wünschen.
Startzeit	Wählen Sie aus der Dropdown-Liste eine neue Startzeit für die täglichen Snapshots aus. Die Auswahl erfolgt in Schritten von einer halben Stunde. Die Startzeit liegt standardmäßig auf eine halbe Stunde vor der aktuellen Zeit.
Zeitzone	Wählen Sie aus der Dropdown-Liste die Zeitzone Ihres Speicher-Arrays aus.
Snapshots pro Tag Zeit zwischen Snapshots	Wählen Sie die Anzahl der pro Tag zu erstellenden Snapshot-Bilder aus. Wenn Sie mehrere auswählen, wählen Sie auch die Zeit zwischen den Wiederherstellungspunkten aus. Vergewissern Sie sich bei mehreren Wiederherstellungspunkten, dass Sie über ausreichend reservierte Kapazität verfügen.
Startdatum Enddatum Kein Enddatum	Geben Sie das Startdatum für die Synchronisierung ein. Geben Sie auch ein Enddatum ein oder wählen Sie **kein Enddatum**.

5. Klicken Sie Auf **Speichern**.

Aktivieren und Anhalten des Snapshot-Zeitplans

Sie können die geplante Sammlung von Snapshot-Images vorübergehend unterbrechen, wenn Sie Speicherplatz sparen müssen. Diese Methode ist effizienter als das Löschen und das spätere Erstellen des Snapshot-Zeitplans.

Über diese Aufgabe

Der Status des Snapshot-Zeitplans bleibt ausgesetzt, bis Sie die Option **Aktivieren** verwenden, um die geplanten Snapshot-Aktivitäten wieder aufzunehmen.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wenn er nicht bereits angezeigt wird, klicken Sie auf die Registerkarte **Zeitpläne**.

   Die Zeitpläne sind auf der Seite aufgeführt.

3. Wählen Sie einen aktiven Snapshot-Zeitplan aus, den Sie aussetzen möchten, und klicken Sie dann auf **Aktivieren/Deaktivieren**.

   Der Status der Spalte Status ändert sich in **suspended**, und der Snapshot-Zeitplan stoppt die Sammlung aller Snapshot-Bilder.

4. Um das Sammeln von Snapshot-Bildern fortzusetzen, wählen Sie den suspendierten Snapshot-Zeitplan aus, den Sie fortsetzen möchten, und klicken Sie dann auf **Aktivieren / anhalten**.

   Der Status der Spalte Status ändert sich in **aktiv**.

Löschen Sie den Snapshot Zeitplan

Wenn Sie keine Snapshot-Images mehr erstellen möchten, können Sie einen vorhandenen Snapshot-Zeitplan löschen.

Über diese Aufgabe

Wenn Sie einen Snapshot-Zeitplan löschen, werden die zugehörigen Snapshot-Images nicht zusammen mit ihm gelöscht. Wenn Sie der Meinung sind, dass die Sammlung von Snapshot-Bildern irgendwann wieder aufgenommen werden könnte, sollten Sie den Snapshot-Zeitplan unterbrechen, anstatt ihn zu löschen.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Klicken Sie auf die Registerkarte **Zeitpläne**.
3. Wählen Sie den Snapshot-Zeitplan aus, den Sie löschen möchten, und bestätigen Sie den Vorgang.

Ergebnisse

Das System entfernt alle Zeitplanattribute vom Basis-Volume oder der Snapshot-Konsistenzgruppe.

Snapshot-Images verwalten

Anzeigen der Einstellungen für Snapshot-Images

Sie können die Eigenschaften, den Status, die reservierte Kapazität und die zugehörigen Objekte anzeigen, die jedem Snapshot-Image zugewiesen sind.

Über diese Aufgabe

Zu den zugehörigen Objekten für ein Snapshot Image zählen das Basis-Volume oder die Snapshot Konsistenzgruppe, für die dieses Snapshot Image ein Wiederherstellungspunkt ist, die zugehörige Snapshot Gruppe und alle aus dem Snapshot Image erstellten Snapshot Volumes. Bestimmen Sie mithilfe der Snapshot-Einstellungen, ob Sie das Snapshot-Image kopieren oder konvertieren möchten.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Klicken Sie auf die Registerkarte **Snapshot Images**.
3. Wählen Sie das Snapshot-Bild aus, das Sie anzeigen möchten, und klicken Sie dann auf **Einstellungen anzeigen**.

   Das Dialogfeld Snapshot-Bildeinstellungen wird angezeigt.

4. Zeigen Sie die Einstellungen für das Snapshot-Image an.

Starten Sie das Rollback von Snapshot Images für ein Basisvolumen

Sie können einen Rollback-Vorgang durchführen, um den Inhalt eines Basisvolumes an den Inhalt eines Snapshot-Bilds anzupassen.

Durch den Rollback-Vorgang wird der Inhalt der Snapshot-Images, die mit dem Basisvolumen verknüpft sind, nicht geändert.

Bevor Sie beginnen

- Genügend reservierte Kapazität ist verfügbar, um einen Rollback-Vorgang zu starten.
- Das ausgewählte Snapshot-Image ist optimal und das ausgewählte Volume ist optimal.
- Für das ausgewählte Volume wird kein Rollback durchgeführt.

Über diese Aufgabe

Mit der Rollback-Startsequenz können Sie ein Rollback auf einem Snapshot-Image eines Basis-Volumes durchführen und gleichzeitig zusätzliche Speicherkapazität bereitstellen. Sie können nicht mehr als einen Rollback-Vorgang für ein Basis-Volume gleichzeitig starten.

> Der Host kann sofort auf das neue Rollback-Basis-Volume zugreifen, aber das vorhandene Basis-Volume lässt den Lese-/Schreibzugriff des Hosts nach dem Rollback nicht zu. Sie können einen Snapshot des Basis-Volumes unmittelbar vor dem Start des Rollback erstellen, um das vorRollback-Basisvolume für die Wiederherstellung zu erhalten.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wählen Sie die Registerkarte **Snapshot Images** aus.
3. Wählen Sie das Snapshot-Bild aus, und wählen Sie dann Menü:Rollback[Start].

   Das Dialogfeld Rollback bestätigen wird angezeigt.

4. **Optional:** Wählen Sie bei Bedarf die Option zur **Erhöhung der Kapazität** aus.

   Das Dialogfeld reservierte Kapazität erhöhen wird angezeigt.

   a. Verwenden Sie die Spinner-Box, um den Kapazitätsanteil einzustellen.

      Wenn im Pool oder in der Volume-Gruppe keine freie Kapazität vorhanden ist, die das ausgewählte Speicherobjekt enthält und das Speicherarray nicht zugewiesene Kapazität hat, können Sie die Kapazität hinzufügen. Sie können einen neuen Pool oder eine neue Volume-Gruppe erstellen und diesen Vorgang anschließend mit der neuen freien Kapazität in diesem Pool oder dieser Volume-

Gruppe wiederholen.

b. Klicken Sie Auf **Erhöhen**.

5. Bestätigen Sie, dass Sie diesen Vorgang ausführen möchten, und klicken Sie dann auf **Rollback**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Stellt das Volume mit dem auf dem ausgewählten Snapshot-Image gespeicherten Inhalt wieder her.
- Rollback-Volumes stehen sofort für Host-Zugriff zur Verfügung. Sie müssen nicht warten, bis der Rollback-Vorgang abgeschlossen ist.

Nachdem Sie fertig sind

Wählen Sie MENU:Startseite[Vorgänge in Bearbeitung anzeigen], um den Fortschritt des Rollback-Vorgangs anzuzeigen.

Ist der Rollback-Vorgang nicht erfolgreich, wird der Vorgang angehalten. Sie können den angehaltenen Vorgang fortsetzen und, falls dieser weiterhin nicht erfolgreich war, das Recovery Guru-Verfahren befolgen, um das Problem zu beheben oder sich an den technischen Support zu wenden.

Starten Sie das Rollback von Snapshot Image für Volumes von Mitgliedern der Snapshot Consistency Group

Sie können einen Rollback-Vorgang durchführen, um den Inhalt der Snapshot Consistency Group Member Volumes an den Inhalt anzupassen, der in einem Snapshot-Image gespeichert ist.

Durch den Rollback-Vorgang wird der Inhalt der Snapshot-Images, die mit der Snapshot-Konsistenzgruppe verknüpft sind, nicht geändert.

Bevor Sie beginnen

- Genügend reservierte Kapazität ist verfügbar, um einen Rollback-Vorgang zu starten.
- Das ausgewählte Snapshot-Image ist optimal und das ausgewählte Volume ist optimal.
- Für das ausgewählte Volume wird kein Rollback durchgeführt.

Über diese Aufgabe

Mit der Rollback-Startsequenz können Sie ein Rollback auf ein Snapshot-Image einer Snapshot-Consistency Group starten und gleichzeitig zusätzliche Speicherkapazität bereitstellen. Sie können nicht mehr als einen Rollback-Vorgang für eine Snapshot-Konsistenzgruppe gleichzeitig starten.

Der Host hat sofortigen Zugriff auf die neuen Rollback-Volumes, aber die vorhandenen Mitglieder-Volumes ermöglichen keinen Lese-/Schreibzugriff auf den Host nach dem Rollback-Start. Sie können ein Snapshot-Image der Mitgliedsvolumes unmittelbar vor dem Start des Rollbacks erstellen, um die vorRollback-Basisvolumes für Wiederherstellungszwecke zu erhalten.

Der Vorgang zum Starten des Rollbacks eines Snapshot-Images einer Snapshot-Consistency Group ist ein mehrstufiges Verfahren.

Schritt 1: Mitglieder auswählen

Sie müssen die Mitgliedvolumes auswählen, die zurückgerollt werden sollen.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wählen Sie die Registerkarte **Snapshot Images** aus.
3. Wählen Sie das Snapshot-Snapshot-Image der Snapshot-Konsistenzgruppe aus, und wählen Sie dann Menü:Rollback[Start].

   Das Dialogfeld Rollback starten wird angezeigt.

4. Wählen Sie das Mitgliedsvolumen oder die Volumes aus.
5. Klicken Sie auf **Weiter**, und führen Sie einen der folgenden Schritte aus:
   - Wenn einer der ausgewählten Mitgliedvolumes mehr als einem Objekt mit reservierter Kapazität zugeordnet ist, in dem Snapshot-Bilder gespeichert werden, wird das Dialogfeld Kapazität prüfen angezeigt. Gehen Sie zu Schritt 2: Kapazität überprüfen.
   - Wenn keiner der ausgewählten Mitgliedvolumes mehr als einem Objekt mit reservierter Kapazität zugeordnet ist, in dem Snapshot-Bilder gespeichert werden, wird das Dialogfeld Priorität bearbeiten angezeigt. Gehen Sie zu Schritt 3: Priorität bearbeiten.

Schritt 2: Kapazität überprüfen

Wenn Sie Mitgliedvolumes ausgewählt haben, die mehr als einem reservierten Kapazitätsobjekt zugeordnet sind, z. B. einer Snapshot-Gruppe und einem reservierten Kapazitätsvolumen, können Sie die reservierte Kapazität für die zurückgerollten Volumes überprüfen und erhöhen.

Schritte

1. Klicken Sie in der Spalte **Bearbeiten** neben einem Mitgliedsvolumen mit sehr geringer (oder Null) reservierter Kapazität auf den Link **Erhöhung der Kapazität**.

   Das Dialogfeld reservierte Kapazität erhöhen wird angezeigt.

2. Verwenden Sie das Spinner-Feld, um den Kapazitätsanteil anzupassen, und klicken Sie dann auf **Erhöhen**.

   Wenn im Pool oder in der Volume-Gruppe keine freie Kapazität vorhanden ist, die das ausgewählte Speicherobjekt enthält und das Speicherarray nicht zugewiesene Kapazität hat, können Sie die Kapazität hinzufügen. Sie können einen neuen Pool oder eine neue Volume-Gruppe erstellen und diesen Vorgang mit der neuen freien Kapazität in diesem Pool oder dieser Volume-Gruppe wiederholen.

3. Klicken Sie auf **Weiter**, und gehen Sie zu Schritt 3: Priorität bearbeiten.

   Das Dialogfeld Priorität bearbeiten wird angezeigt.

Schritt 3: Priorität bearbeiten

Sie können bei Bedarf die Priorität des Rollback-Vorgangs bearbeiten.

Über diese Aufgabe

Die Rollback-Priorität bestimmt, wie viele Systemressourcen auf Kosten der System-Performance für den Rollback-Vorgang reserviert sind.

Schritte

1. Mit dem Schieberegler können Sie die Rollback-Priorität nach Bedarf anpassen.
2. Bestätigen Sie, dass Sie diesen Vorgang ausführen möchten, und klicken Sie dann auf **Fertig stellen**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Stellt die Mitgliedsvolumes der Snapshot-Konsistenzgruppe mit dem auf dem ausgewählten Snapshot-Image gespeicherten Inhalt wieder her.
- Rollback-Volumes stehen sofort für Host-Zugriff zur Verfügung. Sie müssen nicht warten, bis der Rollback-Vorgang abgeschlossen ist.

Nachdem Sie fertig sind

Wählen Sie MENU:Startseite[Vorgänge in Bearbeitung anzeigen], um den Fortschritt des Rollback-Vorgangs anzuzeigen.

Ist der Rollback-Vorgang nicht erfolgreich, wird der Vorgang angehalten. Sie können den angehaltenen Vorgang fortsetzen und, falls dieser weiterhin nicht erfolgreich war, das Recovery Guru-Verfahren befolgen, um das Problem zu beheben oder sich an den technischen Support zu wenden.

Setzen Sie das Rollback von Snapshot-Bildern fort

Wenn während eines Rollback-Vorgangs eines Snapshot-Images ein Fehler auftritt, wird der Vorgang automatisch angehalten. Sie können einen Rollback-Vorgang fortsetzen, der sich im Status „Pause“ befindet.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Klicken Sie auf die Registerkarte **Snapshot Images**.
3. Markieren Sie das angehaltene Rollback, und wählen Sie dann Menü:Rollback[Resume].

   Der Vorgang wird fortgesetzt.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Wenn der Rollback-Vorgang erfolgreich fortgesetzt wird, können Sie den Fortschritt des Rollback-Vorgangs im Fenster „Vorgänge in Bearbeitung“ anzeigen.
- Ist der Rollback-Vorgang nicht erfolgreich, wird der Vorgang erneut angehalten. Sie können das Problem durch die Recovery Guru-Prozedur beheben oder sich an den technischen Support wenden.

Abbrechen des Zurücksetzvorgangs von Snapshot-Bildern

Sie können ein aktives Rollback abbrechen, das gerade läuft (Daten aktiv kopieren), ein ausstehendes Rollback (in einer Warteschlange, in der auf den Start warten) oder ein Rollback, das aufgrund eines Fehlers angehalten wurde.

Über diese Aufgabe

Wenn Sie einen laufenden Rollback-Vorgang abbrechen, wird das Basis-Volume in einen unbrauchbaren

Zustand zurückgesetzt und wird als fehlgeschlagen angezeigt. Daher sollten Sie einen Rollback-Vorgang nur dann abbrechen, wenn Recovery-Optionen zur Wiederherstellung des Inhalts des Basis-Volumes vorhanden sind.

> Wenn in der Snapshot-Gruppe, auf der sich das Snapshot-Image befindet, ein oder mehrere Snapshot-Images vorhanden sind, die automatisch gelöscht wurden, ist das für den Rollback-Vorgang verwendete Snapshot-Image möglicherweise nicht für künftige Rollbacks verfügbar.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Klicken Sie auf die Registerkarte **Snapshot Images**.
3. Wählen Sie den aktiven oder unterbrochenen Rollback aus und wählen Sie dann Menü:Rollback[Abbrechen].

   Das Dialogfeld Rollback bestätigen wird angezeigt.
4. Klicken Sie zur Bestätigung auf **Ja**.

Ergebnisse

System Manager stoppt den Rollback-Vorgang. Das Basis-Volume ist zwar nutzbar, kann aber Daten enthalten, die inkonsistent oder nicht intakt sind.

Nachdem Sie fertig sind

Nachdem Sie einen Rollback-Vorgang abgebrochen haben, müssen Sie eine der folgenden Aktionen durchführen:

- Initialisieren Sie den Inhalt des Basis-Volume neu.
- Führen Sie einen neuen Rollback-Vorgang durch, um das Basisvolume entweder mit demselben Snapshot-Image wiederherzustellen, das beim Rollback abbrechen verwendet wurde, oder mit einem anderen Snapshot-Image, um den neuen Rollback-Vorgang durchzuführen.

Snapshot Image löschen

Sie löschen Snapshot Images, um das älteste Snapshot Image aus einer Snapshot-Gruppe oder einer Snapshot-Konsistenzgruppe aufzuräumen.

Über diese Aufgabe

Sie können ein einzelnes Snapshot-Image löschen oder Snapshot-Images aus Snapshot-Konsistenzgruppen löschen, die denselben Zeitstempel für die Erstellung haben. Sie können Snapshot-Images auch aus einer Snapshot-Gruppe löschen.

Ein Snapshot Image kann nicht gelöscht werden, wenn es nicht das älteste Snapshot Image des zugehörigen Basis-Volumes oder der Snapshot-Konsistenzgruppe ist.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Klicken Sie auf die Registerkarte **Snapshot Images**.
3. Wählen Sie das Snapshot-Image aus, das Sie löschen möchten, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

   Wenn Sie ein Snapshot-Image einer Snapshot-Konsistenzgruppe ausgewählt haben, wählen Sie jedes

Mitgliedvolume aus, das Sie löschen möchten, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

4. Klicken Sie Auf **Löschen**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Löscht das Snapshot-Image aus dem Speicher-Array.
- Gibt die reservierte Kapazität zur Wiederverwendung innerhalb der Snapshot-Gruppe oder der Snapshot-Konsistenzgruppe frei.
- Deaktiviert alle zugeordneten Snapshot-Volumes, die für das gelöschte Snapshot-Image vorhanden sind.
- Beim Löschen einer Snapshot Konsistenzgruppe wird jedes dem gelöschten Snapshot Image zugeordnete Mitglied-Volume in einen Status „angehalten“ verschoben.

Verwalten von Snapshot Konsistenzgruppen

Fügen Sie einer Snapshot-Konsistenzgruppe ein Mitgliedsvolume hinzu

Sie können einer vorhandenen Snapshot-Konsistenzgruppe ein neues Mitgliedsvolume hinzufügen. Wenn Sie ein neues Mitgliedsvolumen hinzufügen, müssen Sie auch Kapazität für das Mitgliedervolumen reservieren.

Bevor Sie beginnen

- Das Mitgliedervolumen muss optimal sein.
- Die Snapshot-Consistency-Gruppe muss weniger als die maximale Anzahl zulässiger Volumes aufweisen (gemäß Ihrer Konfiguration).
- Jedes reservierte Kapazitäts-Volume muss dieselben Data Assurance (da) und Sicherheitseinstellungen haben wie das zugehörige Mitglied-Volume.

Über diese Aufgabe

Sie können der Snapshot-Konsistenzgruppe Standard-Volumes oder Thin Volumes hinzufügen. Das Basis-Volume kann sich entweder in einem Pool oder in einer Volume-Gruppe befinden.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wählen Sie die Registerkarte **Snapshot Consistency Groups** aus.

   Die Tabelle wird angezeigt und zeigt alle Snapshot-Konsistenzgruppen an, die dem Speicher-Array zugeordnet sind.

3. Wählen Sie die Snapshot Consistency Group aus, die Sie ändern möchten, und klicken Sie dann auf **Mitglieder hinzufügen**.

   Das Dialogfeld Mitglieder hinzufügen wird angezeigt.

4. Wählen Sie die Mitglieder aus, die Sie hinzufügen möchten, und klicken Sie dann auf **Weiter**.

   Der Schritt Reserve Kapazität wird angezeigt. In der Tabelle Volume Candidate werden nur die Kandidaten angezeigt, die die angegebene reservierte Kapazität unterstützen.

5. Verwenden Sie den Spinner-Kasten, um die reservierte Kapazität für das Mitgliedervolumen zuzuweisen. Führen Sie eine der folgenden Aktionen aus:
   - **Die Standardeinstellungen akzeptieren.**

     Verwenden Sie diese empfohlene Option, um die reservierte Kapazität für das Mitglied-Volume mit den Standardeinstellungen zuzuweisen.

   - **Zuweisen Ihrer eigenen reservierten Kapazitätseinstellungen entsprechend Ihren Datenspeicheranforderungen.**

     Wenn Sie die Standardeinstellung für reservierte Kapazität ändern, klicken Sie auf **Kandidaten aktualisieren**, um die Kandidatenliste für die von Ihnen angegebene reservierte Kapazität zu aktualisieren.

     Weisen Sie die reservierte Kapazität mithilfe der folgenden Richtlinien zu.

     - Die Standardeinstellung für die reservierte Kapazität ist 40 % der Kapazität des Basis-Volumes, und in der Regel reicht diese Kapazität aus.
     - Die benötigte Kapazität ist unterschiedlich, abhängig von der Häufigkeit und Größe der I/O-Schreibvorgänge auf den Volumes sowie von der Menge und Dauer der Snapshot-Image-Erfassung.
6. Klicken Sie auf **Fertig stellen**, um die Mitgliedervolumes hinzuzufügen.

Entfernen eines Mitglieds-Volumes aus einer Snapshot-Konsistenzgruppe

Sie können ein Mitglied-Volume aus einer vorhandenen Snapshot-Konsistenzgruppe entfernen.

Über diese Aufgabe

Wenn Sie ein Mitglied-Volume aus einer Snapshot Konsistenzgruppe entfernen, löscht der System Manager automatisch die Snapshot Objekte, die diesem Mitglied-Volume zugeordnet sind.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Klicken Sie auf die Registerkarte **Snapshot Consistency Groups**.
3. Erweitern Sie die Snapshot Consistency Group, die Sie ändern möchten, indem Sie das Pluszeichen (+) neben ihr auswählen.
4. Wählen Sie das Mitgliedvolume aus, das Sie entfernen möchten, und klicken Sie dann auf **Entfernen**.
5. Bestätigen Sie, dass Sie den Vorgang ausführen möchten, und klicken Sie dann auf **Entfernen**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Löscht alle Snapshot-Images und Snapshot-Volumes, die dem Mitgliedvolume zugeordnet sind.
- Löscht die dem Mitgliedvolume zugeordnete Snapshot-Gruppe.
- Das Mitgliedvolume wird nicht anders geändert oder gelöscht.

Ändern Sie die Einstellungen für eine Snapshot Konsistenzgruppe

Ändern Sie die Einstellungen für eine Snapshot Konsistenzgruppe, wenn Sie ihren Namen, die Einstellungen zum automatischen Löschen oder die maximale Anzahl von Snapshot Images ändern möchten.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Klicken Sie auf die Registerkarte **Snapshot Consistency Groups**.
3. Wählen Sie die Snapshot Consistency Group aus, die Sie bearbeiten möchten, und klicken Sie dann auf **View/Edit Settings**.

   Das Dialogfeld Einstellung für Snapshot-Konsistenzgruppen wird angezeigt.

4. Ändern Sie ggf. die Einstellungen für die Snapshot-Konsistenzgruppe.

Felddetails

Einstellung	Beschreibung
Snapshot Consistency Group Einstellungen	Name
Sie können den Namen für die Snapshot Konsistenzgruppe ändern.	Automatisches Löschen
Aktivieren Sie das Kontrollkästchen, wenn Snapshot-Bilder nach dem festgelegten Limit automatisch gelöscht werden sollen. Ändern Sie die Begrenzung mit dem Spinner-Feld. Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Erstellung von Snapshot-Bildern nach 32 Bildern angehalten.	Begrenzung des Snapshot Images
Sie können die maximale Anzahl von Snapshot Images ändern, die für eine Snapshot-Gruppe zulässig sind.	Snapshot Zeitplan
Dieses Feld gibt an, ob ein Zeitplan der Snapshot-Konsistenzgruppe zugeordnet ist.	**Assoziierte Objekte**
Member-Volumes	Sie können die Anzahl der Mitglied-Volumes anzeigen, die der Snapshot-Konsistenzgruppe zugeordnet sind.

5. Klicken Sie Auf **Speichern**.

Löschen der Snapshot Konsistenzgruppe

Sie können Snapshot-Konsistenzgruppen löschen, die nicht mehr benötigt werden.

Bevor Sie beginnen

Vergewissern Sie sich, dass die Images aller Mitgliedsvolumes nicht mehr für Backup- oder Testzwecke benötigt werden.

Über diese Aufgabe

Durch diesen Vorgang werden alle Snapshot-Images oder -Zeitpläne gelöscht, die mit der Snapshot-Konsistenzgruppe verknüpft sind.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wählen Sie die Registerkarte **Snapshot Consistency Groups** aus.
3. Wählen Sie die Snapshot-Konsistenzgruppe aus, die Sie löschen möchten, und wählen Sie dann Menü:Sonstige Aufgaben[Löschen].

   Das Dialogfeld „Konsistenzgruppe löschen bestätigen“ wird angezeigt.

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

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Löscht alle vorhandenen Snapshot-Images und Snapshot-Volumes aus der Snapshot-Konsistenzgruppe.
- Löscht alle zugehörigen Snapshot-Images, die für jedes Mitgliedsvolume in der Snapshot-Konsistenzgruppe vorhanden sind.
- Löscht alle zugehörigen Snapshot-Volumes, die für jedes Mitgliedsvolume in der Snapshot-Konsistenzgruppe vorhanden sind.
- Löscht alle zugeordneten reservierten Kapazitäten für jedes Mitglied-Volume in der Snapshot-Konsistenzgruppe (wenn ausgewählt).

Managen von Snapshot Volumes

Konvertieren des Snapshot-Volumes in den Lese-/Schreibmodus

Sie können bei Bedarf ein schreibgeschütztes Snapshot Volume oder ein Snapshot Consistency Group Snapshot Volume in den Lese-/Schreibmodus konvertieren.

Ein Snapshot Volume, das in den Zugriff auf Lese- und Schreibvorgänge umgewandelt wird, enthält seine eigene reservierte Kapazität. Mit dieser Kapazität werden nachfolgende Änderungen der Host-Applikation auf dem Basis-Volume gespeichert, ohne dass das referenzierte Snapshot Image beeinträchtigt wird.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wählen Sie die Registerkarte **Snapshot Volumes** aus.

   Die Tabelle Snapshot Volumes wird angezeigt und zeigt alle dem Speicher-Array zugeordneten Snapshot-Volumes an.

3. Wählen Sie das schreibgeschützte Snapshot-Volumen aus, das Sie konvertieren möchten, und klicken Sie dann auf **in Lesen/Schreiben konvertieren**.

Das Dialogfeld in Lesen/Schreiben konvertieren wird angezeigt, wenn der Schritt **Reservekapazität** aktiviert ist. In der Tabelle Volume Candidate werden nur die Kandidaten angezeigt, die die angegebene reservierte Kapazität unterstützen.

4. Um die reservierte Kapazität für das Lese- und Schreib-Snapshot-Volume zuzuweisen, führen Sie eine der folgenden Aktionen aus:
   - **Übernehmen Sie die Standardeinstellungen** — Verwenden Sie diese empfohlene Option, um die reservierte Kapazität für das Snapshot-Volumen mit den Standardeinstellungen zuzuweisen.
   - **Zuweisen Ihrer eigenen reservierten Kapazitätseinstellungen entsprechend Ihren Datenspeicheranforderungen** — Zuweisen der reservierten Kapazität unter Verwendung der folgenden Richtlinien.
     - Die Standardeinstellung für die reservierte Kapazität ist 40 % der Kapazität des Basis-Volumes, und in der Regel reicht diese Kapazität aus.
     - Die benötigte Kapazität ist abhängig von der Häufigkeit und der Größe der I/O-Schreibvorgänge auf dem Volume.
5. Wählen Sie **Weiter**, um die Einstellungen zu überprüfen oder zu bearbeiten.

   Das Dialogfeld Einstellungen bearbeiten wird angezeigt.

6. Akzeptieren oder geben Sie die Einstellungen für das Snapshot-Volumen an, und wählen Sie dann **Fertig**, um das Snapshot-Volumen zu konvertieren.

   Felddetails

Einstellung	Beschreibung
Reservierte Kapazitätseinstellungen	Benachrichtigen, wenn…

Ändern Sie die Volume-Einstellungen für ein Snapshot-Volume

Sie können die Einstellungen für ein Snapshot-Volume oder Snapshot-Konsistenzgruppenvolume ändern, um es umzubenennen, das SSD-Caching zu aktivieren oder zu deaktivieren oder die Zuweisung von Host, Host-Cluster oder Logical Unit Number (LUN) zu ändern.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Klicken Sie auf die Registerkarte **Snapshot Volumes**.
3. Wählen Sie das Snapshot-Volumen aus, das Sie ändern möchten, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld Snapshot-Volume-Einstellungen wird angezeigt.

4. Zeigen Sie die Einstellungen für das Snapshot-Volume an, oder bearbeiten Sie sie entsprechend.

Felddetails

Einstellung	Beschreibung
Snapshot Volumen	Name
Sie können den Namen für das Snapshot-Volume ändern.	Zugewiesen zu
Sie können die Host- oder Host-Cluster-Zuweisung für das Snapshot-Volume ändern.	LUN
Sie können die LUN-Zuweisung für das Snapshot-Volume ändern.	SSD Cache
Sie können die schreibgeschützte Cache-Speicherung bei Solid State Disks (SSDs) aktivieren/deaktivieren.	**Assoziierte Objekte**
Snapshot Image	Sie können die Snapshot-Images anzeigen, die dem Snapshot-Volume zugeordnet sind. Ein Snapshot-Image ist eine logische Kopie der Volume-Daten, die zu einem bestimmten Zeitpunkt erfasst werden. Wie bei einem Wiederherstellungspunkt können Sie durch Snapshot Images ein Rollback zu einem bekannten fehlerfreien Datensatz durchführen. Obwohl der Host auf das Snapshot-Image zugreifen kann, kann er nicht direkt lesen oder darauf schreiben.
Basis-Volume	Sie können das Basisvolumen anzeigen, das mit dem Snapshot-Volume verknüpft ist. Ein Basis-Volume ist die Quelle, aus der ein Snapshot Image erstellt wird. Es kann sich um ein Thick- oder Thin-Volume handeln, das in der Regel einem Host zugewiesen ist. Das Basis-Volume kann entweder in einer Volume-Gruppe oder im Laufwerk-Pool gespeichert werden.
Snapshot-Gruppe	Sie können die Snapshot-Gruppe anzeigen, die dem Snapshot-Volumen zugeordnet ist. Eine Snapshot-Gruppe ist eine Sammlung von Snapshot Images aus einem einzigen Basis-Volume.

Snapshot Volume kopieren

Sie können einen Prozess zum Kopieren von Volumes auf einem Snapshot-Volume oder

einem Snapshot-Snapshot-Volume der Konsistenzgruppe durchführen.

Über diese Aufgabe

Sie können ein Snapshot-Volume wie bei einem normalen Kopiervorgang auf das Ziel-Volume kopieren. Snapshot-Volumen können jedoch während des Kopiervorgangs nicht online bleiben.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wählen Sie die Registerkarte **Snapshot Volumes** aus.

   Die Tabelle Snapshot Volumes wird angezeigt und zeigt alle dem Speicher-Array zugeordneten Snapshot-Volumes an.

3. Wählen Sie das Snapshot-Volume aus, das Sie kopieren möchten, und wählen Sie dann **Volume kopieren** aus.

   Das Dialogfeld Volume kopieren wird angezeigt, in dem Sie aufgefordert werden, ein Ziel auszuwählen.

4. Wählen Sie das Zielvolume, das als Kopierziel verwendet werden soll, und klicken Sie dann auf **Fertig stellen**.

Snapshot Volumen neu erstellen

Sie können ein Snapshot-Volumen oder ein Snapshot-Snapshot-Volumen, das Sie zuvor deaktiviert haben, neu erstellen. Das erneute Erstellen eines Snapshot Volumes dauert weniger Zeit als das Erstellen eines neuen.

Bevor Sie beginnen

- Das Snapshot Volume muss sich entweder im optimalen oder deaktivierten Zustand befinden.
- Alle Snapshot-Volumes der Mitglieder müssen sich im deaktivierten Zustand befinden, bevor Sie das Snapshot-Volume der Snapshot-Konsistenzgruppe neu erstellen können.

Über diese Aufgabe

Sie können ein Snapshot-Volumen eines einzelnen Mitglieds nicht neu erstellen, sondern nur das gesamte Snapshot-Consistency Group-Snapshot-Volumen neu erstellen.

> Wenn das Snapshot-Volumen oder das Snapshot-Snapshot-Volumen Teil einer Online-Kopie-Beziehung ist, können Sie die Option zur erneuten Erstellung auf dem Volume nicht ausführen.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wählen Sie die Registerkarte **Snapshot Volumes** aus.

   Die Tabelle Snapshot Volumes wird angezeigt und zeigt alle dem Speicher-Array zugeordneten Snapshot-Volumes an.

3. Wählen Sie das Snapshot-Volumen aus, das Sie neu erstellen möchten, und wählen Sie dann Menü:Sonstige Aufgaben[recreate].

   Das Dialogfeld Snapshot-Volume neu erstellen wird angezeigt.

4. Wählen Sie eine der folgenden Optionen:
   - **Ein vorhandenes Snapshot-Image, das aus Volume <Name>** erstellt wurde

     Wählen Sie diese Option aus, um ein vorhandenes Snapshot-Image anzuzeigen, aus dem das Snapshot-Volume neu erstellt werden soll.

   - **Ein neues (Instant) Snapshot-Image des Datenträgers <Name>**

     Wählen Sie diese Option aus, um ein neues Snapshot-Image zu erstellen, aus dem das Snapshot-Volume neu erstellt werden soll.
5. Klicken Sie Auf **Reproduzieren**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Löscht alle `write` Daten auf einem zugehörigen Snapshot Repository Volume.
- Die Parameter des Snapshot-Volumes oder des Snapshot-Volumes von Konsistenzgruppen bleiben mit den zuvor deaktivierten Volume-Parametern identisch.
- Behält die ursprünglichen Namen für das Snapshot Volume oder das Snapshot Consistency Group Snapshot Volume bei.

Deaktivieren Sie das Snapshot-Volumen

Sie können ein Snapshot-Volume oder ein Snapshot-Volume in einer Snapshot-Konsistenzgruppe deaktivieren, wenn Sie es nicht mehr benötigen oder vorübergehend nicht verwenden möchten.

Über diese Aufgabe

Verwenden Sie die Option Deaktivieren, wenn eine dieser Bedingungen zutrifft:

- Sie sind mit dem Snapshot-Volumen oder dem Snapshot-Volumen der Konsistenzgruppen fertig.
- Sie beabsichtigen, das Snapshot Volume oder das Snapshot Consistency Group Snapshot Volume (das als Lesen-Schreiben bezeichnet wird) zu einem späteren Zeitpunkt neu zu erstellen und die damit verbundene reservierte Kapazität beizubehalten, damit Sie es nicht erneut erstellen müssen.
- Sie möchten die Performance des Speicher-Arrays erhöhen, indem Sie die Schreibaktivität auf einem Lese-/Schreib-Snapshot-Volume stoppen.

Wenn das Snapshot Volume oder das Snapshot Consistency Group Snapshot Volume als Lese-/Schreibzugriff festgelegt ist, können Sie mit dieser Option auch weitere Schreibaktivität für sein reserviertes Kapazitäts-Volume anhalten. Wenn Sie das Snapshot-Volumen oder das Snapshot-Snapshot-Volumen der Consistency Group neu erstellen möchten, müssen Sie ein Snapshot-Image aus dem gleichen Basis-Volume auswählen.

> Wenn das Snapshot-Volumen oder das Snapshot-Snapshot-Volumen einer Snapshot-Consistency Group Teil einer Online-Kopierbeziehung ist, können Sie auf dem Datenträger die Option Disable nicht ausführen.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wählen Sie die Registerkarte **Snapshot Volumes** aus.

System Manager zeigt alle Snapshot Volumes an, die dem Speicher-Array zugeordnet sind.

3. Wählen Sie die Snapshot-Lautstärke aus, die Sie deaktivieren möchten, und wählen Sie dann Menü:Sonstige Aufgaben[Deaktivieren].
4. Bestätigen Sie, dass Sie den Vorgang ausführen möchten, und klicken Sie dann auf **Deaktivieren**.

Ergebnisse

- Das Snapshot Volume bleibt in Verbindung mit dem Basis-Volume.
- Der Snapshot-Volume behält seinen World Wide Name (WWN) bei.
- Bei Lese- und Schreibvorgängen behält das Snapshot Volume seine zugehörige reservierte Kapazität bei.
- Das Snapshot-Volume behält alle Host-Zuweisungen und den Zugriff bei. Lese-/Schreibanfragen schlagen jedoch fehl.
- Der Snapshot-Volumen verliert seine Verbindung mit seinem Snapshot-Image.

Snapshot Volume löschen

Sie können ein Snapshot-Volume oder ein Snapshot-Snapshot-Snapshot-Snapshot-Volume löschen, das nicht mehr für Backup- oder Softwareanwendungen-Tests benötigt wird.

Sie können auch angeben, ob das zu einem zugeordnete Snapshot-Kapazitätsvolume gelöscht werden soll `read-write` snapshot Volume oder Beibehaltung des reservierten Kapazitäts-Volumes des Snapshots als nicht zugewiesenes Volume.

Über diese Aufgabe

Durch das Löschen eines Basis-Volumes werden automatisch alle zugehörigen Snapshot-Volumes oder Snapshot-Volumes der Konsistenzgruppe gelöscht. Ein Snapshot-Volume, das sich in einer Volume-Kopie befindet, kann nicht mit dem Status **in Bearbeitung** gelöscht werden.

Schritte

1. Wählen Sie Menü:Storage[Snapshots].
2. Wählen Sie die Registerkarte **Snapshot Volumes** aus.

   System Manager zeigt alle Snapshot Volumes an, die dem Speicher-Array zugeordnet sind.

3. Wählen Sie das Snapshot-Volumen aus, das Sie löschen möchten, und wählen Sie dann Menü:Sonstige Aufgaben[Löschen].
4. Bestätigen Sie, dass Sie den Vorgang ausführen möchten, und klicken Sie dann auf **Löschen**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Löscht alle Snapshot-Volumes der Mitglieder (für ein Snapshot-Snapshot-Snapshot-Volumen der Konsistenzgruppe).
- Entfernt alle zugeordneten Host-Zuweisungen.

FAQs

Warum sehe ich nicht alle meine Bände, 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.

Was ist ein Snapshot Image?

Ein Snapshot-Image ist eine logische Kopie des Volume-Inhalts, der zu einem bestimmten Zeitpunkt erfasst wurde. Snapshot Images belegen minimalen Speicherplatz.

Die Snapshot Image-Daten werden wie folgt gespeichert:

- Ein erstelltes Snapshot Image entspricht genau dem Basis-Volume. Sobald der Snapshot erstellt wurde, werden die ursprünglichen Daten für Datenblöcke oder Blöcke auf dem Basis-Volume in die reservierte Snapshot Kapazität kopiert, bevor die neuen Daten auf das Basis-Volume geschrieben werden.
- Nachfolgende Snapshots enthalten nur Datenblöcke, die sich seit dem ersten Snapshot Image geändert haben. Bei jedem folgenden Kopiervorgang werden Originaldaten gespeichert, die im Basis-Volume überschrieben werden, bevor die neuen Daten auf das Basis-Volume geschrieben werden.

Warum Snapshot-Bilder verwenden?

Snapshots schützen vor versehentlichem oder böswillig herbeigeführten Verlust oder Beschädigung von Daten und ermöglichen so die Recovery.

Wählen Sie ein Basis-Volume oder eine Gruppe von Basis-Volumes aus, eine Snapshot-Konsistenzgruppe genannt, und erfassen Sie dann Snapshot Images auf eine oder mehrere der folgenden Arten:

- Sie können ein Snapshot Image eines einzelnen Basis-Volumes oder eine Snapshot Konsistenzgruppe aus mehreren Basis-Volumes erstellen.
- Sie können Snapshots manuell erstellen oder einen Zeitplan für ein Basis-Volume oder eine Snapshot-Consistency Group erstellen, um periodische Snapshot-Images automatisch zu erfassen.
- Sie können ein Host-zugängliches Snapshot-Volume eines Snapshot-Images erstellen.
- Sie können einen Rollback-Vorgang durchführen, um ein Snapshot-Image wiederherzustellen.

Das System speichert mehrere Snapshot-Images als Wiederherstellungspunkte, mit denen Sie ein Rollback zu bekannten guten Datensätzen zu bestimmten Zeitpunkten durchführen können. Durch die Möglichkeit eines Rollback ist Schutz vor versehentlichem Löschen von Daten und Datenbeschädigung möglich.

Welche Arten von Volumen können für Snapshots verwendet werden?

Standard-Volumes und Thin-Volumes sind die einzigen Arten von Volumes, die zum Speichern von Snapshot-Images verwendet werden können. Nicht standardmäßige Volumes können nicht verwendet werden. Das Basis-Volume kann entweder auf einem Pool oder einer Volume-Gruppe residieren.

Warum sollte ich eine Snapshot Konsistenzgruppe erstellen?

Sie erstellen eine Snapshot-Konsistenzgruppe, wenn Sie sicherstellen möchten, dass Snapshot-Images gleichzeitig auf mehreren Volumes erstellt werden.

Beispielsweise würde eine Datenbank aus mehreren Volumes, die für Recovery-Zwecke konsistent bleiben müssen, eine Snapshot-Konsistenzgruppe benötigen, um koordinierte Snapshots aller Volumes zu erstellen und sie zum Wiederherstellen der gesamten Datenbank zu verwenden.

Die Volumes, die in einer Snapshot Konsistenzgruppe enthalten sind, werden „*Member Volumes*“ genannt.

Sie können die folgenden Snapshot-Vorgänge auf einer Snapshot-Konsistenzgruppe durchführen:

- Erstellen Sie ein Snapshot-Image einer Snapshot-Konsistenzgruppe, um gleichzeitige Images der Mitglieder-Volumes zu erhalten.
- Erstellen Sie einen Zeitplan für die Snapshot-Konsistenzgruppe, um automatisch gleichzeitig periodische Images der Mitglieder-Volumes zu erfassen.
- Erstellen Sie ein über Host zugängliches Snapshot Volume eines Snapshot-Konsistenzgruppenabbilds.
- Führen Sie einen Rollback-Vorgang für eine Snapshot-Konsistenzgruppe durch.

Was ist ein Snapshot Volume und wann braucht es reservierte Kapazität?

Ein Snapshot-Volume ermöglicht dem Host den Zugriff auf Daten im Snapshot Image. Das Snapshot Volume verfügt über eine eigene reservierte Kapazität, um alle Änderungen am Basis-Volume ohne Beeinträchtigung des ursprünglichen Snapshot Images zu speichern. Snapshot Images sind für Hosts nicht Lese- oder Schreibzugriff möglich. Wenn Sie Snapshot-Daten lesen oder schreiben möchten, erstellen Sie ein Snapshot-Volume und weisen Sie es einem Host zu.

Sie können zwei Typen von Snapshot Volumes erstellen. Der Typ des Snapshot Volume bestimmt, ob die reservierte Kapazität genutzt wird.

- **Schreibgeschützt** — Ein Snapshot-Volumen, das als schreibgeschützt erstellt wird, bietet eine Host-Anwendung mit Lesezugriff auf eine Kopie der Daten im Snapshot-Image. Ein schreibgeschütztes Snapshot Volume verwendet keine reservierte Kapazität.
- **Lesen-Schreiben** — Ein Snapshot-Volumen, das als Lesen-Schreiben erstellt wird, ermöglicht es Ihnen, Änderungen am Snapshot-Volumen zu machen, ohne das referenzierte Snapshot-Bild zu beeinflussen. Ein Lese-Schreib-Snapshot-Volume nutzt die reservierte Kapazität, um diese Änderungen zu speichern. Sie können ein schreibgeschütztes Snapshot-Volumen jederzeit in Lese-/Schreibzugriff konvertieren.

Was ist eine Snapshot Gruppe?

Eine Snapshot-Gruppe ist eine Sammlung von zeitpunktgenauen Snapshot-Images eines

einzelnen verbundenen Basis-Volumes.

System Manager organisiert Snapshot Images in *Snapshot Gruppen*. Snapshot-Gruppen erfordern keine Benutzeraktion, Sie können jedoch jederzeit die reservierte Kapazität einer Snapshot-Gruppe anpassen. Darüber hinaus werden Sie möglicherweise aufgefordert, eine reservierte Kapazität zu erstellen, wenn die folgenden Bedingungen erfüllt sind:

- Jedes Mal, wenn Sie einen Snapshot eines Basis-Volumes erstellen, das noch keine Snapshot-Gruppe besitzt, erstellt System Manager automatisch eine Snapshot-Gruppe. Dadurch wird für das Basis-Volume reservierte Kapazität erstellt, mit dem nachfolgende Snapshot Images gespeichert werden können.
- Jedes Mal, wenn Sie einen Snapshot-Zeitplan für ein Basis-Volume erstellen, erstellt System Manager automatisch eine Snapshot-Gruppe.

Warum sollte ich ein Snapshot-Volumen deaktivieren?

Sie deaktivieren ein Snapshot-Volume, wenn Sie dem Snapshot-Image ein anderes Snapshot-Volume zuweisen möchten. Sie können das deaktivierte Snapshot-Volumen für die spätere Verwendung reservieren.

Wenn Sie das Snapshot Volume oder das Snapshot Volume der Konsistenzgruppe nicht mehr benötigen und zu einem späteren Zeitpunkt keine erneute Erstellung beabsichtigen, sollten Sie das Volume löschen statt es zu deaktivieren.

Was ist der deaktivierte Zustand?

Ein Snapshot-Volume im Status „deaktiviert“ ist derzeit keinem Snapshot-Image zugewiesen. Um das Snapshot-Volumen zu aktivieren, müssen Sie den Vorgang „erneut erstellen“ verwenden, um dem deaktivierten Snapshot-Volume ein neues Snapshot-Image zuzuweisen.

Die Merkmale des Snapshot-Volumes werden durch das ihm zugewiesene Snapshot-Image definiert. Lese-Schreib-Aktivität wird auf einem Snapshot-Volume im Status „deaktiviert“ angehalten.

Warum sollte ich einen Snapshot Zeitplan aussetzen?

Wenn ein Zeitplan unterbrochen wird, werden die geplanten Snapshot-Bilder-Kreationen nicht durchgeführt. Sie können einen Snapshot-Zeitplan anhalten, um Speicherplatz zu sparen, und die geplanten Snapshots zu einem späteren Zeitpunkt wieder aufnehmen.

Wenn Sie den Snapshot-Zeitplan nicht benötigen, sollten Sie den Zeitplan löschen, anstatt ihn zu sperren.

Spiegelung

Überblick

Übersicht über asynchrones Spiegeln

Die Funktion zur asynchronen Spiegelung bietet einen auf Firmware basierenden Mechanismus auf Controller-Ebene zur Datenreplizierung zwischen einem lokalen Storage-Array und einem Remote Storage Array.

Was ist asynchrones Spiegeln?

Asynchronous Mirroring erfasst den Status des primären Volumes zu einem bestimmten Zeitpunkt und kopiert nur die Daten, die sich seit der letzten Bildaufzeichnung geändert haben. Der primäre Standort kann sofort aktualisiert werden, während der sekundäre Standort mit der Bandbreite aktualisiert werden kann. Die Informationen werden im Cache gespeichert und später gesendet, sobald Netzwerkressourcen verfügbar sind.

Asynchrones Spiegeln wird auf Volume-Basis erstellt, jedoch auf Gruppenebene gemanagt. Es ermöglicht Ihnen, ein bestimmtes gespiegeltes Remote-Volume mit einem beliebigen primären Volume in einem bestimmten Storage Array zu verknüpfen. Diese Art der Spiegelung ist ideal für die Erfüllung der Anforderungen an einen unterbrechungsfreien Betrieb und im Allgemeinen ist weit mehr Netzwerkeffizienz für periodische Prozesse.

Weitere Informationen:

- "Funktionsweise der asynchronen Spiegelung"
- "Terminologie für asynchrone Spiegelung"
- "Status der asynchronen Spiegelung"
- "Volume-Eigentum"
- "Rollenwechsel einer SpiegelungsConsistency Group"

Wie konfiguriere ich asynchrone Spiegelung?

Sie müssen die ursprüngliche Spiegelungskonfiguration zwischen den Arrays über die Unified Manager-Schnittstelle durchführen. Sobald diese konfiguriert ist, können Sie gespiegelte Paare und Konsistenzgruppen in System Manager managen.

Weitere Informationen:

- "Anforderungen für die Verwendung von asynchronem Spiegeln"
- "Workflow für die asynchrone Spiegelung eines Volumes"
- "Asynchrones gespiegeltes Paar erstellen (in Unified Manager)"

Verwandte Informationen

Weitere Informationen zu Konzepten zur asynchronen Spiegelung:

- "Was Sie wissen müssen, bevor Sie eine gespiegelte Konsistenzgruppe erstellen"
- "Was Sie wissen müssen, bevor Sie ein gespiegeltes Paar erstellen"
- "Unterschiede zwischen der asynchronen Spiegelung und der synchronen Spiegelung"

Übersicht über synchrones Spiegeln

Die Funktion synchrone Spiegelung bietet Online-Datenreplizierung in Echtzeit zwischen Storage-Arrays über eine Remote-Entfernung.

Diese Funktion ist für das Speichersystem EF600/EF600C oder EF300/EF300C nicht verfügbar.

Was ist synchrones Spiegeln?

Synchronous Mirroring repliziert Daten-Volumes in Echtzeit, um eine kontinuierliche Verfügbarkeit zu gewährleisten. Storage Array Controller managen den Spiegelungsvorgang, der für Host Machines und Softwareapplikationen transparent ist.

Diese Art von Spiegelung ist ideal für Business Continuity-Zwecke wie Disaster Recovery.

Weitere Informationen:

- "Funktionsweise der synchronen Spiegelung"
- "Terminologie für synchrones Spiegeln"
- "Status der synchronen Spiegelung"
- "Volume-Eigentum"
- "Rollenänderung zwischen Volumes in einem gespiegelten Paar"

Wie konfiguriere ich die synchrone Spiegelung?

Sie müssen die ursprüngliche Spiegelungskonfiguration zwischen den Arrays über die Unified Manager-Schnittstelle durchführen. Sobald diese konfiguriert ist, können Sie gespiegelte Paare in System Manager managen.

Weitere Informationen:

- "Anforderungen für die Nutzung von synchroner Spiegelung"
- "Workflow für synchrones Spiegeln eines Volumes"
- "Synchrones gespiegeltes Paar erstellen (in Unified Manager)"

Verwandte Informationen

Erfahren Sie mehr über Konzepte zur synchronen Spiegelung:

- "Was Sie wissen müssen, bevor Sie ein gespiegeltes Paar erstellen"
- "Unterschiede zwischen der asynchronen Spiegelung und der synchronen Spiegelung"

Asynchrone Konzepte

Funktionsweise der asynchronen Spiegelung

Die asynchrone Spiegelung kopiert Daten-Volumes nach Bedarf oder nach einem Zeitplan. So werden Ausfallzeiten, die auf Datenbeschädigung oder -Verlust zurückzuführen sind, minimiert oder vermieden.

Das asynchrone Spiegeln erfasst den Status des primären Volumes zu einem bestimmten Zeitpunkt und kopiert nur die Daten, die sich seit der letzten Bildaufzeichnung geändert haben. Der primäre Standort kann sofort aktualisiert werden, während der sekundäre Standort mit der Bandbreite aktualisiert werden kann. Die Informationen werden im Cache gespeichert und später gesendet, sobald Netzwerkressourcen verfügbar sind.

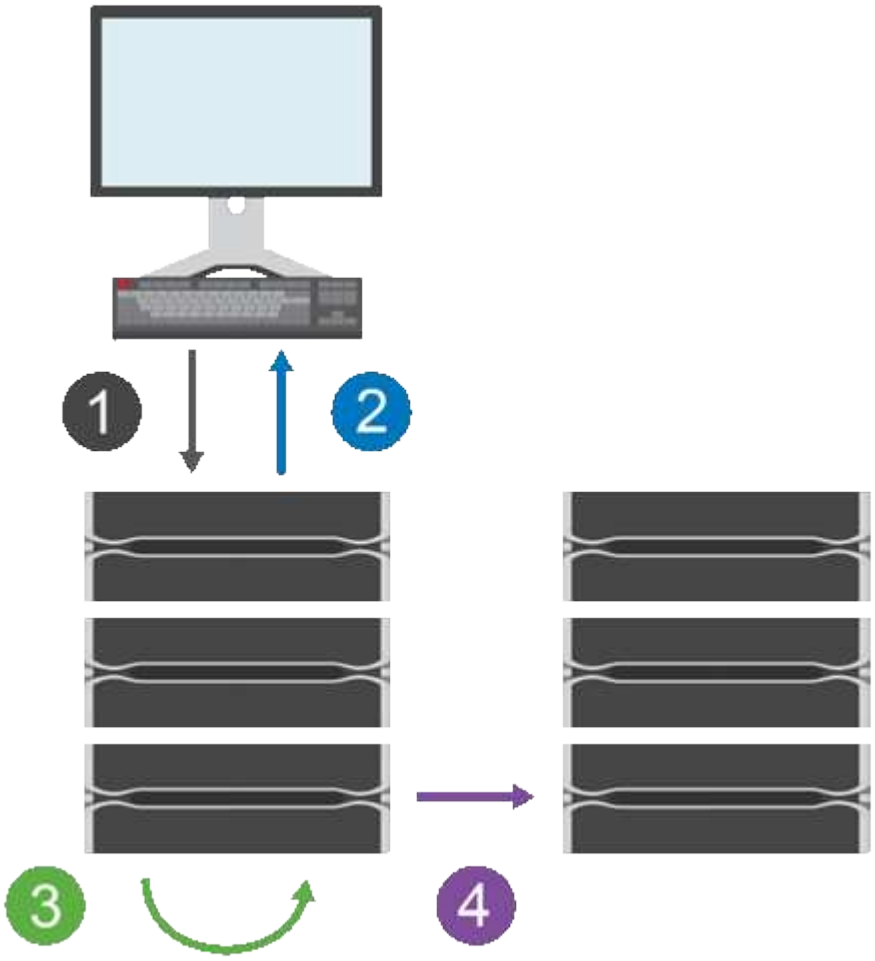
Diese Art der Spiegelung ist ideal für die Anforderungen an einen unterbrechungsfreien Betrieb und im Allgemeinen für periodische Prozesse wie Backup und Archivierung. Die Gründe für die Verwendung von asynchronem Spiegeln umfassen Folgendes:

- Remote-Backup-Konsolidierung:
- Schutz vor lokalen oder Wide-Area-Ausfällen
- Applikationsentwicklung und -Tests in einem zeitpunktgenauen Image von Live-Daten

Asynchrone Spiegelungssitzung

Das asynchrone Spiegeln erfasst den Status des primären Volumes zu einem bestimmten Zeitpunkt und kopiert nur die Daten, die sich seit der letzten Bildaufzeichnung geändert haben. Durch das asynchrone Spiegeln kann der primäre Standort sofort aktualisiert werden, während der sekundäre Standort mit der Bandbreite aktualisiert werden kann. Die Informationen werden im Cache gespeichert und später gesendet, sobald Netzwerkressourcen verfügbar sind.

Es gibt vier Hauptschritte in einer aktiven asynchronen Spiegelungssitzung.



1. Ein Schreibvorgang erfolgt zuerst auf dem Storage-Array des primären Volumes.
2. Der Status des Vorgangs wird an den Host zurückgegeben.
3. Alle Änderungen auf dem primären Volume werden protokolliert und nachverfolgt.
4. Alle Änderungen werden als Hintergrundprozess an das Storage-Array des sekundären Volume gesendet.

Diese Schritte werden gemäß den definierten Synchronisierungsintervallen wiederholt oder die Schritte können manuell wiederholt werden, wenn keine Intervalle definiert sind.

Bei der asynchronen Spiegelung werden Daten nur in festen Intervallen an den Remote Standort übertragen,

sodass lokale I/O-Vorgänge von langsamen Netzwerkverbindungen fast ebenso wenig beeinträchtigt werden. Da dieser Transfer nicht an den lokalen I/O gebunden ist, wird die Applikations-Performance nicht beeinträchtigt. Daher nutzt die asynchrone Spiegelung langsamere Verbindungen wie iSCSI und kann über größere Entfernungen zwischen lokalen und Remote-Storage-Systemen ausgeführt werden.

Die Speicher-Arrays müssen eine Firmware-Version von mindestens 7.84 aufweisen. (Beide können unterschiedliche OS-Versionen ausführen.)

Konsistenzgruppen und gespiegelte Paare spiegeln

Sie erstellen eine SpiegelungsConsistency Group, um die Spiegelbeziehung zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array herzustellen. Die Beziehung zur asynchronen Spiegelung besteht aus einem gespiegelten Paar: Einem primären Volume auf einem Storage Array und einem sekundären Volume auf einem anderen Storage Array.

Das Storage-Array, das das primäre Volume enthält, befindet sich normalerweise am primären Standort und dient den aktiven Hosts. Das Storage-Array mit dem sekundären Volume befindet sich normalerweise an einem sekundären Standort und enthält ein Replikat der Daten. Das sekundäre Volume enthält typischerweise eine Backup-Kopie der Daten und wird für Disaster Recovery verwendet.

Synchronisierungseinstellungen

Beim Erstellen eines gespiegelten Paares definieren Sie außerdem die Synchronisierungspriorität und die Resynchronisierungsrichtlinie, mit der das gespiegelte Paar den Neusynchronisierung nach einer Kommunikationsunterbrechung abgeschlossen.

Beim Erstellen einer Konsistenzgruppe für Spiegelungen definieren Sie außerdem die Synchronisierungspriorität und die Resynchronisierungsrichtlinie für alle gespiegelten Paare innerhalb der Gruppe. Die gespiegelten Paare verwenden die Synchronisierungspriorität und die Resynchronisierungsrichtlinie, um die Neusynchronisierung nach einer Kommunikationsunterbrechung abzuschließen.

Das primäre und sekundäre Volume in einem gespiegelten Paar können nicht synchronisiert werden, wenn das Storage-Array des primären Volume keine Daten auf das sekundäre Volume schreiben kann. Diese Bedingung kann durch folgende Probleme verursacht werden:

- Netzwerkprobleme zwischen lokalen und Remote-Speicher-Arrays.
- Ein ausgefallenes sekundäres Volume.
- Die Synchronisierung wird manuell auf dem gespiegelten Paar ausgesetzt.
- Konflikt mit der Spiegelgruppe.

Sie können Daten auf dem Remote-Speicher-Array entweder manuell oder automatisch synchronisieren.

Reservierte Kapazität und asynchrone Spiegelung

Mithilfe der reservierten Kapazität werden die Unterschiede zwischen dem primären und dem sekundären Volume nachverfolgt, wenn keine Synchronisierung stattfindet. Zudem überwacht er die Synchronisierungsstatistiken für jedes gespiegelte Paar.

Jedes Volume in einem gespiegelten Paar benötigt eine eigene reservierte Kapazität.

Konfiguration und Management

Um die Spiegelung zwischen zwei Arrays zu aktivieren und zu konfigurieren, müssen Sie die Unified Manager-

Schnittstelle verwenden. Sobald die Spiegelung aktiviert ist, können Sie gespiegelte Paare und Synchronisierungseinstellungen in System Manager verwalten.

Terminologie für asynchrone Spiegelung

Erfahren Sie, wie die Bedingungen für asynchrone Spiegelung auf Ihr Storage Array angewendet werden.

Laufzeit	Beschreibung
Lokales Storage-Array	Das lokale Storage-Array ist das Storage-Array, auf dem Sie arbeiten. Wenn in der Spalte Lokale Rolle **Primary** angezeigt wird, zeigt dies an, dass das Speicherarray das Volume enthält, das die primäre Rolle in der Spiegelbeziehung enthält. Wenn in der Spalte Lokale Rolle **sekundär** angezeigt wird, weist dies darauf hin, dass das Speicherarray das Volume enthält, das die sekundäre Rolle in der Spiegelbeziehung enthält.
Spiegelung der Konsistenzgruppe	Eine gespiegelte Konsistenzgruppe ist ein Container für ein oder mehrere gespiegelte Paare. Für asynchrone Spiegelungsvorgänge müssen Sie eine Konsistenzgruppe erstellen.
Gespiegeltes Paar	Ein gespiegeltes Paar besteht aus zwei Volumes, einem primären Volume und einem sekundären Volume. Bei der asynchronen Spiegelung gehört ein gespiegeltes Paar immer einer gespiegelten Konsistenzgruppe an. Schreibvorgänge werden zunächst auf dem primären Volume durchgeführt und dann auf das sekundäre Volume repliziert. Jedes gespiegelte Paar in einer Spiegelkonsistent-Gruppe verwendet dieselben Synchronisierungseinstellungen.
Primäres Volume	Das primäre Volume eines gespiegelten Paars ist das zu spiegelnden Quell-Volume.
Remote Storage Array	Das Remote Storage Array wird in der Regel als sekundärer Standort bezeichnet, der in der Regel ein Replikat der Daten in einer Spiegelungskonfiguration enthält.
Reservierte Kapazität	Reservierte Kapazität ist die zugewiesene physische Kapazität, die für jeden Kopierdienst- und Storage-Objekt verwendet wird. Er ist nicht direkt vom Host lesbar.
Rollenänderung	Rollenänderung bedeutet, dass dem sekundären Volume die primäre Rolle zugewiesen wird und umgekehrt.
Sekundäres Volume	Das sekundäre Volume eines gespiegelten Paars befindet sich normalerweise an einem sekundären Standort und enthält ein Replikat der Daten.

Laufzeit	Beschreibung
Synchronisierung	Die Synchronisierung erfolgt bei der ersten Synchronisierung zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array. Die Synchronisierung findet auch statt, wenn primäre und sekundäre Volumes nach einer Kommunikationsunterbrechung nicht mehr synchronisiert werden. Wenn die Kommunikationsverbindung wieder funktioniert, werden alle nicht replizierten Daten mit dem Storage-Array des sekundären Volumes synchronisiert.

Workflow für die asynchrone Spiegelung eines Volumes

Sie konfigurieren die asynchrone Spiegelung mithilfe des folgenden Workflows.

1. Die Erstkonfiguration in Unified Manager durchführen:
   a. Wählen Sie das lokale Speicher-Array als Quelle für den Datentransfer aus.
   b. Erstellen oder Auswählen einer vorhandenen SpiegelungsConsistency Group: Dies ist ein Container für das primäre Volume auf dem lokalen Array und dem sekundären Volume auf dem Remote-Array. Das primäre und sekundäre Volume werden als „gespiegeltes Paar“ bezeichnet. Wenn Sie zum ersten Mal die Spiegelkonsistent-Gruppe erstellen, legen Sie fest, ob Sie manuelle oder geplante Synchronisierungen durchführen möchten.
   c. Wählen Sie ein primäres Volume aus dem lokalen Speicher-Array aus, und bestimmen Sie dann die reservierte Kapazität. Die reservierte Kapazität ist die physisch zugewiesene Kapazität, die für den Kopiervorgang verwendet werden soll.
   d. Wählen Sie ein Remote-Speicher-Array als Ziel des Transfers, ein sekundäres Volume, und legen Sie dann seine reservierte Kapazität fest.
   e. Beginnen Sie den ersten Datentransfer vom primären Volume zum sekundären Volume. Je nach Volume-Größe kann dieser erste Transfer mehrere Stunden dauern.
2. Den Fortschritt der ersten Synchronisierung überprüfen:
   a. Starten Sie in Unified Manager den System Manager für das lokale Array.
   b. Zeigen Sie in System Manager den Status des Spiegelungsvorgangs an. Nach Abschluss der Spiegelung ist der Status des gespiegelten Paares „optimal“.
3. **Optional:** Sie können nachfolgende Datenüberweisungen in System Manager neu terminieren oder manuell durchführen. Es werden nur neue und geänderte Blöcke vom primären Volume auf das sekundäre Volume übertragen.

> Da die asynchrone Replizierung periodisch erfolgt, kann das System die geänderten Blöcke konsolidieren und Netzwerkbandbreite sparen. Der Schreibdurchsatz und die Schreiblatenz sind nur minimal beeinträchtigt.

Anforderungen für die Verwendung von asynchronem Spiegeln

Wenn Sie asynchrone Spiegelung verwenden möchten, beachten Sie die folgenden Anforderungen.

Unified Manager

Um die Spiegelung zwischen zwei Arrays zu aktivieren und zu konfigurieren, müssen Sie die Unified Manager-Schnittstelle verwenden. Unified Manager wird auf einem Host-System zusammen mit dem Web Services

Proxy installiert.

- Der Web Services Proxy-Dienst muss ausgeführt werden.
- Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung ausgeführt werden.
- Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr eigenes Sicherheitszertifikat mit Unified Manager installieren und zum Menü:Zertifikat[Zertifikatverwaltung] navigieren.

Storage-Arrays durchführt

- Sie müssen über zwei Storage-Arrays verfügen.
- Jedes Speicher-Array muss zwei Controller haben.
- Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
- Jeder Controller im primären Array und im sekundären Array muss über einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk verbunden sein.
- Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens 7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
- Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays kennen.
- Sie benötigen genügend freie Kapazität auf dem Remote-Speicher-Array, um ein sekundäres Volume zu erstellen, das dem primären Volume entspricht oder dessen Größe Sie spiegeln möchten.
- Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel Fabric- oder iSCSI-Schnittstelle verbunden.

Unterstützte Verbindungen

Beim asynchronen Spiegeln können FC- oder iSCSI-Verbindungen genutzt werden oder für die Kommunikation zwischen lokalen und Remote-Storage-Systemen. Beim Erstellen einer SpiegelungsConsistency Group kann der Administrator entweder FC oder iSCSI für diese Gruppe auswählen, wenn beide mit dem Remote-Speicher-Array verbunden sind. Es gibt kein Failover von einem Kanaltyp zum anderen.

Die asynchrone Spiegelung nutzt die Host-seitigen I/O-Ports des Storage-Arrays, um gespiegelte Daten von der primären Seite zur sekundären Seite zu übermitteln.

- **Spiegelung über eine Fibre-Channel-Schnittstelle**

  Jeder Controller des Storage-Arrays ordnet den am höchsten nummerierten FC-Host-Port der Spiegelung zu.

  Wenn der Controller sowohl Basis-FC-Ports als auch Host-Schnittstellenkarte (HIC) FC-Ports aufweist, ist der Port mit der höchsten Nummer auf einer HIC. Alle Hosts, die am dedizierten Port angemeldet sind, werden abgemeldet, und es werden keine Anmeldeanforderungen für den Host akzeptiert. I/O-Anfragen auf diesem Port werden nur von Controllern akzeptiert, die an Spiegelungsvorgängen beteiligt sind.

  Die dedizierten Spiegelungs-Ports müssen an eine FC-Fabric-Umgebung angeschlossen werden, die den Verzeichnisdienst und die Nameservice-Schnittstellen unterstützt. Insbesondere werden FC-AL und Point-to-Point nicht als Konnektivitätsoptionen zwischen den Controllern unterstützt, die an gespiegelten Beziehungen beteiligt sind.

- **Spiegelung über eine iSCSI-Schnittstelle**

Im Gegensatz zu FC erfordert iSCSI keinen dedizierten Port. Wenn Sie asynchrone Spiegelung in iSCSI-Umgebungen einsetzen, müssen Sie keine der Front-End iSCSI-Ports des Storage-Arrays für die asynchrone Spiegelung verwenden. Diese Ports werden sowohl für asynchronen Spiegeldatenverkehr als auch für Array-I/O-Verbindungen gemeinsam genutzt.

Der Controller verfügt über eine Liste der Remote-Speichersysteme, mit denen der iSCSI-Initiator versucht, eine Sitzung einzurichten. Der erste Port, der eine iSCSI-Verbindung erfolgreich herstellt, wird für die anschließende Kommunikation mit dem Remote-Speicher-Array verwendet. Wenn die Kommunikation fehlschlägt, wird eine neue Sitzung unter Verwendung aller verfügbaren Ports versucht.

ISCSI-Ports werden auf Array-Ebene für Port konfiguriert. Intercontroller Kommunikation für Konfigurationsnachrichten und Datentransfer verwendet die globalen Einstellungen, einschließlich Einstellungen für:

- VLAN: Sowohl lokale als auch Remote-Systeme müssen die gleiche VLAN-Einstellung für die Kommunikation haben
- ISCSI-Listening-Port
- Jumbo-Frames
- Ethernet-Priorität

> Die iSCSI-Intercontroller-Kommunikation muss einen Host-Connect-Port und nicht den Management-Ethernet-Port verwenden.

Die asynchrone Spiegelung nutzt die Host-seitigen I/O-Ports des Storage-Arrays, um gespiegelte Daten von der primären Seite zur sekundären Seite zu übermitteln. Da asynchrones Spiegeln für latenzarme, kostengünstigere Netzwerke ausgelegt ist, eignen sich iSCSI- (und damit TCP/IP-basierte) Verbindungen hervorragend für die IT. Wenn in iSCSI-Umgebungen asynchrone Spiegelung verwendet wird, müssen keine der Front-End-iSCSI-Ports des Arrays für asynchrone Spiegelung verwendet werden. Diese Ports werden sowohl für asynchronen Spiegeldatenverkehr als auch für Array-I/O-Verbindungen gemeinsam genutzt

Kandidaten für gespiegelte Volumes

- RAID-Level, Caching-Parameter und Segmentgröße können auf den primären und sekundären Volumes eines asynchronen gespiegelten Paars unterschiedlich sein.

> Bei EF600- und EF300-Controllern müssen die primären und sekundären Volumes eines asynchronen gespiegelten Paares dasselbe Protokoll, Tray-Level, Segmentgröße, Sicherheitstyp und RAID-Level erfüllen. Nicht geeignete asynchrone gespiegelte Paare werden nicht in der Liste der verfügbaren Volumes angezeigt.

- Das sekundäre Volume muss mindestens so groß sein wie das primäre Volume.
- Ein Volume kann nur an einer Spiegelbeziehung beteiligt sein.
- Volume-Kandidaten müssen dieselben Datensicherheitsfunktionen nutzen.
  - Wenn das primäre Volume FIPS-fähig ist, muss das sekundäre Volume FIPS-fähig sein.
  - Wenn das primäre Volume FDE-fähig ist, muss das sekundäre Volume FDE-fähig sein.
  - Wenn das primäre Volume keine Laufwerkssicherheit verwendet, darf das sekundäre Volume keine Laufwerkssicherheit verwenden.
- Primäre und sekundäre Volumes müssen denselben Laufwerkstyp verwenden. Die Kombination von NVMe

und SAS-Laufwerken zwischen primären und sekundären Volumes wird nicht unterstützt.

Reservierte Kapazität

- Ein reserviertes Kapazitäts-Volume ist für ein primäres Volume und ein sekundäres Volume in einem gespiegelten Paar für das Protokollieren von Schreibinformationen erforderlich, um nach einem Controller-Reset und anderen temporären Unterbrechungen wiederherzustellen.
- Da sowohl das primäre Volume als auch das sekundäre Volume in einem gespiegelten Paar zusätzliche reservierte Kapazität benötigen, müssen Sie sicherstellen, dass auf beiden Storage-Arrays in der Spiegelbeziehung freie Kapazität verfügbar ist.
- Das reservierte Volume mit Kapazität muss denselben Laufwerkstyp wie die zugehörigen Spiegelvolumes verwenden.
  - Wenn das reservierte Kapazitäts-Volume auf NVMe-Laufwerken erstellt wird, müssen auch seine Spiegelungs-Volumes auf NVMe-Laufwerken erstellt werden.
  - Wenn das reservierte Kapazitätsvolume auf SAS-Laufwerken erstellt wird, müssen auch seine Spiegelvolumes auf SAS-Laufwerken erstellt werden.

Laufwerkssicherheit

- Wenn Sie sichere Laufwerke verwenden, müssen das primäre und das sekundäre Volume über kompatible Sicherheitseinstellungen verfügen. Diese Beschränkung wird nicht durchgesetzt, deshalb müssen Sie sie selbst überprüfen.
- Bei Verwendung von sicheren Laufwerken sollten das primäre Volume und das sekundäre Volume denselben Laufwerkstyp verwenden. Diese Beschränkung wird nicht durchgesetzt, deshalb müssen Sie sie selbst überprüfen.
- Wenn Sie Data Assurance (da) verwenden, müssen das primäre Volume und das sekundäre Volume über dieselben da-Einstellungen verfügen.

Status der asynchronen Spiegelung

Der Status der Spiegelung definiert den Status von Konsistenzgruppen und gespiegelten Volume-Paaren.

Der Status von Spiegelungskonsistency Groups

Status	Beschreibung
Synchronisieren (erste Synchronisierung)	Der Fortschritt der ersten Datensynchronisation, die zwischen den gespiegelten Volume-Paaren abgeschlossen wurde. Während einer ersten Synchronisierung können die Volumes in folgende Zustände überführt werden: Degraded/failed/optimal/Unbekannt.
Synchronisieren (Intervallsynch)	Der Fortschritt der periodischen Datensynchronisierung, die zwischen den gespiegelten Volume-Paaren abgeschlossen wurde.

Status	Beschreibung
System unterbrochen	Speichersystemsuspendierte Synchronisierung von Daten auf allen gespiegelten Paaren auf der Ebene der Consistency Group als Spiegelung. Mindestens ein gespiegeltes Paar in der gespiegelten Konsistenzgruppe befindet sich in einem Status „angehalten“ oder „fehlgeschlagen“.
Benutzer ausgesetzt	Vom Benutzer suspendierte Synchronisierung von Daten auf allen gespiegelten Paaren auf der Ebene der Consistency Group Mirror. Dieser Status reduziert die Performance-Einbußen für die Host-Applikation, die auftreten können, während geänderte Daten im lokalen Storage-Array in das Remote Storage Array kopiert werden.
Angehalten	Die Datensynchronisierung wurde vorübergehend unterbrochen, weil ein Fehler beim Zugriff auf das Remote-Speicher-Array aufgetreten ist.
„Verlorene“	Ein verwaistes gespiegeltes Paar-Volume ist vorhanden, wenn ein Mitglied-Volume in einer Konsistenzgruppe entfernt wurde auf einer Seite der Consistency Mirror-Gruppe (entweder auf der primären oder sekundären Seite), nicht jedoch auf der anderen Seite. Verwaiste gespiegelte Paar-Volumes werden erkannt, wenn die Kommunikation zwischen den Arrays wiederhergestellt wird und die beiden Seiten der Spiegelkonfiguration die Spiegelparameter in Einklang bringen. Sie können ein gespiegeltes Paar entfernen, um den Status eines verwaisten gespiegelten Paares zu korrigieren.
Rollenänderung ausstehend/in-progress	Eine Rollenänderung zwischen den gespiegelten Konsistenzgruppen steht an oder wird gerade ausgeführt. Die Änderung der Rollenumkehr (entweder in eine primäre Rolle oder eine sekundäre Rolle) betrifft alle asynchronen gespiegelten Paare innerhalb der ausgewählten SpiegelConsistency Group. Sie können eine ausstehende Rollenänderung abbrechen, jedoch keine in Bearbeitung laufende Rollenänderung.
Rollenkonflikt	Ein Rollenkonflikt zwischen den Spiegelkonsistency Groups ist aufgetreten, weil bei einem Rollenänderungsvorgang ein Kommunikationsproblem zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array aufgetreten ist. Wenn das Kommunikationsproblem gelöst wurde, tritt ein Rollenkonflikt auf. Verwenden Sie den Recovery Guru zur Wiederherstellung nach diesem Fehler. Eine erzwungene Beförderung ist nicht zulässig, wenn ein Rollenkonflikt gelöst wird.

Status der gespiegelten Paare

Der Status eines gespiegelten Paars gibt an, ob die Daten auf dem primären Volume und auf dem sekundären Volume synchronisiert werden.

Status	Beschreibung
Synchronisieren	Der Fortschritt der anfänglichen oder periodischen Datensynchronisierung, die zwischen den gespiegelten Paaren abgeschlossen wurde. Es gibt zwei Arten der Synchronisierung: Die erste Synchronisierung und die periodische Synchronisierung. Der anfängliche Synchronisierungsfortschritt wird auch im Dialogfeld Long Running Operations angezeigt.
Optimal	Die Volumes im gespiegelten Paar sind synchronisiert, was bedeutet, dass die Verbindung zwischen den Speicher-Arrays betriebsbereit ist und jedes Volume sich in dem gewünschten Betriebszustand befindet.
Unvollständig	Das asynchrone gespiegelte Paar ist auf dem Remote-Speicher-Array unvollständig, da die Sequenz zur Erstellung eines gespiegelten Paares auf einem Speicher-Array initiiert wurde, das von System Manager nicht unterstützt wird und das gespiegelte Paar auf dem sekundären nicht abgeschlossen wurde. Der Erstellungsvorgang für gespiegelte Paare ist abgeschlossen, wenn der Konsistenzgruppe der Spiegelung im Remote-Speicher-Array ein Volume hinzugefügt wird. Dieses Volume wird zum sekundären Volume im asynchronen gespiegelten Paar. Das gespiegelte Paar wird automatisch abgeschlossen, wenn das Remote-Speicher-Array von System Manager verwaltet wird.
Fehlgeschlagen	Der asynchrone Spiegelungsvorgang kann aufgrund eines Fehlers bei den primären Volumes, sekundären Volumes oder der reservierten Spiegelkapazität nicht normal ausgeführt werden.
„Verlorene“	Ein verwaistes gespiegeltes Paar-Volume ist vorhanden, wenn ein Mitglied-Volume in einer Konsistenzgruppe entfernt wurde auf einer Seite der Consistency Mirror-Gruppe (entweder auf der primären oder sekundären Seite), nicht jedoch auf der anderen Seite. Verwaiste gespiegelte Paar-Volumes werden erkannt, wenn die Kommunikation zwischen den beiden Speicher-Arrays wiederhergestellt wird und die beiden Seiten der Spiegelkonfiguration die Spiegelparameter abstimmen. Sie können ein gespiegeltes Paar entfernen, um den Status eines verwaisten gespiegelten Paares zu korrigieren.
Angehalten	Das gespiegelte Paar befindet sich in einem Status „angehalten“, da sich die Konsistenzgruppe der Spiegelung in einem System befindet.

Volume-Eigentum

Sie können den bevorzugten Controller-Eigentümer in einem gespiegelten Paar ändern.

Wenn das primäre Volume des gespiegelten Paars Eigentum von Controller A ist, dann befindet sich das sekundäre Volume auch im Besitz von Controller A des Remote Storage Array. Wenn Sie den Eigentümer des primären Volume ändern, wird automatisch der Eigentümer des sekundären Volumes geändert, um sicherzustellen, dass beide Volumes Eigentum des gleichen Controllers sind. Aktuelle Eigentumsänderungen auf der primären Seite werden automatisch an die entsprechenden aktuellen Eigentumsänderungen auf der sekundären Seite übernommen.

Beispielsweise befindet sich ein primäres Volume im Besitz von Controller A, und dann ändern Sie den Controller-Inhaber in Controller B. In diesem Fall ändert der nächste Remote-Schreibvorgang den Controller-Eigentümer des sekundären Volumes von Controller A zu B. Da Änderungen an der Eigentumsrechte am Controller auf der sekundären Seite vom primären Standort gesteuert werden, sind keine besonderen Eingriffe durch den Storage-Administrator erforderlich.

Controller wird zurückgesetzt

Ein Reset des Controllers bewirkt eine Änderung des Volume-Eigentumsrechts auf der primären Seite vom bevorzugten Controller-Eigentümer zum alternativen Controller im Storage Array.

Manchmal wird ein Remote-Schreibvorgang durch einen Controller-Reset oder das aus- und Wiedereinschalten des Storage Arrays unterbrochen, bevor dieser auf das sekundäre Volume geschrieben werden kann. Der Controller muss in diesem Fall keine vollständige Synchronisation des gespiegelten Paares durchführen.

Wenn während eines Reset des Controllers ein Remote-Schreibvorgang unterbrochen wurde, liest der neue Controller-Eigentümer auf der primären Seite die in einer Protokolldatei im reservierten Kapazitäts-Volume des bevorzugten Controller-Inhabers gespeicherten Informationen. Der neue Controller-Eigentümer kopiert dann die betroffenen Datenblöcke vom primären Volume auf das sekundäre Volume, sodass keine vollständige Synchronisierung der gespiegelten Volumes erforderlich ist.

Rollenwechsel einer SpiegelungsConsistency Group

Sie können die Rolle zwischen gespiegelten Paaren in einer gespiegelten Consistency Group ändern. Hierzu können Sie die Konsistenzgruppe der primären Spiegelung auf die sekundäre Rolle zurückstufen oder die Konsistenzgruppe für die sekundäre Spiegelung in die primäre Rolle heraufstufen.

Überprüfen Sie die folgenden Informationen über den Rollenänderungsvorgang:

- Die Rollenänderung betrifft alle gespiegelten Paare innerhalb der ausgewählten SpiegelConsistency Group.
- Wenn eine SpiegelungsConsistency Group auf die sekundäre Rolle herabgestuft wird, werden alle gespiegelten Paare innerhalb dieser SpiegelConsistency Group auch auf die sekundäre Rolle herabgestuft und umgekehrt.
- Wenn die primäre SpiegelungsConsistency Group auf die sekundäre Rolle herabgestuft wird, haben Hosts, die den Mitgliedvolumes innerhalb dieser Gruppe zugewiesen wurden, keinen Schreibzugriff mehr auf sie.
- Wenn eine gespiegelte Konsistenzgruppe in die primäre Rolle heraufgestuft wird, können alle Hosts, die auf die Mitglied-Volumes innerhalb dieser Gruppe zugreifen, diese nun schreiben.
- Wenn das lokale Speicher-Array nicht mit dem Remote-Speicher-Array kommunizieren kann, können Sie

die Rollenänderung im lokalen Speicher-Array erzwingen.

Rollenänderung erzwingen

Sie können eine Rollenänderung zwischen gespiegelten Konsistenzgruppen erzwingen, wenn ein Kommunikationsproblem zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array verhindert, dass die Mitglied-Volumes innerhalb der Konsistenzgruppe der sekundären Spiegelung befördert werden oder die Herabstufung der Mitglied-Volumes innerhalb der Konsistenz der primären Spiegelung ausfällt Gruppieren.

Sie können die gespiegelte Konsistenzgruppe auf der sekundären Seite zu der primären Rolle zwingen. Anschließend ist der Recovery-Host in der Lage, auf die neu beworbenen Mitglieder-Volumes innerhalb dieser SpiegelKonsistenzgruppe zuzugreifen, und Geschäftsprozesse können fortgesetzt werden.

Wann ist eine erzwungene Promotion zulässig und nicht zulässig?

Die erzwungene Beförderung einer SpiegelungsConsistency Group ist nur zulässig, wenn alle Mitglied-Volumes der Consistency Group synchronisiert wurden und über konsistente Recovery-Punkte verfügen.

Die erzwungene Beförderung einer SpiegelungsConsistency Group ist unter den folgenden Bedingungen nicht zulässig:

- Jedes der Mitgliedsvolumes einer SpiegelungsConsistency Group befindet sich im Prozess einer ersten Synchronisation.
- Jedes Mitglied-Volume einer SpiegelungsConsistency Group verfügt über kein Point-in-Time-Image des Wiederherstellungspunkts (beispielsweise aufgrund eines vollständigen Kapazitätsfehlers).
- Die Konsistenzgruppe der Spiegelung enthält keine Mitglied-Volumes.
- Die Konsistenzgruppe der Spiegelung befindet sich im Status „Fehlgeschlagen“, „Role-Change-Pending“ oder „Role-Change-in-Progress“ oder „Failed eines der zugehörigen Mitglied-Volumes oder reservierten Kapazitäts-Volumes“.

Konflikt mit der Spiegelgruppe

Wenn ein Kommunikationsproblem zwischen den lokalen und den Remote-Speicher-Arrays behoben wurde, tritt ein Konflikt zwischen den Spiegelgruppen-Rollen auf. Verwenden Sie den Recovery Guru zur Wiederherstellung nach diesem Fehler. Eine erzwungene Beförderung ist nicht zulässig, wenn ein Konflikt mit zwei Rollen gelöst wird.

Um den Konflikt zwischen den Spiegelgruppen und den nachfolgenden Wiederherstellungsschritten zu vermeiden, warten Sie, bis die Verbindung zwischen den Speicherarrays betriebsbereit ist, um die Rollenänderung zu erzwingen.

Rollenänderung in Bearbeitung

Wenn zwei Speicher-Arrays in einer Spiegelungskonfiguration getrennt werden, und die primäre Seite einer SpiegelungsConsistency Group zum Zurückstufen auf eine sekundäre Rolle geherabgestuft wird und die sekundäre Seite einer SpiegelungsConsistency Group erzwingen wird, wird sie zu einer primären Rolle heraufgestuft. Wenn die Kommunikation wiederhergestellt wird, werden die gespiegelten Konsistenzgruppen auf beiden Storage Arrays in den Status „Role Change-in-Progress“ versetzt.

Das System führt den Rollenänderungsprozess durch, indem die Änderungsprotokolle übertragen, neu synchronisiert, der Zustand der Consistency Group auf den normalen Betriebszustand zurückversetzt und regelmäßig synchronisiert wird.

Konzepte synchronisieren

Funktionsweise der synchronen Spiegelung

Bei der synchronen Spiegelung werden Daten-Volumes in Echtzeit repliziert, um eine kontinuierliche Verfügbarkeit zu gewährleisten.

Synchrones Spiegeln ist für das EF600/EF600C oder EF300/EF300C Storage-Array nicht verfügbar.

Beim synchronen Spiegeln wird ein Recovery Point Objective (RPO) von null verloren gegangene Daten erreicht, da eine Kopie wichtiger Daten verfügbar ist, falls auf einem der beiden Storage Arrays ein Ausfall auftritt. Die Kopie ist zu jedem Zeitpunkt identisch mit den Produktionsdaten. Jedes Mal, wenn ein Schreibvorgang auf dem primären Volume ausgeführt wird, wird auf dem sekundären Volume ein Schreibvorgang vorgenommen. Der Host erhält keine Bestätigung, dass der Schreibvorgang erfolgreich war, bis das sekundäre Volume mit den Änderungen auf dem primären Volume erfolgreich aktualisiert wurde.

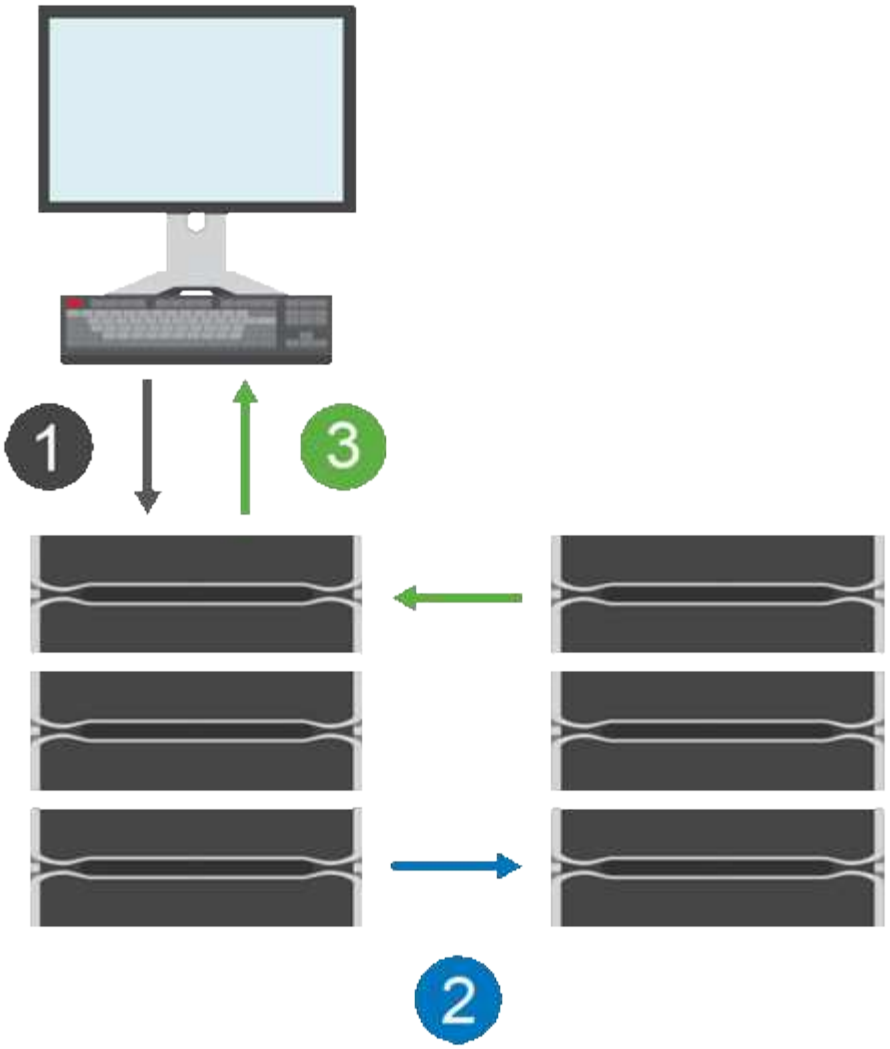
Diese Art von Spiegelung ist ideal für Business Continuity-Zwecke wie Disaster Recovery.

Beziehung zwischen synchronem Spiegeln

Eine synchrone Spiegelbeziehung besteht aus einem primären Volume und einem sekundären Volume auf separaten Storage Arrays. Das Storage-Array, das das primäre Volume enthält, befindet sich normalerweise am primären Standort und dient den aktiven Hosts. Das Storage-Array mit dem sekundären Volume befindet sich normalerweise an einem sekundären Standort und enthält ein Replikat der Daten. Das sekundäre Volume wird verwendet, wenn das Storage Array des primären Volumes nicht verfügbar ist, beispielsweise wegen eines vollständigen Stromausfalls, eines Brandes oder eines Hardware-Ausfalls am primären Standort.

Sitzung zur synchronen Spiegelung

Bei der Konfiguration der synchronen Spiegelung müssen Volumes zu Paaren konfiguriert werden. Nachdem Sie ein gespiegeltes Paar erstellt haben, das aus einem primären Volume auf einem Storage Array und einem sekundären Volume auf einem anderen Storage Array besteht, können Sie mit der synchronen Spiegelung beginnen. Die Schritte im synchronen Spiegeln sind unten dargestellt.



1. Ein Schreibvorgang erfolgt vom Host.
2. Der Schreibvorgang wird an das primäre Volume übertragen, an das Remote-System übertragen und anschließend an das sekundäre Volume übertragen.
3. Das Storage-Array des primären Volumes sendet eine I/O-Abschlussmeldung an das Host-System *nachdem* beide Schreibvorgänge erfolgreich abgeschlossen wurden.

Die reservierte Kapazität wird verwendet, um Informationen über die eingehende Schreibanforderung von einem Host zu protokollieren.

Wenn der aktuelle Controller-Eigentümer des primären Volume eine Schreibanforderung von einem Host empfängt, protokolliert der Controller zuerst Informationen über den Schreibzugriff auf die reservierte Kapazität des primären Volumes. Anschließend werden die Daten auf das primäre Volume geschrieben. Anschließend initiiert der Controller einen Remote-Schreibvorgang, um die betroffenen Datenblöcke in das sekundäre Volume des Remote-Storage Arrays zu kopieren.

Da die Host-Anwendung warten muss, bis der Schreibvorgang auf dem lokalen Speicher-Array und im Netzwerk auf dem Remote-Speicher-Array erfolgt, Eine sehr schnelle Verbindung zwischen dem lokalen Storage Array und dem Remote Storage Array ist erforderlich, um die Spiegelbeziehung aufrechtzuerhalten, ohne die lokale I/O Performance zu übermäßig zu reduzieren.

Disaster Recovery

Bei der synchronen Spiegelung werden eine Kopie von Daten gespeichert, die sich physisch vom Standort entfernt befindet. Falls am primären Standort – beispielsweise bei einem Stromausfall oder einer Überflutung – ein Ausfall auftritt, ist der Zugriff auf die Daten vom sekundären Standort aus schnell möglich.

Das sekundäre Volume ist zum Hosten von Applikationen nicht verfügbar, während der Synchronous Mirroring-Vorgang läuft. Somit kann bei einem Ausfall des lokalen Storage-Arrays ein Failover auf das Remote-Storage-Array durchgeführt werden. Setzen Sie das sekundäre Volume für die primäre Rolle ein, um ein Failover zu ermöglichen. Anschließend kann der Recovery-Host auf das neu beworbene Volume zugreifen, und die Geschäftsabläufe können fortgesetzt werden.

Synchronisierungseinstellungen

Beim Erstellen eines gespiegelten Paares definieren Sie außerdem die Synchronisierungspriorität und die Resynchronisierungsrichtlinie, mit der das gespiegelte Paar den Neusynchronisierung nach einer Kommunikationsunterbrechung abgeschlossen.

Wenn die Kommunikationsverbindung zwischen den beiden Speicherarrays nicht mehr funktioniert, erhalten Hosts weiterhin Bestätigungen vom lokalen Speicher-Array, um einen Zugriffsverlust zu verhindern. Wenn die Kommunikationsverbindung wieder funktioniert, können alle nicht replizierten Daten automatisch oder manuell zum Remote-Speicher-Array resynchronisiert werden.

Ob Daten automatisch neu synchronisiert werden, hängt von der Resynchronisierung des gespiegelten Paars ab. Eine automatische Neusynchronisierung ermöglicht dem gespiegelten Paar die automatische Neusynchronisierung, wenn die Verbindung wieder funktioniert. Bei einer manuellen Neusynchronisierung müssen Sie die Synchronisierung nach einem Kommunikationsproblem manuell fortsetzen. Eine manuelle Neusynchronisierung ist die empfohlene Richtlinie.

Sie können die Synchronisierungseinstellungen für ein gespiegeltes Paar nur auf dem Speicher-Array bearbeiten, das das primäre Volume enthält.

Nicht synchronisierte Daten

Das primäre und das sekundäre Volume werden nicht synchronisiert, wenn das Storage-Array des primären Volumes keine Daten auf das sekundäre Volume schreiben kann. Dies kann durch folgende Probleme verursacht werden:

- Netzwerkprobleme zwischen lokalen und Remote-Speicher-Arrays
- Ein ausgefallenes sekundäres Volume
- Die Synchronisierung wird manuell auf dem gespiegelten Paar ausgesetzt

Verwaiste gespiegelte Paare

Ein verwaistes gespiegeltes Paar-Volume ist vorhanden, wenn ein Mitglied-Volume auf einer Seite entfernt wurde (entweder auf der primären oder sekundären Seite), aber nicht auf der anderen Seite.

Verwaiste gespiegelte Paar-Volumes werden erkannt, wenn die Kommunikation zwischen den Arrays wiederhergestellt wird und die beiden Seiten der Spiegelkonfiguration die Spiegelparameter in Einklang bringen.

Sie können ein gespiegeltes Paar entfernen, um den Status eines verwaisten gespiegelten Paares zu korrigieren.

Konfiguration und Management

Um die Spiegelung zwischen zwei Arrays zu aktivieren und zu konfigurieren, müssen Sie die Unified Manager-Schnittstelle verwenden. Sobald die Spiegelung aktiviert ist, können Sie gespiegelte Paare und Synchronisierungseinstellungen in System Manager verwalten.

Terminologie für synchrones Spiegeln

Erfahren Sie, wie die Bedingungen für synchrone Spiegelung auf Ihr Storage Array angewendet werden.

Laufzeit	Beschreibung
Lokales Storage-Array	Das lokale Storage-Array ist das Storage-Array, auf dem Sie arbeiten. Wenn in der Spalte Lokale Rolle **Primary** angezeigt wird, zeigt dies an, dass das Speicherarray das Volume enthält, das die primäre Rolle in der Spiegelbeziehung enthält. Wenn in der Spalte Lokale Rolle **sekundär** angezeigt wird, weist dies darauf hin, dass das Speicherarray das Volume enthält, das die sekundäre Rolle in der Spiegelbeziehung enthält.
Gespiegeltes Paar	Ein gespiegeltes Paar besteht aus zwei Volumes, einem primären Volume und einem sekundären Volume.
Primäres Volume	Das primäre Volume eines gespiegelten Paars ist das zu spiegelnden Quell-Volume.
Recovery-Zeitpunkt (RPO)	Der Recovery-Zeitpunkt (Recovery Point Objective, RPO) bezeichnet ein Ziel, das die als akzeptabel berücksichtigende Differenz zwischen dem primären Volume und dem sekundären Volume in einem gespiegelten Paar angibt. Ein RPO von null zeigt an, dass kein Unterschied zwischen dem primären Volume und dem sekundären Volume toleriert werden kann. Ein RPO größer als null zeigt an, dass das sekundäre Volume weniger aktuell ist oder weniger hinter dem primären Volume liegt.
Remote Storage Array	Das Remote Storage Array wird in der Regel als sekundärer Standort bezeichnet, der in der Regel ein Replikat der Daten in einer Spiegelungskonfiguration enthält.
Reservierte Kapazität	Reservierte Kapazität ist die zugewiesene physische Kapazität, die für jeden Kopierdienst- und Storage-Objekt verwendet wird. Er ist nicht direkt vom Host lesbar.
Rollenänderung	Rollenänderung bedeutet, dass dem sekundären Volume die primäre Rolle zugewiesen wird und umgekehrt.
Sekundäres Volume	Das sekundäre Volume eines gespiegelten Paars befindet sich normalerweise an einem sekundären Standort und enthält ein Replikat der Daten.

Laufzeit	Beschreibung
Synchronisierung	Die Synchronisierung erfolgt bei der ersten Synchronisierung zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array. Die Synchronisierung findet auch statt, wenn primäre und sekundäre Volumes nach einer Kommunikationsunterbrechung nicht mehr synchronisiert werden. Wenn die Kommunikationsverbindung wieder funktioniert, werden alle nicht replizierten Daten mit dem Storage-Array des sekundären Volumes synchronisiert.

Workflow für synchrones Spiegeln eines Volumes

Sie konfigurieren die synchrone Spiegelung unter Verwendung des folgenden Workflows.

Diese Funktion ist für das Speichersystem EF600/EF600C oder EF300/EF300C nicht verfügbar.

1. Die Erstkonfiguration in Unified Manager durchführen:
   a. Wählen Sie ein lokales Speicher-Array als Quelle für den Datentransfer aus.
   b. Wählen Sie ein primäres Volume aus dem lokalen Speicher-Array aus.
   c. Wählen Sie ein Remote-Speicher-Array als Ziel für den Datentransfer aus, und wählen Sie dann ein sekundäres Volume aus.
   d. Wählen Sie Synchronisierungsprioritäten und Neusynchronisierung aus.
   e. Beginnen Sie den ersten Datentransfer vom primären Volume zum sekundären Volume. Je nach Volume-Größe kann dieser erste Transfer mehrere Stunden dauern.
2. Den Fortschritt der ersten Synchronisierung überprüfen:
   a. Starten Sie in Unified Manager den System Manager für das lokale Array.
   b. Zeigen Sie in System Manager den Status des Spiegelungsvorgangs an. Nach Abschluss der Spiegelung ist der Status des gespiegelten Paares „optimal“. Die beiden Arrays versuchen, während des normalen Betriebs synchronisiert zu bleiben. Es werden nur neue und geänderte Blöcke vom primären Volume auf das sekundäre Volume übertragen.
3. **Optional:** die Synchronisationseinstellungen können in System Manager geändert werden.

Da die synchrone Replizierung kontinuierlich erfolgt, muss die Replizierungsverbindung zwischen den beiden Standorten ausreichend Bandbreitenkapazität bereitstellen.

Anforderungen für die Nutzung von synchroner Spiegelung

Wenn Sie die synchrone Spiegelung verwenden möchten, beachten Sie die folgenden Anforderungen.

Unified Manager

Um die Spiegelung zwischen zwei Arrays zu aktivieren und zu konfigurieren, müssen Sie die Unified Manager-Schnittstelle verwenden. Unified Manager wird auf einem Host-System zusammen mit dem Web Services Proxy installiert.

- Der Web Services Proxy-Dienst muss ausgeführt werden.

- Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung ausgeführt werden.
- Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr eigenes Sicherheitszertifikat mit Unified Manager installieren und zum Menü:Zertifikat[Zertifikatverwaltung] navigieren.

Storage-Arrays durchführt

Synchrones Spiegeln ist für das Storage-Array EF300/EF300C oder EF600/EF600C nicht verfügbar.

- Sie müssen über zwei Storage-Arrays verfügen.
- Jedes Speicher-Array muss zwei Controller haben.
- Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
- Jeder Controller im primären Array und im sekundären Array muss über einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk verbunden sein.
- Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens 7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
- Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays kennen.
- Sie benötigen genügend freie Kapazität auf dem Remote-Speicher-Array, um ein sekundäres Volume zu erstellen, das dem primären Volume entspricht oder dessen Größe Sie spiegeln möchten.
- Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel Fabric verbunden.

Unterstützte Verbindungen

Kommunikation für synchrones Spiegeln wird nur auf Controllern mit Fibre Channel (FC) Host Ports unterstützt.

Bei der synchronen Spiegelung wird der am höchsten nummerierte Host Port auf jedem Controller verwendet, sowohl auf dem lokalen Storage-Array als auch auf dem Remote-Storage-Array. Der Controller Host Bus Adapter (HBA) Host-Port 4 ist normalerweise für die Übertragung von Spiegeldaten reserviert.

Kandidaten für gespiegelte Volumes

- RAID-Level, Caching-Parameter und Segmentgröße können auf den primären und sekundären Volumes eines synchronen gespiegelten Paars unterschiedlich sein.
- Die primären und sekundären Volumes in einem synchronen gespiegelten Paar müssen Standard-Volumes sein. Es können keine dünnen Volumes oder Snapshot Volumes sein.
- Das sekundäre Volume muss mindestens so groß sein wie das primäre Volume.
- Mit dem primären Volume sind möglicherweise nur Snapshots verknüpft, und/oder das Quell- oder Ziel-Volume während eines Volume-Kopiervorgangs.
- Ein Volume kann nur an einer Spiegelbeziehung beteiligt sein.
- Die Anzahl der Volumes, die auf einem bestimmten Storage Array unterstützt werden, ist begrenzt. Stellen Sie sicher, dass die Anzahl der konfigurierten Volumes in Ihrem Speicher-Array kleiner als das unterstützte Limit ist. Wenn das synchrone Spiegeln aktiv ist, werden die zwei reservierten Kapazitäts-Volumes, die erstellt werden, mit der Volume-Obergrenze verglichen.

Reservierte Kapazität

- Für ein primäres Volume und ein sekundäres Volume zur Protokollierung von Schreibinformationen zum Wiederherstellen nach Controller-Resets und anderen vorübergehenden Unterbrechungen ist die reservierte Kapazität erforderlich.
- Die reservierten Kapazitäts-Volumes werden automatisch bei aktivierter synchronen Spiegelung erstellt. Da sowohl das primäre Volume als auch das sekundäre Volume in einem gespiegelten Paar reservierte Kapazität benötigen, müssen Sie sicherstellen, dass auf beiden Storage-Arrays, die an der Beziehung zur synchronen Spiegelung beteiligt sind, ausreichend freie Kapazität zur Verfügung steht.

Laufwerkssicherheit

- Wenn Sie sichere Laufwerke verwenden, müssen das primäre und das sekundäre Volume über kompatible Sicherheitseinstellungen verfügen. Diese Beschränkung wird nicht durchgesetzt, deshalb müssen Sie sie selbst überprüfen.
- Bei Verwendung von sicheren Laufwerken sollten das primäre Volume und das sekundäre Volume denselben Laufwerkstyp verwenden. Diese Beschränkung wird nicht durchgesetzt, deshalb müssen Sie sie selbst überprüfen.
  - Wenn das primäre Volume vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) verwendet, sollten auf dem sekundären Volume FDE-Laufwerke verwendet werden.
  - Wenn das primäre Volume gemäß FIPS (Federal Information Processing Standards 140-2) zertifizierte Laufwerke verwendet, sollte auf dem sekundären Volume FIPS 140-2-2-zertifizierte Laufwerke verwendet werden.
- Wenn Sie Data Assurance (da) verwenden, müssen das primäre Volume und das sekundäre Volume über dieselben da-Einstellungen verfügen.

Status der synchronen Spiegelung

Der Status eines synchronen gespiegelten Paars gibt an, ob die Daten auf dem primären Volume und auf dem sekundären Volume synchronisiert werden. Ein Spiegelstatus ist unabhängig vom Komponentenstatus der Volumes im gespiegelten Paar.

Diese Funktion ist für das Speichersystem EF600/EF600C oder EF300/EF300C nicht verfügbar.

Synchrone gespiegelte Paare können einen der folgenden Status aufweisen:

- **Optimal**

  Gibt an, dass die Volumes im gespiegelten Paar synchronisiert werden. Das bedeutet, dass die Fabric-Verbindung zwischen den Storage-Arrays funktionsfähig ist und jedes Volume sich in dem gewünschten Betriebszustand befindet.

- **Synchronisieren**

  Zeigt den Fortschritt der Datensynchronisierung zwischen den gespiegelten Paaren an. Dieser Status wird auch während der ersten Synchronisierung angezeigt.

  Nach einer Unterbrechung der Kommunikationsverbindung werden nur die Datenblöcke, die sich während der Verbindungsunterbrechung auf dem primären Volume geändert haben, auf das sekundäre Volume kopiert.

- **Nicht Synchronisiert**

  Zeigt an, dass das Speicher-Array des primären Volumes keine eingehenden Daten auf das Remote-Array schreiben kann. Der lokale Host kann weiterhin auf das primäre Volume schreiben, aber Remote-Schreibvorgänge erfolgen nicht. Verschiedene Bedingungen können verhindern, dass das Storage-Array des primären Volume eingehende Daten auf das sekundäre Volume schreibt, z. B.:

  - Auf das sekundäre Volume ist nicht zugegriffen werden kann.
  - Auf das Remote-Speicher-Array kann nicht zugegriffen werden.
  - Auf die Fabric-Verbindung zwischen den Storage-Arrays kann nicht zugegriffen werden.
  - Das sekundäre Volume kann nicht mit einem neuen World Wide Identifier (WWID) aktualisiert werden.

- * Ausgesetzt*

  Zeigt an, dass der Synchronspiegelungsvorgang vom Benutzer unterbrochen wurde. Wenn ein gespiegeltes Paar ausgesetzt wird, wird kein Versuch unternommen, das sekundäre Volume zu kontaktieren. Alle Schreibvorgänge auf dem primären Volume werden permanent in den reservierten Kapazitäts-Volumes des Spiegels protokolliert.

- **Fehlgeschlagen**

  Zeigt an, dass der Vorgang der synchronen Spiegelung nicht normal ausgeführt werden kann, weil das primäre Volume, das sekundäre Volume oder die reservierte Kapazität des Spiegels ausfällt.

Volume-Eigentum

Sie können den bevorzugten Controller-Eigentümer in einem gespiegelten Paar ändern.

> Diese Funktion ist für die synchrone Spiegelung auf dem Storage-System EF600/EF600C oder EF300/EF300C nicht verfügbar.

Wenn das primäre Volume des gespiegelten Paars Eigentum von Controller A ist, dann befindet sich das sekundäre Volume auch im Besitz von Controller A des Remote Storage Array. Wenn Sie den Eigentümer des primären Volume ändern, wird automatisch der Eigentümer des sekundären Volumes geändert, um sicherzustellen, dass beide Volumes Eigentum des gleichen Controllers sind. Aktuelle Eigentumsänderungen auf der primären Seite werden automatisch an die entsprechenden aktuellen Eigentumsänderungen auf der sekundären Seite übernommen.

Beispielsweise befindet sich ein primäres Volume im Besitz von Controller A, und dann ändern Sie den Controller-Inhaber in Controller B. In diesem Fall ändert der nächste Remote-Schreibvorgang den Controller-Eigentümer des sekundären Volumes von Controller A zu B. Da Änderungen an der Eigentumsrechte am Controller auf der sekundären Seite vom primären Standort gesteuert werden, sind keine besonderen Eingriffe durch den Storage-Administrator erforderlich.

Controller wird zurückgesetzt

Ein Reset des Controllers bewirkt eine Änderung des Volume-Eigentumsrechts auf der primären Seite vom bevorzugten Controller-Eigentümer zum alternativen Controller im Storage Array.

Manchmal wird ein Remote-Schreibvorgang durch einen Controller-Reset oder das aus- und Wiedereinschalten des Storage Arrays unterbrochen, bevor dieser auf das sekundäre Volume geschrieben werden kann. Der Controller muss in diesem Fall keine vollständige Synchronisation des gespiegelten Paares durchführen.

Wenn während eines Reset des Controllers ein Remote-Schreibvorgang unterbrochen wurde, liest der neue Controller-Eigentümer auf der primären Seite die in einer Protokolldatei im reservierten Kapazitäts-Volume des bevorzugten Controller-Inhabers gespeicherten Informationen. Der neue Controller-Eigentümer kopiert dann die betroffenen Datenblöcke vom primären Volume auf das sekundäre Volume, sodass keine vollständige Synchronisierung der gespiegelten Volumes erforderlich ist.

Rollenänderung zwischen Volumes in einem gespiegelten Paar

Sie können die Rolle zwischen Volumes in einem gespiegelten Paar ändern. Dazu wird das primäre Volume auf die sekundäre Rolle herabstufen oder das sekundäre Volume auf die primäre Rolle heraufstufen.

Synchrones Spiegeln ist auf dem Storage-System EF600/EF600C oder EF300/EF300C nicht verfügbar.

Überprüfen Sie die folgenden Informationen über den Rollenänderungsvorgang:

- Wenn ein primäres Volume auf die sekundäre Rolle herabgestuft wird, wird das sekundäre Volume in diesem gespiegelten Paar zur primären Rolle heraufgestuft und umgekehrt.
- Wenn das primäre Volume auf die sekundäre Rolle herabgestuft wird, haben Hosts, die diesem Volume zugewiesen wurden, keinen Schreibzugriff mehr.
- Wenn das sekundäre Volume zur primären Rolle heraufgestuft wird, können alle Hosts, die auf das Volume zugreifen, jetzt darauf schreiben.
- Wenn das lokale Speicher-Array nicht mit dem Remote-Speicher-Array kommunizieren kann, können Sie die Rollenänderung im lokalen Speicher-Array erzwingen.

Rollenänderung erzwingen

Sie können eine Rollenänderung zwischen Volumes in einem gespiegelten Paar erzwingen, wenn ein Kommunikationsproblem zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array die Heraufstufung des sekundären Volumes oder die Herabstufung des primären Volumes verhindert.

Sie können das Volume auf der sekundären Seite dazu zwingen, zur primären Rolle zu wechseln. Anschließend kann der Recovery-Host auf das neu aufgestuften Volume zugreifen, und der Geschäftsbetrieb kann fortgesetzt werden.

Wenn das Remote-Speicher-Array wiederhergestellt wurde und eventuelle Kommunikationsprobleme behoben wurden, tritt ein Synchronous Mirroring - Primary Volume Conflict-Zustand auf. Zu den Wiederherstellungsschritten gehört auch die Neusynchronisierung der Volumes. Verwenden Sie den Recovery Guru zur Wiederherstellung nach diesem Fehler.

Wann ist eine erzwungene Promotion zulässig und nicht zulässig?

Die erzwungene Beförderung eines Volumes in einem gespiegelten Paar ist unter den folgenden Bedingungen nicht zulässig:

- Jedes der Volumes in einem gespiegelten Paar ist dabei, eine erste Synchronisierung durchzuführen.
- Das gespiegelte Paar befindet sich im Status „Fehlgeschlagen“, „Role-Change-Pending“ oder „Role-Change-in-Progress“ oder wenn eines der zugehörigen Volumes mit reservierter Kapazität ausfällt.

Rollenänderung in Bearbeitung

Wenn zwei Speicher-Arrays in einer Spiegelungskonfiguration getrennt werden, und das primäre Volume eines gespiegelten Paars erzwingen, dass es zu einer sekundären Rolle herabgestuft wird, und das sekundäre Volume eines gespiegelten Paares wird zu einer primären Rolle heraufgestuft. Wenn die Kommunikation wiederhergestellt wird, werden die Volumes auf beiden Storage Arrays im Status „Role-Change-in-Progress“ platziert.

Das System führt den Rollenänderungsprozess durch, indem die Änderungsprotokolle übertragen, neu synchronisiert, der Zustand des gespiegelten Paares auf einen normalen Betriebszustand zurückversetzt wird und die Synchronisation fortführt.

Management von asynchronen Spiegelungskonzerne

Testen Sie die Kommunikation für Spiegelkonsistency Groups

Sie können den Kommunikationslink testen, um mögliche Kommunikationsprobleme zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array zu diagnostizieren, das mit einer SpiegelKonsistenzgruppe verknüpft ist.

Bevor Sie beginnen

Die zu testenden Mirror Consistency Group muss sich auf den lokalen und Remote Storage Arrays befinden.

Über diese Aufgabe

Sie können vier verschiedene Tests ausführen:

- **Konnektivität** — überprüft, ob die beiden Controller einen Kommunikationspfad haben. Der Konnektivitätstest sendet eine Array-übergreifende Meldung zwischen den Storage Arrays und validiert dann, dass die entsprechende gespiegelte Konsistenzgruppe im Remote-Storage-Array vorhanden ist. Die Software validiert außerdem, dass die Mitglied-Volumes der Consistency Group des Remote Storage Arrays die Mitglied-Volumes der Mirror-Consistency Group auf dem lokalen Speicher-Array entsprechen.
- **Latenz** — sendet einen SCSI Test Unit-Befehl an jedes gespiegelte Volume im Remote-Speicher-Array, das mit der Consistency Mirror-Gruppe verknüpft ist, um die minimale, durchschnittliche und maximale Latenz zu testen.
- **Bandwidth** — sendet zwei Inter-Array-Nachrichten an das Remote-Speicher-Array, um die minimale, durchschnittliche und maximale Bandbreite sowie die ausgehandelte Verbindungsgeschwindigkeit des Ports auf dem Array zu testen, der den Test durchführt.
- **Port Connections** — zeigt den Port, der für die Spiegelung auf dem lokalen Speicher-Array verwendet wird, und den Port, der die gespiegelten Daten auf dem Remote-Speicher-Array empfängt.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Wählen Sie die Registerkarte **Mirror Consistency Groups** aus, und wählen Sie dann die zu testenden Mirror Consistency Group aus.
3. Wählen Sie **Kommunikation Testen**.

   Das Dialogfeld Testkommunikation wird angezeigt.

4. Wählen Sie einen oder mehrere Kommunikationstests aus, die zwischen den lokalen und externen Speicher-Arrays durchgeführt werden sollen, die der ausgewählten SpiegelConsistency Group zugeordnet sind, und klicken Sie dann auf **Test**.

5. Überprüfen Sie die im Ergebnisfenster angezeigten Informationen.

Status Des Kommunikationstests	Beschreibung
Normal ohne Fehler	Die Konsistenzgruppe der Spiegelung kommuniziert ordnungsgemäß.
Status bestanden (aber nicht normal)	Überprüfen Sie mögliche Netzwerk- oder Verbindungsprobleme, und versuchen Sie den Test erneut.
Status fehlgeschlagen	Der Grund für den Fehler wird angezeigt. Verwenden Sie den Recovery Guru zur Behebung des Problems.
Port-Verbindungsfehler	Der Grund kann sein, dass das lokale Speicher-Array nicht verbunden ist oder das Remote-Speicher-Array nicht kontaktiert werden kann. Verwenden Sie den Recovery Guru zur Behebung des Problems.

Ergebnisse

Nach Abschluss des Kommunikationstests wird in diesem Dialogfeld ein Status „Normal“, ein Status „bestanden“ oder ein Status „Fehlgeschlagen“ angezeigt.

Wenn der Kommunikationstest einen fehlgeschlagenen Status zurückgibt, wird der Test nach dem Schließen dieses Dialogfelds weiter ausgeführt, bis die Kommunikation zwischen den gespiegelten Konsistenzgruppen wiederhergestellt ist.

Unterbrechen oder Fortsetzen der Synchronisierung für die SpiegelungsConsistency Group

Die Synchronisation der Daten auf allen gespiegelten Paaren innerhalb einer Spiegelkonsistent-Gruppe kann unterbrochen oder fortgesetzt werden. Dies ist effizienter als das Unterbrechen oder Wiederaufnehmen der Synchronisierung auf einzelnen gespiegelten Paaren.

Über diese Aufgabe

Durch das Anhalten und Wiederaufnehmen der Synchronisierung mit Gruppen werden die Auswirkungen auf die Performance der Host-Applikation verringert. Dies kann auftreten, wenn geänderte Daten im lokalen Speicher-Array in das Remote-Speicher-Array kopiert werden.

Der Status der SpiegelungsConsistency Group und die gespiegelten Paare bleiben ausgesetzt, bis Sie die Option Resume verwenden, um die Synchronisationstätigkeit wieder aufzunehmen.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Wählen Sie die Registerkarte * Consistency Groups spiegeln* aus.

   Die Tabelle der gespiegelten Consistency Group wird angezeigt und zeigt alle dem Speicher-Array zugeordneten Spiegelkonsistency Groups an.

3. Wählen Sie die Konsistenzgruppe „Mirror“ aus, die Sie aussetzen oder fortsetzen möchten, und wählen Sie dann entweder Menü:Mehr[Suspend] oder Menü:Mehr[Fortsetzen].

Das System zeigt eine Bestätigung an.

4. Wählen Sie zur Bestätigung * Ja* aus.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Pausiert oder setzt den Datentransfer zwischen allen gespiegelten Paaren in einer Spiegelkonsistent-Gruppe fort, ohne die Spiegelbeziehung zu entfernen.
- Protokolliert alle Daten, die auf die primäre Seite der Spiegelgruppe geschrieben wurden, während die Spiegelgruppe ausgesetzt wird und die Daten automatisch auf die sekundäre Seite der Spiegelgruppe schreibt, wenn die Spiegelgruppe wieder aufgenommen wird. Eine vollständige Synchronisation ist nicht erforderlich.
- Für eine Consistency Groups *suspended* mirror zeigt in der Tabelle Mirror Consistency Groups **user-suspended** an.
- Im Rahmen einer _wiederaufgenommenen Spiegelung Konsistenzgruppe werden Daten, die auf die primären Volumes geschrieben wurden, während die Konsistenzgruppe der Spiegelung unterbrochen wurde, sofort auf die sekundären Volumes geschrieben. Die regelmäßige Synchronisierung wird fortgesetzt, wenn ein Intervall für die automatische Synchronisierung festgelegt wurde.

Ändern Sie die Synchronisierungseinstellungen für eine gespiegelte Konsistenzgruppe

Sie können die Synchronisierungseinstellungen und die Warnschwellenwerte ändern, die von der Spiegelkonsistent-Gruppe im lokalen Speicher-Array verwendet werden, wenn Daten zu Beginn synchronisiert werden oder wenn Daten während der asynchronen Spiegelung neu synchronisiert werden.

Über diese Aufgabe

Das Ändern der Synchronisationseinstellungen wirkt sich auf die Synchronisierungsvorgänge aller gespiegelten Paare innerhalb der Consistency Mirror-Gruppe aus.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Wählen Sie die Registerkarte * Consistency Groups spiegeln* aus.

   Die Tabelle der gespiegelten Consistency Group wird angezeigt und zeigt alle dem Speicher-Array zugeordneten Spiegelkonsistency Groups an.

3. Wählen Sie die Konsistenzgruppe „Spiegel“ aus, die Sie bearbeiten möchten, und wählen Sie dann Menü:Mehr[Einstellungen bearbeiten].

   Das Dialogfeld „Einstellungen bearbeiten“ wird angezeigt.

4. Bearbeiten Sie die Synchronisierungseinstellungen und die Einstellungen für Warnmeldungen, und klicken Sie dann auf **Speichern**.

Felddetails

Feld	Beschreibung
Die gespiegelten Paare synchronisieren…	Geben Sie an, ob Sie die gespiegelten Paare auf dem Remote-Speicher-Array manuell oder automatisch synchronisieren möchten. • **Manuell** – Wählen Sie diese Option, um die gespiegelten Paare auf dem Remote-Speicher-Array manuell zu synchronisieren. • **Automatisch jedes** – Wählen Sie diese Option, um die gespiegelten Paare auf dem Remote-Speicher-Array automatisch zu synchronisieren, indem Sie das Zeitintervall vom Beginn des vorherigen Updates bis zum Beginn des nächsten Updates angeben. Das Standardintervall beträgt 10 Minuten.
Warnung…	Wenn Sie die Synchronisationsmethode auf automatisch einstellen, legen Sie die folgenden Warnungen fest: • **Synchronisation** – Einstellen der Zeitdauer, nach der der System Manager eine Warnung sendet, dass die Synchronisierung noch nicht abgeschlossen ist. • **Remote Recovery Point** – Festlegen eines Zeitlimits, nach dem System Manager eine Warnmeldung ausgibt, die angibt, dass die Recovery Point-Daten auf dem Remote-Speicher-Array älter als die festgelegte Zeitgrenze sind. Definieren Sie die Zeitgrenze ab dem Ende der vorherigen Aktualisierung. • **Schwellenwert für reservierte Kapazität** – Definieren Sie einen reservierten Kapazitätsbetrag, bei dem System Manager eine Warnung sendet, dass Sie sich dem Schwellenwert für die reservierte Kapazität nähern. Definieren Sie den Schwellenwert um den Prozentsatz der verbleibenden Kapazität.

Ergebnisse

System Manager ändert die Synchronisierungseinstellungen für jedes gespiegelte Paar in der Consistency Group.

Die SpiegelungsConsistency Group manuell neu synchronisieren

Sie können die Neusynchronisierung für alle gespiegelten Paare innerhalb einer SpiegelungsConsistency Group manuell starten.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Wählen Sie die Registerkarte * Consistency Groups spiegeln* aus.

   Die Tabelle Mirror Consistency Group wird angezeigt und zeigt alle dem Speicher-Array zugeordneten Spiegelkonsistency Groups an.

3. Wählen Sie die SpiegelungsConsistency Group aus, die Sie erneut synchronisieren möchten, und wählen

Sie dann Menü:Mehr[manuell neu synchronisieren].

Das System zeigt eine Bestätigung an.

4. Wählen Sie zur Bestätigung * Ja* aus.

Ergebnisse

Das System führt die folgenden Aktionen durch:

- Initiiert die erneute Synchronisation von Daten auf allen gespiegelten Paaren innerhalb der ausgewählten SpiegelungsConsistency Group.
- Aktualisiert geänderte Daten vom lokalen Speicher-Array auf das Remote-Speicher-Array.

Zeigen Sie die nicht synchronisierte Datenmenge zwischen gespiegelten Konsistenzgruppen an

Sie können die Menge der nicht synchronisierten Daten zwischen den Spiegelungskonsistenzgruppen im lokalen Speicher-Array und auf dem Remote-Speicher-Array anzeigen. Während sich die Konsistenzgruppe der Spiegelung in einem nicht synchronisierten Status befindet, erfolgt keine Spiegelungsaktivität.

Über diese Aufgabe

Sie können diese Aufgabe ausführen, wenn die ausgewählte SpiegelungsConsistency Group gespiegelte Paare enthält und die Synchronisierung derzeit nicht ausgeführt wird.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Wählen Sie die Registerkarte * Consistency Groups spiegeln* aus.

   Die Tabelle Mirror Consistency Group wird angezeigt und zeigt alle dem Speicher-Array zugeordneten Spiegelkonsistency Groups an.

3. Klicken Sie auf Menü:Mehr[Unsynchronisierte Datenmenge anzeigen].

   Wenn nicht synchronisierte Daten vorhanden sind, spiegeln die Tabellenwerte dies wider. In der Spalte Datenbetrag wird der nicht synchronisierte Datenbetrag in MiB aufgelistet.

Remote-IP-Adresse aktualisieren

Sie können die iSCSI-IP-Adresse für Ihr Remote-Speicher-Array aktualisieren, um die Verbindung mit dem lokalen Speicher-Array wiederherzustellen.

Bevor Sie beginnen

Das lokale Storage-Array und das Remote-Storage-Array müssen für asynchrone Spiegelung über eine iSCSI-Verbindung konfiguriert werden.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Wählen Sie die Registerkarte * Consistency Groups spiegeln* aus.

   In der Tabelle Mirror Consistency Group werden alle dem Speicher-Array zugeordneten Spiegelkonsistency Groups angezeigt.

3. Wählen Sie die zu aktualisierenden Spiegelkonsistent-Gruppe aus, und wählen Sie dann Menü:Mehr[Remote-IP-Adresse aktualisieren].

   Das Dialogfeld Remote-IP-Adresse aktualisieren wird angezeigt.

4. Wählen Sie **Update**, um die iSCSI-IP-Adresse für Ihr Remote-Speicher-Array zu aktualisieren.

Ergebnisse

Das System setzt die IP-Adresse des Remote-Speicher-Arrays zurück, um die Verbindung zum lokalen Speicher-Array wiederherzustellen.

Ändern Sie die Rolle der gespiegelten Consistency Group auf primär oder sekundär

Sie können die Rolle zwischen gespiegelten Konsistenzgruppen für administrative Zwecke oder im Falle einer Störung im lokalen Speicher-Array ändern.

Über diese Aufgabe

Die primäre Rolle wird durch Spiegelkonsistency Groups, die auf dem lokalen Speicher-Array erstellt wurden, übernommen. Spiegelung von auf dem Remote-Speicher-Array erstellten Konsistenzgruppen enthalten die sekundäre Rolle. Sie können die Konsistenzgruppe der lokalen Spiegelung auf eine sekundäre Rolle herabstufen oder die Consistency Group für Remote-Spiegelungen auf eine primäre Rolle hochstufen.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Wählen Sie die Registerkarte * Consistency Groups spiegeln* aus.

   Die Tabelle Mirror Consistency Group wird angezeigt und zeigt alle dem Speicher-Array zugeordneten Spiegelkonsistency Groups an.

3. Wählen Sie die Consistency Mirror-Gruppe aus, für die Sie die Rolle ändern möchten, und wählen Sie dann Menü:Mehr[Rolle ändern in <Primär > Sekundär>]**>**.

   Das System zeigt eine Bestätigung an.

4. Bestätigen Sie, dass Sie die Rolle der Consistency Mirror-Gruppe ändern möchten, und klicken Sie dann auf **Rolle ändern**.

> ⓘ Das Dialogfeld „Speicher-Array nicht kontaktieren“ wird angezeigt, wenn eine Rollenänderung angefordert wird, aber das Remote-Speicher-Array kann nicht kontaktiert werden. Klicken Sie auf **Ja**, um die Rollenänderung zu erzwingen.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- In der Tabelle Mirror Consistency Group wird neben der SpiegelConsistency Group, die die Rollenänderung durchläuft, der Status „ausstehend“ oder „in Bearbeitung“ angezeigt. Sie können einen ausstehenden Rollenänderungsvorgang abbrechen, indem Sie auf den Link **Abbrechen** in der Tabellenzelle klicken.
- Wenn die zugehörige gespiegelte Konsistenzgruppe kontaktiert werden kann, ändern sich die Rollen zwischen den Konsistenzgruppen für die Spiegelung. System Manager unterstützt die Konsistenzgruppe der sekundären Spiegelung auf eine primäre Rolle oder stuft die Konsistenzgruppe der primären Spiegelung auf eine sekundäre Rolle ein (abhängig von Ihrer Auswahl). Die Rollenänderung betrifft alle

gespiegelten Paare innerhalb der ausgewählten SpiegelConsistency Group.

Löschen der gespiegelten Konsistenzgruppe

Sie können gespiegelte Konsistenzgruppen löschen, die nicht mehr im lokalen Storage Array und im Remote-Storage Array benötigt werden.

Bevor Sie beginnen

Alle gespiegelten Paare müssen aus der Consistency Mirror-Gruppe entfernt werden.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Wählen Sie die Registerkarte * Consistency Groups spiegeln* aus.

   Die Tabelle Mirror Consistency Group wird angezeigt und zeigt alle dem Speicher-Array zugeordneten Spiegelkonsistency Groups an.

3. Wählen Sie die zu löschende SpiegelungsConsistency Group aus, und wählen Sie dann Menü:Sonstige Aufgaben[Löschen] aus.

   Das System zeigt eine Bestätigung an.

4. Wählen Sie **Ja** aus, um die Consistency Mirror-Gruppe zu löschen.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Löscht zuerst die SpiegelConsistency Group auf dem lokalen Speicher-Array und löscht dann die SpiegelConsistency Group auf dem Remote-Speicher-Array.
- Entfernt die gespiegelte Konsistenzgruppe aus der Tabelle „Konsistenzgruppe spiegeln“.

Nachdem Sie fertig sind

Gelegentlich kann es vorkommen, dass die gespiegelte Konsistenzgruppe erfolgreich aus dem lokalen Speicher-Array gelöscht wird, aber ein Kommunikationsfehler verhindert, dass die gespiegelte Konsistenzgruppe aus dem Remote-Speicher-Array gelöscht wird. In diesem Fall müssen Sie auf das Remote-Speicher-Array zugreifen, um die entsprechende gespiegelte Konsistenzgruppe zu löschen.

Management von asynchronen gespiegelten Paaren

Entfernen Sie die asynchrone Spiegelbeziehung

Ein gespiegeltes Paar entfernen Sie die gespiegelte Beziehung vom primären Volume auf dem lokalen Storage Array und dem sekundären Volume im Remote Storage Array.

Über diese Aufgabe

Prüfen Sie die folgenden Informationen zu verwaisten gespiegelten Paaren:

- Ein verwaister gespiegeltes Paar ist vorhanden, wenn ein Mitglied-Volume einer Consistency Mirror-Gruppe auf einer Seite entfernt wurde (entweder auf der Seite des lokalen Speicher-Arrays oder auf der Seite des Remote-Speicher-Arrays), jedoch nicht auf der anderen Seite.
- Verwaiste gespiegelte Paare werden erkannt, wenn die Kommunikation zwischen den Arrays

wiederhergestellt wird und die beiden Seiten der Spiegelkonfiguration die Spiegelparameter abgleichen.

- Sie können ein gespiegeltes Paar entfernen, um den Status eines verwaisten gespiegelten Paares zu korrigieren.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Wählen Sie die Registerkarte **gespiegeltes Paar** aus.

   Die Tabelle mit gespiegelten Paaren wird angezeigt und zeigt alle gespiegelten Paare an, die dem Speicher-Array zugeordnet sind.

3. Wählen Sie das gespiegelte Paar aus, das Sie entfernen möchten, und klicken Sie dann auf **Entfernen**.
4. Bestätigen Sie, dass Sie das gespiegelte Paar entfernen möchten, und klicken Sie dann auf **Entfernen**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Entfernt die Spiegelbeziehung aus der SpiegelungsConsistency Group auf dem lokalen Speicher-Array und auf dem Remote-Speicher-Array und löscht die reservierte Kapazität.
- Liefert das primäre und das sekundäre Volume zu hostfreien, nicht gespiegelten Volumes zurück.
- Aktualisiert die Kachel „Asynchronous Mirroring“ beim Entfernen des asynchronen gespiegelten Paares.

Reservierte Kapazität wird erhöht

Sie können die reservierte Kapazität erhöhen, die die physisch zugewiesene Kapazität, die für jeden Kopiervorgang auf einem Storage-Objekt genutzt wird.

Bei Snapshot-Vorgängen beträgt dieser Anteil normalerweise 40 % des Basis-Volumes. Bei asynchronen Spiegelungsvorgängen beträgt der Anteil des Basis-Volumes normalerweise 20 %. Normalerweise erhöhen Sie die reservierte Kapazität, wenn Sie eine Warnung erhalten, dass die reservierte Kapazität des Storage-Objekts voll wird.

Bevor Sie beginnen

- Das Volume im Pool oder in der Volume-Gruppe muss den optimalen Status aufweisen und darf sich nicht in einem bestimmten Zustand befinden.
- Freie Kapazität muss im Pool bzw. in der Volume-Gruppe vorhanden sein, mit der die Kapazität erhöht werden soll.

  Wenn auf einem Pool oder Volume-Gruppen keine freie Kapazität vorhanden ist, können Sie einem Pool oder einer Volume-Gruppe nicht zugewiesene Kapazität in Form nicht verwendeter Laufwerke hinzufügen.

Über diese Aufgabe

Sie können die reservierte Kapazität nur in Schritten von 8 gib für die folgenden Storage-Objekte erhöhen:

- Snapshot-Gruppe
- Snapshot Volume
- Mitgliedsvolume der Konsistenzgruppe
- Gespiegeltes Paar-Volume

Verwenden Sie einen hohen Prozentsatz, wenn Sie glauben, dass das primäre Volume viele Änderungen durchlaufen hat oder wenn die Lebensdauer eines bestimmten Kopierdienstes sehr lang ist.

> Sie können die reservierte Kapazität für ein schreibgeschütztes Snapshot-Volume nicht erhöhen. Nur Snapshot Volumes mit Lese- und Schreibvorgängen erfordern reservierte Kapazität.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Wählen Sie die Registerkarte **reservierte Kapazität** aus.
3. Wählen Sie das Speicherobjekt aus, für das Sie die reservierte Kapazität erhöhen möchten, und klicken Sie dann auf **Kapazität erhöhen**.

   Das Dialogfeld reservierte Kapazität erhöhen wird angezeigt.

4. Verwenden Sie die Spinner-Box, um den Kapazitätsanteil einzustellen.

   Wenn im Pool oder in der Volume-Gruppe keine freie Kapazität vorhanden ist, die das ausgewählte Speicherobjekt enthält, und das Speicher-Array über nicht zugewiesene Kapazität verfügt, können Sie einen neuen Pool oder eine neue Volume-Gruppe erstellen. Sie können diesen Vorgang dann mit der neuen freien Kapazität in diesem Pool bzw. dieser Volume-Gruppe wiederholen.

5. Klicken Sie Auf **Erhöhen**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Erhöht die reservierte Kapazität für das Storage-Objekt.
- Zeigt die neu hinzugefügte reservierte Kapazität an.

Ändern Sie die Einstellungen für die reservierte Kapazität eines gespiegelten Paar-Volumes

Sie können die Einstellungen für ein Volume mit gespiegelten Paaren ändern, um den Prozentpunkt anzupassen, an dem SANtricity System Manager eine Warnmeldung sendet, wenn die reservierte Kapazität für ein Volume mit gespiegelten Paaren fast voll ist.

Schritte

1. Wählen Sie Menü:Speicher[Pools & Volume Groups].
2. Wählen Sie die Registerkarte **reservierte Kapazität** aus.
3. Wählen Sie das zu bearbeitende gespiegelte Paar-Volume aus und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld Einstellungen für die reservierte Kapazität des gespiegelten Paar-Volumes wird angezeigt.

4. Ändern Sie gegebenenfalls die Einstellungen für die reservierte Kapazität des gespiegelten Paar-Volumes.

Felddetails

Einstellung	Beschreibung
Benachrichtigen, wenn…	Verwenden Sie das Spinner-Feld, um den Prozentpunkt anzupassen, an dem System Manager eine Benachrichtigung sendet, wenn die reservierte Kapazität eines gespiegelten Paares sich der vollen Kapazität nähert. Wenn die reservierte Kapazität für das gespiegelte Paar den angegebenen Schwellenwert überschreitet, sendet System Manager eine Warnmeldung, sodass Sie die reservierte Kapazität erweitern können. Durch Ändern der Alarmeinstellung für ein gespiegeltes Paar wird die Alarmeinstellung für alle gespiegelten Paare, die zur gleichen SpiegelungsConsistency Group gehören, geändert.

5. Klicken Sie auf **Speichern**, um Ihre Änderungen anzuwenden.

Vollständiges gespiegeltes Paar für auf dem alten System erstellte primäre Volumes

Wenn Sie ein primäres Volume auf einem älteren Storage-Array erstellt haben, das nicht durch SANtricity System Manager gemanagt werden kann, können Sie das sekundäre Volume auf diesem Array mit SANtricity System Manager erstellen.

Über diese Aufgabe

Sie können asynchrone Spiegelungen zwischen älteren Arrays durchführen, die eine andere Schnittstelle verwenden, und neuere Arrays, die von System Manager gemanagt werden können.

- Wenn Sie zwischen zwei Speicher-Arrays, die System Manager verwenden, spiegeln, können Sie diese Aufgabe überspringen, da Sie das gespiegelte Paar in der Erstellungsreihenfolge für gespiegelte Paare bereits abgeschlossen haben.
- Führen Sie diese Aufgabe auf dem Remote-Speicher-Array aus.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Wählen Sie die Registerkarte **gespiegeltes Paar** aus.

   Die Tabelle mit gespiegelten Paaren wird angezeigt und zeigt alle gespiegelten Paare an, die dem Speicher-Array zugeordnet sind.

3. Suchen Sie das gespiegelte Paar-Volume mit dem Status „unvollständig“ und klicken Sie dann auf den in der Spalte „gespiegeltes Paar“ angezeigten Link **complete mirrored Pair**.
4. Wählen Sie aus, ob Sie die Sequenz zur Erzeugung des gespiegelten Paares automatisch oder manuell abschließen möchten, indem Sie eine der folgenden Optionsfelder auswählen:
   - **Automatisch** — Erstellen Sie ein neues sekundäres Volumen.

     Akzeptieren Sie die Standardeinstellungen für die Remote-Seite des gespiegelten Paars, indem Sie einen vorhandenen Pool oder eine Volume-Gruppe auswählen, in dem das sekundäre Volume erstellt

werden soll. Verwenden Sie diese empfohlene Option, um die reservierte Kapazität für das sekundäre Volume mit den Standardeinstellungen zuzuweisen.

- **Manual** — Wählen Sie ein vorhandenes Volumen aus.

  Definieren Sie Ihre eigenen Parameter für das sekundäre Volume.

  i. Klicken Sie auf **Weiter**, um das sekundäre Volume auszuwählen.

  ii. Wählen Sie ein vorhandenes Volume aus, das Sie als sekundäres Volume verwenden möchten, und klicken Sie dann auf **Weiter**, um die reservierte Kapazität zuzuweisen.

  iii. Weisen Sie die reservierte Kapazität zu. Führen Sie einen der folgenden Schritte aus:

  - Übernehmen Sie die Standardeinstellungen.

    Die Standardeinstellung für die reservierte Kapazität ist 20 % der Kapazität des Basis-Volumes, und in der Regel reicht diese Kapazität aus.

  - Weisen Sie Ihre eigenen reservierten Kapazitätseinstellungen zu, um Ihre Storage-Anforderungen im Zusammenhang mit der asynchronen Spiegelung zu erfüllen.

    Die erforderliche Kapazität variiert abhängig von der Häufigkeit und Größe der I/O-Schreibvorgänge auf dem primären Volume und wie lange Sie die Kapazität beibehalten müssen. Im Allgemeinen wählen Sie eine größere Kapazität für reservierte Kapazität aus, wenn eine oder beide Bedingungen vorhanden sind:

    - Sie beabsichtigen, das gespiegelte Paar für einen langen Zeitraum zu halten.
    - Ein großer Prozentsatz an Datenblöcken ändert sich auf dem primären Volume aufgrund von hoher I/O-Aktivität. Mithilfe von historischen Performance-Daten oder anderen Betriebssystem-Utilities können Sie typische I/O-Aktivitäten für das primäre Volume ermitteln.

5. Wählen Sie **Vollständig**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Erstellt das sekundäre Volume auf dem Remote-Storage-Array und weist der Remote-Seite des gespiegelten Paars reservierte Kapazität zu.
- Startet die erste Synchronisierung zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array.
- Wenn es sich bei dem zu spiegelnden Volume um ein Thin Volume handelt, werden während der ersten Synchronisierung nur die zugewiesenen Blöcke auf das sekundäre Volume übertragen. Diese Übertragung reduziert die Menge der Daten, die übertragen werden müssen, um die erste Synchronisierung abzuschließen.
- Legt die reservierte Kapazität für das gespiegelte Paar auf dem lokalen Speicher-Array und auf dem Remote-Speicher-Array fest.

Management von synchronen, gespiegelten Paaren

Testen Sie die Kommunikation zur synchronen Spiegelung

Sie können die Kommunikation zwischen einem lokalen Speicher-Array und einem Remote-Speicher-Array testen, um mögliche Kommunikationsprobleme für ein

gespiegeltes Paar zu diagnostizieren, das an der synchronen Spiegelung beteiligt ist.

Über diese Aufgabe

Es werden zwei verschiedene Tests durchgeführt:

- **Kommunikation** — überprüft, ob die beiden Speicher-Arrays einen Kommunikationspfad haben. Der Kommunikationstest überprüft, ob das lokale Speicher-Array mit dem Remote-Speicher-Array kommunizieren kann und ob das mit dem gespiegelten Paar verbundene sekundäre Volume auf dem Remote-Speicher-Array vorhanden ist.
- **Latenz** — sendet einen SCSI-Testeinheit-Befehl an das sekundäre Volume auf dem Remote-Speicher-Array, das mit dem gespiegelten Paar verbunden ist, um die minimale, durchschnittliche und maximale Latenz zu testen.

Schritte

1. Wählen Sie Menü:Speicher[Synchronous Mirroring].
2. Wählen Sie das gespiegelte Paar aus, das Sie testen möchten, und wählen Sie dann **Kommunikation testen**.
3. Überprüfen Sie die im Ergebnisfenster angezeigten Informationen und befolgen Sie bei Bedarf die angezeigten Korrekturmaßnahmen.

> Wenn der Kommunikationstest fehlschlägt, wird der Test nach dem Schließen dieses Dialogfelds fortgesetzt, bis die Kommunikation zwischen dem gespiegelten Paar wiederhergestellt ist.

Die Synchronisierung für ein gespiegeltes Paar unterbrechen und fortsetzen

Sie können die Option „anhalten“ und „Wiederaufnehmen“ verwenden, um zu steuern, wann die Daten auf dem primären Volume und dem sekundären Volume in einem gespiegelten Paar synchronisiert werden sollen.

Über diese Aufgabe

Wenn ein gespiegeltes Paar manuell unterbrochen wird, synchronisiert das gespiegelte Paar erst dann, wenn es manuell wieder aufgenommen wird.

Schritte

1. Wählen Sie Menü:Speicher[Synchronous Mirroring].
2. Wählen Sie das gespiegelte Paar aus, das Sie aussetzen oder fortsetzen möchten, und wählen Sie dann entweder Menü:Mehr[Suspend] oder Menü:Mehr[Fortsetzen].

   Das System zeigt eine Bestätigung an.

3. Wählen Sie zur Bestätigung * Ja* aus.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Pausiert oder setzt die Datenübertragung zwischen dem gespiegelten Paar ein, ohne die gespiegelte Beziehung zu entfernen.
- Für ein *suspended* gespiegeltes Paar:

- Zeigt **suspended** in der Tabelle Mirrored Pair an.
- Protokolliert alle Daten, die während der Synchronisierung auf das primäre Volume des gespiegelten Paars geschrieben wurden.

- Bei einem *fortgesetzten* gespiegelten Paar werden die Daten automatisch auf das sekundäre Volume des gespiegelten Paars geschrieben, wenn die Synchronisierung wieder aufgenommen wird. Eine vollständige Synchronisation ist nicht erforderlich.

Ändern Sie die Rolle zwischen Volumes in einem gespiegelten Paar

Sie können eine Rollenumkehr zwischen den beiden Volumes in einem gespiegelten Paar, das an der synchronen Spiegelung beteiligt ist, durchführen. Diese Aufgabe kann für administrative Zwecke oder im Falle eines Disasters auf dem lokalen Speicher-Array notwendig sein.

Über diese Aufgabe

Sie können das primäre Volume entweder auf die sekundäre Rolle zurückstufen oder das sekundäre Volume zur primären Rolle heraufstufen. Alle Hosts, die auf das primäre Volume zugreifen, haben Lese-/Schreibzugriff auf das Volume. Wenn das primäre Volume zum sekundären Volume wird, werden nur durch den primären Controller initiierte Remote-Schreibvorgänge auf das Volume geschrieben.

Schritte

1. Wählen Sie Menü:Speicher[Synchronous Mirroring].
2. Wählen Sie das gespiegelte Paar aus, das die Volumes enthält, für die Sie die Rolle ändern möchten, und wählen Sie dann Menü:Mehr[Rolle ändern].

   Das System zeigt eine Bestätigung an.

3. Bestätigen Sie, dass Sie die Rolle der Volumes ändern möchten, und wählen Sie dann **Rolle ändern**.

> Wenn das lokale Speicher-Array nicht mit dem Remote-Speicher-Array kommunizieren kann, zeigt das System das Dialogfeld Speicher-Array nicht kontaktieren an, wenn eine Rollenänderung angefordert wird, aber das Remote-Speicher-Array kann nicht kontaktiert werden. Klicken Sie auf **Ja**, um die Rollenänderung zu erzwingen.

Ergebnisse

System Manager führt die folgende Aktion durch:

- Wenn das zugehörige Volume im gespiegelten Paar kontaktiert werden kann, ändern sich die Rollen zwischen den Volumes. System Manager befördert das sekundäre Volume im gespiegelten Paar in die primäre Rolle oder deprisiert das primäre Volume im gespiegelten Paar auf die sekundäre Rolle (je nach Auswahl).

Ändern Sie die Synchronisierungseinstellungen für ein gespiegeltes Paar

Sie können die Synchronisierungspriorität und die Resynchronisierungsrichtlinie ändern, die das gespiegelte Paar verwendet, um die Neusynchronisierung nach einer Kommunikationsunterbrechung abzuschließen.

Über diese Aufgabe

Sie können die Synchronisierungseinstellungen für ein gespiegeltes Paar nur auf dem Speicher-Array

bearbeiten, das das primäre Volume enthält.

Schritte

1. Wählen Sie Menü:Speicher[Synchronous Mirroring].
2. Wählen Sie das gespiegelte Paar aus, das Sie bearbeiten möchten, und wählen Sie dann Menü:Mehr[Einstellungen bearbeiten].

   Das Dialogfeld Einstellungen anzeigen/bearbeiten wird angezeigt.

3. Verwenden Sie den Schieberegler, um die Synchronisationspriorität zu bearbeiten.

   Die Synchronisierungspriorität legt fest, wie viele der Systemressourcen verwendet werden, um den Neusynchronisierung nach einer Kommunikationsunterbrechung im Vergleich zu Service-I/O-Anfragen abzuschließen.

   Mehr zu Synchronisierungsraten

   Es gibt fünf Prioritätsraten für die Synchronisierung:

   - Am Niedrigsten
   - Niedrig
   - Mittel
   - Hoch
   - Höchste

   Wenn die Synchronisierungspriorität auf die niedrigste Rate eingestellt ist, wird die I/O-Aktivität priorisiert und die Neusynchronisierung dauert länger. Wenn die Synchronisierungspriorität auf die höchste Rate festgelegt ist, wird der Neusynchronisierung nach Priorität geordnet, aber die I/O-Aktivität für das Speicher-Array ist möglicherweise betroffen.

4. Bearbeiten Sie die Resynchronisierung-Richtlinie nach Bedarf.

   Sie können die gespiegelten Paare auf dem Remote-Speicher-Array entweder manuell oder automatisch neu synchronisieren.

   - **Manuell** (die empfohlene Option) — Wählen Sie diese Option aus, damit die Synchronisierung manuell fortgesetzt werden muss, nachdem die Kommunikation auf einem gespiegelten Paar wiederhergestellt wurde. Diese Option bietet die beste Möglichkeit für die Wiederherstellung von Daten.
   - **Automatisch** — Wählen Sie diese Option, um die Neusynchronisierung automatisch zu starten, nachdem die Kommunikation auf einem gespiegelten Paar wiederhergestellt wurde.

5. Wählen Sie **Speichern**.

Entfernen Sie die synchrone Spiegelbeziehung

Ein gespiegeltes Paar entfernen Sie die gespiegelte Beziehung vom primären Volume auf dem lokalen Storage Array und dem sekundären Volume im Remote Storage Array.

Über diese Aufgabe

Sie können auch ein gespiegeltes Paar entfernen, um den Status eines verwaisten gespiegelten Paares zu korrigieren. Prüfen Sie die folgenden Informationen zu verwaisten gespiegelten Paaren:

- Ein verwaister gespiegeltes Paar ist vorhanden, wenn ein Mitglied-Volume auf einer Seite entfernt wurde (lokal/Remote), jedoch nicht auf der anderen Seite.
- Verwaiste gespiegelte Paare werden erkannt, wenn die Kommunikation zwischen den Arrays wiederhergestellt wird.

Schritte

1. Wählen Sie Menü:Speicher[Synchronous Mirroring].
2. Wählen Sie das gespiegelte Paar aus, das Sie entfernen möchten, und wählen Sie dann das Menü:Sonstige Aufgaben[Entfernen].

   Das Dialogfeld Mirror-Beziehung entfernen wird angezeigt.

3. Bestätigen Sie, dass Sie das gespiegelte Paar entfernen möchten, und klicken Sie dann auf **Entfernen**.

Ergebnisse

System Manager führt die folgenden Aktionen durch:

- Entfernt die gespiegelte Beziehung vom gespiegelten Paar auf dem lokalen Speicher-Array und auf dem Remote-Speicher-Array.
- Liefert das primäre und das sekundäre Volume zu hostfreien, nicht gespiegelten Volumes zurück.
- Aktualisiert die Kachel „Synchronous Mirroring“ beim Entfernen des synchronen gespiegelten Paares.

Spiegelung deaktivieren

Deaktivieren Sie die asynchrone Spiegelung

Sie können die asynchrone Spiegelung auf den lokalen und Remote-Speicher-Arrays deaktivieren, um die normale Nutzung dedizierter Ports auf den Speicher-Arrays wiederherzustellen.

Bevor Sie beginnen

- Sie müssen alle Spiegelbeziehungen gelöscht haben. Stellen Sie sicher, dass alle Spiegelkonsistency Groups und gespiegelten Paare aus den lokalen und Remote Storage Arrays gelöscht wurden.
- Das lokale Speicher-Array und das Remote-Speicher-Array müssen über eine Fibre-Channel Fabric- oder iSCSI-Schnittstelle verbunden sein.

Über diese Aufgabe

Wenn Sie die asynchrone Spiegelung deaktivieren, können auf den lokalen und Remote-Storage-Arrays keine Spiegelungsaktivitäten stattfinden.

Schritte

1. Wählen Sie Menü:Speicher[Asynchronous Mirroring].
2. Menü wählen:Sonstige Aufgaben[Deaktivieren].

   Das System zeigt eine Bestätigung an.

3. Wählen Sie zur Bestätigung * Ja* aus.

Ergebnisse

- Die HBA-Host-Kanäle des Controllers, die für die Kommunikation mit asynchroner Spiegelung reserviert waren, können nun Lese- und Schreibanfragen des Hosts akzeptieren.
- Keine der Volumes in diesem Speicher-Array sind in der Lage, an Spiegelbeziehungen entweder als primäre Volumen oder als sekundäre Volumen teilzunehmen.

Deaktivieren Sie die synchrone Spiegelung

Sie können die Funktion Synchronous Mirroring auf einem Speicher-Array deaktivieren, um die normale Nutzung des Host Bus Adapters (HBA) Host-Ports 4, der für die Datenübertragung an der Spiegelung reserviert war, wiederherzustellen.

Bevor Sie beginnen

Sie müssen alle synchronen Spiegelbeziehungen gelöscht haben. Überprüfen Sie, ob alle gespiegelten Paare aus dem Speicher-Array gelöscht wurden.

Schritte

1. Wählen Sie Menü:Speicher[Synchronous Mirroring].
2. Menü wählen:Sonstige Aufgaben[Deaktivieren].

   Das System zeigt eine Bestätigung an.

3. Wählen Sie zur Bestätigung * Ja* aus.

Ergebnisse

- Der HBA-Host-Port 4 des Controllers, der für die Kommunikation mit synchroner Spiegelung vorgesehen war, kann jetzt Lese- und Schreibanfragen des Hosts akzeptieren.
- Die Volumes mit reservierter Kapazität im Speicher-Array werden gelöscht.

Async FAQs

Wie unterscheidet sich die asynchrone Spiegelung von der synchronen Spiegelung?

Die asynchrone Spiegelung unterscheidet sich grundlegend von der Funktion zum synchronen Spiegeln: Sie erfasst den Status des Quell-Volumes zu einem bestimmten Zeitpunkt und kopiert nur die Daten, die sich seit der letzten Bildaufzeichnung geändert haben.

Bei der synchronen Spiegelung wird der Status des primären Volume nicht zu einem bestimmten Zeitpunkt erfasst, sondern gibt alle Änderungen wieder, die am primären Volume auf das sekundäre Volume vorgenommen wurden. Das sekundäre Volume ist zu jedem Zeitpunkt mit dem primären Volume identisch, da bei dieser Art von Spiegelung jedes Mal, wenn ein Schreibvorgang auf dem primären Volume ausgeführt wird, ein Schreibvorgang auf das sekundäre Volume vorgenommen wird. Der Host erhält keine Bestätigung, dass der Schreibvorgang erfolgreich war, bis das sekundäre Volume mit den Änderungen auf dem primären Volume erfolgreich aktualisiert wurde.

Bei der asynchronen Spiegelung ist das Remote-Storage-Array nicht vollständig mit dem lokalen Storage-Array synchronisiert. Falls die Applikation aufgrund eines Verlusts des lokalen Storage-Arrays zum Remote Storage-Array wechseln muss, können einige Transaktionen verloren gehen.

Vergleich der Spiegelungsfunktionen:

Asynchrones Spiegeln	Synchrones Spiegeln
Replikationsmethode	• **Point-in-Time** Die Spiegelung erfolgt nach Bedarf oder automatisch gemäß einem benutzerdefinierten Zeitplan. Zeitpläne können mit der Granularität von Minuten definiert werden. Die Mindestzeit zwischen den Synchronisierungen beträgt 10 Minuten.
• * Kontinuierlich* Die Spiegelung wird kontinuierlich ausgeführt und kopiert Daten von jedem Host-Schreibvorgang.	**Reservierte Kapazität**
• **Mehrfach** Für jedes gespiegelte Paar ist ein reserviertes Kapazitäts-Volume erforderlich.	• **Single** Für alle gespiegelten Volumes ist ein einzelnes reserviertes Kapazitäts-Volume erforderlich.
Kommunikation	• **ISCSI und Fibre Channel** Unterstützt iSCSI- und Fibre Channel-Schnittstellen zwischen Storage Arrays.
• * Fibre Channel* Unterstützt nur Fibre Channel-Schnittstellen zwischen Storage Arrays.	**Entfernung**
• **Unlimited** Unterstützung nahezu unbegrenzter Entfernungen zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array, wobei die Entfernung in der Regel nur durch die Fähigkeiten des Netzwerks und der Channel-Erweiterungstechnologie begrenzt wird.	• **Eingeschränkt** Normalerweise muss das lokale Storage-Array innerhalb von etwa 10 km Entfernung (6.2 Meilen) liegen, um die Anforderungen an Latenz und Applikations-Performance zu erfüllen.

Warum kann ich nicht auf meine gewählte Spiegelfunktion zugreifen?

Spiegelung wird in der Schnittstelle des SANtricity Unified Managers konfiguriert.

Synchrones Spiegeln ist für das EF600/EF600C oder EF300/EF300C Storage-Array nicht verfügbar.

Um die Spiegelung zwischen zwei Arrays zu aktivieren und zu konfigurieren, überprüfen Sie Folgendes:

- Der Web Services Proxy-Dienst muss ausgeführt werden. (Unified Manager wird auf einem Host-System zusammen mit dem Web Services Proxy installiert.)
- Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung ausgeführt werden.
- Die beiden Storage Arrays, die Sie für die Spiegelung verwenden möchten, müssen in Unified Manager erkannt werden.
- Unified Manager muss über gültige SSL-Zertifikate für die Speicher-Arrays verfügen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder CA-signierte Zertifikate von Unified Manager installieren.

Anweisungen zur Konfiguration finden Sie im folgenden Abschnitt:

- "Asynchrones gespiegeltes Paar erstellen (in Unified Manager)"
- "Synchrones gespiegeltes Paar erstellen (in Unified Manager)"

Was muss ich wissen, bevor ich eine gespiegelte Konsistenzgruppe erstellt?

Befolgen Sie die folgenden Richtlinien, bevor Sie eine gespiegelte Konsistenzgruppe erstellen.

Synchrones Spiegeln ist auf dem Storage-System EF600/EF600C oder EF300/EF300C nicht verfügbar.

Sie erstellen eine Konsistenzgruppe in Unified Manager im Assistenten zum Erstellen gespiegelter Paare.

Erfüllen Sie die folgenden Anforderungen für Unified Manager:

- Der Web Services Proxy-Dienst muss ausgeführt werden.
- Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung ausgeführt werden.
- Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr eigenes Sicherheitszertifikat mit Unified Manager installieren und zum Menü:Zertifikat[Zertifikatverwaltung] navigieren.

Erfüllen Sie außerdem die folgenden Anforderungen an Storage-Arrays:

- Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
- Jedes Speicher-Array muss zwei Controller haben.
- Jeder Controller im primären Array und im sekundären Array muss über einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk verbunden sein.
- Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens 7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
- Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays kennen.
- Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel Fabric- oder iSCSI-Schnittstelle verbunden.

Asynchrones Spiegeln - Was muss ich wissen, bevor ich ein gespiegeltes Paar erstellt habe?

Sie konfigurieren gespiegelte Paare in der Oberfläche von SANtricity Unified Manager und verwalten dann die Paare in SANtricity System Manager.

Befolgen Sie vor dem Erstellen eines gespiegelten Paares diese Richtlinien.

- Sie müssen über zwei Storage-Arrays verfügen.
- Jedes Speicher-Array muss zwei Controller haben.
- Jeder Controller im primären Array und im sekundären Array muss über einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk verbunden sein.
- Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel Fabric- oder iSCSI-Schnittstelle verbunden.
- Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens 7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
- Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays kennen.
- Sie benötigen genügend freie Kapazität auf dem Remote-Speicher-Array, um ein sekundäres Volume zu erstellen, das dem primären Volume entspricht oder dessen Größe Sie spiegeln möchten.
- Sie haben Web Services Proxy und Unified Manager installiert. Gespiegelte Paare werden in der Unified Manager Schnittstelle konfiguriert.
- Die beiden Storage Arrays werden in Unified Manager erkannt.
- Ihr Speicher-Array muss mindestens eine gespiegelte Konsistenzgruppe enthalten. Sie erstellen eine Konsistenzgruppe in Unified Manager im Assistenten zum Erstellen gespiegelter Paare.

Was muss ich wissen, bevor ich meine reservierte Kapazität auf einem gespiegelten Paar-Volume erhöhen kann?

Normalerweise sollten Sie die reservierte Kapazität erhöhen, wenn Sie eine Warnung erhalten, dass die reservierte Kapazität eines gespiegelten Paares voll wird. Sie können die reservierte Kapazität nur in Schritten von 8 gib erhöhen.

Bei asynchronen Spiegelungsvorgängen beträgt die reservierte Kapazität normalerweise 20 Prozent des Basis-Volumes. Wählen Sie eine größere Kapazität für reservierte Kapazität, wenn eine oder beide Bedingungen vorliegen:

- Sie beabsichtigen, das gespiegelte Paar für einen langen Zeitraum zu halten.
- Ein großer Prozentsatz an Datenblöcken ändert sich auf dem primären Volume aufgrund von hoher I/O-Aktivität. Mithilfe von historischen Performance-Daten oder anderen Betriebssystem-Utilities können Sie typische I/O-Aktivitäten für das primäre Volume ermitteln.

Sie können die reservierte Kapazität für ein gespiegeltes Paar erhöhen, indem Sie eine der folgenden Aktionen durchführen:

- Passen Sie den Kapazitätsprozentsatz für ein gespiegeltes Paar-Volumen an, indem Sie Menü:Speicher[Pools und Volumes Groups] auswählen und dann auf die Registerkarte **Reservierte Kapazität** klicken.
- Erstellen Sie ein neues Volume mithilfe von freier Kapazität, die in einem Pool oder einer Volume-Gruppe verfügbar ist.

  Wenn in einem Pool oder einer Volume-Gruppe keine freie Kapazität vorhanden ist, können Sie nicht konfigurierte Kapazität in Form von nicht verwendeten Laufwerken zu einem Pool oder einer Volume-Gruppe hinzufügen.

Warum kann ich die reservierte Kapazität nicht mit meinem angeforderten Betrag erhöhen?

Sie können die reservierte Kapazität nur in Schritten von 4 gib erhöhen.

Lesen Sie sich die folgenden Richtlinien durch:

- Sie müssen über ausreichende freie Kapazitäten im Pool oder Volume-Gruppe verfügen, damit diese bei Bedarf erweitert werden kann.

  Wenn auf einem Pool oder Volume-Gruppen keine freie Kapazität vorhanden ist, können Sie einem Pool oder einer Volume-Gruppe nicht zugewiesene Kapazität in Form nicht verwendeter Laufwerke hinzufügen.

- Das Volume im Pool oder in der Volume-Gruppe muss den optimalen Status aufweisen und darf sich nicht in einem bestimmten Zustand befinden.
- Freie Kapazität muss im Pool bzw. in der Volume-Gruppe vorhanden sein, mit der die Kapazität erhöht werden soll.

Bei asynchronen Spiegelungsvorgängen beträgt die reservierte Kapazität in der Regel 20 Prozent des Basis-Volumes. Verwenden Sie einen höheren Prozentsatz, wenn Sie glauben, dass das Basis-Volume viele Änderungen durchlaufen wird oder wenn die geschätzte Lebensdauer des Kopierservice eines Storage-Objekts sehr lang sein wird.

Warum sollte ich diesen Prozentsatz ändern?

Die reservierte Kapazität beträgt normalerweise 40 % des Basis-Volumes für Snapshot-Vorgänge und 20 % des Basis-Volumes für asynchrone Spiegelungsvorgänge.

In der Regel ist diese Kapazität ausreichend. Die benötigte Kapazität ist abhängig von Häufigkeit und Größe der I/O-Schreibvorgänge auf dem Basis-Volume und wie lange Sie den Kopierdienst des Storage-Objekts verwenden möchten.

Im Allgemeinen wählen Sie einen größeren Prozentsatz für die reservierte Kapazität aus, wenn eine oder beide Bedingungen vorhanden sind:

- Wenn sich der Kopierdienst eines bestimmten Storage-Objekts sehr lange Lebensdauer hat.
- Wenn sich ein großer Prozentsatz an Datenblöcken auf dem Basis-Volume aufgrund von hoher I/O-Aktivität ändert. Mithilfe von historischen Performance-Daten oder anderen Betriebssystem-Dienstprogrammen können Sie die typischen I/O-Aktivitäten für das Basis-Volume ermitteln.

Warum kann ich mehr als einen Kandidaten für reservierte Kapazität sehen?

Wenn sich mehrere Volumes in einem Pool oder einer Volume-Gruppe befinden, die dem für das Storage-Objekt ausgewählten Kapazitätsprozentsatz entsprechen, werden mehrere Kandidaten angezeigt.

Sie können die Liste der empfohlenen Kandidaten aktualisieren, indem Sie den Prozentsatz des physischen Speicherplatzes ändern, den Sie im Basis-Volume für Kopierdienste reservieren möchten. Die besten Kandidaten werden basierend auf Ihrer Auswahl angezeigt.

Warum werden in der Tabelle keine verfügbaren Werte angezeigt?

In der Tabelle sind die Werte aufgeführt, die nicht verfügbar sind, wenn die Daten im

Remote-Speicher-Array nicht angezeigt werden können.

Um die Daten des Remote-Speicher-Arrays anzuzeigen, starten Sie System Manager von Unified Manager.

Warum sehe ich nicht alle meine Pools und Volume-Gruppen?

Wenn Sie ein sekundäres Volume für das asynchrone gespiegelte Paar erstellen, zeigt das System eine Liste aller infrage kommenden Pools und Volume-Gruppen für das asynchrone gespiegelte Paar an. Pools oder Volume-Gruppen, die nicht verwendet werden können, werden in dieser Liste nicht angezeigt.

Pools oder Volume-Gruppen können aus den folgenden Gründen nicht berechtigt sein.

- Die Sicherheitsfunktionen von Pools oder Volume-Gruppen stimmen nicht überein.
- Ein Pool oder eine Volume-Gruppe befindet sich in einem nicht optimalen Zustand.
- Die Kapazität eines Pools oder einer Volume-Gruppe ist zu klein.

Asynchrones Spiegeln - Warum sehe ich nicht alle meine Volumen?

Wenn Sie ein primäres Volume für ein gespiegeltes Paar auswählen, werden in einer Liste alle berechtigten Volumes angezeigt.

Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser Liste nicht angezeigt. Die Volumes können aus den folgenden Gründen nicht berechtigt sein:

- Die Lautstärke ist nicht optimal.
- Das Volume beteiligt sich bereits an einer Spiegelbeziehung.
- Bei Thin Volumes muss die automatische Erweiterung aktiviert sein.

> Bei EF600- und EF300-Controllern müssen die primären und sekundären Volumes eines asynchronen gespiegelten Paares dasselbe Protokoll, Tray-Level, Segmentgröße, Sicherheitstyp und RAID-Level erfüllen. Nicht geeignete asynchrone gespiegelte Paare werden nicht in der Liste der verfügbaren Volumes angezeigt.

Asynchrones Spiegeln - Warum sehe ich nicht alle Volumen auf dem Remote-Speicher-Array?

Wenn Sie ein sekundäres Volume auf dem Remote-Speicher-Array auswählen, werden alle für dieses gespiegelte Paar geeigneten Volumes in einer Liste angezeigt.

Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser Liste nicht angezeigt. Volumes sind aus folgenden Gründen möglicherweise nicht verfügbar:

- Die Lautstärke ist nicht optimal.
- Das Volume beteiligt sich bereits an einer Spiegelbeziehung.
- Die Thin-Volume-Attribute des primären Volume und des sekundären Volumes stimmen nicht überein.
- Wenn Sie Data Assurance (da) verwenden, müssen das primäre Volume und das sekundäre Volume über dieselben da-Einstellungen verfügen.
  - Wenn das primäre Volume mit da aktiviert ist, muss das sekundäre Volume mit da aktiviert sein.

- Wenn das primäre Volume nicht da aktiviert ist, darf das sekundäre Volume nicht als da-aktiviert verwendet werden.

Warum sollte ich die IP-Adresse meines Remote-Speicherarrays aktualisieren?

Sie aktualisieren die IP-Adresse des Remote-Speicher-Arrays, wenn sich die IP-Adresse eines iSCSI-Ports ändert und das lokale Speicher-Array nicht mit dem Remote-Speicher-Array kommunizieren kann.

Beim Einrichten einer asynchronen Spiegelbeziehung mit einer iSCSI-Verbindung speichern sowohl die lokalen als auch die Remote-Speicher-Arrays einen Datensatz der IP-Adresse des Remote-Speicher-Arrays in der Konfiguration zur asynchronen Spiegelung. Wenn sich die IP-Adresse eines iSCSI-Ports ändert, tritt auf dem Remote-Speicher-Array, das versucht, diesen Port zu verwenden, ein Kommunikationsfehler auf.

Das Speicher-Array mit der geänderten IP-Adresse sendet eine Nachricht an jedes Remote-Speicher-Array, das mit den Spiegelungskonsistency Groups verknüpft ist, die für die Spiegelung über eine iSCSI-Verbindung konfiguriert sind. Speicher-Arrays, die diese Meldung erhalten, aktualisieren automatisch ihre Remote-Ziel-IP-Adresse.

Wenn das Speicher-Array mit der geänderten IP-Adresse seine Array-übergreifende Meldung nicht an ein Remote-Speicher-Array senden kann, sendet das System eine Warnmeldung über das Verbindungsproblem. Verwenden Sie die Option Remote IP-Adresse aktualisieren, um die Verbindung zum lokalen Speicher-Array wiederherzustellen.

FAQs synchronisieren

Wie unterscheidet sich die asynchrone Spiegelung von der synchronen Spiegelung?

Die asynchrone Spiegelung unterscheidet sich grundlegend von der Funktion zum synchronen Spiegeln: Sie erfasst den Status des Quell-Volumes zu einem bestimmten Zeitpunkt und kopiert nur die Daten, die sich seit der letzten Bildaufzeichnung geändert haben.

Bei der synchronen Spiegelung wird der Status des primären Volume nicht zu einem bestimmten Zeitpunkt erfasst, sondern gibt alle Änderungen wieder, die am primären Volume auf das sekundäre Volume vorgenommen wurden. Das sekundäre Volume ist zu jedem Zeitpunkt mit dem primären Volume identisch, da bei dieser Art von Spiegelung jedes Mal, wenn ein Schreibvorgang auf dem primären Volume ausgeführt wird, ein Schreibvorgang auf das sekundäre Volume vorgenommen wird. Der Host erhält keine Bestätigung, dass der Schreibvorgang erfolgreich war, bis das sekundäre Volume mit den Änderungen auf dem primären Volume erfolgreich aktualisiert wurde.

Bei der asynchronen Spiegelung ist das Remote-Storage-Array nicht vollständig mit dem lokalen Storage-Array synchronisiert. Falls die Applikation aufgrund eines Verlusts des lokalen Storage-Arrays zum Remote Storage-Array wechseln muss, können einige Transaktionen verloren gehen.

Vergleich der Spiegelungsfunktionen:

Asynchrones Spiegeln	Synchrones Spiegeln
Replikationsmethode	• **Point-in-Time** Die Spiegelung erfolgt nach Bedarf oder automatisch gemäß einem benutzerdefinierten Zeitplan. Zeitpläne können mit der Granularität von Minuten definiert werden. Die Mindestzeit zwischen den Synchronisierungen beträgt 10 Minuten.
• * Kontinuierlich* Die Spiegelung wird kontinuierlich ausgeführt und kopiert Daten von jedem Host-Schreibvorgang.	**Reservierte Kapazität**
• **Mehrfach** Für jedes gespiegelte Paar ist ein reserviertes Kapazitäts-Volume erforderlich.	• **Single** Für alle gespiegelten Volumes ist ein einzelnes reserviertes Kapazitäts-Volume erforderlich.
Kommunikation	• **ISCSI und Fibre Channel** Unterstützt iSCSI- und Fibre Channel-Schnittstellen zwischen Storage Arrays.
• * Fibre Channel* Unterstützt nur Fibre Channel-Schnittstellen zwischen Storage Arrays.	**Entfernung**
• **Unlimited** Unterstützung nahezu unbegrenzter Entfernungen zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array, wobei die Entfernung in der Regel nur durch die Fähigkeiten des Netzwerks und der Channel-Erweiterungstechnologie begrenzt wird.	• **Eingeschränkt** Normalerweise muss das lokale Storage-Array innerhalb von etwa 10 km Entfernung (6.2 Meilen) liegen, um die Anforderungen an Latenz und Applikations-Performance zu erfüllen.

Synchronous Mirroring - Warum sehe ich nicht alle meine Volumen?

Wenn Sie ein primäres Volume für ein gespiegeltes Paar auswählen, werden in einer Liste alle berechtigten Volumes angezeigt.

Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser Liste nicht angezeigt. Volumes sind aus folgenden Gründen möglicherweise nicht verfügbar:

- Das Volume ist ein nicht standardmäßiges Volume, wie beispielsweise ein Snapshot-Volume oder ein Thin Volume.
- Die Lautstärke ist nicht optimal.
- Das Volume beteiligt sich bereits an einer Spiegelbeziehung.

Synchrones Spiegeln - Warum sehe ich nicht alle Volumes auf dem Remote Storage Array?

Wenn Sie ein sekundäres Volume auf dem Remote-Speicher-Array auswählen, werden alle für dieses gespiegelte Paar geeigneten Volumes in einer Liste angezeigt.

Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser Liste nicht angezeigt. Volumes sind aus folgenden Gründen möglicherweise nicht verfügbar:

- Das Volume ist ein nicht standardmäßiges Volume, wie beispielsweise ein Snapshot-Volume oder ein Thin Volume.
- Die Lautstärke ist nicht optimal.
- Das Volume beteiligt sich bereits an einer Spiegelbeziehung.
- Wenn Sie Data Assurance (da) verwenden, müssen das primäre Volume und das sekundäre Volume über dieselben da-Einstellungen verfügen.
  - Wenn das primäre Volume mit da aktiviert ist, muss das sekundäre Volume mit da aktiviert sein.
  - Wenn das primäre Volume nicht da aktiviert ist, darf das sekundäre Volume nicht als da-aktiviert verwendet werden.

Synchrones Spiegeln - Was muss ich wissen, bevor ein gespiegeltes Paar erstellt wird?

Sie konfigurieren gespiegelte Paare in der Oberfläche von SANtricity Unified Manager und verwalten dann die Paare in SANtricity System Manager.

Befolgen Sie vor dem Erstellen eines gespiegelten Paares die folgenden Richtlinien:

- Sie müssen über zwei Storage-Arrays verfügen.
- Jedes Speicher-Array muss zwei Controller haben.
- Jeder Controller im primären Array und im sekundären Array muss über einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk verbunden sein.
- Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel Fabric verbunden.
- Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens 7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
- Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays kennen.
- Sie benötigen genügend freie Kapazität auf dem Remote-Speicher-Array, um ein sekundäres Volume zu erstellen, das dem primären Volume entspricht oder dessen Größe Sie spiegeln möchten.
- Sie haben Web Services Proxy und Unified Manager installiert. Gespiegelte Paare werden in der Unified Manager Schnittstelle konfiguriert.
- Die beiden Storage Arrays werden in Unified Manager erkannt.

Welche Auswirkungen hat die Synchronisierungspriorität auf die Synchronisierungsraten?

Die Synchronisierungspriorität definiert, wie viel Verarbeitungszeit für Synchronisierungsaktivitäten im Verhältnis zur Systemleistung zugewiesen wird.

Der Controller-Eigentümer des primären Volume führt diesen Vorgang im Hintergrund durch. Gleichzeitig verarbeitet der Controller-Inhaber lokale I/O-Schreibvorgänge auf das primäre Volume und verbundene Remote-Schreibvorgänge auf das sekundäre Volume. Da durch die Resynchronisierung der Controller-Verarbeitungsressourcen von der I/O-Aktivität umgeleitet werden, kann eine Neusynchronisierung die Performance der Host-Applikation nach sich ziehen.

Beachten Sie diese Richtlinien, um zu ermitteln, wie lange eine Synchronisierungspriorität dauern könnte und wie sich die Synchronisierungsprioritäten auf die Systemleistung auswirken können.

Allgemeines zu Prioritätsraten für die Synchronisierung

Diese Prioritätsraten sind verfügbar:

- Am Niedrigsten
- Niedrig
- Mittel
- Hoch
- Höchste

Die niedrigste Prioritätsrate unterstützt die System-Performance, die Neusynchronisierung dauert jedoch länger. Die höchste Prioritätsrate unterstützt eine Neusynchronisierung, aber die System-Performance ist möglicherweise beeinträchtigt.

Diese Leitlinien entsprechen ungefähr den Unterschieden zwischen den Prioritäten.

Prioritätsrate für vollständige Synchronisierung	Verstrichene Zeit im Vergleich zur höchsten Synchronisationsrate
Am Niedrigsten	Etwa achtmal so lange wie bei der höchsten Prioritätsrate.
Niedrig	Etwa sechsmal so lange wie bei der höchsten Prioritätsrate.
Mittel	Etwa dreieinhalb Mal so lang wie bei der höchsten Prioritätsrate.
Hoch	Etwa doppelt so lange wie bei der höchsten Prioritätsrate.

Volume-Größe und Host-I/O-Rate-Lasten wirken sich auf den Vergleich der Synchronisierungszeit aus.

Warum wird empfohlen, eine manuelle Synchronisierungsrichtlinie zu verwenden?

Die manuelle Neusynchronisierung wird empfohlen, da Sie damit den Neusynchronisierung so verwalten können, dass dadurch keine Möglichkeit zum Wiederherstellen von Daten besteht.

Wenn Sie eine automatische Resynchronisierung verwenden und während der Neusynchronisierung intermittierende Kommunikationsprobleme auftreten, können die Daten auf dem sekundären Volume vorübergehend beschädigt werden. Nach Abschluss der Resynchronisierung werden die Daten korrigiert.

Remote Storage

Übersicht über die Funktionen von Remote Storage

Wenn Sie über die Funktion Remote Storage verfügen, können Sie Daten von einem Remote-Speichersystem auf Ihr Speicher-Array importieren.

Was ist die Remote Storage Funktion?

Die Funktion *Remote Storage* ermöglicht das Importieren von Daten aus einem Remote Storage-System in ein lokales E-Series Storage-System. Das Remote-System kann ein anderes E-Series System oder ein System eines anderen Anbieters sein. Diese Funktion ist hilfreich, wenn Sie die Datenmigration mit minimalen Ausfallzeiten, z. B. bei Geräte-Upgrades, rationalisieren möchten.

Um Remote-Speicher zu verwenden, muss diese Funktion in der Submodell-ID (SMID) aktiviert sein.

Weitere Informationen:

- "Funktionsweise von Remote Storage"
- "Remote Storage – Terminologie"
- "Remote-Storage-Anforderungen"
- "Anforderungen für Remote Storage Volumes"

Wie importiere ich Daten mit dieser Funktion?

Mit dem Remote Storage Wizard ordnen Sie ein Remote Storage-Gerät (die Quelle für den Datenimport) einem Ziel-Volume auf dem E-Series System zu. Dieser Assistent ist über das Menü:Speicher[Remote-Speicher] verfügbar.

Weitere Informationen:

- "Remote-Speicher importieren"
- "Den Fortschritt des Datenimports managen"

Konzepte

Funktionsweise von Remote Storage

Mit der Remote Storage-Funktion können Sie Daten von einem Remote Storage-System auf ein lokales E-Series Storage-System importieren. Diese Funktion ist hilfreich, wenn Sie die Datenmigration mit minimalen Ausfallzeiten, z. B. bei Geräte-Upgrades, rationalisieren möchten.

Zum Konfigurieren der Remote-Speicherfunktion müssen Sie die Hardware einrichten und dann mit System Manager ein Remote-Speicherobjekt erstellen. Sobald diese Konfiguration abgeschlossen ist, beginnt der

Importvorgang.

Hardware-Einrichtung

Verwenden Sie den folgenden Workflow, um die Hardwareverbindungen vorzubereiten.

Diese Schritte finden Sie im Benutzerhandbuch zur Remote-Speicherfunktion, die im E-Series and SANtricity Dokumentationszentrum unter verfügbar ist "Remote Storage Volumes: Überblick", Und im "Technischer Bericht Zu Remote-Storage".

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

In dem lokalen E-Series Storage-System:

1. Stellen Sie sicher, dass jeder Controller über eine iSCSI-Verbindung zum Remote-Speichersystem verfügt. Mit dieser Verbindung fungiert das lokale E-Series System als iSCSI-Initiator, der als Host auf dem Remote-System eingerichtet werden kann.
2. Erstellen Sie ein Zielvolume für den Importvorgang. Stellen Sie sicher, dass das Volume über eine Kapazität verfügt, die dem Quell-Volume des Remote-Storage-Systems entspricht oder größer ist, über eine passende Blockgröße verfügt und nicht zugeordnet ist. Siehe "Volumes erstellen".
3. Sammeln Sie den iSCSI Qualified Name (IQN) für das lokale E-Series System von der System Manager-Schnittstelle aus. Der IQN wird später zum Einrichten des lokalen E-Series Systems als Host auf dem Remote-Speichersystem verwendet. Wechseln Sie in System Manager zu Menü:Einstellungen[System > iSCSI-Einstellungen > Ziel-IQN].

Auf dem Remote Storage-System:

1. Richten Sie das lokale E-Series-System mit seinem IQN als Host auf dem Remote-System ein. Stellen Sie sicher, dass Sie den entsprechenden Host-Typ festlegen:
   - Wenn es sich bei dem Remote-System um ein Modell der E-Series handelt, lesen Sie "Übersicht über Hosts und Host-Cluster". Verwenden Sie einen Host-Typ von „Factory Standard“.
   - Wenn das Remotesystem von einem anderen Anbieter stammt, wählen Sie je nach den verfügbaren Optionen einen entsprechenden Hosttyp aus.
2. Beenden Sie alle I/OS, heben Sie die Mounten von Dateisystemen ab und entfernen Sie alle Zuweisungen zu Hosts oder Anwendungen für das Quell-Volume.
3. Weisen Sie das Volume dem neu erstellten lokalen Host des E-Series Storage-Systems zu.
4. Erfassen Sie für das ausgewählte Quell-Volume die folgenden Informationen aus dem Remote-Speichersystem, damit der Import erstellt werden kann:
   - Qualifizierter iSCSI-Name (IQN)
   - ISCSI-IP-Adresse
   - Die LUN-Nummer des Quell-Volume

Einrichtung von System Manager

Verwenden Sie den folgenden Workflow, um ein Remote-Speicherobjekt für den Import zu erstellen:

1. Ordnen Sie mit dem Remote Storage-Assistenten von System Manager in der Benutzeroberfläche ein Remote-Storage-Gerät (die Quelle für den Datenimport) auf einem Ziel-Volume auf dem E-Series System zu. Wenn Sie **Fertig stellen** wählen, beginnt der Importvorgang.

2. Überwachen Sie den Import aus dem Dialogfeld „Anzeigevorgänge“ oder dem Fenster „Vorgänge in Bearbeitung“. Bei Bedarf können Sie den Prozess auch unterbrechen und fortsetzen.
3. Wenn der Import abgeschlossen ist, können Sie die Verbindung zwischen Quell- und Ziel-Volumes unterbrechen oder die Verbindung für zukünftige Importe beibehalten.

Remote Storage – Terminologie

Erfahren Sie, wie Remote Storage-Bedingungen auf Ihr Storage Array angewendet werden.

Laufzeit	Beschreibung
IQN	ISCSI Qualified Name (IQN) Identifier, die einen eindeutigen Namen für einen iSCSI-Initiator oder ein iSCSI-Ziel darstellen.
LUN	Logische Gerätenummer, mit der eine logische Einheit identifiziert wird, die einem Host für den Zugriff angezeigt werden kann.
Remote Storage-System	Dem Storage-System, in dem die Daten zu Beginn gespeichert sind. Das Remote Storage-System kann entweder ein E-Series Modell oder ein System eines anderen Anbieters sein.
Remote-Storage-Gerät	Das physische oder logische Gerät, auf dem die Daten ursprünglich auf dem Remote-System gespeichert werden. In einem Storage-System der E-Series wird dies als „Volume“ bezeichnet.
Remote Storage Objekt	Ein Objekt mit Informationen, das es dem E-Series System ermöglicht, das Remote-Storage-System zu identifizieren und eine Verbindung herzustellen. Diese Informationen enthalten die IQN- und IP-Adressen für das Remote-Speichersystem. Das Remote-Storage-Objekt stellt die Kommunikation zwischen dem Remote-Storage-System und dem E-Series System dar.
Remote Storage Volume	Standard-Volume auf dem E-Series System, das den Datenzugriff auf ein Remote Storage-Gerät ermöglicht
Datenmenge	Ein Container, in dem Daten gespeichert werden. Dies ist die logische Komponente, die für den Host für den Zugriff auf die Daten erstellt wurde.

Anforderungen für Remote Storage-Funktionen

Überprüfen Sie vor der Verwendung der Remote-Speicherfunktion die folgenden Anforderungen und Einschränkungen.

Unterstützte Protokolle

Folgende Protokolle werden unterstützt:

- ISCSI
- IPv4

Aktuelle Informationen zu E-Series Support und Konfiguration finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Hardwareanforderungen

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. Sie muss Folgendes umfassen:

- ISCSI-fähige Schnittstellen

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.

Anforderungen für Remote Storage Volumes

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 Abschluss des Imports 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.

Remote-Storage managen

Remote-Speicher importieren

Verwenden Sie den Assistenten zum Importieren von Remote Storage, um einen Storage-Import von einem Remote-System auf ein lokales E-Series Storage-System zu initiieren.

Bevor Sie beginnen

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

> Die Hardwarekonfiguration wird im Benutzerhandbuch zur Remote-Speicherfunktion beschrieben, die im E-Series und im SANtricity Dokumentationszentrum unter verfügbar ist "Hardware konfigurieren", Und im "Technischer Bericht Zu Remote-Storage".

- 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. Siehe "Volumes erstellen". 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 für Remote Storage-Volumes".

- **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 Fertigstellungszeit auswirken können, empfehlen wir Ihnen, zuerst kleinere Importe von „`Test`“ durchzuführen. Mit diesen Tests stellen Sie sicher, dass alle Verbindungen wie erwartet funktionieren und dass der Importvorgang in einem angemessenen Zeitraum abgeschlossen wird.

Schritte

1. Wählen Sie Menü:Speicher[Remote-Speicher].
2. Klicken Sie Auf **Remote Storage Importieren**.

   Ein Assistent zum Importieren von Remote-Speicher wird angezeigt.

3. Geben Sie im Fenster „Quelle konfigurieren“ in **Schritt 1a** die Verbindungsinformationen ein. 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**.

Felddetails

Einstellung	Beschreibung
Name	Geben Sie einen Namen für das Remote-Speichergerät ein, um es in der System Manager-Schnittstelle zu identifizieren. Ein Name kann bis zu 30 Zeichen enthalten und darf nur Buchstaben, Ziffern und die folgenden Sonderzeichen enthalten: Unterstrich (_), Bindestrich (-) und das Hash-Zeichen (#). Ein Name darf keine Leerzeichen enthalten.
Eigenschaften der iSCSI-Verbindung	Geben Sie die Verbindungseigenschaften des Remote-Speichergeräts ein: • **ISCSI Qualified Name (IQN)**: Geben Sie den iSCSI-IQN ein. • **IP-Adresse**: Geben Sie die IPv4-Adresse ein. • **Port**: Geben Sie die Portnummer ein, die für die Kommunikation zwischen den Quell- und Zielgeräten verwendet werden soll. Standardmäßig ist die Portnummer 3260.

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

4. Wählen Sie im Feld **LUN** die LUN-Nummer des Remote-Speichergeräts aus, das als Quelle verwendet werden soll, 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 im Fenster Überprüfung, ob die Einstellungen korrekt sind, und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

   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 zurück zu **Schritt 1a** im Fenster Quelle konfigurieren, wo 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.

Ergebnisse

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.

Nachdem Sie fertig sind

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.

Fortschritt der Remote-Storage-Importe managen

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

Über diese Aufgabe

Für jeden Importvorgang wird im Dialogfeld „Vorgänge in Bearbeitung“ ein Prozentsatz der Fertigstellung 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 (Menü:Startseite[Vorgänge in Bearbeitung anzeigen]).

Schritte

1. Wählen Sie auf der Seite Remote Storage die Option **Operationen anzeigen**.

   Das Dialogfeld „laufende Vorgänge“ wird angezeigt.

2. Wenn gewünscht, verwenden Sie die Links in der Spalte **Aktionen**, um zu stoppen und wieder aufzunehmen, 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**.
   - **Stop** — Wählen Sie **Stop**, 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**. Dieser Vorgang startet den Import von Anfang an neu. 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.

Verbindungseinstellungen für Remote-Speicher ändern

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

Über diese Aufgabe

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 Menü:Speicher[Remote-Speicher].
2. Wählen Sie in der Liste das Remote-Speicherobjekt aus, das Sie ändern möchten.
3. Klicken Sie Auf **Einstellungen Anzeigen/Bearbeiten**.

   Das Dialogfeld Einstellungen für Remote-Speicher wird angezeigt.

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

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

5. Führen Sie eine der folgenden Aktionen aus:
   - **Bearbeiten** — Klicken Sie auf **Bearbeiten** neben dem entsprechenden Zeilenelement für das entfernte Speicherobjekt. 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.
6. Klicken Sie Auf **Speichern**.

   Die geänderten Verbindungseinstellungen werden auf das Remote-Speicherobjekt angewendet.

Remote-Storage-Objekt entfernen

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

Bevor Sie beginnen

Stellen Sie sicher, dass dem Remote-Speicherobjekt, das Sie entfernen möchten, keine Importe zugeordnet sind.

Über diese Aufgabe

Wenn Sie ein Remote-Speicherobjekt entfernen, werden Verbindungen zwischen den lokalen und den Remote-Geräten entfernt.

Schritte

1. Wählen Sie Menü:Speicher[Remote-Speicher].
2. Wählen Sie aus der Liste das Remote-Speicherobjekt aus, das Sie entfernen möchten.
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 Remote-Speicherobjekt wird entfernt.

FAQs

Was muss ich vor der Erstellung einer Remote-Speicherverbindung wissen?

Zur Konfiguration der Remote-Speicherfunktion müssen Sie das Remote-Gerät und die Zielspeichersysteme direkt über iSCSI verbinden.

Informationen zum Einrichten der iSCSI-Systemverbindung finden Sie unter:

- "Konfigurieren Sie die iSCSI-Ports"
- "Technischer Bericht Zu Remote-Storage"

Warum wird ich aufgefordert, meine Remote-Volumes zu entfernen?

Wenn die maximale Anzahl an Remote-Volumes erreicht ist, erkennt das Speichersystem automatisch alle nicht verwendeten Remote-Volumes und fordert Sie auf, diese zu entfernen.

In einigen Fällen werden die nicht verwendeten Remote-Volumes während des Erstellungsprozesses nicht bereinigt. Bevor Sie weitere Importvorgänge starten, überprüfen Sie, ob Ihre Systeme optimal sind und die Netzwerkverbindungen stabil sind.

Warum sehe ich nicht alle meine Volumen auf meinem Ziel-Array?

Bei der Konfiguration eines Imports für die Remote-Speicherfunktion können Sie feststellen, dass einige Volumes aufgrund von Blockgröße, Kapazität oder Volume-Verfügbarkeit nicht in der Liste der Zielkandidaten angezeigt werden.

Um in der Liste angezeigt zu werden, müssen Volumenkandidaten Folgendes haben:

- Kapazität, die dem Remote-Volume entspricht oder größer ist.
- Blockgröße, die mit dem Remote Volume identisch ist.
- Aktueller Status von optimal.

Volumes-Kandidaten werden aus der Liste ausgeschlossen, wenn sie:

- Jede der folgenden Beziehungen: Volume-Kopie, Snapshot oder Spiegelung.
- Neukonfigurierung wird ausgeführt.

- Zuordnung zu einem anderen Gerät (Host oder Host-Cluster)
- Lese-Flash-Cache aktiviert.

Was muss ich über das Remote Volume bei einem Import wissen?

Bei Verwendung der Remote-Storage-Funktion ist zu beachten, dass das Remote-Volume die Quelle ist, aus der die Daten stammen.

Wenn der Import ausgeführt wird, werden die Daten vom Remote-Volume auf das Ziel-Volume auf dem Ziel-Storage-System übertragen. Diese beiden Volumes müssen eine passende Blockgröße aufweisen.

Was muss ich vor dem Start eines Remote-Storage-Imports beachten?

Mit der Remote Storage-Funktion können Sie Daten von einem Remote Storage-System auf ein Volume auf einem lokalen E-Series Storage-System kopieren. Bevor Sie diese Funktion verwenden, lesen Sie die folgenden Richtlinien durch.

Konfiguration

Bevor Sie den Remote-Speicherimport erstellen, müssen Sie die folgenden Aktionen durchführen und die folgenden Bedingungen überprüfen:

- Stellen Sie sicher, dass jeder Controller des lokalen E-Series Storage-Systems über eine iSCSI-Verbindung zum Remote Storage-System verfügt.
- Erstellen Sie auf Ihrem lokalen E-Series Storage-System ein Ziel-Volume für den Importvorgang. Stellen Sie sicher, dass das Volume über eine Kapazität verfügt, die dem Quell-Volume entspricht oder größer ist als das Quell-Volume, über eine Blockgröße verfügt, die dem Quell-Volume entspricht und nicht zugeordnet ist. Siehe "Volumes erstellen".
- Richten Sie das lokale E-Series Storage-System mithilfe des iSCSI Qualified Name (IQN) als Host auf dem Remote-System ein. Sie können den IQN über Menü:Einstellungen[System > iSCSI-Einstellungen > Ziel-IQN] anzeigen. Stellen Sie außerdem sicher, dass Sie den entsprechenden Host-Typ auf Grundlage des verwendeten Systems festlegen.
- Beenden Sie alle I/OS, heben Sie die Mounten von Dateisystemen ab und entfernen Sie alle Zuweisungen zu Hosts oder Anwendungen für das ausgewählte Volume auf dem Remote-Speichersystem.
- Weisen Sie das Volume dem Remote-Storage-System dem neu erstellten lokalen Host des E-Series Storage-Systems zu.
- Sammeln Sie die folgenden Informationen aus dem Remote-Speichersystem, damit der Import erstellt werden kann:
  - Qualifizierter iSCSI-Name (IQN)
  - ISCSI-IP-Adresse
  - Die LUN-Nummer des Remote-Storage-Geräts, aus dem die Quelldaten stammen
- Sobald der Importvorgang beginnt, wird das gesamte lokale Zielvolume mit den kopierten Daten überschrieben. Alle neuen Daten, die auf das lokale Ziel-Volume geschrieben werden, werden nach der Importerstellung auf dem Volume des Remote-Speichergeräts übertragen. Daher empfehlen wir, vor Beginn des Importvorgangs Backups von Volumes auf dem Remote-Storage-System durchzuführen.

Importvorgang

Die folgenden Schritte beschreiben den Importvorgang.

1. Öffnen Sie die System Manager-Schnittstelle und gehen Sie dann zur Seite **Remote Storage**. Wählen Sie **Import**, um eine neue Importerstellung zu starten. Ausführliche Anweisungen finden Sie unter "Remote-Speicher importieren".

   Wenn Sie einen Offline-Import durchführen möchten, weisen Sie das Zielvolume erst nach Abschluss des Imports zu.

2. Überwachen Sie den Importfortschritt.

   Sobald der Import gestartet wurde, kann das Zielvolume zugeordnet werden. Wie lange der Importvorgang abgeschlossen werden muss, hängt von der Größe des Remote-Speichergeräts (Quell-Volume), der Prioritätseinstellung für den Import und der Menge der I/O-Last sowohl auf den Speichersystemen als auch den zugehörigen Volumes ab.

   Nach Abschluss des Imports handelt es sich bei dem Zielvolume um ein Duplikat der Quelle.

3. Wenn Sie bereit sind, die Mapping-Beziehung zu brechen, führen Sie im Fenster **Operationen in Progress** ein **Trennen** auf dem Importobjekt aus.

Sobald der Import getrennt ist, kehrt die Leistung des lokalen Ziels wieder in den Normalzustand zurück und wird nicht mehr von der Remote-Verbindung beeinträchtigt.

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.

Weitere Informationen

Weitere Informationen zur Remote-Speicherung finden Sie auf der "Technischer Bericht Zu Remote-Storage".

Hardwarekomponenten

Übersicht über Hardwarekomponenten

Sie können den Komponentenstatus auf der Seite Hardware überprüfen und einige Funktionen ausführen, die mit diesen Komponenten zusammenhängen.

Welche Komponenten kann ich managen?

Sie können den Komponentenstatus prüfen und einige Funktionen im Zusammenhang mit diesen Komponenten ausführen:

- **Regale** — A *Shelf* ist eine Komponente, die die Hardware für das Speicher-Array (Controller, Power/Fan Kanister und Laufwerke) enthält. Die Einlegeböden sind in drei Größen für Gehäuse mit bis zu 12, 24 oder 60 Laufwerken erhältlich.
- **Controller** — A *Controller* ist die kombinierte Hardware und Firmware, die Speicher-Array und Verwaltungsfunktionen implementiert. Sie enthält Cache-Speicher, Laufwerksunterstützung und die Ports für Host-Verbindungen.
- **Laufwerke** — Ein Laufwerk_ kann entweder ein Festplattenlaufwerk (HDD) oder ein Solid State Drive (SSD) sein. Je nach Shelf-Größe können bis zu 12, 24 oder 60 Laufwerke im Shelf installiert werden.

Weitere Informationen:

- "Hardware-Seite"
- "Terminologie der Hardware"

Wie werden Hardwarekomponenten angezeigt?

Wechseln Sie zur Hardware-Seite, die eine grafische Darstellung der physischen Komponenten des Storage Arrays bietet. Sie können zwischen der Vorder- und der Rückansicht der Array-Shelfs wechseln, indem Sie oben rechts in der Shelf-Ansicht die Registerkarte **Laufwerke** oder **Controller** auswählen.

Weitere Informationen:

- "Zeigt den Status und die Einstellungen von Shelf-Komponenten an"
- "Zeigen Sie Controller-Einstellungen an"
- "Zeigen Sie den Laufwerkstatus und die Einstellungen an"

Verwandte Informationen

Erfahren Sie mehr über Hardwarekonzepte:

- "Controller-Status"
- "Laufwerksstatus"
- "Schutz vor Regalverlust und Schutz vor Schubladenverlust"

Konzepte

Hardwareseiten und -Komponenten

Die Seite Hardware bietet eine grafische Darstellung der physischen Komponenten des Storage Arrays. Hier können Sie den Komponentenstatus prüfen und einige Funktionen ausführen, die mit diesen Komponenten zusammenhängen.

Shelfs

Ein Shelf ist eine Komponente, die die Hardware für das Storage-Array enthält (Controller, Strom-/Lüfterbehälter und Laufwerke). Es gibt zwei Arten von Shelfs:

- **Controller-Regal** — enthält die Laufwerke, Power/Fan-Kanister und Controller.
- **Laufwerk-Shelf** (oder **Erweiterungs-Shelf**) — enthält Laufwerke, Strom-/Lüfterbehälter und zwei Eingangs-/Ausgangsmodule (IOMs). Die IOMs, auch als Environmental Service Modules (ESMs) bekannt, umfassen SAS-Ports, die das Festplatten-Shelf mit dem Controller-Shelf verbinden.

Die Einlegeböden sind in drei Größen für Gehäuse mit bis zu 12, 24 oder 60 Laufwerken erhältlich. Jedes Shelf enthält eine ID-Nummer, die von der Controller-Firmware zugewiesen wird. Die ID wird oben links in der Shelf-Ansicht angezeigt.

In der Shelf-Ansicht auf der Seite Hardware werden die Komponenten vorne oder hinten angezeigt. Sie können zwischen den beiden Ansichten wechseln, indem Sie entweder die Registerkarten **Drives** oder **Controller** oben rechts in der Shelf-Ansicht auswählen. Sie können auch **Alle anzeigen** oder **Alle anzeigen** von unten auf der Seite auswählen. Die Vorder- und Rückseite zeigen Folgendes:

- **Front Components** — Laufwerke und leere Laufwerksschächte.
- **Back Components** — Controller und Power/Fan Kanister (für Controller-Shelves) oder die IOMs und Power/Fan Kanister (für Laufwerk-Shelfs).

Sie können die folgenden Funktionen in Bezug auf die Shelves ausführen:

- Schalten Sie die Positionsleuchte des Shelfs ein, sodass Sie die physische Position des Shelfs im Schrank oder Rack finden können.
- Ändern Sie die ID-Nummer, die oben links in der Shelf-Ansicht angezeigt wird.
- Zeigen Sie die Shelf-Einstellungen an, z. B. die Typen installierter Laufwerke und die Seriennummer.
- Verschieben Sie die Shelf-Ansichten nach oben oder unten, um das physische Layout im Storage-Array zu entsprechen.

Controller

Ein Controller ist die kombinierte Hardware und Firmware, die Storage-Array- und Managementfunktionen implementiert. Sie umfasst Cache-Speicher, Laufwerksunterstützung und Host-Interface-Unterstützung.

Sie können die folgenden Funktionen für Controller ausführen:

- Konfigurieren Sie die Management-Ports für IP-Adressen und Geschwindigkeit.
- Konfigurieren Sie iSCSI-Hostverbindungen (wenn iSCSI-Hosts vorhanden sind).
- Konfigurieren Sie einen NTP-Server (Network Time Protocol) und einen DNS-Server (Domain Name System).
- Zeigen Sie den Controller-Status und die -Einstellungen an.

- Benutzern außerhalb des lokalen Netzwerks ermöglichen, eine SSH-Sitzung zu starten und die Einstellungen auf dem Controller zu ändern.
- Platzieren Sie den Controller offline, online oder in Servicemodus.

Laufwerke

Das Storage-Array kann Festplattenlaufwerke (HDDs) oder Solid State-Laufwerke (SSDs) umfassen. Je nach Shelf-Größe können bis zu 12, 24 oder 60 Laufwerke im Shelf installiert werden.

Sie können die folgenden Funktionen im Zusammenhang mit Laufwerken ausführen:

- Schalten Sie die Positionsleuchte des Laufwerks ein, damit Sie den physischen Speicherort des Laufwerks im Shelf finden können.
- Zeigen Sie den Laufwerkstatus und die Einstellungen an.
- Weisen Sie ein Laufwerk erneut zu (ersetzen Sie ein ausgefallenes Laufwerk durch ein nicht zugewiesenes Laufwerk logisch), und rekonstruieren Sie es bei Bedarf manuell.
- Ein Laufwerk kann manuell ausfallen, sodass Sie es ersetzen können. (Wenn ein Laufwerk ausfällt, können Sie den Inhalt des Laufwerks kopieren, bevor Sie es ersetzen.)
- Zuweisung oder Zuweisung von Hot Spares
- Laufwerke löschen.

Terminologie der Hardware

Die folgenden Hardwarebedingungen gelten für Storage Arrays.

Allgemeine Begriffe der Hardware:

Komponente	Beschreibung
Bucht	Ein Schacht ist ein Steckplatz im Shelf, in dem ein Laufwerk oder eine andere Komponente installiert ist.
Controller	Ein Controller besteht aus einer Hauptplatine, Firmware und Software. Sie steuert die Laufwerke und implementiert die Funktionen von System Manager.
Controller-Shelf	Ein Controller-Shelf enthält einen Satz von Laufwerken und einen oder mehrere Controller-Behälter. Ein Controller-Behälter enthält die Controller, Host-Schnittstellenkarten (HICs) und Batterien.
Laufwerk	Ein Laufwerk ist ein elektromagnetisches mechanisches Gerät oder ein Solid State-Speichergerät, das die physischen Speichermedien für Daten bereitstellt.
Festplatten-Shelf	Ein Festplatten-Shelf, auch als Erweiterungs-Shelf bezeichnet, enthält mehrere Laufwerke und zwei Input/Output-Module (IOMs). Die IOMs enthalten SAS-Ports, die ein Festplatten-Shelf mit einem Controller-Shelf oder anderen Festplatten-Shelfs verbinden.
IOM (ESM)	Ein IOM ist ein ein ein ein-/Ausgabemodul, das SAS-Ports zum Anschließen des Festplatten-Shelf an das Controller-Shelf enthält. In früheren Controller-Modellen wurde das IOM als Environmental Service Module (ESM) bezeichnet.
Power-/Lüfterbehälter	Ein Power-/Lüfterbehälter ist eine Baugruppe, die in ein Regal gleist. Sie umfasst ein Netzteil und einen integrierten Lüfter.
SFP	Ein SFP ist ein Small Form-factor Pluggable (SFP) Transceiver.
Shelf	Ein Shelf ist ein Gehäuse, das in einem Schrank oder Rack installiert ist. Er enthält die Hardwarekomponenten für das Storage-Array. Es gibt zwei Typen von Shelfs: Ein Controller-Shelf und ein Festplatten-Shelf. Ein Controller Shelf enthält Controller und Laufwerke. Ein Festplatten-Shelf enthält ein-/Ausgabemodule (IOMs) und Laufwerke.
Storage Array erledigen	Ein Storage-Array umfasst Shelfs, Controller, Laufwerke, Software und Firmware.

Controller-Begriffe:

Komponente	Beschreibung
Controller	Ein Controller besteht aus einer Hauptplatine, Firmware und Software. Sie steuert die Laufwerke und implementiert die Funktionen von System Manager.
Controller-Shelf	Ein Controller-Shelf enthält einen Satz von Laufwerken und einen oder mehrere Controller-Behälter. Ein Controller-Behälter enthält die Controller, Host-Schnittstellenkarten (HICs) und Batterien.
DHCP	Dynamic Host Configuration Protocol (DHCP) ist ein Protokoll, das in IP-Netzwerken (Internet Protocol) zur dynamischen Verteilung von Netzwerkkonfigurationsparametern, z. B. IP-Adressen, verwendet wird.
DNS	Domain Name System (DNS) ist ein Benennungssystem für Geräte, die mit dem Internet oder einem privaten Netzwerk verbunden sind. Der DNS-Server verwaltet ein Verzeichnis von Domain-Namen und übersetzt diese in Internet Protocol (IP)-Adressen.
Duplexkonfigurationen	Duplex ist eine Konfiguration mit zwei Controllern im Speicher-Array. Duplex-Systeme sind in Bezug auf Controller, logische Volume-Pfade und Disk-Pfade vollständig redundant. Sollte ein Controller ausfallen, übernimmt der andere Controller dessen I/O, um die Verfügbarkeit zu gewährleisten. Duplex-Systeme verfügen auch über redundante Lüfter und Netzteile.
Vollduplex-/Halbduplex-Anschlüsse	Vollduplex- und Halbduplex-Mode siehe Verbindungsmodi. Im Vollduplex-Modus können zwei Geräte gleichzeitig in beide Richtungen kommunizieren. Im Halbduplex-Modus können Geräte gleichzeitig in eine Richtung kommunizieren (ein Gerät sendet eine Nachricht, während das andere Gerät sie empfängt).
HIC	Eine Host Interface Card (HIC) kann optional in einem Controller-Behälter installiert werden. Host Ports, die in den Controller integriert sind, werden als Baseboard Host Ports bezeichnet. In die HIC integrierte Host Ports werden HIC Ports genannt.
ICMP-PING-Antwort	Internet Control Message Protocol (ICMP) ist ein Protokoll, das von Betriebssystemen vernetzter Computer zum Senden von Nachrichten verwendet wird. ICMP-Meldungen bestimmen, ob ein Host erreichbar ist und wie lange es dauert, bis Pakete von und zu diesem Host gelangen.
MAC-Adresse	Media Access Control Identifier (MAC-Adressen) werden vom Ethernet verwendet, um zwischen separaten logischen Kanälen zu unterscheiden, die zwei Ports auf derselben physischen Transportnetzwerkschnittstelle verbinden.
Management- Client	Ein Management-Client ist der Computer, auf dem ein Browser zum Zugriff auf System Manager installiert ist.

Komponente	Beschreibung
MTU	Eine Maximum Transmission Unit (MTU) ist das größte Paket oder den größten Frame, der in einem Netzwerk gesendet werden kann.
NTP	Network Time Protocol (NTP) ist ein Netzwerkprotokoll für die Uhrsynchronisierung zwischen Computersystemen in Datennetzwerken.
Simplex-Konfigurationen	Simplex ist eine Konfiguration mit einem Controller-Modul innerhalb des Speicher-Arrays. Ein simplex-System bietet keine Controller- oder Disk-Path-Redundanz, sondern redundante Lüfter und Netzteile.
VLAN	Ein Virtual Local Area Network (VLAN) ist ein logisches Netzwerk, das sich so verhält, als sei es physisch getrennt von anderen Netzwerken, die von denselben Geräten (Switches, Router usw.) unterstützt werden.

Laufwerksbedingungen:

Komponente	Beschreibung
DA	Data Assurance (da) ist eine Funktion, die Fehler überprüft und korrigiert, die auftreten können, wenn Daten durch die Controller zu den Laufwerken übertragen werden. Data Assurance kann auf Pool- oder Volume-Gruppenebene aktiviert werden, wobei Hosts über eine da-fähige I/O-Schnittstelle wie Fibre Channel verfügen.
Laufwerkssicherheit	Laufwerkssicherheit ist eine Funktion des Storage Arrays, die eine zusätzliche Sicherheitsschicht bietet – entweder mit vollständigen Festplatten-Verschlüsselung (FDE) oder FIPS-Laufwerken (Federal Information Processing Standard). Wenn diese Laufwerke zusammen mit der Sicherheitsfunktion des Laufwerks verwendet werden, benötigen sie einen Sicherheitsschlüssel für den Zugriff auf ihre Daten. Wenn die Laufwerke physisch aus dem Array entfernt werden, können sie erst betrieben werden, wenn sie in einem anderen Array installiert sind. Zu diesem Zeitpunkt befinden sie sich in einem Sicherheitsstatus, bis der richtige Sicherheitsschlüssel bereitgestellt wird.
Festplatten-Shelf	Ein Festplatten-Shelf, auch als Erweiterungs-Shelf bezeichnet, enthält mehrere Laufwerke und zwei Input/Output-Module (IOMs). Die IOMs enthalten SAS-Ports, die ein Festplatten-Shelf mit einem Controller-Shelf oder anderen Festplatten-Shelfs verbinden.
DULBE	Dezugewiesener oder nicht geschriebener logischer Blockfehler (DULBE) ist eine Option auf NVMe-Laufwerken, mit der das EF300- oder EF600-Storage-Array ressourcenbereitgestellte Volumes unterstützen kann.
FDE-Laufwerke	Vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) ermöglicht die Verschlüsselung auf Festplattenlaufwerken auf Hardware-Ebene. Die Festplatte enthält einen ASIC-Chip, der Daten während des Schreibvorgangs verschlüsselt und die Daten beim Lesen entschlüsselt.
FIPS-Laufwerke	FIPS-Laufwerke verwenden Federal Information Processing Standards (FIPS) 140-2 Level 2. Es handelt sich im Wesentlichen um FDE-Laufwerke, die den Standards der US-Regierung entsprechen, um solide Verschlüsselungsalgorithmen und -Methoden sicherzustellen. FIPS-Laufwerke haben höhere Sicherheitsstandards als FDE-Laufwerke.
HDD	Festplattenlaufwerke (HDDs) sind Datenspeicher-Geräte, die rotierende Metallplatten mit einer magnetischen Beschichtung verwenden.
Hot-Spare-Laufwerke	Hot Spares fungieren als Standby-Laufwerke in RAID 1-, RAID 5- oder RAID 6-Volume-Gruppen. Es handelt sich dabei um voll funktionsfähige Laufwerke, die keine Daten enthalten. Wenn ein Laufwerk in der Volume-Gruppe ausfällt, rekonstruiert der Controller die Daten vom ausgefallenen Laufwerk automatisch auf eine Hot Spare-Festplatte.

Komponente	Beschreibung
NVMe	Non-Volatile Memory Express (NVMe) ist eine Schnittstelle, die für Flash-basierte Storage-Geräte wie SSD-Laufwerke konzipiert wurde. NVMe reduziert den I/O-Overhead und beinhaltet Performance-Verbesserungen im Vergleich zu vorherigen Schnittstellen für logische Geräte.
SAS	Serial Attached SCSI (SAS) ist ein Point-to-Point-Protokoll, bei dem Controller direkt mit Festplatten verbunden werden.
Secure-fähige Laufwerke	Sichere Laufwerke können entweder vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) sein, die Daten während des Schreibvorgangs verschlüsseln und Daten während Lesevorgängen entschlüsseln. Diese Laufwerke gelten als sicher-*fähig*, da sie mit der Sicherheitsfunktion des Laufwerks für zusätzliche Sicherheit verwendet werden können. Wenn die Laufwerkssicherheitsfunktion für Volume-Gruppen und -Pools aktiviert ist, die mit diesen Laufwerken verwendet werden, werden die Laufwerke sicher-*Enabled*.
Secure-Enabled Laufwerke	Secure-Enabled-Laufwerke werden mit der Drive Security-Funktion verwendet. Wenn Sie die Laufwerkssicherheitsfunktion aktivieren und dann Laufwerksicherheit auf einem Pool oder einer Volume-Gruppe auf Secure-*fähigen*-Laufwerken anwenden, werden die Laufwerke sicher-*aktiviert_*. Lese- und Schreibzugriff ist nur über einen Controller verfügbar, der mit dem korrekten Sicherheitsschlüssel konfiguriert ist. Diese zusätzliche Sicherheit verhindert einen nicht autorisierten Zugriff auf die Daten auf einem Laufwerk, das physisch vom Storage-Array entfernt wird.
SSD	Solid State Disks (SSDs) sind Daten-Storage-Geräte, die Solid State Memory (Flash) verwenden, um Daten dauerhaft zu speichern. SSDs bieten herkömmliche Festplatten an und sind mit denselben Schnittstellen verfügbar wie die Festplatten.

Bedingungen für iSCSI:

Laufzeit	Beschreibung
CHAP	Die CHAP-Methode (Challenge Handshake Authentication Protocol) überprüft die Identität von Zielen und Initiatoren während der ersten Verbindung. Die Authentifizierung basiert auf einem gemeinsamen Sicherheitsschlüssel namens CHAP *secret*.
Controller	Ein Controller besteht aus einer Hauptplatine, Firmware und Software. Sie steuert die Laufwerke und implementiert die Funktionen von System Manager.
DHCP	Dynamic Host Configuration Protocol (DHCP) ist ein Protokoll, das in IP-Netzwerken (Internet Protocol) zur dynamischen Verteilung von Netzwerkkonfigurationsparametern, z. B. IP-Adressen, verwendet wird.
IB	InfiniBand (IB) ist ein Kommunikationsstandard für die Datenübertragung zwischen hochperformanten Servern und Storage-Systemen.
ICMP-PING-Antwort	Internet Control Message Protocol (ICMP) ist ein Protokoll, das von Betriebssystemen vernetzter Computer zum Senden von Nachrichten verwendet wird. ICMP-Meldungen bestimmen, ob ein Host erreichbar ist und wie lange es dauert, bis Pakete von und zu diesem Host gelangen.
IQN	Eine IQN-Kennung (iSCSI Qualified Name) ist ein eindeutiger Name für einen iSCSI-Initiator oder ein iSCSI-Ziel.
ISER	ISCSI Extensions for RDMA (iSER) ist ein Protokoll, das das iSCSI-Protokoll für den Betrieb über RDMA-Übertragungen wie InfiniBand oder Ethernet erweitert.
ISNS	Internet Storage Name Service (iSNS) ist ein Protokoll, das die automatische Erkennung, Verwaltung und Konfiguration von iSCSI- und Fibre-Channel-Geräten in TCP/IP-Netzwerken ermöglicht.
MAC-Adresse	Media Access Control Identifier (MAC-Adressen) werden vom Ethernet verwendet, um zwischen separaten logischen Kanälen zu unterscheiden, die zwei Ports auf derselben physischen Transportnetzwerkschnittstelle verbinden.
Management- Client	Ein Management-Client ist der Computer, auf dem ein Browser zum Zugriff auf System Manager installiert ist.
MTU	Eine Maximum Transmission Unit (MTU) ist das größte Paket oder den größten Frame, der in einem Netzwerk gesendet werden kann.

Laufzeit	Beschreibung
RDMA	Remote Direct Memory Access (RDMA) ist eine Technologie, mit der Netzwerkcomputer Daten im Hauptspeicher austauschen können, ohne das Betriebssystem eines jeden Computers zu involvieren.
Nicht benannte Ermittlungssitzung	Wenn die Option für nicht benannte Ermittlungssitzungen aktiviert ist, müssen iSCSI-Initiatoren nicht die Ziel-IQN angeben, um die Controller-Informationen abzurufen.

Begriffe im Zusammenhang mit NVMe:

Laufzeit	Beschreibung
InfiniBand	InfiniBand (IB) ist ein Kommunikationsstandard für die Datenübertragung zwischen hochperformanten Servern und Storage-Systemen.
Namespace	Ein Namespace ist NVM Storage, der für Blockzugriff formatiert ist. Es gleicht einer logischen Einheit in SCSI, die ein Volume im Storage Array bezieht.
Namespace-ID	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.
NQN	NVMe Qualified Name (NQN) wird zur Identifizierung des Remote-Storage-Ziels (des Storage-Arrays) verwendet.
NVM	Non-Volatile Memory (NVM) ist ein persistenter Speicher, der in vielen Arten von Speichergeräten verwendet wird.
NVMe	Non-Volatile Memory Express (NVMe) ist eine Schnittstelle, die für Flash-basierte Storage-Geräte wie SSD-Laufwerke konzipiert wurde. NVMe reduziert den I/O-Overhead und beinhaltet Performance-Verbesserungen im Vergleich zu vorherigen Schnittstellen für logische Geräte.
NVMe-of	Non-Volatile Memory Express over Fabrics (NVMe-of) ist eine Spezifikation, die die Übertragung von NVMe-Befehlen und -Daten über ein Netzwerk zwischen Host und Storage ermöglicht.
NVMe-Controller	Während der Host-Verbindung wird ein NVMe-Controller erstellt. Es stellt einen Zugriffspfad zwischen einem Host und den Namespaces im Storage-Array bereit.
NVMe-Warteschlange	Zum Übergeben von Befehlen und Nachrichten über die NVMe Schnittstelle wird eine Warteschlange verwendet.
NVMe-Subsystem	Das Storage-Array mit einer NVMe-Host-Verbindung.
RDMA	RDMA (Remote Direct Memory Access) ermöglicht eine direktere Datenverschiebung auf einem Server und wieder zurück, indem es ein Transportprotokoll in der NIC-Hardware (Network Interface Card) implementiert.
ROCE	RDMA over Converged Ethernet (RoCE) ist ein Netzwerkprotokoll, das über ein Ethernet-Netzwerk einen Remote Direct Memory Access (RDMA) ermöglicht.

Laufzeit	Beschreibung
SSD	Solid State Disks (SSDs) sind Daten-Storage-Geräte, die Solid State Memory (Flash) verwenden, um Daten dauerhaft zu speichern. SSDs bieten herkömmliche Festplatten an und sind mit denselben Schnittstellen verfügbar wie die Festplatten.

Management von Shelf-Komponenten

Hardwarekomponenten von View

Die Seite Hardware bietet Sortier- und Filterfunktionen, die die Suche nach Komponenten erleichtern.

Schritte

1. Wählen Sie **Hardware**.
2. Verwenden Sie die in der folgenden Tabelle beschriebenen Funktionen, um Hardwarekomponenten anzuzeigen.

Funktion	Beschreibung
Ansichten von Laufwerken, Controllern und Komponenten	Um zwischen Vorder- und Rückansicht zu wechseln, wählen Sie ganz rechts entweder **Laufwerke** oder **Controller & Komponenten** aus (der Link, der angezeigt wird, hängt von der aktuellen Ansicht ab). Die Ansicht **Laufwerke** zeigt Laufwerke und alle leeren Laufwerksschächte an. Die Ansicht **Controller & Komponenten** zeigt die Controller und alle EAM-Module (ESM), Strom-/Lüftereinschübe oder leeren Controller-Einschübe. Unten auf der Seite können Sie auch **Alle Laufwerke anzeigen** auswählen.
Filter für die Laufwerkansicht	Wenn das Speicher-Array Laufwerke mit unterschiedlichen physischen und logischen Attributen enthält, enthält die Seite **Hardware** Laufwerke mit Ansichtsfiltern. Diese Filterfelder helfen Ihnen, bestimmte Laufwerke schnell zu finden, indem Sie die auf der Seite angezeigten Laufwerkstypen begrenzen. Klicken Sie unter **Laufwerke anzeigen, die…** sind, auf das Filterfeld links (standardmäßig wird **beliebiger Laufwerkstyp** angezeigt), um eine Dropdown-Liste mit physischen Attributen (z. B. Kapazität und Geschwindigkeit) anzuzeigen. Klicken Sie auf das Filterfeld rechts (standardmäßig zeigt **Anywhere im Speicherarray** an), um eine Dropdown-Liste mit logischen Attributen (z. B. Zuweisung von Volume-Gruppen) anzuzeigen. Sie können diese Filter zusammen oder separat verwenden. Wenn das Speicher-Array Laufwerke enthält, die alle dieselben physischen Attribute verwenden, wird das Feld **beliebiger Laufwerkstyp** auf der linken Seite nicht angezeigt. Wenn sich die Laufwerke alle an demselben logischen Ort befinden, wird das Feld **Anywhere im Speicher-Array** rechts nicht angezeigt.

Funktion	Beschreibung
Legende	Die Komponenten werden in bestimmten Farben angezeigt, um ihren Rollenzustand darzustellen. Um die Beschreibungen dieser Zustände zu erweitern und zu reduzieren, klicken Sie auf **Legende**.
Zeigt Details zum Statussymbol an	Die Statusanzeigen können Textbeschreibungen für den Verfügbarkeitsstatus enthalten. Klicken Sie auf **Statusanzeige anzeigen**, um diesen Statustext ein- oder auszublenden.
Shelf-/Shelf-Symbole	Jede Shelf-Ansicht enthält eine Liste mit verwandten Befehlen sowie Eigenschaften und Status. Klicken Sie auf **Regal**, um eine Dropdown-Liste mit Befehlen anzuzeigen. Sie können auch eines der Symbole oben auswählen, um Status und Eigenschaften für einzelne Komponenten anzuzeigen: Controller, IOMs (ESMs), Netzteile, Lüfter, Temperatur, Batterien und SFPs.
Shelf-Reihenfolge	Die Regale können auf der Hardware-Seite neu angeordnet werden. Verwenden Sie die nach-oben- bzw. nach-unten-Pfeile oben rechts in jeder Shelf-Ansicht, um die Shelfs oben/unten zu ändern.

Komponentenstatus ein- oder ausblenden

Sie können Statusbeschreibungen für Laufwerke, Controller, Lüfter und Netzteile anzeigen.

Schritte

1. Wählen Sie **Hardware**.
2. So sehen Sie die Komponenten auf der Rückseite oder auf der Vorderseite:
   - Wenn Sie die Komponenten des Controllers und des Power/Fan-Kanisters sehen möchten, aber die Laufwerke angezeigt werden, klicken Sie auf die Registerkarte **Controller & Komponenten**.
   - Wenn Sie die Laufwerke sehen möchten, aber die Komponenten des Controllers und des Netzstromanzeigebehälters angezeigt werden, klicken Sie auf die Registerkarte **Laufwerke**.
3. So zeigen Sie Pop-over-Statusbeschreibungen an oder verbergen sie:
   - Wenn Sie eine Pop-over-Beschreibung der Statussymbole sehen möchten, klicken Sie oben rechts in der Shelf-Ansicht auf **Statussymbol anzeigen**. (Aktivieren Sie das Kontrollkästchen).
   - Um die Pop-over-Beschreibungen auszublenden, klicken Sie erneut auf **Statusanzeige-Symboldetails** (deaktivieren Sie das Kontrollkästchen).
4. Wenn Sie vollständige Statusdetails sehen möchten, wählen Sie die Komponente in der Shelf-Ansicht aus, und wählen Sie dann **Einstellungen anzeigen**.
5. Wenn Sie die Beschreibungen der farbigen Komponenten anzeigen möchten, wählen Sie **Legende**.

Wechseln Sie zwischen Vorder- und Rückseite

Die Hardware-Seite kann entweder die Vorder- oder die Rückseite des Shelfs anzeigen.

Über diese Aufgabe

Die Ansicht auf der Rückseite zeigt die Controller/IOMs und die Power-Fan-Kanister. In der Vorderansicht

werden die Laufwerke angezeigt.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte **Controller & Komponenten**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

3. Wenn die Grafik die Controller anzeigt, klicken Sie auf die Registerkarte **Laufwerke**.

   Die Grafik ändert sich, um die Laufwerke anstelle der Controller anzuzeigen.

4. Optional können Sie **Alle anzeigen** oder **Alle anzeigen zurück** wählen, die sich am unteren Rand der Seite befinden.

Ansichtsreihenfolge der Shelfs ändern

Sie können die Reihenfolge der auf der Seite Hardware angezeigten Shelfs ändern, um sie der physischen Reihenfolge der Regale in einem Schrank anzupassen.

Schritte

1. Wählen Sie **Hardware**.
2. Wählen Sie oben rechts in einer Shelf-Ansicht die nach-oben- bzw. nach-unten-Pfeile aus, um die Reihenfolge der auf der Hardware-Seite angezeigten Shelfs neu anzuordnen.

Die Positionsleuchte für den Regal einschalten

Um den physischen Speicherort eines auf der Hardware-Seite gezeigten Shelfs zu ermitteln, können Sie die Locator-LED des Shelfs einschalten.

Schritte

1. Wählen Sie **Hardware**.
2. Wählen Sie die Dropdown-Liste für das Controller-Shelf oder Laufwerk-Shelf aus, und wählen Sie dann **Locator einschalten**.

   Die Positionsleuchte für das Regal leuchtet auf.

3. Wenn Sie das Regal physisch gefunden haben, kehren Sie zum Dialogfeld zurück und wählen Sie **Ausschalten**.

Ändern Sie Shelf-IDs

Die Shelf-ID ist eine Nummer, die ein Shelf im Storage Array eindeutig identifiziert. Die Regale werden nacheinander nummeriert, beginnend mit entweder 00 oder 01, oben links von jeder Regalansicht.

Über diese Aufgabe

Die Controller-Firmware weist automatisch die Shelf-ID zu. Sie können diese Nummer jedoch ändern, wenn Sie ein anderes Bestellschema erstellen möchten.

Schritte

1. Wählen Sie **Hardware**.
2. Wählen Sie die Dropdown-Liste für das Controller-Shelf oder Laufwerk-Shelf aus, und wählen Sie dann **ID ändern** aus.
3. Wählen Sie im Dialogfeld Shelf-ID ändern die Dropdown-Liste aus, um die verfügbaren Nummern anzuzeigen.

   In diesem Dialogfeld werden keine IDs angezeigt, die derzeit aktiven Shelfs zugewiesen sind.

4. Wählen Sie eine verfügbare Nummer aus, und klicken Sie dann auf **Speichern**.

   Je nach gewählter Nummer kann die Shelf-Reihenfolge auf der Hardware-Seite neu angeordnet werden. Auf Wunsch können Sie mit den nach-oben/unten-Pfeilen oben rechts auf jedem Regal die Reihenfolge neu einlesen.

Zeigt den Status und die Einstellungen von Shelf-Komponenten an

Die Seite Hardware enthält Status und Einstellungen für Shelf-Komponenten, einschließlich Netzteile, Lüfter und Batterien.

Über diese Aufgabe

Die verfügbaren Komponenten sind vom Shelf-Typ abhängig:

- **Laufwerk-Shelf** — enthält einen Satz von Laufwerken, Strom-/Lüfterkanistern, ein-/Ausgangsmodulen (IOMs) und anderen unterstützenden Komponenten in einem einzigen Shelf.
- **Controller-Shelf** — enthält einen Satz von Laufwerken, ein oder zwei Controller-Kanister, Power/Fan-Kanister und andere unterstützende Komponenten in einem einzigen Shelf.

Schritte

1. Wählen Sie **Hardware**.
2. Wählen Sie die Dropdown-Liste für das Controller-Shelf oder Laufwerk-Shelf aus, und wählen Sie dann **Anzeigeeinstellungen** aus.

   Das Dialogfeld Einstellungen für Shelf-Komponenten wird geöffnet. Auf diesen Registerkarten werden der Status und die Einstellungen für die Shelf-Komponenten angezeigt. Je nach ausgewähltem Shelf werden einige in der Tabelle beschriebene Registerkarten möglicherweise nicht angezeigt.

Registerkarte	Beschreibung
Shelf	Auf der Registerkarte **Shelf** werden folgende Eigenschaften angezeigt: • **Shelf ID** — identifiziert eindeutig ein Regal im Speicher-Array. Die Controller-Firmware weist diese Nummer zu, Sie können sie aber durch Auswahl des Menüs:Shelf[Change ID] ändern. • **Shelf-Pfadredundanz** — gibt an, ob Verbindungen zwischen dem Regal und dem Controller alternative Methoden haben (ja) oder nicht (Nein). • **Aktuelle Laufwerkstypen** — zeigt den in die Laufwerke eingebauten Technologietyp an (zum Beispiel ein sicheres SAS-Laufwerk). Wenn es mehrere Laufwerkstypen gibt, werden beide Technologien angezeigt. • **Seriennummer** — zeigt die Seriennummer des Shelfs an.

Registerkarte	Beschreibung
IOMs (ESMs)	Auf der Registerkarte **IOMs (ESM)** wird der Status des ein-/Ausgangsmoduls (EAM) angezeigt, das auch als Umgebungsservicemodul (ESM) bezeichnet wird. Es überwacht den Status der Komponenten in einem Laufwerk-Shelf und dient als Verbindungspunkt zwischen dem Laufwerksfach und dem Controller. Der Status kann „optimal“, „Fehlgeschlagen“, „optimal“ (Fehlgeschlagen) oder „nicht zertifiziert“ lauten. Weitere Informationen sind die Firmware-Version und die Version der Konfigurationseinstellungen. Wählen Sie **Weitere Einstellungen anzeigen**, um die maximale und aktuelle Datenrate und den Zustand der Kartenkommunikation anzuzeigen (entweder Ja oder Nein). Sie können diesen Status auch anzeigen, indem Sie das IOM-Symbol auswählen , Neben der Dropdown-Liste Regal.
Netzteile	Auf der Registerkarte **Netzteile** wird der Status des Netzteilbehälter und des Netzteils selbst angezeigt. Der Status kann „optimal“, „Fehlgeschlagen“, „Entfernen“ oder „Unbekannt“ lauten. Sie zeigt auch die Teilenummer des Netzteils an. Sie können diesen Status auch anzeigen, indem Sie das Netzteil-Symbol auswählen , Neben der Dropdown-Liste Regal.
Lüfter	Auf der Registerkarte **Fans** wird der Status des Lüfterbehälter und des Lüfters selbst angezeigt. Der Status kann „optimal“, „Fehlgeschlagen“, „Entfernen“ oder „Unbekannt“ lauten. Sie können diesen Status auch anzeigen, indem Sie das Symbol Lüfter auswählen , Neben der Dropdown-Liste Regal.
Temperatur	Auf der Registerkarte **Temperatur** wird der Temperaturstatus der Regalkomponenten angezeigt, z. B. Sensoren, Controller und Strom-/Lüfterbehälter. Status kann optimal sein, Nominaltemperatur überschritten, maximale Temperatur überschritten oder Unbekannt. Sie können diesen Status auch anzeigen, indem Sie das Temperatursymbol auswählen , Neben der Dropdown-Liste Regal.

Registerkarte	Beschreibung
Batterien	Auf der Registerkarte **Batteries** wird der Status der Controller-Batterien angezeigt. Der Status kann „optimal“, „Fehlgeschlagen“, „Entfernen“ oder „Unbekannt“ lauten. Weitere Informationen umfassen das Alter der Batterie, Tage bis zum Austausch, Lernzyklen und Wochen zwischen den Lernzyklen. Sie können diesen Status auch anzeigen, indem Sie das Batteriesymbol auswählen, Neben der Dropdown-Liste Regal.
SFPs	Die Registerkarte **SFPs** zeigt den Status von SFP-Transceivern (Small Form-factor Pluggable) auf den Controllern an. Der Status kann „optimal“, „Fehlgeschlagen“ oder „Unbekannt“ lauten. Wählen Sie **Weitere Einstellungen anzeigen** aus, um die Teilenummer, die Seriennummer und den Anbieter der SFPs anzuzeigen. Sie können diesen Status auch anzeigen, indem Sie das SFP-Symbol auswählen, Neben der Dropdown-Liste Regal.

3. Klicken Sie Auf **Schließen**.

Aktualisieren Sie die Lernzyklen der Batterie

Ein Lernzyklus ist ein automatischer Zyklus zum Kalibrieren der intelligenten Akkuanzeige. Die Zyklen werden in 8-Wochen-Intervallen (pro Controller) automatisch, am selben Tag und zur gleichen Zeit, gestartet. Wenn Sie einen anderen Zeitplan festlegen möchten, können Sie die Lernzyklen anpassen.

Über diese Aufgabe

Die Aktualisierung der Lernzyklen wirkt sich auf beide Controller-Batterien aus.

Schritte

1. Wählen Sie **Hardware**.
2. Wählen Sie die Dropdown-Liste für das Controller-Shelf aus, und wählen Sie dann **Einstellungen anzeigen** aus.
3. Wählen Sie die Registerkarte **Akkus** aus.
4. Wählen Sie **Akku-Lernzyklen aktualisieren**.

   Das Dialogfeld Akku-Lernzyklen aktualisieren wird geöffnet.

5. Wählen Sie aus den Dropdown-Listen einen neuen Tag und eine neue Uhrzeit aus.
6. Klicken Sie Auf **Speichern**.

Management von Controllern

Controller-Status

Ein Controller kann in drei verschiedene Zustände versetzt werden: „Online“, „Offline“ und „Service“.

Online-Status

Der Status „Online“ lautet der normale Betriebsstatus des Controllers. Dies bedeutet, dass der Controller ordnungsgemäß funktioniert und für I/O-Vorgänge verfügbar ist.

Wenn Sie einen Controller online schalten, wird dessen Status auf „optimal“ gesetzt.

Offline-Status

Der Offline-Status wird normalerweise verwendet, um einen Controller zum Austausch vorzubereiten, wenn es im Storage Array zwei Controller gibt. Ein Controller kann auf zwei Arten in den Offline-Status eintreten: Sie können einen expliziten Befehl ausgeben oder der Controller kann ausfallen. Ein Controller kann den Offline-Status nur durch Eingabe eines anderen expliziten Befehls oder durch Ersetzen des ausgefallenen Controllers beenden. Sie können einen Controller nur offline schalten, wenn sich zwei Controller im Storage-Array befinden.

Wenn ein Controller den Status „Offline“ aufweist, gelten die folgenden Bedingungen:

- Der Controller ist für I/O nicht verfügbar
- Sie können das Storage Array nicht über diesen Controller verwalten.
- Alle Volumes, die aktuell dem Controller gehören, werden auf den anderen Controller verschoben.
- Die Cache-Spiegelung ist deaktiviert und alle Volumes werden in den Schreib-Cache-Modus geändert.

Servicemodus

Service Mode wird normalerweise nur vom technischen Support verwendet, um alle Storage Array Volumes zu einem Controller zu verschieben, sodass die Diagnose des anderen Controllers gestellt werden kann. Ein Controller muss manuell in den Servicemodus versetzt werden und muss nach Abschluss des Servicevorgangs manuell wieder online geschaltet werden.

Wenn sich ein Controller im Servicemodus befindet, gelten die folgenden Bedingungen:

- Der Controller ist für I/O nicht verfügbar
- Der technische Support kann über den seriellen Port oder die Netzwerkverbindung auf den Controller zugreifen, um potenzielle Probleme zu analysieren.
- Alle Volumes, die aktuell dem Controller gehören, werden auf den anderen Controller verschoben.
- Die Cache-Spiegelung ist deaktiviert und alle Volumes werden in den Schreib-Cache-Modus geändert.

Überlegungen beim Zuweisen von IP-Adressen

Standardmäßig werden Controller bei beiden Netzwerk-Ports mit aktiviertem DHCP ausgeliefert. Sie können statische IP-Adressen zuweisen, die statischen Standardadressen verwenden oder DHCP-zugewiesene IP-Adressen verwenden. Sie können auch eine statusfreie IPv6-Konfiguration verwenden.

IPv6 ist bei neuen Controllern standardmäßig deaktiviert, Sie können jedoch die Management-Port-IP-Adressen mit einer alternativen Methode konfigurieren und dann IPv6 auf den Management-Ports mit System Manager aktivieren.

Wenn sich der Netzwerk-Port in einem Status „Link down“ befindet, d. h. von einem LAN getrennt, meldet das System seine Konfiguration entweder statisch, zeigt eine IP-Adresse von 0.0.0.0 (frühere Freigaben) an oder DHCP ist aktiviert, ohne dass eine IP-Adresse gemeldet wurde (spätere Freigaben). Wenn sich der Netzwerkport im Status „Verbindung nach oben“ befindet (d. h., verbunden mit einem LAN), versucht er, eine IP-Adresse über DHCP abzurufen.

Wenn der Controller bei einem bestimmten Netzwerkport keine DHCP-Adresse erhalten kann, wird auf eine Standard-IP-Adresse zurückgesetzt, die bis zu 3 Minuten dauert. Folgende Standard-IP-Adressen sind vorgesehen:

```
Controller 1 (port 1): IP Address: 192.168.128.101
```

```
Controller 1 (port 2): IP Address: 192.168.129.101
```

```
Controller 2 (port 1): IP Address: 192.168.128.102
```

```
Controller 2 (port 2): IP Address: 192.168.129.102
```

Beim Zuweisen von IP-Adressen:

- Reservieren Sie Port 2 auf den Controllern für den Kunden-Support. Ändern Sie nicht die Standard-Netzwerkeinstellungen (DHCP ist aktiviert).
- Verwenden Sie SANtricity System Manager, um statische IP-Adressen für E4000, E2800 und E5700 Controller festzulegen. Verwenden Sie SANtricity Storage Manager, um statische IP-Adressen für E2700 und E5600 Controller festzulegen. Nach der Konfiguration einer statischen IP-Adresse bleibt sie durch alle Verbindungs-Down-/Up-Ereignisse festgelegt.
- Um DHCP zum Zuweisen der IP-Adresse des Controllers zu verwenden, verbinden Sie den Controller mit einem Netzwerk, das DHCP-Anfragen verarbeiten kann. Verwenden Sie einen permanenten DHCP-Leasing.

Die Standardadressen werden nicht über Ereignisse mit Verbindungsabfällen hinweg beibehalten. Wenn ein Netzwerk-Port auf einem Controller auf DHCP eingestellt ist, versucht der Controller bei jedem Link-Ereignis eine DHCP-Adresse zu erhalten, einschließlich Einführungen von Kabeln, Neustarts und Energiezyklen. Jedes Mal, wenn ein DHCP-Versuch fehlschlägt, wird die statische Standard-IP-Adresse für diesen Port verwendet.

Konfigurieren Sie den Managementport

Der Controller enthält einen für das Systemmanagement verwendeten Ethernet-Port. Bei

Bedarf können Sie die Übertragungsparameter und IP-Adressen ändern.

Über diese Aufgabe

Während dieses Verfahrens wählen Sie Port 1 und bestimmen dann die Geschwindigkeit und Port Addressing-Methode. Port 1 stellt eine Verbindung zum Netzwerk her, in dem der Management-Client auf den Controller und System Manager zugreifen kann.

> Verwenden Sie nicht Port 2 auf beiden Controllern. Port 2 ist dem technischen Support vorbehalten.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte **Controller & Komponenten**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.
3. Klicken Sie auf den Controller mit dem Managementport, den Sie konfigurieren möchten.

   Das Kontextmenü des Controllers wird angezeigt.
4. Wählen Sie **Management Ports konfigurieren**.

   Das Dialogfeld Management-Ports konfigurieren wird geöffnet.
5. Stellen Sie sicher, dass Port 1 angezeigt wird, und klicken Sie dann auf **Weiter**.
6. Wählen Sie die Einstellungen für den Konfigurationsanschluss aus, und klicken Sie dann auf **Weiter**.

   Felddetails

Feld	Beschreibung
Geschwindigkeit und Duplexmodus	Behalten Sie die Einstellung für die automatische Aushandlung bei, wenn der System Manager die Übertragungsparameter zwischen dem Speicher-Array und dem Netzwerk bestimmen soll. Wenn Sie die Geschwindigkeit und den Modus Ihres Netzwerks kennen, wählen Sie die Parameter aus der Dropdown-Liste aus. In der Liste werden nur die gültigen Geschwindigkeits- und Duplexkombinationen angezeigt.
IPv4 aktivieren/IPv6 aktivieren	Wählen Sie eine oder beide Optionen aus, um die Unterstützung für IPv4- und IPv6-Netzwerke zu aktivieren.

   Wenn Sie **IPv4 aktivieren** wählen, wird ein Dialogfeld zur Auswahl von IPv4-Einstellungen geöffnet, nachdem Sie auf **Weiter** geklickt haben. Wenn Sie **IPv6** aktivieren auswählen, wird ein Dialogfeld zur Auswahl von IPv6-Einstellungen geöffnet, nachdem Sie auf **Weiter** geklickt haben. Wenn Sie beide Optionen auswählen, wird zuerst das Dialogfeld für IPv4-Einstellungen geöffnet, und nach dem Klicken auf **Weiter** wird das Dialogfeld für IPv6-Einstellungen geöffnet.
7. Konfigurieren Sie die IPv4- und/oder IPv6-Einstellungen automatisch oder manuell.

Felddetails

Feld	Beschreibung
Konfiguration automatisch vom DHCP-Server beziehen	Wählen Sie diese Option aus, um die Konfiguration automatisch abzurufen.
Statische Konfiguration manuell festlegen	Wählen Sie diese Option aus, und geben Sie dann die IP-Adresse des Controllers ein. (Bei Bedarf können Sie Adressen in die Felder ausschneiden und einfügen.) Geben Sie bei IPv4 die Subnetzmaske und das Gateway des Netzwerks an. Geben Sie für IPv6 die routingfähige IP-Adresse und die Router-IP-Adresse ein. Wenn Sie die Konfiguration der IP-Adresse ändern, geht der Verwaltungspfad zum Speicher-Array verloren. Wenn Sie Arrays in Ihrem Netzwerk global mit SANtricity Unified Manager verwalten, öffnen Sie die Benutzeroberfläche und gehen Sie zum Menü:Managen[Entdecken]. Wenn Sie SANtricity-Speicher-Manager verwenden, müssen Sie das Gerät aus dem Enterprise Management-Fenster (EMW) entfernen, es wieder zum EMW hinzufügen, indem Sie Menü:Bearbeiten[Speicher-Array hinzufügen] auswählen und dann die neue IP-Adresse eingeben.

8. Klicken Sie Auf **Fertig Stellen**.

Ergebnisse

Die Konfiguration des Managementport wird auf der Registerkarte Controller-Einstellungen, Management Ports, angezeigt.

Konfigurieren Sie NTP-Serveradressen

Sie können eine Verbindung zum NTP-Server (Network Time Protocol) konfigurieren, sodass der Controller regelmäßig den NTP-Server abfragen muss, um seine interne Uhrzeit zu aktualisieren.

Bevor Sie beginnen

- Ein NTP-Server muss in Ihrem Netzwerk installiert und konfiguriert sein.
- Sie müssen die Adresse des primären NTP-Servers und einen optionalen Backup-NTP-Server kennen. Dabei können es sich um vollständig qualifizierte Domain-Namen, IPv4-Adressen oder IPv6-Adressen handeln.

Wenn Sie einen oder mehrere Domänennamen für die NTP-Server eingeben, müssen Sie auch einen DNS-Server konfigurieren, um die NTP-Serveradresse aufzulösen. Sie müssen den DNS-Server nur auf den Controllern konfigurieren, auf denen Sie NTP konfiguriert und einen Domain-Namen angegeben haben.

Über diese Aufgabe

NTP ermöglicht dem Speicher-Array die automatische Synchronisierung der Uhren des Controllers mit einem externen Host mithilfe des Simple Network Time Protocol (SNTP). Der Controller fragt regelmäßig den konfigurierten NTP-Server ab und aktualisiert dann seine interne Uhrzeit mit den Ergebnissen. Wenn nur ein Controller NTP aktiviert ist, synchronisiert der alternative Controller regelmäßig seine Uhr mit dem Controller, auf dem NTP aktiviert ist. Wenn auf keinem der Controller NTP aktiviert ist, synchronisieren die Controller regelmäßig ihre Uhren miteinander.

Sie müssen nicht auf beiden Controllern NTP konfigurieren. Dadurch wird jedoch die Fähigkeit des Storage-Arrays verbessert, während der Hardware- oder Kommunikationsausfälle synchronisiert zu bleiben.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte **Controller & Komponenten**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

3. Klicken Sie auf den Controller, den Sie konfigurieren möchten.

   Das Kontextmenü des Controllers wird angezeigt.

4. Wählen Sie **NTP-Server konfigurieren**.

   Das Dialogfeld Configure Network Time Protocol (NTP) Server wird geöffnet.

5. Wählen Sie **Ich möchte NTP auf Controller** (**A** oder **B**) aktivieren.

   Im Dialogfeld werden weitere Auswahlmöglichkeiten angezeigt.

6. Wählen Sie eine der folgenden Optionen:
   - **NTP-Serveradressen werden automatisch vom DHCP-Server abgerufen** — die erkannten NTP-Serveradressen werden angezeigt.

     Wenn das Speicher-Array auf die Verwendung einer statischen NTP-Adresse eingestellt ist, werden keine NTP-Server angezeigt.

   - **NTP-Server-Adressen manuell angeben** — Geben Sie die primäre NTP-Serveradresse und eine Backup-NTP-Serveradresse ein. Der Backup-Server ist optional. (Diese Adressfelder werden angezeigt, nachdem Sie das Optionsfeld ausgewählt haben.) Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
7. **Optional:** Geben Sie Serverinformationen und Authentifizierungsdaten für einen Backup-NTP-Server ein.
8. Klicken Sie Auf **Speichern**.

Ergebnisse

Die NTP-Serverkonfiguration wird auf der Registerkarte Controllereinstellungen **DNS/NTP** angezeigt.

Konfigurieren Sie DNS-Serveradressen

Mit dem Domain Name System (DNS) werden vollständig qualifizierte Domain-Namen für die Controller und ein NTP-Server (Network Time Protocol) aufgelöst. Die Management-Ports auf dem Speicher-Array können IPv4- oder IPv6-Protokolle gleichzeitig

unterstützen.

Bevor Sie beginnen

- Ein DNS-Server muss in Ihrem Netzwerk installiert und konfiguriert sein.
- Sie kennen die Adresse des primären DNS-Servers und einen optionalen Backup-DNS-Server. Bei diesen Adressen können es sich um IPv4-Adressen oder IPv6-Adressen handeln.

Über diese Aufgabe

In diesem Verfahren wird beschrieben, wie Sie eine primäre DNS-Serveradresse und eine DNS-Backup-Adresse angeben. Der Backup-DNS-Server kann optional so konfiguriert werden, dass er verwendet wird, wenn ein primärer DNS-Server ausfällt.

> Wenn Sie bereits die Management-Ports des Storage-Arrays mit DHCP (Dynamic Host Configuration Protocol) konfiguriert haben und ein oder mehrere DNS- oder NTP-Server mit dem DHCP-Setup verbunden sind, müssen Sie DNS oder NTP nicht manuell konfigurieren. In diesem Fall sollte das Speicher-Array bereits automatisch die DNS/NTP-Serveradressen erhalten haben. Sie sollten jedoch weiterhin die folgenden Anweisungen befolgen, um das Dialogfeld zu öffnen und sicherzustellen, dass die richtigen Adressen erkannt werden.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte **Controller & Komponenten**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

3. Wählen Sie den zu konfigurierenden Controller aus.

   Das Kontextmenü des Controllers wird angezeigt.

4. Wählen Sie **DNS-Server konfigurieren**.

   Das Dialogfeld DNS-Server konfigurieren wird geöffnet.

5. Wählen Sie eine der folgenden Optionen:
   - **DNS-Serveradressen werden automatisch vom DHCP-Server abgerufen** — die erkannten DNS-Serveradressen werden angezeigt.

     > Wenn das Speicherarray auf eine statische DNS-Adresse eingestellt ist, werden keine DNS-Server angezeigt.

   - **DNS-Server-Adressen manuell angeben** — Geben Sie eine primäre DNS-Server-Adresse und eine Backup-DNS-Server-Adresse ein. Der Backup-Server ist optional. (Diese Adressfelder werden angezeigt, nachdem Sie das Optionsfeld ausgewählt haben.) Bei diesen Adressen können es sich um IPv4-Adressen oder IPv6-Adressen handeln.
6. Klicken Sie Auf **Speichern**.
7. Wiederholen Sie diese Schritte für den anderen Controller.

Ergebnisse

Die DNS-Konfiguration wird auf der Registerkarte Controllereinstellungen **DNS/NTP** angezeigt.

Zeigen Sie Controller-Einstellungen an

Sie können Informationen zu einem Controller anzeigen, z. B. den Status der Host-Schnittstellen, Laufwerksschnittstellen und Management-Ports.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte **Controller & Komponenten**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

3. Führen Sie eine der folgenden Aktionen durch, um die Controller-Einstellungen anzuzeigen:
   - Klicken Sie auf den Controller, um das Kontextmenü anzuzeigen, und wählen Sie dann **Einstellungen anzeigen**.
   - Wählen Sie das Controller-Symbol aus (neben der Dropdown-Liste **Shelf**). Wählen Sie bei Duplexkonfigurationen entweder **Controller A** oder **Controller B** aus dem Dialogfeld aus, und klicken Sie dann auf **Weiter**.

     Das Dialogfeld Controller-Einstellungen wird geöffnet.

4. Wählen Sie die Registerkarten aus, die zwischen den Eigenschaftseinstellungen verschoben werden sollen.

   Einige Registerkarten haben einen Link für **Weitere Einstellungen anzeigen** oben rechts.

Felddetails

Registerkarte	Beschreibung
Basis	Zeigt den Controller-Status, den Modellnamen, die Ersatzteilnummer des Ersatzteils, die aktuelle Firmware-Version und die Version des nichtflüchtigen statischen Random Access Memory (NVSRAM) an.
Cache	Zeigt die Cache-Einstellungen des Controllers an, zu denen der Daten-Cache, der Prozessor-Cache und das Cache-Backup-Gerät gehören. Das Cache-Backup-Gerät wird verwendet, um Daten im Cache zu sichern, wenn Sie den Controller bei einem Stromausfall verlieren. Status kann optimal, fehlgeschlagen, entfernt, Unbekannt, schreibgeschützt, Oder nicht kompatibel.
Host-Schnittstellen	Zeigt die Informationen zur Host-Schnittstelle und den Linkstatus der einzelnen Ports an. Die Host-Schnittstelle ist die Verbindung zwischen dem Controller und dem Host, z. B. Fibre Channel oder iSCSI. Der Standort der Host Interface Card (HIC) befindet sich entweder in der Baseboard oder in einem Steckplatz (Schacht). „Baseboard“ zeigt, dass die HIC-Ports in den Controller integriert sind. Die „Steckplatz“-Ports befinden sich auf der optionalen HIC.
Festplattenschnittstellen	Zeigt die Informationen zur Laufwerkschnittstelle und den Linkstatus jedes Ports an. Die Laufwerksschnittstelle ist die Verbindung zwischen dem Controller und den Laufwerken, z. B. SAS.
Management-Ports	Zeigt Details zum Management-Port an, z. B. den Host-Namen, der für den Zugriff auf den Controller verwendet wurde, und ob eine Remote-Anmeldung aktiviert wurde. Der Managementport verbindet den Controller und den Management-Client. Hier wird ein Browser zum Zugriff auf System Manager installiert.
DNS/NTP	Zeigt die Adressmethode und die IP-Adressen für den DNS-Server und den NTP-Server an, wenn diese Server in System Manager konfiguriert wurden. Domain Name System (DNS) ist ein Benennungssystem für Geräte, die mit dem Internet oder einem privaten Netzwerk verbunden sind. Der DNS-Server verwaltet ein Verzeichnis von Domain-Namen und übersetzt diese in Internet Protocol (IP)-Adressen. Network Time Protocol (NTP) ist ein Netzwerkprotokoll für die Uhrsynchronisierung zwischen Computersystemen in Datennetzwerken.

5. Klicken Sie Auf **Schließen**.

Remote-Anmeldung konfigurieren (SSH)

Durch die Aktivierung der Remote-Anmeldung können Benutzer außerhalb des lokalen Netzwerks eine SSH-Sitzung starten und auf den Controller zugreifen.

Bei SANtricity Version 11.74 und höher ist auch die Multi-Faktor-Autorisierung (MFA) möglich, indem Benutzer einen SSH-Schlüssel und/oder SSH-Passwort eingeben müssen. Bei SANtricity Version 11.73 und früher enthält diese Funktion eine Option für Multi-Faktor-Autorisierung mit SSH-Schlüsseln und -Passwörtern.

Sicherheitsrisiko — aus Sicherheitsgründen sollten nur Mitarbeiter des technischen Supports die Remote-Login-Funktion verwenden.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte **Controller & Komponenten**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

3. Klicken Sie auf den Controller, für den Sie die Remote-Anmeldung konfigurieren möchten.

   Das Kontextmenü des Controllers wird angezeigt.

4. Wählen Sie **Remote-Anmeldung konfigurieren (SSH)** aus. (Für SANtricity Version 11.73 und früher lautet dieser Menüpunkt **Remote Login ändern**.)

   Das Dialogfeld wird geöffnet, um die Remote-Anmeldung zu aktivieren.

5. Aktivieren Sie das Kontrollkästchen * Remote-Anmeldung aktivieren*.

   Diese Einstellung bietet eine Remote-Anmeldung mit drei Optionen für die Autorisierung:

   - **Nur Passwort**. Für diese Option sind Sie fertig und können auf **Speichern** klicken. Wenn Sie über ein Duplex-System verfügen, können Sie die Remote-Anmeldung auf dem zweiten Controller aktivieren, indem Sie die vorherigen Schritte durchführen.
   - * Entweder SSH-Schlüssel oder Passwort*. Für diese Option fahren Sie mit dem nächsten Schritt fort.
   - **Passwort und SSH-Schlüssel**. Aktivieren Sie für diese Option das Kontrollkästchen **autorisierter öffentlicher Schlüssel und Passwort für Remote-Anmeldung erforderlich**, und fahren Sie mit dem nächsten Schritt fort.
6. Füllen Sie das Feld * Public Key* aus. Dieses Feld enthält eine Liste autorisierter öffentlicher Schlüssel im Format der OpenSSH **Authorized_keys**-Datei.

   Beachten Sie beim Ausfüllen des Feldes **autorisierter öffentlicher Schlüssel** die folgenden Richtlinien:

   - Das Feld **autorisierter öffentlicher Schlüssel** gilt für beide Controller und muss nur auf dem ersten Controller konfiguriert werden.
   - Die Datei **Authorized_keys** darf nur einen Schlüssel pro Zeile enthalten. Zeilen, die mit # beginnen und leere Zeilen werden ignoriert. Weitere Informationen zum Dateiformat finden Sie unter "Konfigurieren von autorisierten Schlüsseln für OpenSSH".
   - Eine **authorisierte_keys**-Datei sollte ähnlich wie im folgenden Beispiel aussehen:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
j1tHymwtbdhPuipd2wIDAQAB
```

7. Wenn Sie fertig sind, klicken Sie auf **Speichern**.
8. Bei Duplex-Systemen können Sie die Remote-Anmeldung auf dem zweiten Controller aktivieren, indem Sie die oben beschriebenen Schritte ausführen. Wenn Sie die Option sowohl für ein Passwort als auch für einen SSH-Schlüssel konfigurieren, aktivieren Sie erneut das Kontrollkästchen **autorisierter öffentlicher Schlüssel und Passwort für die Remote-Anmeldung**.
9. Nachdem die Fehlerbehebung für den technischen Support abgeschlossen ist, können Sie die Remote-Anmeldung deaktivieren, indem Sie zum Dialogfeld Remote-Anmeldung konfigurieren zurückkehren und das Kontrollkästchen **Remote-Anmeldung aktivieren** deaktivieren. Wenn die Remote-Anmeldung auf einem zweiten Controller aktiviert ist, wird ein Bestätigungsdialogfeld geöffnet, in dem Sie auch die Remote-Anmeldung auf dem zweiten Controller deaktivieren können.

   Wenn Sie die Remote-Anmeldung deaktivieren, werden alle aktuellen SSH-Sitzungen beendet und neue Anmeldeanfragen werden abgelehnt.

Platzieren Sie den Controller in den Online-Modus

Wenn ein Controller sich im Offlinezustand oder im Servicemodus befindet, können Sie ihn wieder online schalten.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte **Controller & Komponenten**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

3. Klicken Sie auf einen Controller, der sich im Offline- oder Service-Modus befindet.

   Das Kontextmenü des Controllers wird angezeigt.

4. Wählen Sie * Online platzieren* aus, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

Ergebnisse

Die Erkennung eines wiederhergestellten bevorzugten Pfads durch den Multipath-Treiber kann bis zu 10 Minuten dauern.

Alle Volumes, die ursprünglich im Besitz dieses Controllers waren, werden automatisch zurück zum Controller verschoben, sobald I/O-Anfragen für jedes Volume eingegangen sind. In einigen Fällen müssen Sie die Volumes möglicherweise manuell mit dem Befehl **umverteilen Volumes** neu verteilen.

Platzieren Sie den Controller in den Offline-Modus

Wenn Sie dazu aufgefordert werden, können Sie einen Controller in den Offline-Modus versetzen.

Bevor Sie beginnen

- Ihr Storage-Array muss zwei Controller haben. Der Controller, den Sie nicht in den Offline-Modus versetzen, muss den Status „Online“ (im optimalen Status) aufweisen.
- Stellen Sie sicher, dass keine Volumes verwendet werden oder dass auf allen Hosts, die diese Volumes verwenden, ein Multipath-Treiber installiert ist.

Über diese Aufgabe

```
[CAUTION]
====
Setzen Sie einen Controller nicht offline, es sei denn, Sie werden vom
Recovery Guru oder technischen Support dazu aufgefordert.

====
.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte
*Controller & Komponenten*.
+
Die Grafik ändert sich, um die Controller anstelle der Laufwerke
anzuzeigen.

. Klicken Sie auf den Controller, den Sie in den Offline-Modus versetzen
möchten.
+
Das Kontextmenü des Controllers wird angezeigt.

. Wählen Sie *Offline platzieren* aus, und bestätigen Sie, dass Sie den
Vorgang ausführen möchten.


.Ergebnisse
Es kann einige Minuten dauern, bis System Manager den Status des
Controllers auf Offline aktualisiert. Beginnen Sie keine anderen Vorgänge,
bis der Status aktualisiert wurde.



[[IDc7bc1d41441824097caf7eed5af7fce5]]
= Platzieren Sie den Controller in den Servicemodus
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

```
Wenn Sie dazu aufgefordert werden, können Sie einen Controller in den
Servicemodus versetzen.

.Bevor Sie beginnen
* Das Speicher-Array muss zwei Controller haben. Der Controller, den Sie
nicht im Servicemodus platzieren, muss online sein (im optimalen Status).
* Stellen Sie sicher, dass keine Volumes verwendet werden oder dass auf
allen Hosts, die diese Volumes verwenden, ein Multipath-Treiber
installiert ist.


[NOTE]
====
Wenn Sie einen Controller in den Servicemodus schalten, kann dies die
Performance erheblich beeinträchtigen. Setzen Sie einen Controller nicht
in den Servicemodus ein, es sei denn, Sie werden vom technischen Support
dazu aufgefordert.

====
.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte
*Controller & Komponenten*.
+
Die Grafik ändert sich, um die Controller anstelle der Laufwerke
anzuzeigen.

. Klicken Sie auf den Controller, den Sie in den Servicemodus platzieren
möchten.
+
Das Kontextmenü des Controllers wird angezeigt.

. Wählen Sie * im Servicemodus*, und bestätigen Sie, dass Sie den Vorgang
ausführen möchten.




[[ID8445000ee982001a8a9cfad5ca8805e3]]
= Controller zurücksetzen (neu booten
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

```
Einige Probleme erfordern ein Zurücksetzen des Controllers (Neubooten).
Sie können den Controller zurücksetzen, selbst wenn Sie keinen physischen
Zugriff darauf haben.

.Bevor Sie beginnen
* Das Speicher-Array muss zwei Controller haben. Der Controller, den Sie
nicht zurücksetzen, muss online sein (im optimalen Zustand).
* Stellen Sie sicher, dass keine Volumes verwendet werden oder dass auf
allen Hosts, die diese Volumes verwenden, ein Multipath-Treiber
installiert ist.


.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte
*Controller & Komponenten*.
+
Die Grafik ändert sich, um die Controller anstelle der Laufwerke
anzuzeigen.

. Klicken Sie auf den Controller, den Sie zurücksetzen möchten.
+
Das Kontextmenü des Controllers wird angezeigt.

. Wählen Sie *Zurücksetzen*, und bestätigen Sie, dass Sie den Vorgang
ausführen möchten.




:leveloffset: -1


= Verwalten von iSCSI-Ports

:leveloffset: +1


[[IDb191e2b0541085f959f9c898a84e9482]]
= Konfigurieren Sie die iSCSI-Ports
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

Wenn Ihr Controller eine iSCSI-Hostverbindung enthält, können Sie die iSCSI-Porteinstellungen auf der Seite Hardware konfigurieren.

.Bevor Sie beginnen
* Der Controller muss iSCSI-Ports enthalten. Andernfalls sind die iSCSI-Einstellungen nicht verfügbar.
* Sie müssen die Netzwerkgeschwindigkeit (die Datenübertragungsrate zwischen den Ports und dem Host) kennen.

[NOTE]
====
Die iSCSI-Einstellungen und -Funktionen werden nur angezeigt, wenn Ihr Speicherarray iSCSI unterstützt.

====
.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte *Controller & Komponenten*.
+
Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

. Klicken Sie auf den Controller mit den iSCSI-Ports, die Sie konfigurieren möchten.
+
Das Kontextmenü des Controllers wird angezeigt.

. Wählen Sie *iSCSI-Ports konfigurieren*.
+
[NOTE]
====
Die Option *iSCSI-Ports konfigurieren* wird nur angezeigt, wenn System Manager iSCSI-Ports am Controller erkennt.

====
+
Das Dialogfeld iSCSI-Ports konfigurieren wird geöffnet.

. Wählen Sie in der Dropdown-Liste den Port aus, den Sie konfigurieren möchten, und klicken Sie dann auf *Weiter*.
. Wählen Sie die Einstellungen für den Konfigurationsanschluss aus, und klicken Sie dann auf *Weiter*.
+
Um alle Porteinstellungen anzuzeigen, klicken Sie rechts im Dialogfeld auf

```
den Link *Weitere Porteinstellungen anzeigen*.

+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Port-Einstellung | Beschreibung


 a|
Konfigurierte ethernet-Port-Geschwindigkeit (erscheint nur für bestimmte
Arten von Host-Schnittstellenkarten)
 a|
Wählen Sie die Geschwindigkeit aus, die der Geschwindigkeitsfähigkeit des
SFP am Port entspricht.



 a|
FEC-Modus (Forward Error Correction) (wird nur für bestimmte Arten von
Host Interface Cards angezeigt)
 a|
Wählen Sie bei Bedarf einen der FEC-Modi für den angegebenen Host-Port
aus.


NOTE: Der Reed Solomon-Modus unterstützt die 25-Gbit/s-Port-
Geschwindigkeit nicht.



 a|
IPv4 aktivieren/IPv6 aktivieren
 a|
Wählen Sie eine oder beide Optionen aus, um die Unterstützung für IPv4-
und IPv6-Netzwerke zu aktivieren.


NOTE: Wenn Sie den Portzugriff deaktivieren möchten, deaktivieren Sie
beide Kontrollkästchen.



 a|
TCP-Listening-Port (verfügbar durch Klicken auf *Weitere Port-
```

```
Einstellungen anzeigen*.)
 a|
Geben Sie bei Bedarf eine neue Portnummer ein.

Der Listening-Port ist die TCP-Port-Nummer, die der Controller zum Abhören
von iSCSI-Anmeldungen von Host-iSCSI-Initiatoren verwendet. Der
standardmäßige Listenanschluss ist 3260. Sie müssen 3260 oder einen Wert
zwischen 49152 und 65535 eingeben.



 a|
MTU-Größe (verfügbar durch Klicken auf *Weitere Porteinstellungen
anzeigen*.)
 a|
Geben Sie bei Bedarf eine neue Größe in Byte für die maximale
Übertragungseinheit (MTU) ein.

Die Standardgröße für maximale Übertragungseinheit (Maximum Transmission
Unit, MTU) beträgt 1500 Byte pro Frame. Sie müssen einen Wert zwischen
1500 und 9000 eingeben.



 a|
ICMP PING-Antworten aktivieren
 a|
Wählen Sie diese Option aus, um das ICMP (Internet Control Message
Protocol) zu aktivieren. Die Betriebssysteme von vernetzten Computern
verwenden dieses Protokoll zum Senden von Meldungen. Diese ICMP-Meldungen
bestimmen, ob ein Host erreichbar ist und wie lange es dauert, bis Pakete
von und zu diesem Host gelangen.

|===
====
+
Wenn Sie *IPv4 aktivieren* ausgewählt haben, wird ein Dialogfeld zur
Auswahl von IPv4-Einstellungen geöffnet, nachdem Sie auf *Weiter* geklickt
haben. Wenn Sie *IPv6* aktivieren ausgewählt haben, wird ein Dialogfeld
zur Auswahl von IPv6-Einstellungen geöffnet, nachdem Sie auf *Weiter*
geklickt haben. Wenn Sie beide Optionen ausgewählt haben, wird zuerst das
Dialogfeld für IPv4-Einstellungen geöffnet, und nach dem Klicken auf
*Weiter* wird das Dialogfeld für IPv6-Einstellungen geöffnet.

. Konfigurieren Sie die IPv4- und/oder IPv6-Einstellungen automatisch oder
manuell. Um alle Porteinstellungen anzuzeigen, klicken Sie rechts im
Dialogfeld auf den Link *Weitere Einstellungen anzeigen*.
```

```
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Port-Einstellung | Beschreibung


 a|
Automatische Ermittlung der Konfiguration
 a|
Wählen Sie diese Option aus, um die Konfiguration automatisch abzurufen.



 a|
Statische Konfiguration manuell festlegen
 a|
Wählen Sie diese Option aus, und geben Sie dann eine statische Adresse in die Felder ein. (Bei Bedarf können Sie Adressen in die Felder ausschneiden und einfügen.) Geben Sie bei IPv4 die Subnetzmaske und das Gateway des Netzwerks an. Geben Sie für IPv6 die routingfähige IP-Adresse und die Router-IP-Adresse ein.



 a|
Aktivieren Sie die VLAN-Unterstützung (verfügbar durch Klicken auf *Weitere Einstellungen anzeigen*.)
 a|
Wählen Sie diese Option aus, um ein VLAN zu aktivieren und seine ID einzugeben. Ein VLAN ist ein logisches Netzwerk, das sich verhält, als sei es physisch von anderen physischen und virtuellen lokalen Netzwerken (LANs) getrennt, die von denselben Switches, denselben Routern oder beiden unterstützt werden.



 a|
ethernet-Priorität aktivieren (verfügbar durch Klicken auf *Weitere Einstellungen anzeigen*.)
 a|
Wählen Sie diese Option aus, um den Parameter zu aktivieren, der die Priorität des Zugriffs auf das Netzwerk bestimmt. Verwenden Sie den Schieberegler, um eine Priorität zwischen 1 (niedrigste) und 7 (höchste) auszuwählen.
```

In einer gemeinsamen LAN-Umgebung (Local Area Network) wie Ethernet könnten viele Stationen den Zugang zum Netzwerk zu schaffen haben. Der Zugriff erfolgt in der Reihenfolge der eingehenden Reservierungen. Zwei Stationen versuchen möglicherweise gleichzeitig, auf das Netzwerk zuzugreifen, was dazu führt, dass beide Stationen wieder aus- und abschalten und warten, bevor sie es erneut versuchen. Dieser Vorgang wird bei geswitchten Ethernet minimiert, bei dem nur eine Station mit einem Switch-Port verbunden ist.

|===
====
. Klicken Sie Auf *Fertig Stellen*.

[[ID1f703dcfd90ae924c13812c24966d428]]
= Konfigurieren Sie die iSCSI-Authentifizierung
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Für zusätzliche Sicherheit in einem iSCSI-Netzwerk können Sie die Authentifizierung zwischen Controllern (Zielen) und Hosts (Initiatoren) festlegen.

System Manager 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 namens _CHAP Secret_.

.Bevor Sie beginnen
Sie können den CHAP-Schlüssel für die Initiatoren (iSCSI-Hosts) entweder vor oder nach dem Festlegen des CHAP-Geheimschlüssels für die Ziele (Controller) festlegen. Bevor Sie die Anweisungen in dieser Aufgabe befolgen, sollten Sie warten, bis die Hosts zuerst eine iSCSI-Verbindung hergestellt haben, und dann den CHAP-Schlüssel auf den einzelnen Hosts festlegen. Nachdem die Verbindungen hergestellt wurden, werden die IQN-Namen der Hosts und ihre CHAP-Schlüssel im Dialogfeld für die iSCSI-Authentifizierung (siehe in dieser Aufgabe) aufgelistet, und Sie müssen sie nicht manuell eingeben.

.Über diese Aufgabe
Sie können eine der folgenden Authentifizierungsmethoden auswählen:

* *Einweg-Authentifizierung* - Verwenden Sie diese Einstellung, um dem Controller die Identität der iSCSI-Hosts zu authentifizieren (unidirektionale Authentifizierung).
* *Zwei-Wege-Authentifizierung* - Verwenden Sie diese Einstellung, um sowohl dem Controller als auch den iSCSI-Hosts die Authentifizierung (bidirektionale Authentifizierung) zu ermöglichen. Diese Einstellung bietet eine zweite Sicherheitsstufe, indem der Controller die Identität der iSCSI-Hosts authentifizieren kann. Und wiederum können die iSCSI-Hosts die Identität des Controllers authentifizieren.

[NOTE]
====
Die iSCSI-Einstellungen und -Funktionen werden nur auf der Seite Einstellungen angezeigt, wenn Ihr Speicher-Array iSCSI unterstützt.

====
.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Klicken Sie unter iSCSI-Einstellungen auf *Authentifizierung konfigurieren*.
+
Das Dialogfeld Authentifizierung konfigurieren wird angezeigt, in dem die derzeit festgelegte Methode angezeigt wird. Außerdem wird angezeigt, ob auf Hosts CHAP-Schlüssel konfiguriert sind.

. Wählen Sie eine der folgenden Optionen:
+
** *Keine Authentifizierung* -- Wenn der Controller die Identität von iSCSI-Hosts nicht authentifizieren soll, wählen Sie diese Option aus und klicken Sie auf *Fertig stellen*. Das Dialogfeld wird geschlossen, und die Konfiguration ist abgeschlossen.
** *Einweg-Authentifizierung* -- damit der Controller die Identität der iSCSI-Hosts authentifizieren kann, wählen Sie diese Option aus und klicken Sie auf *Weiter*, um das Dialogfeld Ziel-CHAP konfigurieren anzuzeigen.
** *Zwei-Wege-Authentifizierung* -- damit sowohl der Controller als auch die iSCSI-Hosts die Authentifizierung durchführen können, wählen Sie diese Option aus und klicken Sie auf *Weiter*, um das Dialogfeld Target CHAP konfigurieren anzuzeigen.

. Geben Sie für eine ein- oder zweiseitige Authentifizierung den CHAP-Schlüssel für den Controller (das Ziel) ein oder bestätigen Sie ihn. Der

```
CHAP-Schlüssel muss zwischen 12 und 57 druckbaren ASCII-Zeichen liegen.
+
[NOTE]
====
Wenn der CHAP-Schlüssel für den Controller zuvor konfiguriert wurde,
werden die Zeichen im Feld maskiert. Falls erforderlich, können Sie die
vorhandenen Zeichen ersetzen (neue Zeichen werden nicht maskiert).

====
. Führen Sie einen der folgenden Schritte aus:
+
** Wenn Sie die Authentifizierung _One-Way_ konfigurieren, klicken Sie auf
*Finish*. Das Dialogfeld wird geschlossen, und die Konfiguration ist
abgeschlossen.
** Wenn Sie die Authentifizierung _zwei-Wege_ konfigurieren, klicken Sie
auf *Weiter*, um das Dialogfeld Initiator-CHAP konfigurieren anzuzeigen.


. Geben Sie für die Zweiwege-Authentifizierung einen CHAP-Schlüssel für
einen der iSCSI-Hosts (die Initiatoren) ein, der zwischen 12 und 57
druckbaren ASCII-Zeichen liegen kann. Wenn Sie die zwei-Wege-
Authentifizierung für einen bestimmten Host nicht konfigurieren möchten,
lassen Sie das Feld Initiator CHAP Secret leer.
+
[NOTE]
====
Wenn der CHAP-Schlüssel für einen Host zuvor konfiguriert wurde, werden
die Zeichen im Feld maskiert. Falls erforderlich, können Sie die
vorhandenen Zeichen ersetzen (neue Zeichen werden nicht maskiert).

====
. Klicken Sie Auf *Fertig Stellen*.


.Ergebnisse
Die Authentifizierung erfolgt während der iSCSI-Anmeldesequenz zwischen
den Controllern und iSCSI-Hosts, es sei denn, Sie haben keine
Authentifizierung angegeben.



[[IDdf81ddcde74049425b661b15856afb22]]
= Aktivieren Sie die iSCSI-Erkennungseinstellungen
:allow-uri-read:
:experimental:
:icons: font
```

```
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können Einstellungen für die Ermittlung von Speichergeräten in einem
iSCSI-Netzwerk aktivieren.

Mit den Einstellungen für die Zielerkennung können Sie die iSCSI-
Informationen des Speicherarrays über das iSNS-Protokoll (Internet Storage
Name Service) registrieren und bestimmen, ob nicht benannte
Ermittlungssitzungen zugelassen werden sollen.

.Bevor Sie beginnen
Wenn der iSNS-Server eine statische IP-Adresse verwendet, muss diese
Adresse für die iSNS-Registrierung verfügbar sein. IPv4 und IPv6 werden
unterstützt.

.Über diese Aufgabe
Sie können die folgenden Einstellungen für die iSCSI-Ermittlung
aktivieren:

* *ISNS-Server aktivieren, um ein Ziel zu registrieren* -- Wenn es
aktiviert ist, registriert das Speicherarray seinen iSCSI-qualifizierten
Namen (IQN) und Port-Informationen vom iSNS-Server. Diese Einstellung
ermöglicht die iSNS-Erkennung, sodass ein Initiator die IQN- und
Portinformationen vom iSNS-Server abrufen kann.
* *Nicht benannte Ermittlungssitzungen aktivieren* -- Wenn nicht benannte
Ermittlungssitzungen aktiviert sind, muss der Initiator (iSCSI-Host)
während der Anmeldesequenz keine IQN des Ziels (Controller) für eine
Ermittlungsverbindung bereitstellen. Wenn diese Option deaktiviert ist,
müssen die Hosts den IQN zur Einrichtung einer Erkennungssitzung für den
Controller bereitstellen. Die Ziel-IQN ist jedoch immer für eine normale
(E/A-Lagersitzung) erforderlich. Wenn Sie diese Einstellung deaktivieren,
kann dies verhindern, dass nicht autorisierte iSCSI-Hosts nur über ihre
IP-Adresse eine Verbindung zum Controller herstellen.


[NOTE]
====
Die iSCSI-Einstellungen und -Funktionen werden nur auf der Seite
Einstellungen angezeigt, wenn Ihr Speicher-Array iSCSI unterstützt.

====
.Schritte
. Wählen Sie Menü:Einstellungen[System].
```

. Klicken Sie unter *iSCSI-Einstellungen* auf *Zielermittlungs-Einstellungen anzeigen/bearbeiten*.
+
Das Dialogfeld Einstellungen für die Zielerkennung wird angezeigt. Unter dem Feld *iSNS-Server aktivieren*... wird im Dialogfeld angezeigt, ob der Controller bereits registriert ist.

. Um den Controller zu registrieren, wählen Sie *iSNS-Server aktivieren, um mein Ziel zu registrieren*, und wählen Sie dann eine der folgenden Optionen aus:
+
** *Konfiguration automatisch vom DHCP-Server beziehen* -- Wählen Sie diese Option, wenn Sie den iSNS-Server mit einem DHCP-Server (Dynamic Host Configuration Protocol) konfigurieren möchten. Wenn Sie diese Option verwenden, müssen alle iSCSI-Ports des Controllers auch für die Verwendung von DHCP konfiguriert sein. Aktualisieren Sie gegebenenfalls die iSCSI-Port-Einstellungen des Controllers, um diese Option zu aktivieren.
+
[NOTE]
====
Damit der DHCP-Server die iSNS-Serveradresse bereitstellen kann, müssen Sie den DHCP-Server so konfigurieren, dass Option 43 -- „`anbieterspezifische Informationen`“ verwendet wird. Diese Option muss die IPv4-Adresse des iSNS-Servers in Datenbytes 0xA-0xd (10-13) enthalten.

====
** *Statische Konfiguration festlegen* -- Wählen Sie diese Option aus, wenn Sie eine statische IP-Adresse für den iSNS-Server eingeben möchten. (Bei Bedarf können Sie Adressen in die Felder ausschneiden und einfügen.) Geben Sie im Feld eine IPv4-Adresse oder eine IPv6-Adresse ein. Wenn Sie beide konfiguriert haben, ist IPv4 die Standardeinstellung. Geben Sie auch einen TCP-Listening-Port ein (verwenden Sie die Standardeinstellung 3205 oder geben Sie einen Wert zwischen 49152 und 65535 ein).

. Um die Teilnahme des Speicher-Arrays an nicht benannten Ermittlungssitzungen zu ermöglichen, wählen Sie *nicht benannte Ermittlungssitzungen aktivieren* aus.
+
** Wenn diese Option aktiviert ist, müssen iSCSI-Initiatoren nicht den Ziel-IQN angeben, um die Controller-Informationen abzurufen.
** Wenn diese Option deaktiviert ist, werden Ermittlungssitzungen verhindert, es sei denn, der Initiator stellt die Ziel-IQN bereit. Durch das Deaktivieren von nicht benannten Ermittlungssitzungen wird zusätzliche Sicherheit gewährleistet.

. Klicken Sie Auf *Speichern*.

.Ergebnisse
Es wird eine Statusleiste angezeigt, da der System Manager versucht, den Controller beim iSNS-Server zu registrieren. Dieser Vorgang kann bis zu fünf Minuten dauern.

[[ID2e31c9cfef7b0c630eb2e71b85b90d78]]
= Anzeigen von iSCSI-Statistikpaketen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können Daten über die iSCSI-Verbindungen zu Ihrem Speicher-Array anzeigen.

.Über diese Aufgabe
System Manager zeigt diese Typen von iSCSI-Statistiken. Alle Statistiken sind schreibgeschützt und können nicht festgelegt werden.

NOTE: Die in System Manager angezeigten Statistiktypen basieren auf den für Ihr Speicher-Array verfügbaren Statistiken.

* *Ethernet MAC Statistics* -- stellt Statistiken für die Media Access Control (MAC) bereit. MAC bietet auch einen Adressierungsmechanismus, der als physische Adresse oder MAC-Adresse bezeichnet wird. Die MAC-Adresse ist eine eindeutige Adresse, die jedem Netzwerkadapter zugewiesen wird. Die MAC-Adresse unterstützt die Übertragung von Datenpaketen an ein Ziel innerhalb des Subnetzwerks.
* *Ethernet TCP/IP-Statistiken* -- liefert Statistiken für das TCP/IP, welches das Transmission Control Protocol (TCP) und das Internet Protocol (IP) für das iSCSI-Gerät ist. Mit TCP können Anwendungen auf vernetzten Hosts Verbindungen miteinander herstellen, über die sie Daten in Paketen austauschen können. Die IP ist ein datenorientiertes Protokoll, das Daten über ein paketgeschaltetes Inter-Netzwerk kommuniziert. Die IPv4-Statistiken und die IPv6-Statistiken werden separat angezeigt.
* *Ethernet Kernel Statistik* -- liefert Statistiken für die Plattform Kernel Treiber des iSCSI Gerätes. In der Kernelstatistik werden ähnliche Netzwerkdaten wie die TCP/IP-Statistikoption angezeigt. Die

Kernelstatistikdaten werden jedoch nicht direkt von der iSCSI-Hardware, sondern von den Plattformkerneltreibern erfasst.
* *Local Target/Initiator (Protocol) Statistics* -- zeigt Statistiken für das iSCSI-Ziel an, die Zugriff auf seine Speichermedien auf Blockebene ermöglichen, und zeigt die iSCSI-Statistiken für das Speicher-Array an, wenn es als Initiator bei asynchronen Spiegelungsvorgängen verwendet wird.
* *DCBX Betriebszustände* -- zeigt die Betriebszustände der verschiedenen Funktionen von Data Center Bridging Exchange (DCBX) an.
* *LLDP-TLV-Statistiken* -- zeigt die Statistiken zum Typ Length Value (TLV) des Link Layer Discovery Protocol (LLDP) an.
* *DCBX TLV Statistics* -- zeigt die Informationen an, die die Speicher-Array-Host-Ports in einer Data Center Bridging (DCB)-Umgebung identifizieren. Diese Informationen werden zu Identifikations- und Funktionszwecken an Kollegen des Netzwerks weitergegeben.

Sie können jede dieser Statistiken als RAW-Statistiken oder als Baseline-Statistiken anzeigen. RAW-Statistiken sind alle Statistiken, die seit dem Start der Controller gesammelt wurden. Baseline-Statistiken sind zeitpunktgenaue Statistiken, die seit dem Festlegen der Baseline-Zeit erfasst wurden.

.Schritte
. Wählen Sie MENU:Support[Support Center > Diagnose].
. Wählen Sie *Anzeigen von iSCSI-Statistikpaketen* aus.
. Klicken Sie auf eine Registerkarte, um die verschiedenen Statistikgruppen anzuzeigen.
. Klicken Sie zum Festlegen des Basisplans auf *Neue Baseline festlegen*.
+
Durch das Festlegen der Baseline wird ein neuer Ausgangspunkt für die Erfassung der Statistiken festgelegt. Dieselbe Baseline wird für alle iSCSI-Statistiken verwendet.

[[ID50d09c58bb7292a3c11e8d1fe900982f]]
= Anzeigen von iSCSI-Sitzungen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

```
Sie können detaillierte Informationen über die iSCSI-Verbindungen zu Ihrem
Speicher-Array anzeigen. ISCSI-Sitzungen können bei Hosts oder Remote-
Storage-Arrays in einer asynchronen Spiegelbeziehung durchgeführt werden.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie *Anzeigen/Beenden von iSCSI-Sitzungen*.
+
Eine Liste der aktuellen iSCSI-Sitzungen wird angezeigt.

. *Optional:* um zusätzliche Informationen zu einer bestimmten iSCSI-
Sitzung anzuzeigen, wählen Sie eine Sitzung aus, und klicken Sie dann auf
*Details anzeigen*.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Element | Beschreibung


 a|
Session Identifier (SSID)
 a|
Eine hexadezimale Zeichenfolge, die eine Sitzung zwischen einem iSCSI-
Initiator und einem iSCSI-Ziel identifiziert. Die SSID besteht aus ISID
und TPGT.



 a|
Initiator-Sitzungs-ID (ISID)
 a|
Der Initiator-Teil der Session-ID. Der Initiator gibt während der
Anmeldung die ISID an.



 a|
Zielportalgruppe
 a|
Das iSCSI-Ziel.



 a|
```

```
Ziel-Portal-Gruppen-Tag (TPGT)
 a|
Der Zielteil der Sitzungs-ID. Eine 16-Bit numerische Kennung für eine
iSCSI-Zielportalgruppe.



 a|
ISCSI-Name des Initiators
 a|
Der eindeutige weltweite Name des Initiators.



 a|
ISCSI-Etikett des Initiators
 a|
Die in System Manager festgelegte Benutzerbezeichnung.



 a|
ISCSI-Alias des Initiators
 a|
Ein Name, der auch einem iSCSI-Knoten zugeordnet werden kann. Mit dem
Alias kann eine Organisation eine benutzerfreundliche Zeichenfolge mit dem
iSCSI-Namen verknüpfen. Der Alias ist jedoch kein Ersatz für den iSCSI-
Namen. Der iSCSI-Alias des Initiators kann nur auf dem Host festgelegt
werden, nicht im System Manager



 a|
Host
 a|
Ein Server, der ein- und Ausgang an das Speicherarray sendet.



 a|
Verbindungs-ID (CID)
 a|
Ein eindeutiger Name für eine Verbindung innerhalb der Sitzung zwischen
dem Initiator und dem Ziel. Der Initiator generiert diese ID und stellt
sie während der Login-Anforderungen dem Ziel bereit. Die Verbindungs-ID
wird auch während der Abmeldung angezeigt, die Verbindungen schließen.
```

```
 a|
Port-ID
 a|
Der der Verbindung zugeordnete Controller-Port.


 a|
Initiator-IP-Adresse
 a|
Die IP-Adresse des Initiators.


 a|
Ausgehandelte Anmeldeparameter
 a|
Die Parameter, die während der Anmeldung der iSCSI-Sitzung bearbeitet
werden.


 a|
Authentifizierungsmethode
 a|
Die Technik, um Benutzer zu authentifizieren, die Zugriff auf das iSCSI-
Netzwerk wollen. Gültige Werte sind *CHAP* und *Keine*.


 a|
Header-Digest-Methode
 a|
Die Technik, um mögliche Kopfzeilenwerte für die iSCSI-Sitzung anzuzeigen.
HeaderDigest und DataDigest können entweder *Keine* oder *CRC32C* sein.
Der Standardwert für beide ist *Keine*.


 a|
Data Digest-Methode
 a|
Die Technik, um mögliche Datenwerte für die iSCSI-Sitzung anzuzeigen.
HeaderDigest und DataDigest können entweder *Keine* oder *CRC32C* sein.
Der Standardwert für beide ist *Keine*.
```

```
 a|
Maximale Anzahl der Verbindungen
 a|
Die größte Anzahl von Verbindungen, die für die iSCSI-Sitzung zulässig
sind. Die maximale Anzahl der Verbindungen kann 1 bis 4 sein. Der
Standardwert ist *1*.



 a|
Ziel-Alias
 a|
Die dem Ziel zugeordnete Bezeichnung.



 a|
Alias des Initiators
 a|
Die dem Initiator zugeordnete Bezeichnung.



 a|
Ziel-IP-Adresse
 a|
Die IP-Adresse des Ziels für die iSCSI-Sitzung. DNS-Namen werden nicht
unterstützt.



 a|
Anfängliche R2T
 a|
Der anfängliche Status für die Übertragung bereit. Der Status kann
entweder *Ja* oder *Nein* sein.



 a|
Maximale Burst-Länge
 a|
Die maximale SCSI-Nutzlast in Byte für diese iSCSI-Sitzung. Die maximale
Burst-Länge kann zwischen 512 und 262,144 (256 KB) liegen. Der
```

Standardwert ist *262,144 (256 KB)*.

a|
Erste Burst-Länge
a|
Die SCSI-Nutzlast in Byte für unaufgeforderte Daten für diese iSCSI-Sitzung. Die erste Burst-Länge kann von 512 bis 131,072 (128 KB) liegen. Der Standardwert ist *65,536 (64 KB)*.

a|
Standardzeit zu warten
a|
Die minimale Anzahl von Sekunden, die gewartet werden müssen, bevor Sie nach einer Verbindungsabbruch oder einem Zurücksetzen der Verbindung eine Verbindung herstellen. Der Standardwert für die Wartezeit kann zwischen 0 und 3600 liegen. Der Standardwert ist *2*.

a|
Standardzeit für die Aufbewahrung
a|
Die maximale Anzahl von Sekunden, die nach Beendigung einer Verbindung oder Zurücksetzen der Verbindung noch möglich ist. Die Standardzeit für die Aufbewahrung kann von 0 bis 3600 liegen. Der Standardwert ist *20*.

a|
Max. Ausstehender R2T
a|
Die maximale Anzahl der ausstehenden „Ready to Transfers“ für diese iSCSI-Sitzung. Der maximale Wert für den Wert für den Wert für den ausstehenden Transfer kann zwischen 1 und 16 liegen. Der Standardwert ist *1*.

a|
Fehler bei Recovery-Stufe
a|
Die Ebene der Fehlerwiederherstellung für diese iSCSI-Sitzung. Der Wert für die Fehlerwiederherstellung ist immer auf *0* gesetzt.

```
 a|
Maximale Länge des Segments für Empfangsdaten
 a|
Die maximale Datenmenge, die entweder der Initiator oder das Ziel in einer
beliebigen iSCSI-Nutzlastdateneinheit (PDU) empfangen kann.



 a|
Zielname
 a|
Der offizielle Name des Ziels (nicht der Alias). Der Zielname mit dem
Format _iqn_.



 a|
Name des Initiators
 a|
Der offizielle Name des Initiators (nicht der Alias). Der Initiatorname,
der entweder das Format _iqn_ oder _eui_ verwendet.

|===
====
. *Optional:* um den Bericht in einer Datei zu speichern, klicken Sie auf
*Speichern*.
+
Die Datei wird im Ordner Downloads für Ihren Browser mit dem Dateinamen
gespeichert `iscsi-session-connections.txt`.




[[ID426c5802e999f76f50e7b47d10032161]]
= ISCSI-Sitzung beenden
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können eine nicht mehr benötigte iSCSI-Sitzung beenden. ISCSI-
```

Sitzungen können bei Hosts oder Remote-Storage-Arrays in einer asynchronen Spiegelbeziehung durchgeführt werden.

.Über diese Aufgabe
Aus folgenden Gründen können Sie eine iSCSI-Sitzung beenden:

* *Nicht autorisierter Zugriff* -- Wenn ein iSCSI-Initiator angemeldet ist und keinen Zugriff haben sollte, können Sie die iSCSI-Sitzung beenden, um den iSCSI-Initiator vom Speicher-Array zu erzwingen. Der iSCSI-Initiator konnte angemeldet sein, da die Authentifizierungsmethode „Keine“ verfügbar war.
* *System Downtime* -- Wenn Sie ein Speicher-Array herunternehmen müssen und sehen, dass iSCSI-Initiatoren noch angemeldet sind, können Sie die iSCSI-Sitzungen beenden, um die iSCSI-Initiatoren vom Speicher-Array zu erhalten.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie *Anzeigen/Beenden von iSCSI-Sitzungen*.
+
Eine Liste der aktuellen iSCSI-Sitzungen wird angezeigt.

. Wählen Sie die Sitzung aus, die Sie beenden möchten
. Klicken Sie auf *Sitzung beenden*, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

[[ID1f5c81fd5bea64bd9eaedcf1cc5caf8c]]
= Konfigurieren Sie iSER-over-InfiniBand-Ports
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Wenn der Controller einen iSER-over-InfiniBand-Port enthält, können Sie die Netzwerkverbindung zu dem Host konfigurieren.

.Bevor Sie beginnen
* Der Controller muss einen iSER-over-InfiniBand-Port umfassen, andernfalls sind die iSER-over-InfiniBand-Einstellungen in System Manager nicht verfügbar.
* Sie müssen die IP-Adresse der Hostverbindung kennen.

```
.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte
*Controller & Komponenten*.
+
Die Grafik ändert sich, um die Controller anstelle der Laufwerke
anzuzeigen.

. Klicken Sie auf den Controller mit dem iSER-over-InfiniBand-Port, den
Sie konfigurieren möchten.
+
Das Kontextmenü des Controllers wird angezeigt.

. Wählen Sie *iSER-over-InfiniBand-Ports konfigurieren*.
+
Das Dialogfeld iSER-over-InfiniBand-Ports konfigurieren wird geöffnet.

. Wählen Sie in der Dropdown-Liste den HIC-Port aus, den Sie konfigurieren
möchten, und geben Sie dann die IP-Adresse des Hosts ein.
. Klicken Sie Auf *Konfigurieren*.
. Vervollständigen Sie die Konfiguration, und setzen Sie dann den iSER-
over-InfiniBand-Port zurück, indem Sie auf *Ja* klicken.




[[IDd4af5a2eb0014c7d9b172821df95d491]]
= Zeigen Sie iSER-over-InfiniBand-Statistiken an
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn der Controller Ihres Storage-Arrays einen iSER-over-InfiniBand-Port
umfasst, können Sie Daten zu den Host-Verbindungen anzeigen.

.Über diese Aufgabe
System Manager zeigt die folgenden Arten von iSER-over-InfiniBand-
Statistiken an. Alle Statistiken sind schreibgeschützt und können nicht
festgelegt werden.

* *Statistiken zu lokalen Zielen (Protokoll)* -- stellt Statistiken für
```

```
das iSER-over-InfiniBand-Ziel bereit, das den Zugriff auf die
Speichermedien auf Blockebene anzeigt.
* *ISER-over-InfiniBand-Interface-Statistik* -- stellt Statistiken für
alle iSER-Ports der InfiniBand-Schnittstelle bereit, die Performance-
Statistiken und Link-Fehlerinformationen zu jedem Switch-Port enthalten.


Sie können jede dieser Statistiken als RAW-Statistiken oder als Baseline-
Statistiken anzeigen. RAW-Statistiken sind alle Statistiken, die seit dem
Start der Controller gesammelt wurden. Baseline-Statistiken sind
zeitpunktgenaue Statistiken, die seit dem Festlegen der Baseline-Zeit
erfasst wurden.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie *Anzeigen iSER über InfiniBand Statistik*.
. Klicken Sie auf eine Registerkarte, um die verschiedenen
Statistikgruppen anzuzeigen.
. *Optional:* um den Basisplan festzulegen, klicken Sie auf *Neue
Basislinie festlegen*.
+
Durch das Festlegen der Baseline wird ein neuer Ausgangspunkt für die
Erfassung der Statistiken festgelegt. Dieselbe Baseline wird für sämtliche
iSER-over-InfiniBand-Statistiken verwendet.




:leveloffset: -1


= Managen Sie NVMe-Ports

:leveloffset: +1


[[IDaadf54bd3305db97f5c886acebf44a42]]
= NVMe Übersicht
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Einige Controller enthalten einen Port für die Implementierung von NVMe
```

(Non-Volatile Memory Express) über Fabrics. NVMe ermöglicht eine High-Performance-Kommunikation zwischen Hosts und dem Storage-Array.

== Was ist NVMe?

NVM steht für „nichtflüchtiger Speicher“ und ist persistenter Speicher, der in vielen Arten von Speichergeräten verwendet wird. _NVMe_ (NVM Express) ist eine standardisierte Schnittstelle oder ein standardisiertes Protokoll, das speziell für eine hochperformante Multi-Queue-Kommunikation mit NVM-Geräten entwickelt wurde.

== Was ist NVMe over Fabrics?

NVMe over Fabrics (NVMe-of) ist eine Technologiespezifikation, die den Datentransfer zwischen einem Host-Computer und Storage über ein Netzwerk zwischen messenbasierten NVMe-Befehlen und -Daten ermöglicht. Auf ein NVMe-Storage-Array (sog. _Subsystem_) kann ein Host über eine Fabric zugreifen. NVMe Befehle sind sowohl auf der Host- als auch auf der Subsystemseite in transportabstrahierten Schichten aktiviert und eingekapselt. Damit erweitert sich die End-to-End-NVMe-High-Performance-Schnittstelle vom Host bis zum Storage und standardisiert und vereinfacht die Befehlszeilen.

NVMe-of-Storage wird einem Host als lokales Block-Storage-Gerät präsentiert. Das Volume (auch „_Namespace_“ genannt) kann wie jedes andere Block-Storage-Gerät in ein Dateisystem eingebunden werden. Mit DER REST-API, dem SMcli oder SANtricity System Manager wird der Storage nach Bedarf bereitgestellt.

== Was ist ein qualifizierter NVMe-Name (NVMe Qualified Name, NQN)?

Der NVMe Qualified Name (NQN) wird zur Identifizierung des Remote-Storage-Ziels verwendet. Der für das Storage-Array qualifizierte NVMe-Name wird immer vom Subsystem zugewiesen und darf nicht geändert werden. Es gibt nur einen für NVMe qualifizierten Namen für das gesamte Array. Der qualifizierte NVMe-Name ist auf 223 Zeichen begrenzt. Sie können ihn mit einem qualifizierten iSCSI-Namen vergleichen.

== Was ist ein Namespace und eine Namespace-ID?

```
Ein Namespace entspricht einer logischen Einheit in SCSI, die ein Volume
im Array betrifft. Die Namespace-ID (NSID) entspricht einer Logical Unit
Number (LUN) in SCSI. Sie erstellen die NSID zum Erstellungszeitpunkt des
Namespace und können sie auf einen Wert zwischen 1 und 255 setzen.



== Was ist ein NVMe Controller?

Ähnlich wie bei einem SCSI I_T nexus, der den Pfad vom Host-Initiator zum
Ziel des Storage-Systems darstellt, stellt ein während des Host-
Verbindungsvorgangs erstellter NVMe-Controller einen Zugriffspfad zwischen
einem Host und den Namespaces im Storage-Array bereit. Ein NQN für den
Host und eine Host-Port-Kennung identifizieren einen NVMe-Controller
eindeutig. Ein NVMe-Controller kann zwar nur einem einzelnen Host
zugewiesen werden, kann aber auf diverse Namespaces zugreifen.

Sie konfigurieren, welche Hosts auf welche Namespaces zugreifen können und
legen die Namespace-ID für den Host mit dem SANtricity System Manager
fest. Anschließend wird bei der Erstellung des NVMe Controllers die Liste
der Namespace-IDs, auf die der NVMe Controller zugreifen kann, erstellt
und zum Konfigurieren der zulässigen Verbindungen verwendet.



[[IDa98169d81570521ce9cd892b61651e86]]
= Konfigurieren Sie NVMe-over-InfiniBand-Ports
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Ihr Controller eine NVMe-over-InfiniBand-Verbindung enthält, können
Sie die NVMe-Port-Einstellungen auf der Seite Hardware konfigurieren.

.Bevor Sie beginnen
* Der Controller muss einen NVMe-over-InfiniBand-Host-Port enthalten.
Andernfalls stehen die NVMe-over-InfiniBand-Einstellungen in System
Manager nicht zur Verfügung.
* Sie müssen die IP-Adresse der Hostverbindung kennen.


[NOTE]
====
```

Die NVMe-over-InfiniBand-Einstellungen und -Funktionen werden nur angezeigt, wenn der Controller des Storage-Arrays einen NVMe-over-InfiniBand-Port enthält.

====
.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte *Controller & Komponenten*.
+
Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

. Klicken Sie auf den Controller mit dem NVMe over InfiniBand-Port, den Sie konfigurieren möchten.
+
Das Kontextmenü des Controllers wird angezeigt.

. Wählen Sie *NVMe über InfiniBand-Ports konfigurieren* aus.
+
Das Dialogfeld NVMe-over-InfiniBand-Ports konfigurieren wird geöffnet.

. Wählen Sie den HIC-Port aus der Dropdown-Liste aus, und geben Sie dann die IP-Adresse ein.
+
Wenn Sie ein EF600 Speicher-Array mit einer 200-GB-fähigen HIC konfigurieren, werden in diesem Dialogfeld zwei IP-Adressfelder angezeigt, eines für einen physischen Port (extern) und eines für einen virtuellen Port (intern). Sie sollten für beide Ports eine eindeutige IP-Adresse zuweisen. Mit diesen Einstellungen kann der Host einen Pfad zwischen jedem Port und für die HIC einrichten, um eine maximale Performance zu erzielen. Wenn Sie dem virtuellen Port keine IP-Adresse zuweisen, läuft die HIC mit etwa der Hälfte ihrer fähigen Geschwindigkeit.

. Klicken Sie Auf *Konfigurieren*.
. Führen Sie die Konfiguration aus, und setzen Sie den NVMe over InfiniBand-Port zurück, indem Sie auf *Ja* klicken.

[[ID15e7fb270fc8afae1c2c30c37e2abc32]]
= Konfigurieren Sie NVMe over RoCE-Ports
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

```
[role="lead"]
Wenn Ihr Controller eine Verbindung für NVMe over RoCE (RDMA over
Converged Ethernet) umfasst, können Sie die NVMe-Port-Einstellungen auf
der Hardware-Seite konfigurieren.

.Bevor Sie beginnen
* Der Controller muss einen NVMe-over-RoCE-Host-Port umfassen. Andernfalls
sind die NVMe-over-RoCE-Einstellungen in System Manager nicht verfügbar.
* Sie müssen die IP-Adresse der Hostverbindung kennen.


.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf die Registerkarte
*Controller & Komponenten*.
+
Die Grafik ändert sich, um die Controller anstelle der Laufwerke
anzuzeigen.

. Klicken Sie auf den Controller mit dem NVMe-over-RoCE-Port, den Sie
konfigurieren möchten.
+
Das Kontextmenü des Controllers wird angezeigt.

. Wählen Sie *NVMe over RoCE Ports konfigurieren* aus.
+
Das Dialogfeld NVMe-over-RoCE-Ports konfigurieren wird geöffnet.

. Wählen Sie in der Dropdown-Liste den HIC-Port aus, den Sie konfigurieren
möchten.
. Klicken Sie Auf *Weiter*.
+
Um alle Porteinstellungen anzuzeigen, klicken Sie rechts im Dialogfeld auf
den Link *Weitere Porteinstellungen anzeigen*.

+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Port-Einstellung | Beschreibung


 a|
```

```
Konfigurierte Geschwindigkeit des ethernet-Ports
 a|
Wählen Sie die Geschwindigkeit aus, die der Geschwindigkeitsfähigkeit des
SFP am Port entspricht.



 a|
IPv4 aktivieren/IPv6 aktivieren
 a|
Wählen Sie eine oder beide Optionen aus, um die Unterstützung für IPv4-
und IPv6-Netzwerke zu aktivieren.


NOTE: Wenn Sie den Portzugriff deaktivieren möchten, deaktivieren Sie
beide Kontrollkästchen.



 a|
MTU-Größe (verfügbar durch Klicken auf *Weitere Porteinstellungen
anzeigen*.)
 a|
Geben Sie bei Bedarf eine neue Größe in Byte für die maximale
Übertragungseinheit (MTU) ein.

Die Standardgröße für maximale Übertragungseinheit (Maximum Transmission
Unit, MTU) beträgt 1500 Byte pro Frame. Sie müssen einen Wert zwischen
1500 und 9000 eingeben.

|===
====
+
Wenn Sie *IPv4 aktivieren* ausgewählt haben, wird ein Dialogfeld zur
Auswahl von IPv4-Einstellungen geöffnet, nachdem Sie auf *Weiter* geklickt
haben. Wenn Sie *IPv6* aktivieren ausgewählt haben, wird ein Dialogfeld
zur Auswahl von IPv6-Einstellungen geöffnet, nachdem Sie auf *Weiter*
geklickt haben. Wenn Sie beide Optionen ausgewählt haben, wird zuerst das
Dialogfeld für IPv4-Einstellungen geöffnet, und nach dem Klicken auf
*Weiter* wird das Dialogfeld für IPv6-Einstellungen geöffnet.

. Konfigurieren Sie die IPv4- und/oder IPv6-Einstellungen automatisch oder
manuell.
+
.Felddetails
[%collapsible]
====
```

```
[cols="25h,~"]
|===
| Port-Einstellung | Beschreibung


 a|
Automatische Ermittlung der Konfiguration
 a|
Wählen Sie diese Option aus, um die Konfiguration automatisch abzurufen.



 a|
Statische Konfiguration manuell festlegen
 a|
Wählen Sie diese Option aus, und geben Sie dann eine statische Adresse in die Felder ein. (Bei Bedarf können Sie Adressen in die Felder ausschneiden und einfügen.) Geben Sie bei IPv4 die Subnetzmaske und das Gateway des Netzwerks an. Geben Sie für IPv6 die routingfähige IP-Adresse und die Router-IP-Adresse ein. Wenn Sie ein EF600 Speicher-Array mit einer 200-GB-fähigen HIC konfigurieren, werden in diesem Dialogfeld zwei Feldsätze für Netzwerkparameter angezeigt: Eines für einen physischen Port (extern) und eines für einen virtuellen Port (intern). Sie sollten für beide Ports eindeutige Parameter zuweisen. Mit diesen Einstellungen kann der Host einen Pfad zwischen jedem Port und für die HIC einrichten, um eine maximale Performance zu erzielen. Wenn Sie dem virtuellen Port keine IP-Adresse zuweisen, läuft die HIC mit etwa der Hälfte ihrer fähigen Geschwindigkeit.

|===
====
. Klicken Sie Auf *Fertig Stellen*.




[[IDa8f0b7a92da7050fe89faad7943f0a6d]]
= Anzeigen der NVMe over Fabrics Statistiken
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Daten über die NVMe over Fabrics-Verbindungen mit Ihrem Storage-Array
```

anzeigen lassen,

.Über diese Aufgabe
System Manager zeigt diese Arten von NVMe over Fabrics Statistiken. Alle Statistiken sind schreibgeschützt und können nicht festgelegt werden.

* *NVMe Subsystem-Statistik* -- zeigt Statistiken für den NVMe-Controller und seine Queue an. Der NVMe Controller stellt einen Zugriffspfad zwischen einem Host und den Namespaces im Storage-Array bereit. Sie können die NVMe-Subsystem-Statistiken für Elemente wie Verbindungsfehler, Zurücksetzen und Herunterfahren überprüfen.
* *RDMA Interface Statistics* -- stellt Statistiken für alle NVMe over Fabrics Ports auf der RDMA-Schnittstelle bereit, die Performance-Statistiken und Link-Fehlerinformationen enthält, die mit jedem Switch-Port verbunden sind. Diese Registerkarte wird nur angezeigt, wenn NVMe over Fabrics-Ports verfügbar sind.

Sie können jede dieser Statistiken als RAW-Statistiken oder als Baseline-Statistiken anzeigen. RAW-Statistiken sind alle Statistiken, die seit dem Start der Controller gesammelt wurden. Baseline-Statistiken sind zeitpunktgenaue Statistiken, die seit dem Festlegen der Baseline-Zeit erfasst wurden.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie *View NVMe over Fabrics Statistics* aus.
. *Optional:* um den Basisplan festzulegen, klicken Sie auf *Neue Basislinie festlegen*.
+
Durch das Festlegen der Baseline wird ein neuer Ausgangspunkt für die Erfassung der Statistiken festgelegt. Dieselbe Baseline wird für alle NVMe-Statistiken verwendet.

:leveloffset: -1

= Verwalten Sie Laufwerke

:leveloffset: +1

[[ID5bca18c3639cd606532d312c19b1d5aa]]

```
= Laufwerksstatus
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
SANtricity System Manager meldet verschiedene Status für Laufwerke.



== Zugänglichkeitszustände

[cols="25h,~"]
|===
| Bundesland | Definition


 a|
Umgangen
 a|
Das Laufwerk ist physisch vorhanden, aber der Controller kann nicht mit
ihm über einen Port kommunizieren.



 a|
Inkompatibel
 a|
Eine der folgenden Bedingungen besteht:

* Das Laufwerk ist nicht für die Verwendung im Speicher-Array
zertifiziert.
* Das Laufwerk hat eine andere Sektorgröße.
* Das Laufwerk verfügt über unbrauchbare Konfigurationsdaten von einer
älteren oder neueren Firmware-Version.




 a|
Entfernt
 a|
Das Laufwerk wurde nicht ordnungsgemäß aus dem Speicher-Array entfernt.
```

```
 a|
Präsent
 a|
Der Controller kann an beiden Ports mit dem Laufwerk kommunizieren.



 a|
Nicht Ansprechbar
 a|
Das Laufwerk antwortet nicht auf Befehle.

|===


== Rollenstaaten

[cols="25h,~"]
|===
| Bundesland | Definition


 a|
Zugewiesen
 a|
Das Laufwerk ist Mitglied eines Pools oder einer Volume-Gruppe.



 a|
In-Use-Hot-Spare
 a|
Das Laufwerk wird derzeit als Ersatz für ein ausgefallenes Laufwerk
verwendet. Hot Spares werden nur in Volume-Gruppen verwendet, nicht Pools.



 a|
Standby-Hot-Spare
 a|
Das Laufwerk kann als Ersatz für ein ausgefallenes Laufwerk verwendet
werden. Hot Spares werden nur in Volume-Gruppen verwendet, nicht Pools.



 a|
```

```
Nicht Zugewiesen
 a|
Das Laufwerk ist kein Mitglied eines Pools oder einer Volume-Gruppe.

|===


== Verfügbarkeitsstatus

[cols="25h,~"]
|===
| Bundesland | Definition


 a|
Fehlgeschlagen
 a|
Das Laufwerk funktioniert nicht. Die Daten auf dem Laufwerk sind nicht
verfügbar.



 a|
Drohender Ausfall
 a|
Es wurde festgestellt, dass das Laufwerk bald ausfallen könnte. Die Daten
auf dem Laufwerk sind weiterhin verfügbar.



 a|
Offline
 a|
Das Laufwerk ist normalerweise nicht zum Speichern von Daten verfügbar,
weil es Teil einer Volume-Gruppe ist, die exportiert wird oder ein
Firmware-Upgrade durchgeführt wird.



 a|
Optimal
 a|
Das Laufwerk funktioniert ordnungsgemäß.

|===
```

```
[[IDd28c8e20ef2c7464e84fd7129c6218fe]]
= Solid State Disks (SSDs)
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Solid State Disks (SSDs) sind Daten-Storage-Geräte, die Solid State Memory
(Flash) verwenden, um Daten dauerhaft zu speichern. SSDs bieten
herkömmliche Festplatten an und sind mit denselben Schnittstellen
verfügbar wie die Festplatten.



== Vorteile von SSDs

SSDs bieten im Vergleich zu Festplatten folgende Vorteile:

* Schnellerer Start (kein Hochfahren)
* Geringere Latenz
* Höhere I/O-Operationen pro Sekunde (IOPS)
* Höhere Zuverlässigkeit mit weniger beweglichen Teilen
* Geringerer Stromverbrauch
* Geringerer Wärmeaufwand und geringerer Kühlungsbedarf




== SSDs werden identifiziert

Auf der Hardware-Seite finden Sie die SSDs in der Front-Shelf-Ansicht.
Suchen Sie nach Laufwerksschächten, die ein Blitzsymbol anzeigen, das
darauf hinweist, dass eine SSD installiert ist.



== Volume-Gruppen

Alle Laufwerke in einer Volume-Gruppe müssen vom gleichen Medientyp
(entweder alle SSDs oder alle Festplatten) sein. Volume-Gruppen können
keine Mischung aus Medientypen oder Schnittstellentypen haben.
```

```
== Caching

Das Schreib-Caching des Controllers ist immer für SSDs aktiviert. Schreib-
Caching verbessert die Performance und verlängert die Lebensdauer der
SSDs.

Zusätzlich zum Controller-Cache können Sie die SSD-Cache-Funktion
implementieren, um die Performance des gesamten Systems zu verbessern. Im
SSD-Cache werden die Daten aus Volumes kopiert und auf zwei internen RAID-
Volumes (eine pro Controller) gespeichert.



[[ID32b5ca2d154f6f96ca0e5d5a72474b26]]
= Begrenzen Sie die Laufwerkansicht
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn das Speicher-Array Laufwerke mit unterschiedlichen physischen und
logischen Attributen enthält, bietet die Seite Hardware Filterfelder, die
Ihnen helfen, die Laufwerkansicht zu begrenzen und bestimmte Laufwerke zu
finden.

.Über diese Aufgabe
Mit den Laufwerksfiltern kann die Ansicht auf bestimmte Typen physischer
Laufwerke (z. B. alle SAS) mit bestimmten Sicherheitsattributen (z. B.
sicher-fähig) an bestimmten logischen Standorten (z. B. Volume-Gruppe 1)
beschränkt werden. Sie können diese Filter zusammen oder separat
verwenden.

[NOTE]
====
Wenn alle Laufwerke dieselben physischen Attribute verwenden, wird das
Filterfeld *Laufwerke anzeigen, die...* sind, nicht angezeigt. Wenn alle
Laufwerke dieselben logischen Attribute verwenden, wird das Filterfeld
*Anywhere im Speicherarray* nicht angezeigt.

====
.Schritte
. Wählen Sie *Hardware*.
. Klicken Sie im ersten Filterfeld (unter *Laufwerke anzeigen, die...*
sind) auf den Dropdown-Pfeil, um die verfügbaren Laufwerkstypen und
Sicherheitsattribute anzuzeigen.
```

+
Folgende Laufwerktypen können enthalten:

+
** Laufwerkstyp (SSD, HDD)
** Typ der Laufwerksschnittstelle
** Laufwerkskapazität (höchste bis niedrigste)
** Fahrgeschwindigkeit (höchste bis niedrigste) Sicherheitsattribute können Folgendes umfassen:
** Sicher
** Sicher aktiviert
** DA (Data Assurance)-fähig
** FIPS-konform
** FIPS-konform (FIPS 140-2)
** FIPS-konform (FIPS 140-3)
+
Wenn eines dieser Attribute für alle Laufwerke gleich ist, werden sie in der Dropdown-Liste nicht angezeigt. Wenn das Storage-Array beispielsweise alle SSD-Laufwerke mit SAS-Schnittstellen und Geschwindigkeiten von 15000 U/min umfasst, aber einige SSDs unterschiedliche Kapazitäten haben, werden in der Dropdown-Liste nur die Kapazitäten als Filteroption angezeigt.

+
Wenn Sie eine Option aus dem Feld auswählen, werden die Laufwerke, die nicht Ihren Filterkriterien entsprechen, in der grafischen Ansicht ausgegraut.

. Klicken Sie im zweiten Filterfeld auf den Dropdown-Pfeil, um die verfügbaren logischen Positionen für die Laufwerke anzuzeigen.
+
[NOTE]
====
Wenn Sie Ihre Filterkriterien löschen möchten, wählen Sie *Löschen* ganz rechts neben den Filterfeldern aus.

====
+
Logische Standorte:

+
** Pools
** Volume-Gruppen
** Hot Spare
** SSD Cache

```
** Nicht Zugewiesen
+
Wenn Sie eine Option aus dem Feld auswählen, werden die Laufwerke, die
nicht Ihren Filterkriterien entsprechen, in der grafischen Ansicht
ausgegraut.



. Optional können Sie *Locator Lights* ganz rechts neben den Filterfeldern
einschalten, um die Locator-Leuchten für die angezeigten Laufwerke
einzuschalten.
+
Diese Aktion unterstützt Sie dabei, die Laufwerke im Speicher-Array
physisch zu finden.




[[ID35019df682fe85ca532c7d25ef09972c]]
= Schalten Sie die Anzeige der Laufwerksuchhilfe ein
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Auf der Seite Hardware können Sie die Locator-LED einschalten, um den
physischen Standort eines Laufwerks im Speicher-Array zu finden.

.Über diese Aufgabe
Sie können einzelne oder mehrere Laufwerke finden, die auf der Seite
Hardware angezeigt werden.

.Schritte
. Wählen Sie *Hardware*.
. Um ein oder mehrere Laufwerke zu finden, führen Sie einen der folgenden
Schritte aus:
+
** *Einzelantrieb* -- aus der Regalgrafik finden Sie das Laufwerk, das Sie
physisch im Array finden möchten. (Wenn die Grafik die Controller anzeigt,
klicken Sie auf die Registerkarte *Laufwerke*.) Klicken Sie auf das
Laufwerk, um das Kontextmenü anzuzeigen, und wählen Sie dann *Locator
Light einschalten*.
+
Die Positionsanzeige des Laufwerks leuchtet auf. Wenn Sie das Laufwerk
```

physisch gefunden haben, kehren Sie zum Dialog zurück und wählen Sie *Ausschalten*.

** *Mehrere Laufwerke* -- Wählen Sie in den Filterfeldern aus der linken Dropdown-Liste einen physischen Laufwerkstyp und einen logischen Laufwerkstyp aus der rechten Dropdown-Liste aus. Die Anzahl der Laufwerke, die Ihren Kriterien entsprechen, wird rechts in den Feldern angezeigt. Als Nächstes können Sie entweder auf *Locator einschalten Lichter* klicken oder im Kontextmenü *Alle gefilterten Laufwerke lokalisieren* wählen. Wenn Sie die Laufwerke physisch lokalisiert haben, kehren Sie zum Dialog zurück und wählen Sie *Ausschalten*.

[[ID8b63f8b2e474e225a2506c4d0dd6c62f]]
= Zeigen Sie den Laufwerkstatus und die Einstellungen an
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können Status und Einstellungen für die Laufwerke anzeigen, z. B. Medientyp, Schnittstellentyp und Kapazität.

.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Controller anzeigt, klicken Sie auf die Registerkarte *Laufwerke*.
+
Die Grafik ändert sich, um die Laufwerke anstelle der Controller anzuzeigen.

. Wählen Sie das Laufwerk aus, für das Sie Status und Einstellungen anzeigen möchten.
+
Das Kontextmenü des Laufwerks wird geöffnet.

. Wählen Sie *Anzeigeeinstellungen*.
+
Das Dialogfeld Laufwerkeinstellungen wird geöffnet.

. Um alle Einstellungen anzuzeigen, klicken Sie oben rechts im Dialogfeld

```
auf *Weitere Einstellungen anzeigen*.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellungen | Beschreibung


 a|
Status
 a|
Anzeige optimal, Offline, nicht-kritischer Fehler und fehlgeschlagen. Der
optimale Status gibt den gewünschten Betriebszustand an.



 a|
Modus
 a|
Zeigt zugewiesene, nicht zugewiesene, Hot Spare Standby oder Hot Spare in
Verwendung an.



 a|
Standort
 a|
Zeigt das Shelf und die Einschubnummer, auf der sich das Laufwerk
befindet.



 a|
Zugewiesen zu/kann für/Schutz schützen
 a|
Wenn das Laufwerk einem Pool, einer Volume-Gruppe oder einem SSD-Cache
zugewiesen ist, wird in diesem Feld „Assigned to“ angezeigt. Der Wert kann
ein Poolname, ein Name der Volume-Gruppe oder ein Name des SSD-Caches
sein. Wenn das Laufwerk einem Hot Spare zugewiesen ist und dessen Modus
Standby ist, wird in diesem Feld „Can Protect for“ angezeigt. Wenn das Hot
Spare eine oder mehrere Volume-Gruppen schützen kann, werden die Namen der
Volume-Gruppen angezeigt. Wenn eine Volume-Gruppe nicht geschützt werden
kann, werden 0 Volume-Gruppen angezeigt.

Wenn das Laufwerk einem Hot Spare zugewiesen ist und dessen Modus
```

verwendet wird, wird in diesem Feld „Schutz“ angezeigt. Der Wert ist der Name der betroffenen Volume-Gruppe.

Wenn die Zuweisung des Laufwerks aufgehoben ist, wird dieses Feld nicht angezeigt.

a|
Medientyp
a|
Zeigt den Typ der Aufzeichnungsmedien an, die vom Laufwerk verwendet werden. Dabei kann es sich um eine Festplatte (HDD) oder ein Solid State Disk (SSD) handeln.

a|
Verwendete Ausdauer in Prozent (nur angezeigt, wenn SSD-Laufwerke vorhanden sind)
a|
Die Menge der Daten, die bisher auf das Laufwerk geschrieben wurden, geteilt durch die theoretische Gesamtbeschreibungsgrenze.

a|
Schnittstellentyp
a|
Zeigt den Schnittstellentyp an, den das Laufwerk verwendet, z. B. SAS.

a|
Redundanz von Laufwerkspfaden
a|
Zeigt an, ob die Verbindungen zwischen dem Laufwerk und dem Controller redundant sind (Ja) oder nicht (Nein).

a|
Kapazität (gib)
a|
Zeigt die nutzbare Kapazität (gesamte konfigurierte Kapazität) des Laufwerks an.

```
 a|
Geschwindigkeit (U/min)
 a|
Zeigt die Geschwindigkeit in RPM an (wird nicht für SSDs angezeigt).



 a|
Aktuelle Datenrate
 a|
Zeigt die Datentransferrate zwischen dem Laufwerk und dem Speicher-Array
an.



 a|
Größe des logischen Sektors (Byte)
 a|
Zeigt die Größe des logischen Sektors an, die das Laufwerk verwendet.



 a|
Größe des physischen Sektors (Bytes)
 a|
Zeigt die physikalische Sektorgröße an, die das Laufwerk verwendet. In der
Regel beträgt die Größe des physischen Sektors 4096 Bytes für Festplatten.



 a|
Die Version der Laufwerk-Firmware
 a|
Zeigt die Versionsebene der Laufwerk-Firmware an.



 a|
Weltweite Kennung
 a|
Zeigt die eindeutige Hexadezimalkennung für das Laufwerk an.



 a|
```

```
Produkt-ID
 a|
Zeigt die vom Hersteller zugewiesene Produktkennung an.



 a|
Seriennummer
 a|
Zeigt die Seriennummer des Laufwerks an.



 a|
Hersteller
 a|
Zeigt den Anbieter des Laufwerks an.



 a|
Herstellungsdatum
 a|
Zeigt das Datum an, an dem das Laufwerk gebaut wurde.

NOTE: Nicht verfügbar für NVMe-Laufwerke.



 a|
Sicher
 a|
Zeigt an, ob das Laufwerk sicher-fähig ist (ja) oder nicht (Nein). Sichere
Laufwerke können entweder vollständige Festplattenverschlüsselung (Full
Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing
Standard) sein (Level 140-2 oder 140 bis 3), die Daten beim Schreiben
verschlüsseln und während Lesevorgänge entschlüsseln. Diese Laufwerke
gelten als sicher-_fähig_, da sie mit der Sicherheitsfunktion des
Laufwerks für zusätzliche Sicherheit verwendet werden können. Wenn die
Laufwerkssicherheitsfunktion für Volume-Gruppen und -Pools aktiviert ist,
die mit diesen Laufwerken verwendet werden, werden die Laufwerke sicher-
_Enabled_.



 a|
```

Sicher aktiviert
 a|
Zeigt an, ob das Laufwerk sicher aktiviert ist (Ja) oder nicht (Nein). Secure-Enabled-Laufwerke werden mit der Drive Security-Funktion verwendet. Wenn Sie die Laufwerkssicherheitsfunktion aktivieren und dann Laufwerksicherheit auf einem Pool oder einer Volume-Gruppe auf Secure-_fähigen_-Laufwerken anwenden, werden die Laufwerke sicher-_enabled_. Lese- und Schreibzugriff ist nur über einen Controller verfügbar, der mit dem korrekten Sicherheitsschlüssel konfiguriert ist. Diese zusätzliche Sicherheit verhindert einen nicht autorisierten Zugriff auf die Daten auf einem Laufwerk, das physisch vom Storage-Array entfernt wird.

 a|
Zugriff auf Lese-/Schreibzugriff
 a|
Zeigt an, ob auf das Laufwerk Lese-/Schreibzugriff möglich ist (Ja) oder nicht (Nein).

 a|
Kennung des Laufwerksicherheitsschlüssels
 a|
Zeigt den Sicherheitsschlüssel für sichere Laufwerke an. Laufwerkssicherheit ist eine Funktion des Storage Arrays, die eine zusätzliche Sicherheitsschicht bietet – entweder mit vollständigen Festplatten-Verschlüsselung (FDE) oder FIPS-Laufwerken (Federal Information Processing Standard). Wenn diese Laufwerke zusammen mit der Sicherheitsfunktion des Laufwerks verwendet werden, benötigen sie einen Sicherheitsschlüssel für den Zugriff auf ihre Daten. Wenn die Laufwerke physisch aus dem Array entfernt werden, können sie erst betrieben werden, wenn sie in einem anderen Array installiert sind. Zu diesem Zeitpunkt befinden sie sich in einem Sicherheitsstatus, bis der richtige Sicherheitsschlüssel bereitgestellt wird.

 a|
Data Assurance (da)-fähig
 a|
Zeigt an, ob die da-Funktion (Data Assurance) aktiviert ist (Ja) oder nicht (Nein). Data Assurance (da) ist eine Funktion, die Fehler überprüft und korrigiert, die auftreten können, wenn Daten durch die Controller zu den Laufwerken übertragen werden. Data Assurance kann auf Pool- oder

```
Volume-Gruppenebene aktiviert werden, wobei Hosts über eine da-fähige I/O-
Schnittstelle wie Fibre Channel verfügen.



 a|
DULBE-fähig
 a|
Gibt an, ob die Option für dezugeordneten oder nicht geschriebenen
logischen Blockfehler (DULBE) aktiviert ist (Ja) oder nicht (Nein). DULBE
ist eine Option auf NVMe-Laufwerken, mit der das EF300- oder EF600-
Storage-Array ressourcenbereitgestellte Volumes unterstützt.

|===
====
. Klicken Sie Auf *Schließen*.




[[ID2581574e03d236e91996903560fdb12b]]
= Laufwerk logisch ersetzen
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn ein Laufwerk ausfällt oder Sie es aus einem anderen Grund ersetzen
möchten, können Sie das ausgefallene Laufwerk logisch durch ein nicht
zugewiesenes Laufwerk oder ein vollständig integriertes Hot Spare
ersetzen.

.Über diese Aufgabe
Wenn Sie ein Laufwerk logisch ersetzen, wird es zugewiesen und ist dann
dauerhaftes Mitglied des zugeordneten Pools oder der Volume-Gruppe.

Sie verwenden die Option „logischer Austausch“, um die folgenden
Laufwerkstypen zu ersetzen:

* Ausgefallene Laufwerke
* Laufwerke fehlen
* SSD-Laufwerke, die der Recovery Guru benachrichtigt hat, dass sich ihrem
Ende ihres Lebenszyklus nähert
* Festplatten, die der Recovery Guru benachrichtigt hat, die über einen
bevorstehenden Laufwerksausfall verfügen
```

* Zugewiesene Laufwerke (nur für Laufwerke in einer Volume-Gruppe, nicht in einem Pool verfügbar)

.Bevor Sie beginnen
Das Ersatzlaufwerk muss die folgenden Eigenschaften aufweisen:

* Im optimalen Zustand
* Im Status nicht zugewiesen
* Die gleichen Attribute wie das zu ersetzende Laufwerk (Medientyp, Schnittstellentyp usw.)
* Dieselben FDE-Funktionen (empfohlen, jedoch nicht erforderlich)
* Die gleiche da-Fähigkeit (empfohlen, aber nicht erforderlich)

.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Controller anzeigt, klicken Sie auf die Registerkarte *Laufwerke*.
+
Die Grafik ändert sich, um die Laufwerke anstelle der Controller anzuzeigen.

. Klicken Sie auf das Laufwerk, das Sie logisch ersetzen möchten.
+
Das Kontextmenü des Laufwerks wird angezeigt.

. Klicken Sie auf *logisch ersetzen*.
. *Optional:* Aktivieren Sie das Kontrollkästchen *fail drive, nachdem es ersetzt wurde*, um das ursprüngliche Laufwerk nach dem Ersetzen zu scheitern.
+
Dieses Kontrollkästchen ist nur aktiviert, wenn das ursprünglich zugewiesene Laufwerk nicht ausgefallen ist oder fehlt.

. Wählen Sie in der Tabelle *Ersatzlaufwerk auswählen* das Ersatzlaufwerk aus, das Sie verwenden möchten.
+
In der Tabelle werden nur die Laufwerke aufgeführt, die mit dem Laufwerk kompatibel sind, das Sie ersetzen. Wenn möglich, wählen Sie ein Laufwerk aus, das den Schutz vor Regalverlust und den Schutz vor Schubladenverlust aufrechterhalten soll.

. Klicken Sie Auf *Ersetzen*.
+
Wenn das ursprüngliche Laufwerk ausgefallen ist oder fehlt, werden die Daten mithilfe der Paritätsinformationen auf dem Ersatzlaufwerk

rekonstruiert. Diese Rekonstruktion beginnt automatisch. Die Fehleranzeige des Laufwerks erlischt, und die Aktivitäts-LED der Laufwerke im Pool oder in der Volume-Gruppe beginnt zu blinken.

+
Wenn das ursprüngliche Laufwerk nicht ausgefallen ist oder fehlt, werden seine Daten auf das Ersatzlaufwerk kopiert. Dieser Kopiervorgang startet automatisch. Nachdem der Kopiervorgang abgeschlossen ist, wechselt das System das ursprüngliche Laufwerk in den Status nicht zugewiesen oder wenn das Kontrollkästchen aktiviert wurde, in den Status fehlgeschlagen.

[[ID58b82ac1abc7d25ce11935e8d51df72d]]
= Manuelles Rekonstruieren des Laufwerks
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Die Laufwerksrekonstruktion wird normalerweise automatisch gestartet, nachdem Sie ein Laufwerk ersetzt haben. Wenn die Datenrekonstruktion nicht automatisch gestartet wird, können Sie die Rekonstruktion manuell starten.

[NOTE]
====
Führen Sie diesen Vorgang nur aus, wenn Sie vom technischen Support oder dem Recovery Guru dazu aufgefordert werden.

====
.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Controller anzeigt, klicken Sie auf die Registerkarte *Laufwerke*.
+
Die Grafik ändert sich, um die Laufwerke anstelle der Controller anzuzeigen.

. Klicken Sie auf das Laufwerk, das Sie manuell rekonstruieren möchten.
+
Das Kontextmenü des Laufwerks wird angezeigt.

. Wählen Sie * rekonstruieren*, und bestätigen Sie, dass Sie den Vorgang

```
ausführen möchten.




[[ID67cb79bfa78f88c4b0c232b495ae5e44]]
= Initialisieren (Formatieren) des Laufwerks
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie zugewiesene Laufwerke von einem Speicher-Array in ein anderes
verschieben, müssen Sie die Laufwerke initialisieren (formatieren), bevor
sie im neuen Speicher-Array verwendet werden können.

.Über diese Aufgabe
Durch Initialisieren werden die vorherigen Konfigurationsinformationen von
einem Laufwerk entfernt und in den Status „nicht zugewiesen“
zurückgeführt. Das Laufwerk kann dann einem neuen Pool oder einer neuen
Volume-Gruppe im neuen Speicher-Array hinzugefügt werden.

Verwenden Sie den Vorgang zum Initialisieren des Laufwerks, wenn Sie ein
einzelnes Laufwerk verschieben. Sie müssen Laufwerke nicht initialisieren,
wenn Sie eine ganze Volume-Gruppe von einem Speicher-Array in ein anderes
verschieben.

[CAUTION]
====
*Möglicher Datenverlust* -- Wenn Sie ein Laufwerk initialisieren, gehen
alle Daten auf dem Laufwerk verloren. Führen Sie diesen Vorgang nur aus,
wenn Sie vom technischen Support dazu aufgefordert werden.

====
.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Controller anzeigt, klicken Sie auf die
Registerkarte *Laufwerke*.
+
Die Grafik ändert sich, um die Laufwerke anstelle der Controller
anzuzeigen.

. Klicken Sie auf das Laufwerk, das Sie initialisieren möchten.
+
Das Kontextmenü des Laufwerks wird angezeigt.
```

```
. Wählen Sie *Initialisieren*, und bestätigen Sie, dass Sie den Vorgang
ausführen möchten.



[[IDd1bccd7480173a51db76d11326a40906]]
= Laufwerk ausfällt
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie dazu aufgefordert werden, können Sie ein Laufwerk manuell
fehlschlagen.

.Über diese Aufgabe
System Manager überwacht die Laufwerke im Speicher-Array. Wenn die
Software feststellt, dass ein Laufwerk viele Fehler verursacht,
benachrichtigt Sie der Recovery Guru über einen bevorstehenden
Laufwerksausfall. Sollte dies der Fall sein und Sie können ein
Ersatzlaufwerk verwenden, um präventiv zu handeln. Wenn kein
Ersatzlaufwerk verfügbar ist, können Sie warten, bis das Laufwerk
ausfällt.

[CAUTION]
====
*Möglicher Verlust des Datenzugriffs* -- dieser Vorgang kann zu
Datenverlust oder Datenverlust führen. Führen Sie diesen Vorgang nur aus,
wenn Sie vom technischen Support oder dem Recovery Guru dazu aufgefordert
werden.

====
.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Controller anzeigt, klicken Sie auf die
Registerkarte *Laufwerke*.
+
Die Grafik ändert sich, um die Laufwerke anstelle der Controller
anzuzeigen.

. Klicken Sie auf das Laufwerk, das Sie fehlschlagen möchten.
+
Das Kontextmenü des Laufwerks wird angezeigt.
```

. Wählen Sie *Fail*.
. Aktivieren Sie das Kontrollkästchen *Inhalt kopieren von Laufwerk vor Ausfall*.
+
Die Kopieroption wird nur für zugewiesene Laufwerke und für nicht-RAID 0-Volume-Gruppen angezeigt.

+
Bevor Sie das Laufwerk ausfallen, müssen Sie den Inhalt des Laufwerks kopieren. Je nach Konfiguration könnten möglicherweise alle Daten- oder Datenredundanz auf dem zugehörigen Pool oder Volume-Gruppe verloren gehen, wenn Sie den Inhalt des Laufwerks nicht zuerst kopieren.

+
Die Kopieroption ermöglicht eine schnellere Wiederherstellung des Laufwerks als zur Rekonstruktion und verringert somit die Möglichkeit eines Volume-Ausfalls, wenn während des Kopiervorgangs ein weiteres Laufwerk ausfällt.

. Bestätigen Sie, dass das Laufwerk ausfallen soll.
+
Warten Sie nach dem Ausfall des Laufwerks mindestens 60 Sekunden, bevor Sie es entfernen.

[[ID3582570f030e26f45a7a3560c24b54ab]]
= Laufwerke löschen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können die Option Löschen verwenden, um ein nicht zugewiesenes Laufwerk zum Entfernen aus dem System vorzubereiten. Durch dieses Verfahren werden die Daten endgültig entfernt, sodass die Daten nicht erneut gelesen werden können.

.Bevor Sie beginnen
Das Laufwerk muss sich im Status „nicht zugewiesen“ befinden.

.Über diese Aufgabe
Verwenden Sie die Option Löschen nur, wenn Sie alle Daten auf einem Laufwerk dauerhaft entfernen möchten. Wenn das Laufwerk sicher aktiviert ist, führt die Option Löschen eine kryptografische Löschung durch und setzt die Sicherheitsattribute des Laufwerks wieder auf sicher-fähig zurück.

[NOTE]
====
Die Löschfunktion unterstützt einige ältere Laufwerksmodelle nicht. Wenn Sie versuchen, eines dieser älteren Modelle zu löschen, wird eine Fehlermeldung angezeigt.

====
.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Controller anzeigt, klicken Sie auf die Registerkarte *Laufwerke*.
+
Die Grafik ändert sich, um die Laufwerke anstelle der Controller anzuzeigen.

. Optional können Sie mithilfe der Filterfelder alle nicht zugewiesenen Laufwerke im Shelf anzeigen. Wählen Sie aus der Dropdown-Liste *Laufwerke anzeigen, die...* sind, die Option *nicht zugewiesen* aus.
+
In der Shelf-Ansicht werden nur die nicht zugewiesenen Laufwerke angezeigt; alle anderen sind ausgegraut.

. Um das Kontextmenü des Laufwerks zu öffnen, klicken Sie auf ein Laufwerk, das Sie löschen möchten. (Wenn Sie mehrere Laufwerke auswählen möchten, können Sie dies im Dialogfeld Laufwerke löschen tun.)
+
[CAUTION]
====
Möglicher Datenverlust -- der Löschvorgang kann nicht rückgängig gemacht werden. Vergewissern Sie sich, dass Sie während des Verfahrens die richtigen Laufwerke auswählen.

====
. Wählen Sie im Kontextmenü *Löschen* aus.
+
Das Dialogfeld Laufwerke löschen wird geöffnet und zeigt alle für einen Löschvorgang geeigneten Laufwerke an.

. Wählen Sie bei Bedarf zusätzliche Laufwerke aus der Tabelle aus. Sie

können keine _alle_ Laufwerke auswählen. Vergewissern Sie sich, dass die Auswahl eines Laufwerks weiterhin aufgehoben ist.
. Bestätigen Sie den Vorgang, indem Sie eingeben `erase`, Und klicken Sie dann auf *Löschen*.
+
[CAUTION]
====
Stellen Sie sicher, dass Sie mit diesem Vorgang fortfahren möchten. Wenn Sie im nächsten Dialogfeld auf Ja klicken, kann der Vorgang nicht abgebrochen werden.

====
. Klicken Sie im Dialogfeld geschätzte Abschlusszeit auf *Ja*, um mit dem Löschvorgang fortzufahren.

.Ergebnisse
Der Löschvorgang kann mehrere Minuten oder mehrere Stunden dauern. Sie können den Status im Menü:Startseite[Vorgänge in Bearbeitung anzeigen] anzeigen. Wenn der Vorgang Löschen abgeschlossen ist, können die Laufwerke in einer anderen Volume-Gruppe oder einem anderen Laufwerk-Pool oder in einem anderen Speicher-Array verwendet werden.

.Nachdem Sie fertig sind
Wenn Sie das Laufwerk wieder verwenden möchten, müssen Sie es zuerst initialisieren. Wählen Sie dazu im Kontextmenü des Laufwerks *Initialisieren* aus.

[[ID7145b1cea7a5e68a9db157628e21ae71]]
= Locked NVMe- oder FIPS-Laufwerke entsperren oder zurücksetzen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Wenn Sie ein oder mehrere gesperrte NVMe- oder FIPS-Laufwerke in ein Storage-Array einfügen, können die Laufwerkdaten entsperrt werden, indem Sie die Sicherheitsschlüsseldatei hinzufügen, die den Laufwerken zugeordnet ist. Wenn Sie keinen Sicherheitsschlüssel haben, können Sie auf jedem gesperrten Laufwerk einen Reset durchführen, indem Sie seine physische Sicherheits-ID (PSID) eingeben, um seine Sicherheitsattribute zurückzusetzen und die Laufwerkdaten zu löschen.

.Bevor Sie beginnen
* Stellen Sie bei der Option Entsperren sicher, dass die Sicherheitsschlüsseldatei (mit einer Erweiterung von) verwendet wird `.slk`) Ist auf dem Management-Client verfügbar (das System mit einem Browser, der für den Zugriff auf System Manager verwendet wird). Sie müssen auch die Passphrase kennen, die mit der Taste verbunden ist.
* Für die Option Zurücksetzen müssen Sie die PSID auf jedem Laufwerk finden, das Sie zurücksetzen möchten. Um die PSID zu finden, entfernen Sie das Laufwerk physisch und suchen Sie die PSID-Zeichenfolge (maximal 32 Zeichen) auf dem Laufwerketikett, und installieren Sie dann das Laufwerk neu.

.Über diese Aufgabe
In dieser Aufgabe wird beschrieben, wie Daten aus NVMe- oder FIPS-Laufwerken durch Importieren einer Sicherheitsschlüsseldatei in das Storage Array entsperrt werden. In Fällen, in denen der Sicherheitsschlüssel nicht verfügbar ist, beschreibt diese Aufgabe auch, wie ein Reset auf einem gesperrten Laufwerk durchgeführt wird.

[NOTE]
====
Wenn das Laufwerk über einen externen Schlüsselverwaltungsserver gesperrt wurde, wählen Sie in System Manager Menü:Einstellungen[System > Sicherheitsschlüsselverwaltung], um die externe Schlüsselverwaltung zu konfigurieren und das Laufwerk zu entsperren.

====
Sie können die Funktion zum Entsperren entweder über die Seite Hardware oder über das Menü:Einstellungen[System > Sicherheitsschlüsselverwaltung] aufrufen. Die folgende Aufgabe enthält Anweisungen auf der Seite Hardware.

.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Controller anzeigt, klicken Sie auf die Registerkarte *Laufwerke*.
+
Die Grafik ändert sich, um die Laufwerke anstelle der Controller anzuzeigen.

. Wählen Sie das NVMe- oder FIPS-Laufwerk aus, das entsperrt oder zurückgesetzt werden soll.
+
Das Kontextmenü des Laufwerks wird geöffnet.

```
. Wählen Sie *Entsperren*, um die Sicherheitsschlüsseldatei anzuwenden,
oder *Zurücksetzen*, wenn Sie keine Sicherheitsschlüsseldatei haben.
+
Diese Optionen werden nur angezeigt, wenn Sie ein gesperrtes NVMe- oder
FIPS-Laufwerk auswählen.

+
[CAUTION]
====
Während eines Reset-Vorgangs werden alle Daten gelöscht. Führen Sie nur
einen Reset aus, wenn Sie keinen Sicherheitsschlüssel haben. Beim
Zurücksetzen eines gesperrten Laufwerks werden alle Daten auf dem Laufwerk
endgültig entfernt und die Sicherheitsattribute auf „sicher-fähig“
zurückgesetzt, aber nicht aktiviert. *Dieser Vorgang ist nicht umkehrbar.*

====
. Führen Sie einen der folgenden Schritte aus:
+
.. *Entsperren*: Klicken Sie im Dialogfeld * Secure Drive entsperren* auf
*Durchsuchen* und wählen Sie dann die Sicherheitsschlüsseldatei aus, die
dem Laufwerk entspricht, das Sie entsperren möchten. Geben Sie dann den
Passphrase ein und klicken Sie dann auf *Entsperren*.
.. *Zurücksetzen*: Geben Sie im Dialogfeld *gesperrtes Laufwerk
zurücksetzen* den PSID-String in das Feld ein, und geben Sie dann ein
`RESET` Zur Bestätigung. Klicken Sie Auf *Zurücksetzen*.
+
Für einen Entsperrvorgang muss dieser Vorgang nur einmal ausgeführt
werden, um alle NVMe- oder FIPS-Laufwerke freizuschalten. Bei einem Reset-
Vorgang müssen Sie jedes Laufwerk einzeln auswählen, das Sie zurücksetzen
möchten.




.Ergebnisse
Das Laufwerk kann nun in einer anderen Volume-Gruppe oder einem anderen
Laufwerk-Pool oder in einem anderen Speicher-Array verwendet werden.



:leveloffset: -1


= Management von Hot Spares

:leveloffset: +1
```

```
[[ID256e52e2e1ca434156e9ed02f851b4d6]]
= Übersicht über Hot-Spare-Laufwerke
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Hot Spares fungieren als Standby-Laufwerke in RAID 1-, RAID 5- oder RAID
6-Volume-Gruppen für SANtricity System Manager.

Es handelt sich dabei um voll funktionsfähige Laufwerke, die keine Daten
enthalten. Wenn ein Laufwerk in der Volume-Gruppe ausfällt, rekonstruiert
der Controller die Daten vom ausgefallenen Laufwerk automatisch auf ein
Laufwerk, das als Hot Spare zugewiesen wurde.

Hot Spares sind nicht für bestimmte Volume-Gruppen bestimmt. Sie können
für jedes ausgefallene Laufwerk im Speicher-Array verwendet werden,
solange das Hot Spare und das Laufwerk diese Attribute teilen:

* Gleiche Kapazität (oder höhere Kapazität für das Hot Spare)
* Derselbe Medientyp (beispielsweise Festplatte oder SSD)
* Gleicher Schnittstellentyp (z. B. SAS)




== Identifizierung von Hot Spares

Sie können Hot Spares über den Setup-Assistenten oder über die Hardware-
Seite zuweisen. Um festzustellen, ob Hot Spares zugewiesen werden, gehen
Sie zur Hardware-Seite und suchen Sie nach den in Rosa angezeigten
Laufwerkschächten.



== Funktionsweise der Hot-Spare-Abdeckung

Hot-Spare-Abdeckung funktioniert wie folgt:

* Sie reservieren ein nicht zugewiesenes Laufwerk als Hot Spare für RAID
1-, RAID 5- oder RAID 6-Volume-Gruppen.
+
[NOTE]
```

====
Hot Spares können nicht für Pools verwendet werden, die eine andere Methode der Datensicherheit haben. Anstatt eine zusätzliche Festplatte zu reservieren, reservieren Pools freie Kapazitäten (sogenannte _freie Kapazität_) innerhalb jedes Laufwerks des Pools. Wenn ein Laufwerk in einem Pool ausfällt, werden Daten in diesem freien Speicherplatz wiederhergestellt.

====
* Wenn ein Laufwerk in einer RAID 1-, RAID 5- oder RAID 6-Volume-Gruppe ausfällt, verwendet der Controller automatisch Redundanzdaten zur Rekonstruktion der Daten vom ausgefallenen Laufwerk. Das Hot Spare wird automatisch durch das ausgefallene Laufwerk ersetzt, ohne dass ein physischer Austausch erforderlich ist.
* Wenn Sie das ausgefallene Laufwerk physisch ersetzt haben, erfolgt ein Kopiervorgang vom Hot-Spare-Laufwerk zum ausgetauschten Laufwerk. Wenn Sie das Hot Spare-Laufwerk als dauerhaftes Mitglied einer Volume-Gruppe angegeben haben, ist der Copyback-Vorgang nicht erforderlich.
* Die Verfügbarkeit von Ablagefach-Verlustschutz und Schubladenschutz für eine Volume-Gruppe hängt von der Position der Laufwerke ab, aus denen die Volume-Gruppe besteht. Der Schutz vor Verlust des Fachs und der Schutz vor Schubladenverlust können aufgrund eines ausgefallenen Laufwerks und der Position des Hot-Spare-Laufwerks verloren gehen. Um sicherzustellen, dass der Schutz vor Verlust des Fachs und der Schutz vor Schubladenverlust nicht beeinträchtigt werden, müssen Sie ein ausgefallenes Laufwerk austauschen, um den Kopiervorgang zu initiieren.
* Das Storage Array Volume bleibt während des Austauschs des ausgefallenen Laufwerks online und zugänglich, da das Hot-Spare-Laufwerk automatisch durch das ausgefallene Laufwerk ersetzt wird.

== Überlegungen zur Kapazität von Hot-Spare-Festplatten

Wählen Sie ein Laufwerk mit einer Kapazität aus, die der Gesamtkapazität des zu schützenden Laufwerks entspricht oder die größer ist. Wenn beispielsweise ein Laufwerk mit 18 gib und einer konfigurierten Kapazität von 8 gib vorhanden ist, können Sie ein Laufwerk mit 9 gib oder mehr als Hot Spare verwenden. Weisen Sie ein Laufwerk grundsätzlich nicht als Hot Spare zu, es sei denn, seine Kapazität entspricht oder ist größer als die Kapazität des größten Laufwerks im Speicher-Array.

[NOTE]
====
Wenn nicht Hot Spares zur Verfügung stehen, die die gleiche physische

Kapazität haben, kann ein Laufwerk mit geringerer Kapazität als Hot Spare verwendet werden, wenn die „genutzte Kapazität" des Laufwerks gleich oder kleiner als die Kapazität des Hot-Spare-Laufwerks ist.

====

== Überlegungen zu Medien- und Schnittstellentypen

Das als Hot Spare verwendete Laufwerk muss denselben Medientyp und dieselbe Schnittstelle verwenden wie die Laufwerke, die es schützen wird. Beispielsweise kann eine Festplatte nicht als Hot Spare für SSD-Laufwerke verwendet werden.

== Überlegungen zu sicheren Laufwerken

Ein sicheres Laufwerk wie FDE oder FIPS kann als Hot Spare für Laufwerke mit oder ohne Sicherheitsmerkmale genutzt werden. Ein nicht sicher fähiges Laufwerk kann jedoch nicht als Hot Spare für Laufwerke mit Sicherheitsfunktionen dienen.

Wenn Sie ein sicheres Laufwerk auswählen, das für ein Hot Spare verwendet werden soll, werden Sie von System Manager aufgefordert, eine sichere Löschung durchzuführen, bevor Sie fortfahren können. Mit Secure Erase werden die Sicherheitsattribute des Laufwerks auf sicher-fähig, aber nicht sicher aktiviert zurückgesetzt.

[NOTE]
====
Wenn Sie die Laufwerkssicherheitsfunktion aktivieren und dann aus sicheren Laufwerken einen Pool oder eine Volume-Gruppe erstellen, werden die Laufwerke _Secure-Enabled_. Lese- und Schreibzugriff ist nur über einen Controller verfügbar, der mit dem korrekten Sicherheitsschlüssel konfiguriert ist. Diese zusätzliche Sicherheit verhindert einen nicht autorisierten Zugriff auf die Daten auf einem Laufwerk, das physisch vom Storage-Array entfernt wird.

====

== Empfohlene Anzahl von Hot-Spare-Laufwerken

Wenn Sie den anfänglichen Setup-Assistenten zur automatischen Erstellung von Hot Spares verwendet haben, erstellt der System Manager ein Hot Spare für alle 30 Laufwerke eines bestimmten Medientyps und eines bestimmten

```
Schnittstellentyps. Andernfalls können Sie manuell Hot-Spare-Laufwerke
zwischen den Volume-Gruppen im Speicher-Array erstellen.



[[ID0a3493653df98267998393a14111b739]]
= Weisen Sie Hot Spares zu
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können ein Hot Spare als Standby-Laufwerk für zusätzlichen Datenschutz
in RAID 1-, RAID 5- oder RAID 6-Volume-Gruppen zuweisen. Wenn ein Laufwerk
in einer dieser Volume-Gruppen ausfällt, rekonstruiert der Controller
Daten vom ausgefallenen Laufwerk auf dem Hot Spare.

.Bevor Sie beginnen
* RAID 1-, RAID 5- oder RAID 6-Volume-Gruppen müssen erstellt werden. (Hot
Spares können nicht für Pools verwendet werden. Stattdessen nutzt ein Pool
zur Datensicherung innerhalb jedes Laufwerks freie Kapazitäten.)
* Ein Laufwerk, das die folgenden Kriterien erfüllt, muss verfügbar sein:
+
** Nicht zugewiesen, mit optimalem Status.
** Derselbe Medientyp wie die Laufwerke in der Volume-Gruppe (z. B. SSDs).
** Derselbe Schnittstellentyp wie die Laufwerke in der Volume-Gruppe (z.
B. SAS).
** Die Kapazität entspricht oder größer als die genutzte Kapazität der
Laufwerke in der Volume-Gruppe.




.Über diese Aufgabe
In dieser Aufgabe wird beschrieben, wie Sie auf der Seite Hardware manuell
ein Hot Spare zuweisen. Die empfohlene Abdeckung beträgt zwei Hot Spares
pro Laufwerk-Set.

[NOTE]
====
Hot Spares können auch über den Einrichtungsassistenten zugewiesen werden.
Sie können feststellen, ob Hot Spares bereits zugeordnet sind, indem Sie
auf der Seite Hardware nach in Rosa angezeigten Laufwerkschächten suchen.

====
```

.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Controller anzeigt, klicken Sie auf die Registerkarte *Laufwerke*.
+
Die Grafik ändert sich, um die Laufwerke anstelle der Controller anzuzeigen.

. Wählen Sie ein nicht zugewiesenes Laufwerk (grau dargestellt) aus, das Sie als Hot Spare verwenden möchten.
+
Das Kontextmenü des Laufwerks wird geöffnet.

. Wählen Sie *Hot Spare zuweisen*.
+
Wenn das Laufwerk sicher aktiviert ist, wird das Secure Erase-Laufwerk verwendet? Das Dialogfeld wird geöffnet. Um ein sicheres Laufwerk als Hot Spare zu verwenden, müssen Sie zuerst einen Secure Erase-Vorgang durchführen, um alle Daten zu entfernen und die Sicherheitsattribute zurückzusetzen.

+
[CAUTION]
====
Möglicher Datenverlust -- stellen Sie sicher, dass Sie das richtige Laufwerk ausgewählt haben. Nach Abschluss des Vorgangs Secure Erase können Sie keine Daten wiederherstellen.

====
+
Wenn das Laufwerk *nicht* sicher aktiviert ist, wird das Dialogfeld Hot Spare Drive bestätigen geöffnet.

. Überprüfen Sie den Text im Dialogfeld, und bestätigen Sie den Vorgang.
+
Das Laufwerk wird auf der Seite Hardware in Rosa angezeigt, was darauf hinweist, dass es sich nun um ein Hot Spare handelt.

.Ergebnisse
Wenn ein Laufwerk in einer RAID 1-, RAID 5- oder RAID 6-Volume-Gruppe ausfällt, verwendet der Controller automatisch Redundanzdaten zur Rekonstruktion der Daten vom ausgefallenen Laufwerk auf dem Hot Spare.

```
[[ID48bc087e6c94307ab1abaa3498f658eb]]
= Heben Sie die Zuweisung von Hot Spares wieder auf
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können ein Hot Spare wieder auf ein nicht zugewiesenes Laufwerk
ändern.

.Bevor Sie beginnen
Das Hot Spare muss im Status optimal, Standby sein.

.Über diese Aufgabe
Sie können die Zuweisung eines Ersatzlaufwerks, das derzeit für ein
ausgefallenes Laufwerk übernimmt, nicht aufheben. Wenn sich das Hot Spare
nicht im optimalen Status befindet, befolgen Sie die Recovery Guru-
Verfahren, um Probleme zu beheben, bevor Sie versuchen, die Zuweisung des
Laufwerks zu aufheben.

.Schritte
. Wählen Sie *Hardware*.
. Wenn die Grafik die Controller anzeigt, klicken Sie auf die
Registerkarte *Laufwerke*.
+
Die Grafik ändert sich, um die Laufwerke anstelle der Controller
anzuzeigen.

. Wählen Sie das Hot-Spare-Laufwerk (in rosa angezeigt) aus, das Sie die
Zuweisung aufheben möchten.
+
Wenn diagonale Linien durch den rosa Laufwerksschacht vorhanden sind, wird
das Hot Spare derzeit verwendet und kann nicht aufgehoben werden.

+
Das Kontextmenü des Laufwerks wird geöffnet.

. Wählen Sie aus der Dropdown-Liste des Laufwerks die Option *Hot Spare
aufheben* aus.
+
Das Dialogfeld zeigt alle Volume-Gruppen an, die durch Entfernen dieses
Hot Spare betroffen sind und wenn andere Hot Spares sie schützen.

. Bestätigen Sie die Zuweisung.
```

```
.Ergebnisse
Das Laufwerk wird an Unassigned (in grau dargestellt) zurückgegeben.



:leveloffset: -1


= Shelf-FAQs

:leveloffset: +1


[[ID94afe2168dbd59ee02c33bb28430bc87]]
= Was ist der Schutz vor Regalverlust und der Schutz vor
Schubladenverlust?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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.

[NOTE]
====
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 sind abhängig von der
Schutzmethode, wie in der folgenden Tabelle beschrieben:

[cols="1a,1a,1a"]
|===
| Ebene | Kriterien für den Schutz vor Shelf-Verlust | Mindestanzahl der
benötigten Shelves


 a|
Pool
 a|
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.
 a|
5



 a|
RAID 6
 a|
Die Volume-Gruppe enthält nicht mehr als zwei Laufwerke in einem einzelnen
Shelf.
 a|
3



 a|
RAID 3 oder RAID 5
 a|
Jedes Laufwerk in der Volume-Gruppe befindet sich in einem separaten
Shelf.
 a|
3



 a|
RAID 1
 a|
```

```
Jedes Laufwerk in einem RAID-1-Paar muss sich in einem separaten Shelf
befinden.
 a|
2



 a|
RAID 0
 a|
Shelf-Verlustschutz kann nicht erreicht werden.
 a|
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.

[NOTE]
====
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:

[cols="1a,1a,1a"]
|===
| Ebene | Kriterien für den Schutz vor Schubladenverlust | Mindestanzahl
der benötigten Schubladen



 a|
```

```
Pool
 a|
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.
 a|
5



 a|
RAID 6
 a|
Die Volume-Gruppe enthält nicht mehr als zwei Laufwerke in einem einzigen
Einschub.
 a|
3



 a|
RAID 3 oder RAID 5
 a|
Jedes Laufwerk in der Volume-Gruppe befindet sich in einem separaten
Einschub.
 a|
3



 a|
RAID 1
 a|
Jedes Laufwerk in einem gespiegelten Paar muss sich in einem separaten
Fach befinden.
 a|
2



 a|
```

```
RAID 0
 a|
Der Schutz vor Schubladenverlust kann nicht erreicht werden.
 a|
Keine Angabe

|===



[[IDf814c2960b0e4d9c54afe173e48b7b9b]]
= Was sind Akkulaufläufe?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Ein Lernzyklus ist ein automatischer Zyklus zum Kalibrieren der
intelligenten Akkuanzeige.

Ein Lernzyklus besteht aus folgenden Phasen:

* Kontrollierte Batterieentladung
* Ruheperiode
* Laden


Die Batterien werden bis zu einem vorgegebenen Schwellenwert entladen. In
dieser Phase wird die Batteriehuchte kalibriert.

Für einen Lernzyklus sind die folgenden Parameter erforderlich:

* Vollständig aufgeladene Batterien
* Keine überhitzten Batterien


Lernzyklen für Duplex-Controller-Systeme werden gleichzeitig ausgeführt.
Für Controller mit Sicherungsstrom aus mehr als einer Batterie oder einer
Reihe von Batteriezellen treten nacheinander Lernzyklen auf.

Die Lernzyklen werden in regelmäßigen Abständen, zur gleichen Zeit und am
selben Tag der Woche, automatisch gestartet. Das Intervall zwischen den
Zyklen wird in Wochen beschrieben.

[NOTE]
```

```
====
Ein Lernzyklus kann mehrere Stunden in Anspruch nehmen.

====



:leveloffset: -1


= Controller-FAQs

:leveloffset: +1


[[IDe5982577f9209761f7f76c388f61e0a7]]
= Was ist Auto-Negotiation?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die automatische Aushandlung ist die Möglichkeit einer
Netzwerkschnittstelle, ihre eigenen Verbindungsparameter (Geschwindigkeit
und Duplex) automatisch mit einer anderen Netzwerkschnittstelle zu
koordinieren.

Die automatische Aushandlung ist in der Regel die bevorzugte Einstellung
für die Konfiguration von Management-Ports. Wenn die Aushandlung jedoch
fehlschlägt, können falsch aufeinander abgestimmte Einstellungen der
Netzwerkschnittstelle die Netzwerkleistung erheblich beeinträchtigen. In
Fällen, in denen diese Bedingung nicht akzeptabel ist, sollten Sie die
Einstellungen der Netzwerkschnittstelle manuell auf eine korrekte
Konfiguration einstellen. Die automatische Aushandlung wird durch die
Ethernet-Management-Ports des Controllers durchgeführt. Die automatische
Aushandlung wird nicht von den iSCSI-Host-Bus-Adaptern durchgeführt.

[NOTE]
====
Wenn die automatische Aushandlung fehlschlägt, versucht der Controller,
eine Verbindung bei 10BASE-T, Halbduplex, herzustellen. Dies ist der
kleinste gemeinsame Nenner.

====
```

```
[[IDdb7b45a6cb10f49199281536391e5284]]
= Was ist eine statusfreie IPv6-Adressenkonfiguration?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Bei einer statusfreien automatischen Konfiguration erhalten Hosts keine
Adressen und andere Konfigurationsinformationen von einem Server.

Die statusfreie automatische Konfiguration in IPv6 bietet Link-lokale
Adressen, Multicasting und das Neighbor Discovery-Protokoll (ND). IPv6
kann die Schnittstellen-ID einer Adresse aus der zugrunde liegenden
Datenverbindungslayer-Adresse generieren.

Eine statusfreie automatische Konfiguration und eine statusorientierte
automatische Konfiguration ergänzen sich gegenseitig. Beispielsweise kann
der Host statusfreie Auto-Konfiguration verwenden, um seine eigenen
Adressen zu konfigurieren, aber verwenden Sie Stateful Auto-Configuration,
um andere Informationen abzurufen. Die zustandsorientierte automatische
Konfiguration ermöglicht Hosts, Adressen und andere
Konfigurationsinformationen von einem Server abzurufen. Internet Protocol
Version 6 (IPv6) definiert auch eine Methode, bei der alle IP-Adressen in
einem Netzwerk gleichzeitig neu nummeriert werden können. IPv6 definiert
eine Methode für Geräte im Netzwerk, um ihre IP-Adresse und andere
Parameter automatisch ohne Server zu konfigurieren.

Geräte führen die folgenden Schritte durch, wenn eine statusfreie
automatische Konfiguration verwendet wird:

. *Generieren Sie eine Link-local-Adresse* -- das Gerät erzeugt eine Link-
local-Adresse, die 10 Bit, gefolgt von 54 Nullen und gefolgt von der 64-
Bit-Schnittstellen-ID hat.
. *Testen Sie die Einzigartigkeit einer Link-local-Adresse* -- der Knoten
testet, um sicherzustellen, dass die von ihm erzeugte Link-local-Adresse
nicht bereits im lokalen Netzwerk verwendet wird. Der Knoten sendet
mithilfe des ND-Protokolls eine „Neighbor"-Aufforderung. Das lokale
Netzwerk wartet auf eine Meldung zur Anzeige des Nachbarn, die darauf
hinweist, dass bereits ein anderes Gerät die Link-local-Adresse verwendet.
In diesem Fall muss entweder eine neue Link-local-Adresse generiert
werden, oder die automatische Konfiguration schlägt fehl, und eine andere
Methode muss verwendet werden.
```

. *Zuweisen einer Link-lokalen Adresse* -- Wenn das Gerät den Eindeutigkeit-Test übergibt, weist das Gerät seiner IP-Schnittstelle die Link-lokale Adresse zu. Die Link-local Adresse kann für die Kommunikation im lokalen Netzwerk, aber nicht über das Internet verwendet werden.
. *Kontaktieren Sie den Router* -- der Knoten versucht, sich an einen lokalen Router zu wenden, um weitere Informationen zum Fortsetzen der Konfiguration zu erhalten. Dieser Kontakt wird entweder durch Abhören von regelmäßig von Routern gesendeten Routern-Werbemitteilungen oder durch Senden einer bestimmten Router-Nachricht ausgeführt, um einen Router um Informationen darüber zu bitten, was als Nächstes zu tun ist.
. *Anweisungen zum Knoten geben* -- der Router gibt dem Knoten Anweisungen, wie mit der automatischen Konfiguration fortzufahren. Alternativ teilt der Router dem Host mit, wie die globale Internetadresse ermittelt werden soll.
. *Konfigurieren Sie die globale Adresse* -- der Host konfiguriert sich mit seiner weltweit einzigartigen Internetadresse. Diese Adresse wird in der Regel aus einem Netzwerkpräfix gebildet, das dem Host vom Router bereitgestellt wird.

[[IDd38b54c404853cd783ef8b3f2b919641]]
= Welche Option wähle ich - DHCP- oder manuelle Konfiguration?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Die Standardmethode für die Netzwerkkonfiguration ist DHCP (Dynamic Host Configuration Protocol). Verwenden Sie diese Option immer, wenn Ihr Netzwerk keinen DHCP-Server hat.

[[ID78a43e1ebade4498398d3b3b67e63147]]
= Was ist ein DHCP-Server?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Dynamic Host Configuration Protocol (DHCP) ist ein Protokoll, das die

```
Aufgabe der Zuweisung einer IP-Adresse (Internet Protocol) automatisiert.

Jedem Gerät, das mit einem TCP/IP-Netzwerk verbunden ist, muss eine
eindeutige IP-Adresse zugewiesen werden. Zu diesen Geräten gehören die
Controller in Ihrem Speicher-Array.

Ohne DHCP gibt ein Netzwerkadministrator diese IP-Adressen manuell ein.
Wenn ein Client TCP/IP-Vorgänge starten muss, sendet der Client eine
Anforderung für Adressinformationen aus. Der DHCP-Server erhält die
Anforderung, weist eine neue Adresse für eine bestimmte Zeitspanne, die
als Leasing-Zeitraum bezeichnet wird, zu und sendet die Adresse an den
Client. Bei DHCP kann ein Gerät bei jeder Verbindung mit dem Netzwerk eine
andere IP-Adresse haben. In einigen Systemen kann sich die IP-Adresse des
Geräts auch dann ändern, wenn das Gerät noch angeschlossen ist.



[[ID05f0bb000f9c8f1ff4fbbf7ca197659b]]
= Wie konfiguriere ich meinen DHCP-Server?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie müssen einen DHCP-Server (Dynamic Host Configuration Protocol)
konfigurieren, damit die Controller im Speicher-Array statische IP-
Adressen (Internet Protocol) verwenden können.

Die IP-Adressen, die Ihrem DHCP-Server zugewiesen werden, sind im
Allgemeinen dynamisch und können sich ändern, da sie über einen
Leasingzeitraum verfügen, der abgelaufen ist. Einige Geräte, zum Beispiel
Server und Router, müssen statische Adressen verwenden. Die Controller im
Speicher-Array benötigen auch statische IP-Adressen.

Informationen zum Zuweisen statischer Adressen finden Sie in der
Dokumentation für Ihren DHCP-Server.



[[ID77f2189ca9c4a7cdd1b0256b42794459]]
= Warum muss ich die Controller-Netzwerkkonfiguration ändern?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Sie müssen die Netzwerkkonfiguration für jeden Controller festlegen: IP-
Adresse (Internet Protocol), Subnetzmaske (Subnetzmaske) und Gateway –
wenn Sie Out-of-Band-Management verwenden.

Sie können die Netzwerkkonfiguration mithilfe eines DHCP-Servers (Dynamic
Host Configuration Protocol) festlegen. Wenn Sie keinen DHCP-Server
verwenden, müssen Sie die Netzwerkkonfiguration manuell eingeben.



[[ID83a1a5a82369c9267188c6e8c09e9de4]]
= Wo erhalte ich die Netzwerkkonfiguration?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die IP-Adresse (Internet Protocol), die Subnetzmaske
(Subnetzmaske) und Gateway-Informationen von Ihrem Netzwerkadministrator
abrufen.

Sie benötigen diese Informationen, wenn Sie Ports auf den Controllern
konfigurieren.



[[ID2e8535cbcbf5960e95554b350d61d5fa]]
= Was sind ICMP PING Antworten?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Internet Control Message Protocol (ICMP) ist eines der Protokolle der
TCP/IP-Suite.

Der `ICMP echo request` Und das(`ICMP echo reply` Nachrichten sind
allgemein bekannt als `ping` Nachrichten. `Ping` Ist ein
Fehlerbehebungstool, das von Systemadministratoren verwendet wird, um die
Verbindung zwischen Netzwerkgeräten manuell zu testen und auch auf
```

```
Netzwerkverzögerung und Paketverlust zu testen. Der `ping` Befehl sendet
ein `ICMP echo request` Auf ein Gerät im Netzwerk, und das Gerät reagiert
sofort mit ein(`ICMP echo reply`. Manchmal erfordert die
Netzwerksicherheitsrichtlinie eines Unternehmens `ping` (`ICMP echo
reply`Auf allen Geräten zu deaktivieren, um sie durch unbefugte Personen
schwieriger zu entdecken.



[[IDe4ea4821951b71f7a0c5e3f475c690dd]]
= Wann sollte ich die Portkonfiguration oder den iSNS-Server vom DHCP-
Server aktualisieren?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Aktualisieren Sie den DHCP-Server jederzeit, wenn der Server geändert oder
aktualisiert wird, und die für das aktuelle Speicher-Array und das
Speicherarray, das Sie verwenden möchten, relevanten DHCP-Informationen
wurden geändert.

Aktualisieren Sie insbesondere die Portkonfiguration oder den iSNS-Server
vom DHCP-Server, wenn Sie wissen, dass der DHCP-Server unterschiedliche
Adressen zugewiesen.

[NOTE]
====
Die Aktualisierung einer Portkonfiguration ist für alle iSCSI-Verbindungen
an diesem Port destruktiv.

====



[[ID466d9f2c7b6b0082aa37d971939ceb0b]]
= Was soll ich nach dem Konfigurieren der Management-Ports tun?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

```
Wenn Sie die IP-Adresse für das Speicher-Array geändert haben, möchten Sie
möglicherweise die Ansicht des globalen Arrays in SANtricity Unified
Manager aktualisieren.

Um die Ansicht des globalen Arrays in Unified Manager zu aktualisieren,
öffnen Sie die Schnittstelle und gehen Sie zum Menü:Verwalten[Entdecken].

Wenn Sie noch den SANtricity-Speicher-Manager verwenden, gehen Sie zum
Enterprise Management-Fenster (EMW), wo Sie die neue IP-Adresse entfernen
und erneut hinzufügen müssen.



[[IDc27bcee5d11d47d8f64325052f7b38af]]
= Warum befindet sich das Storage-System im nicht optimalen Modus?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Ein Speichersystem im nicht optimalen Modus ist auf einen ungültigen
Konfigurationsstatus des Systems zurückzuführen. Trotz dieses Status wird
der normale I/O-Zugriff auf vorhandene Volumes vollständig unterstützt,
der SANtricity System Manager untersagt jedoch einige Vorgänge.

Ein Storage-System könnte aus einem der folgenden Gründe auf eine
ungültige Systemkonfiguration überführen:

* Der Controller ist nicht mehr konform, möglicherweise weil er einen
falschen Untermodell-ID-Code (SMID) hat oder die Obergrenze der Premium-
Features überschritten hat.
* Es wird ein interner Servicevorgang ausgeführt, z. B. ein Download der
Laufwerk-Firmware.
* Der Controller hat den Paritätsfehlerschwellenwert überschritten und
tritt gesperrt auf.
* Eine allgemeine Sperrbedingung ist aufgetreten.




:leveloffset: -1


= ISCSI FAQs
```

```
:leveloffset: +1


[[IDc4ef57f5605298c998e4bb25740a3535]]
= Was passiert, wenn ich einen iSNS Server für die Registrierung verwende?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Informationen zum Internet Storage Name Service (iSNS)-Server
verwendet werden, können die Hosts (Initiatoren) so konfiguriert werden,
dass sie den iSNS-Server abfragen, um Informationen aus dem Ziel (den
Controllern) abzurufen.

Mit dieser Registrierung erhält der iSNS-Server den iSCSI-qualifizierten
Namen (IQN) und die Portinformationen des Controllers und ermöglicht
Abfragen zwischen den Initiatoren (iSCSI-Hosts) und Zielen (Controllern).



[[ID8ef913f3c8c55039b7cc6474d31aa4a5]]
= Welche Registrierungsmethoden werden für iSCSI automatisch unterstützt?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die iSCSI-Implementierung unterstützt entweder die iSCSI-
Ermittlungsmethode (Internet Storage Name Service, iSNS) oder die
Verwendung des Befehls Send Targets.

Die iSNS-Methode ermöglicht die iSNS-Erkennung zwischen den Initiatoren
(iSCSI-Hosts) und den Zielen (den Controllern). Sie registrieren den
Zielcontroller, um dem iSNS-Server den iSCSI-qualifizierten Namen (IQN)
und die Portinformationen des Controllers bereitzustellen.

Wenn Sie iSNS nicht konfigurieren, kann der iSCSI-Host den Befehl Ziele
senden während einer iSCSI-Erkennungssitzung senden. Als Antwort gibt der
Controller die Portinformationen zurück (z. B. Ziel-IQN, Port-IP-Adresse,
Listening-Port und Ziel-Portgruppe). Diese Ermittlungsmethode ist nicht
erforderlich, wenn Sie iSNS verwenden, da der Host-Initiator die Ziel-IPs
vom iSNS-Server abrufen kann.
```

```
[[ID31d33c3aad9ff1ebe228a5734658c094]]
= Wie interpretiere ich iSER-over-InfiniBand-Statistiken?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Das Dialogfeld „iSER-over-InfiniBand-Statistiken“ zeigt Statistiken zu
lokalen Zielen (Protokollen) und iSER-over-InfiniBand-Schnittstellen (IB)
an. Alle Statistiken sind schreibgeschützt und können nicht festgelegt
werden.

* *Statistiken zu lokalen Zielen (Protokoll)* -- stellt Statistiken für
das iSER-over-InfiniBand-Ziel bereit, das den Zugriff auf die
Speichermedien auf Blockebene anzeigt.
* *ISER-over-InfiniBand-Interface-Statistik* -- stellt Statistiken für
alle iSER-over-InfiniBand-Ports auf der InfiniBand-Schnittstelle bereit,
die Performance-Statistiken und Link-Fehlerinformationen zu den einzelnen
Switch-Ports enthalten.


Sie können jede dieser Statistiken als RAW-Statistiken oder als Baseline-
Statistiken anzeigen. RAW-Statistiken sind alle Statistiken, die seit dem
Start der Controller gesammelt wurden. Baseline-Statistiken sind
zeitpunktgenaue Statistiken, die seit dem Festlegen der Baseline-Zeit
erfasst wurden.



[[ID6c71e22dfc6010edb51762acc343820e]]
= Was muss ich noch tun, um iSER over InfiniBand zu konfigurieren oder zu
diagnostizieren?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
In der folgenden Tabelle sind die Funktionen von SANtricity System Manager
aufgeführt, mit denen Sie iSER-over-InfiniBand-Sessions konfigurieren und
```

```
managen können.

[NOTE]
====
Die iSER-over-InfiniBand-Einstellungen sind nur verfügbar, wenn der
Controller Ihres Storage-Arrays einen iSER-over-InfiniBand-Host-
Management-Port umfasst.

====
[cols="35h,~"]
|===
| Aktion | Standort


 a|
Konfigurieren Sie iSER-over-InfiniBand-Ports
 a|
. Wählen Sie *Hardware*.
. Wählen Sie die Registerkarte *Controller & Komponenten* aus.
. Wählen Sie einen Controller aus.
. Wählen Sie *iSER-over-InfiniBand-Ports konfigurieren*.


Oder

. Wählen Sie Menü:Einstellungen[System].
. Scrollen Sie nach unten nach *iSER über InfiniBand-Einstellungen*, und
wählen Sie dann *iSER über InfiniBand-Ports konfigurieren* aus.




 a|
Zeigen Sie iSER-over-InfiniBand-Statistiken an
 a|
. Wählen Sie Menü:Einstellungen[System].
. Scrollen Sie nach unten nach *iSER über InfiniBand-Einstellungen* und
wählen Sie dann *Anzeigen iSER über InfiniBand-Statistik* aus.


|===



[[IDc5d1ecd7f9709386c745a3d17e7f14bd]]
= Was muss ich sonst noch tun, um iSCSI zu konfigurieren oder zu
diagnostizieren?
```

```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
ISCSI-Sitzungen können bei Hosts oder Remote-Storage-Arrays in einer
asynchronen Spiegelbeziehung durchgeführt werden. In den folgenden
Tabellen sind die Funktionen von SANtricity System Manager aufgeführt, mit
denen Sie diese iSCSI-Sitzungen konfigurieren und verwalten können.

[NOTE]
====
Die iSCSI-Einstellungen sind nur verfügbar, wenn Ihr Speicher-Array iSCSI
unterstützt.

====


== Konfigurieren Sie iSCSI

[cols="1a,1a"]
|===
| Aktion | Standort


 a|
ISCSI-Einstellungen verwalten
 a|
. Wählen Sie Menü:Einstellungen[System].
. Blättern Sie nach unten zu *iSCSI-Einstellungen*, um alle
Verwaltungsfunktionen anzuzeigen.




 a|
Konfigurieren Sie die iSCSI-Ports
 a|
. Wählen Sie *Hardware*.
. Wählen Sie die Registerkarte *Controller & Komponenten* aus.
. Wählen Sie einen Controller aus.
. Wählen Sie *iSCSI-Ports konfigurieren*.
```

```
 a|
Legen Sie den Host-CHAP-Schlüssel fest
 a|
. Wählen Sie Menü:Einstellungen[System].
. Blättern Sie nach unten zu *iSCSI-Einstellungen*, und wählen Sie dann
*Authentifizierung konfigurieren*.


Oder

. Wählen Sie Menü:Storage[Hosts].
. Wählen Sie ein Hostmitglied aus.
. Klicken Sie auf Menü:Registerkarte Einstellungen
anzeigen/bearbeiten[Host Ports].


|===


== ISCSI diagnostizieren

[cols="1a,1a"]
|===
| Aktion | Standort


 a|
Anzeigen oder Beenden von iSCSI-Sitzungen
 a|
. Wählen Sie Menü:Einstellungen[System].
. Scrollen Sie nach unten zu *iSCSI-Einstellungen* und wählen Sie dann
*iSCSI-Sitzungen anzeigen/beenden* aus.


Oder

. Wählen Sie MENU:Support[Support Center > Diagnose].
. Wählen Sie *Anzeigen/Beenden von iSCSI-Sitzungen*.




 a|
Anzeigen von iSCSI-Statistiken
 a|
```

```
. Wählen Sie Menü:Einstellungen[System].
. Scrollen Sie nach unten zu *iSCSI-Einstellungen* und wählen Sie dann
*iSCSI-Statistikpakete anzeigen* aus.


Oder

. Wählen Sie MENU:Support[Support Center > Diagnose].
. Wählen Sie *Anzeigen von iSCSI-Statistikpaketen* aus.


|===



:leveloffset: -1


= NVMe FAQs

:leveloffset: +1


[[ID07debf5dedf0fd860048d8e56950790e]]
= Wie interpretiere ich NVMe over Fabrics Statistiken?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Im Dialogfeld „Statistik von NVMe over Fabrics anzeigen“ werden
Statistiken für das NVMe-Subsystem und die RDMA-Schnittstelle angezeigt.
Alle Statistiken sind schreibgeschützt und können nicht festgelegt werden.

* *NVMe Subsystem-Statistik* -- zeigt Statistiken für den NVMe-Controller
und seine Queue an. Der NVMe Controller stellt einen Zugriffspfad zwischen
einem Host und den Namespaces im Storage-Array bereit. Sie können die
NVMe-Subsystem-Statistiken für Elemente wie Verbindungsfehler,
Zurücksetzen und Herunterfahren überprüfen. Für weitere Informationen über
diese Statistiken klicken Sie auf *Legende anzeigen für
Tabellenüberschriften*.
* *RDMA Interface Statistics* -- stellt Statistiken für alle NVMe over
Fabrics Ports auf der RDMA-Schnittstelle bereit, die Performance-
Statistiken und Link-Fehlerinformationen enthält, die mit jedem Switch-
Port verbunden sind. Diese Registerkarte wird nur angezeigt, wenn NVMe
```

```
over Fabrics-Ports verfügbar sind. Für weitere Informationen zu den
Statistiken klicken Sie auf *Legende anzeigen für Tabellenüberschriften*.


Sie können jede dieser Statistiken als RAW-Statistiken oder als Baseline-
Statistiken anzeigen. RAW-Statistiken sind alle Statistiken, die seit dem
Start der Controller gesammelt wurden. Baseline-Statistiken sind
zeitpunktgenaue Statistiken, die seit dem Festlegen der Baseline-Zeit
erfasst wurden.



[[IDd63b6643cae632f2dd4d6b2f4b9aa16f]]
= Was muss ich sonst noch tun, um NVMe over InfiniBand zu konfigurieren
oder zu diagnostizieren?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
In der folgenden Tabelle sind die Funktionen von SANtricity System Manager
aufgeführt, mit denen Sie NVMe over InfiniBand-Sessions konfigurieren und
managen können.

[NOTE]
====
Die NVMe-over-InfiniBand-Einstellungen sind nur verfügbar, wenn der
Controller des Storage-Arrays einen NVMe-over-InfiniBand-Port besitzt.

====
[cols="35h,~"]
|===
| Aktion | Standort


 a|
Konfigurieren Sie NVMe-over-InfiniBand-Ports
 a|
. Wählen Sie *Hardware*.
. Wählen Sie die Registerkarte *Controller & Komponenten* aus.
. Wählen Sie einen Controller aus.
. Wählen Sie *NVMe über InfiniBand-Ports konfigurieren* aus.
```

```
Oder

. Wählen Sie Menü:Einstellungen[System].
. Scrollen Sie nach unten zu *NVMe over InfiniBand settings* und wählen
Sie dann *Configure NVMe over InfiniBand Ports* aus.




 a|
Anzeigen der NVMe-over-InfiniBand-Statistiken
 a|
. Wählen Sie Menü:Einstellungen[System].
. Scrollen Sie nach unten zu *NVMe over InfiniBand settings* und wählen
Sie dann *View NVMe over Fabrics Statistics* aus.


|===



[[ID1f234eb057e3f9089d3560ec14ce221c]]
= Was muss ich sonst noch tun, um NVMe over RoCE zu konfigurieren oder zu
diagnostizieren?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
NVMe over RoCE kann über die Seiten für Hardware und Einstellungen
konfiguriert und gemanagt werden.

[NOTE]
====
Die NVMe-over-RoCE-Einstellungen sind nur verfügbar, wenn der Controller
des Storage-Arrays einen NVMe-over-RoCE-Port umfasst.

====
[cols="35h,~"]
|===
| Aktion | Standort


 a|
```

```
Konfigurieren Sie NVMe over RoCE-Ports
 a|
. Wählen Sie *Hardware*.
. Wählen Sie die Registerkarte *Controller & Komponenten* aus.
. Wählen Sie einen Controller aus.
. Wählen Sie *NVMe over RoCE Ports konfigurieren* aus.


Oder

. Wählen Sie Menü:Einstellungen[System].
. Scrollen Sie nach unten zu *NVMe over RoCE settings* und wählen Sie dann
*Configure NVMe over RoCE Ports* aus.




 a|
Anzeigen der NVMe over Fabrics Statistiken
 a|
. Wählen Sie Menü:Einstellungen[System].
. Scrollen Sie nach unten zu *NVMe over RoCE settings* und wählen Sie dann
*View NVMe over Fabrics Statistics* aus.


|===



[[ID28b6dc8cb2a169e359c270392f5e6e17]]
= Warum gibt es zwei IP-Adressen für einen physischen Port?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Das EF600 Storage-Array kann zwei HICs umfassen – einen externen und einen
internen.

In dieser Konfiguration ist die externe HIC mit einer internen HIC-
Zusatzkarte verbunden. Jeder physische Port, auf den Sie über die externe
HIC zugreifen können, hat einen zugeordneten virtuellen Port von der
internen HIC.

Um eine maximale 200-GB-Performance zu erreichen, müssen Sie sowohl den
```

```
physischen als auch den virtuellen Ports eine eindeutige IP-Adresse
zuweisen, damit der Host Verbindungen zu jedem Server herstellen kann.
Wenn Sie dem virtuellen Port keine IP-Adresse zuweisen, läuft die HIC mit
etwa der Hälfte ihrer fähigen Geschwindigkeit.



[[ID382453f4a6eb41f8a19032debda7cabf]]
= Warum gibt es zwei Parametersätze für einen physischen Port?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Das EF600 Storage-Array kann zwei HICs umfassen – einen externen und einen
internen.

In dieser Konfiguration ist die externe HIC mit einer internen HIC-
Zusatzkarte verbunden. Jeder physische Port, auf den Sie über die externe
HIC zugreifen können, hat einen zugeordneten virtuellen Port von der
internen HIC.

Um eine maximale 200-GB-Performance zu erreichen, müssen Sie Parameter für
die physischen und virtuellen Ports zuweisen, damit der Host Verbindungen
zu jedem herstellen kann. Wenn Sie dem virtuellen Port keine Parameter
zuweisen, läuft die HIC mit ungefähr halber Geschwindigkeit.



:leveloffset: -1


= FAQs zu Laufwerken

:leveloffset: +1


[[ID7729192e397ca0a3cb2c0ac814c5508d]]
= Was ist eine Hot-Spare-Festplatte?
:allow-uri-read:
:icons: font
:relative_path: ./sm-storage/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
Hot Spares fungieren als Standby-Laufwerke in RAID 1-, RAID 5- oder RAID 6-Volume-Gruppen. Es handelt sich dabei um voll funktionsfähige Laufwerke, die keine Daten enthalten. Wenn ein Laufwerk in der Volume-Gruppe ausfällt, rekonstruiert der Controller die Daten vom ausgefallenen Laufwerk automatisch auf eine Hot Spare-Festplatte.

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.

Ein Hot-Spare-Laufwerk ist nicht einer bestimmten Volume-Gruppe zugewiesen. Stattdessen können Sie ein Hot-Spare-Laufwerk für alle ausgefallenen Laufwerke im Storage-Array mit derselben Kapazität oder kleinerer Kapazität verwenden. Ein Hot-Spare-Laufwerk muss vom gleichen Medientyp (HDD oder SSD) sein wie die Laufwerke, die es schützt.

[NOTE]
====
Hot-Spare-Festplatten werden mit Pools nicht unterstützt. Anstatt Hot-Spare-Festplatten nutzen Pools die freie Kapazität in jedem Laufwerk, das den Pool umfasst.

====

[[ID397da828c10d5a0792dffddea609df5f]]
= Was ist Erhaltungskapazität?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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.

[[IDde649bb56b7f3407b3792ab745e1c69b]]
= Warum sollte ich ein Laufwerk logisch ersetzen?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Wenn ein Laufwerk ausfällt oder Sie es aus einem anderen Grund ersetzen möchten und ein nicht zugewiesenes Laufwerk im Speicher-Array vorhanden ist, können Sie das ausgefallene Laufwerk logisch durch das nicht zugewiesene Laufwerk ersetzen. Wenn Sie kein nicht zugewiesenes Laufwerk haben, können Sie stattdessen das Laufwerk physisch ersetzen.

Die Daten aus dem Originallaufwerk werden kopiert oder auf das Ersatzlaufwerk rekonstruiert.

[[ID5a675b0744fea4b9aefeb81c7f37bf7e]]
= Wo kann ich den Status eines Laufwerks sehen, der derzeit rekonstruiert wird?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können den Rekonstruktionsstatus des Laufwerks über die Konsole „Operations in Progress“ anzeigen.

Klicken Sie auf der Startseite oben rechts auf den Link *Vorgänge in Bearbeitung anzeigen*.

Je nach Laufwerk kann die vollständige Rekonstruktion sehr viel Zeit in

```
Anspruch nehmen. Wenn sich die Volume-Eigentümerschaft geändert hat, kann
anstelle der schnellen Wiederherstellung eine vollständige Rekonstruktion
stattfinden.



:leveloffset: -1


:leveloffset: -1


= Meldungen

:leveloffset: +1


[[ID21586e50af483faef01dde4597dc7bcd]]
= Übersicht über Warnungen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können SANtricity System Manager so konfigurieren, dass Speicher-
Array-Warnmeldungen per E-Mail, SNMP-Traps und Syslog-Meldungen gesendet
werden.



== Was sind Warnmeldungen?

_Alerts_ benachrichtigt Administratoren über wichtige Ereignisse, die auf
dem Storage-Array auftreten. Zu den Ereignissen zählen beispielsweise
Probleme mit dem Ausfall der Batterie, der Wechsel von optimal zu Offline
oder Redundanzfehler im Controller. Alle kritischen Ereignisse werden als
„alertable“, zusammen mit einigen Warn- und Informationsereignissen
betrachtet.

Weitere Informationen:

* xref:{relative_path}how-alerts-work.html["Funktionsweise von
Warnmeldungen"]
* xref:{relative_path}alerts-terminology.html["Warnmeldungen zur
```

```
Terminologie"]



== Wie konfiguriere ich Benachrichtigungen?

Sie können Warnungen so konfigurieren, dass sie als Nachricht an eine oder
mehrere E-Mail-Adressen gesendet werden, als SNMP-Trap an einen SNMP-
Server oder als Nachricht an einen Syslog-Server. Die Alarmkonfiguration
ist über das Menü:Einstellungen[Warnmeldungen] verfügbar.

Weitere Informationen:

* xref:{relative_path}configure-mail-server-and-recipients-for-
alerts.html["Konfigurieren Sie E-Mail-Server und Empfänger für
Warnmeldungen"]
* xref:{relative_path}configure-syslog-server-for-
alerts.html["Konfigurieren Sie den Syslog-Server für Warnmeldungen"]
* xref:{relative_path}configure-snmp-alerts.html["Konfigurieren von SNMP-
Warnmeldungen"]




== Verwandte Informationen

Weitere Informationen zu Konzepten im Zusammenhang mit Warnmeldungen:

* xref:{relative_path}../sm-support/overview-event-log.html["Übersicht
über das Ereignisprotokoll"]
* xref:{relative_path}why-are-timestamps-inconsistent-between-the-array-
and-alerts.html["Inkonsistente Zeitstempel"]




= Konzepte

:leveloffset: +1


[[IDcbd10f6b04bc9bd6557496d1a9cfe2d0]]
= Funktionsweise von Warnmeldungen
:allow-uri-read:
:experimental:
:icons: font
```

```
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Warnungen benachrichtigen Administratoren über wichtige Ereignisse im
Speicher-Array. Warnmeldungen können per E-Mail, SNMP-Traps und Syslog
gesendet werden.

Die Warnmeldungen werden wie folgt bearbeitet:

. Ein Administrator konfiguriert mindestens eine der folgenden
Warnmeldungsmethoden in System Manager:
+
** *E-Mail* -- Nachrichten werden an E-Mail-Adressen gesendet.
** *SNMP* -- SNMP-Traps werden an einen SNMP-Server gesendet.
** *Syslog* -- Nachrichten werden an einen Syslog-Server gesendet.


. Wenn die Ereignisüberwachung des Speicherarrays ein Problem erkennt,
schreibt sie Informationen über dieses Problem in das Ereignisprotokoll
(verfügbar über Menü:Support[Ereignisprotokoll]). Beispielsweise können
Probleme auftreten, beispielsweise ein Batterieausfall, eine Komponente,
die von optimal nach Offline verschoben wird oder Redundanzfehler im
Controller sind.
. Wenn der Ereignismonitor feststellt, dass das Ereignis „ertabbar“ ist,
sendet er eine Benachrichtigung mit den konfigurierten Alarmmethoden (E-
Mail, SNMP und/oder Syslog). Alle kritischen Ereignisse werden als
„alertable“, zusammen mit einigen Warn- und Informationsereignissen
betrachtet.




== Konfiguration von Warnungen

Sie können Benachrichtigungen über den Einrichtungsassistenten (nur für E-
Mail-Benachrichtigungen) oder über die Seite „Meldungen“ konfigurieren. Um
die aktuelle Konfiguration zu überprüfen, rufen Sie
Menü:Einstellungen[Alarme] auf.

Im Feld „Meldungen“ wird die Konfiguration der Warnmeldungen angezeigt.
Dabei kann es sich um eine der folgenden Optionen handelt:

* Nicht konfiguriert.
* Konfiguriert; mindestens eine Alarmmethode ist eingerichtet. Um zu
bestimmen, welche Alarmmethoden konfiguriert sind, zeigen Sie den Cursor
```

```
auf die Kachel.



== Warnmeldungsinformationen

Warnmeldungen können die folgenden Informationstypen enthalten:

* Name des Speicher-Arrays.
* Ereignistyp, der mit einem Eintrag im Ereignisprotokoll zusammenhängt.
* Datum und Uhrzeit des Ereignisses.
* Kurze Beschreibung der Veranstaltung.


[NOTE]
====
Syslog-Warnungen folgen dem RFC 5424-Messaging-Standard.

====



[[IDff58e84c54720ac2bc15081c975da6d8]]
= Warnmeldungen zur Terminologie
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Erfahren Sie, wie die Warnmeldungs-Bedingungen auf Ihr Storage Array
angewendet werden.

[cols="25h,~"]
|===
| Komponente | Beschreibung


 a|
Ereignisüberwachung
 a|
Die Ereignisüberwachung befindet sich im Storage-Array und wird als
Hintergrundaufgabe ausgeführt. Wenn die Ereignisüberwachung Anomalien im
Storage Array erkennt, schreibt sie Informationen zu den Problemen in das
Ereignisprotokoll. Zu den Problemen zählen beispielsweise Ereignisse wie
```

Batteriefehler, der Wechsel von optimal zu Offline oder Redundanzfehler im Controller. Wenn der Ereignismonitor feststellt, dass das Ereignis „ertabbar“ ist, sendet er eine Benachrichtigung mit den konfigurierten Alarmmethoden (E-Mail, SNMP und/oder Syslog). Alle kritischen Ereignisse werden als „alertable“, zusammen mit einigen Warn- und Informationsereignissen betrachtet.

 a|
Mailserver
 a|
Der Mail-Server wird zum Senden und Empfangen von E-Mail-Warnungen verwendet. Der Server verwendet das Simple Mail Transfer Protocol (SMTP).

 a|
SNMP
 a|
Das Simple Network Management Protocol (SNMP) ist ein internetbasiertes Protokoll, das zur Verwaltung und gemeinsamen Nutzung von Informationen zwischen Geräten in IP-Netzwerken verwendet wird.

 a|
SNMP-Trap
 a|
Ein SNMP-Trap ist eine Benachrichtigung, die an einen SNMP-Server gesendet wird. Der Trap enthält Informationen zu wichtigen Problemen mit dem Speicher-Array.

 a|
SNMP-Trap-Ziel
 a|
Ein SNMP-Trap-Ziel ist eine IPv4- oder IPv6-Adresse des Servers, auf dem ein SNMP-Dienst ausgeführt wird.

 a|
Community-Name
 a|
Ein Community-Name ist eine Zeichenfolge, die wie ein Kennwort für die

```
Netzwerkserver in einer SNMP-Umgebung fungiert.



 a|
MIB-Datei
 a|
Die Management Information Base (MIB)-Datei definiert die Daten, die im
Speicher-Array überwacht und verwaltet werden. Sie muss mit der SNMP-
Dienst-Anwendung auf dem Server kopiert und kompiliert werden. Diese MIB-
Datei ist mit der System Manager-Software auf der Support-Website
verfügbar.



 a|
MIB-Variablen
 a|
MIB-Variablen (Management Information Base) können Werte wie den Namen des
Speicherarrays, den Array-Speicherort und einen Ansprechpartner als
Antwort auf SNMP GetRequests zurückgeben.



 a|
Syslog
 a|
Syslog ist ein Protokoll, das von Netzwerkgeräten zum Senden von
Ereignismeldungen an einen Protokollierungsserver verwendet wird.



 a|
UDP
 a|
Das User Datagram Protocol (UDP) ist ein Protokoll der Transportschicht,
das eine Quell- und Zielportnummer in ihren Paketheader angibt.

|===



:leveloffset: -1


= Verwalten von E-Mail-Warnmeldungen
```

```
:leveloffset: +1


[[ID8ae6a4972b34f53e1779bba06f203d38]]
= Konfigurieren Sie E-Mail-Server und Empfänger für Warnmeldungen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um E-Mail-Benachrichtigungen zu konfigurieren, müssen Sie eine E-Mail-
Serveradresse und die E-Mail-Adressen der Warnungsempfänger angeben. Es
sind bis zu 20 E-Mail-Adressen zulässig.

.Bevor Sie beginnen
* Die Adresse des Mail-Servers muss vorhanden sein. Bei der Adresse kann
es sich um eine IPv4- oder IPv6-Adresse oder einen vollqualifizierten
Domänennamen handeln.
+
[NOTE]
====
Um einen vollständig qualifizierten Domänennamen zu verwenden, müssen Sie
auf beiden Controllern einen DNS-Server konfigurieren. Sie können einen
DNS-Server auf der Seite Hardware konfigurieren.

====
* Die als Alarmsender zu verwendenden E-Mail-Adresse muss verfügbar sein.
Dies ist die Adresse, die im Feld „von“ der Warnmeldung angezeigt wird. Im
SMTP-Protokoll wird eine Absenderadresse benötigt; ohne diese ergibt sich
ein Fehler.
* Die E-Mail-Adresse(n) der Warnungsempfänger muss verfügbar sein. Der
Empfänger ist in der Regel eine Adresse für einen Netzwerkadministrator
oder Speicheradministrator. Sie können bis zu 20 E-Mail-Adressen eingeben.


.Über diese Aufgabe
Diese Aufgabe beschreibt die Konfiguration des E-Mail-Servers, die Eingabe
von E-Mail-Adressen für den Absender und die Empfänger und das Testen
aller von der Seite Warnungen eingegebenen E-Mail-Adressen.

[NOTE]
====
E-Mail-Benachrichtigungen können auch über den Einrichtungsassistenten
```

konfiguriert werden.

====
.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *E-Mail* aus.
+
Wenn noch kein E-Mail-Server konfiguriert ist, wird auf der Registerkarte E-Mail „Mailserver konfigurieren“ angezeigt.

. Wählen Sie *E-Mail-Server Konfigurieren*.
+
Das Dialogfeld Mailserver konfigurieren wird geöffnet.

. Geben Sie die Informationen zum Mail-Server ein, und klicken Sie dann auf *Speichern*.
+
** *Mail-Server-Adresse* -- Geben Sie einen vollständig qualifizierten Domainnamen, eine IPv4-Adresse oder eine IPv6-Adresse des Mail-Servers ein.
+
[NOTE]
====
Um einen vollständig qualifizierten Domänennamen zu verwenden, müssen Sie auf beiden Controllern einen DNS-Server konfigurieren. Sie können einen DNS-Server auf der Seite Hardware konfigurieren.

====
** *E-Mail-Absender-Adresse* -- Geben Sie eine gültige E-Mail-Adresse ein, die als Absender der E-Mail verwendet werden soll. Diese Adresse wird im Feld „von“ der E-Mail-Nachricht angezeigt.
** *Verschlüsselung* -- Wenn Sie Nachrichten verschlüsseln möchten, wählen Sie für den Verschlüsselungstyp entweder *SMTPS* oder *STARTTLS* aus und wählen Sie dann die Portnummer für verschlüsselte Nachrichten aus. Wählen Sie andernfalls * Keine*.
** *Benutzername und Passwort* -- Geben Sie bei Bedarf einen Benutzernamen und ein Passwort für die Authentifizierung mit dem ausgehenden Absender und dem Mail-Server ein.
** *Kontaktinformationen in E-Mail einfügen* -- um die Kontaktdaten des Absenders in die Warnmeldung aufzunehmen, wählen Sie diese Option aus, und geben Sie dann einen Namen und eine Telefonnummer ein.
+
Nachdem Sie auf *Speichern* geklickt haben, werden die E-Mail-Adressen auf der Seite Warnungen auf der Registerkarte E-Mail angezeigt.

```
. Wählen Sie *E-Mails Hinzufügen*.
+
Das Dialogfeld E-Mails hinzufügen wird geöffnet.

. Geben Sie eine oder mehrere E-Mail-Adressen für die Empfänger der
Warnmeldung ein, und klicken Sie dann auf *Hinzufügen*.
+
Die E-Mail-Adressen werden auf der Seite „Meldungen“ angezeigt.

. Wenn Sie sicherstellen möchten, dass die E-Mail-Adressen gültig sind,
klicken Sie auf *Alle E-Mails testen*, um Testmeldungen an die Empfänger
zu senden.


.Ergebnisse
Nachdem Sie E-Mail-Alarme konfiguriert haben, sendet der Ereignismonitor
immer dann E-Mail-Nachrichten an die angegebenen Empfänger.



[[ID13996af5587d27ba5942bd8b3377dc25]]
= E-Mail-Adressen für Warnmeldungen bearbeiten
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die E-Mail-Adressen der Empfänger, die E-Mail-
Benachrichtigungen erhalten, ändern.

.Bevor Sie beginnen
Die E-Mail-Adresse, die Sie bearbeiten möchten, muss auf der Registerkarte
„E-Mail“ der Seite „Benachrichtigungen“ definiert sein.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *E-Mail* aus.
. Wählen Sie in der Tabelle *E-Mail-Adresse* die Adresse aus, die Sie
ändern möchten, und klicken Sie dann rechts auf das Symbol *Bearbeiten*
(Bleistift).
+
Die Zeile wird zu einem bearbeitbaren Feld.

. Geben Sie eine neue Adresse ein, und klicken Sie auf das Symbol
```

```
*Speichern* (Häkchen).
+
[NOTE]
====
Wenn Sie die Änderungen abbrechen möchten, wählen Sie das Symbol
*Abbrechen* (X).

====


.Ergebnisse
Auf der Registerkarte „E-Mail“ der Seite „Meldungen“ werden die
aktualisierten E-Mail-Adressen angezeigt.



[[ID14b61e9f9628e8b954920251657c4aa8]]
= Fügen Sie E-Mail-Adressen für Warnungen hinzu
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können bis zu 20 Empfänger für E-Mail-Benachrichtigungen hinzufügen.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *E-Mail* aus.
. Wählen Sie *E-Mails Hinzufügen*.
+
Das Dialogfeld E-Mails hinzufügen wird geöffnet.

. Geben Sie in das leere Feld eine neue E-Mail-Adresse ein. Wenn Sie mehr
als eine Adresse hinzufügen möchten, wählen Sie *Weitere E-Mail
hinzufügen*, um ein anderes Feld zu öffnen.
. Klicken Sie Auf *Hinzufügen*.


.Ergebnisse
Auf der Registerkarte „E-Mail“ der Seite „Meldungen“ werden die neuen E-
Mail-Adressen angezeigt.
```

```
[[IDdf47507eba1ef2683348a62373237aea]]
= Löschen Sie E-Mail-Server oder E-Mail-Adressen für Warnmeldungen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können den zuvor definierten Mail-Server so entfernen, dass
Warnmeldungen nicht mehr an die E-Mail-Adressen gesendet werden, oder Sie
können einzelne E-Mail-Adressen entfernen.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *E-Mail* aus.
. Führen Sie in der Tabelle einen der folgenden Schritte aus:
+
** Um einen E-Mail-Server zu entfernen, damit Warnmeldungen nicht mehr an
die E-Mail-Adressen gesendet werden, wählen Sie die Zeile für den Mail-
Server aus.
** Um eine E-Mail-Adresse zu entfernen, damit Benachrichtigungen nicht
mehr an diese Adresse gesendet werden, wählen Sie die Zeile für die zu
löschende E-Mail-Adresse aus. Die Schaltfläche *Löschen* oben rechts in
der Tabelle steht zur Auswahl.


. Klicken Sie auf *Löschen* und bestätigen Sie den Vorgang.




[[IDe03804dde15adf6f1cefb3b9a27dfb07]]
= E-Mail-Server für Warnmeldungen bearbeiten
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die E-Mail-Server-Adresse und die E-Mail-Absenderadresse
ändern, die für E-Mail-Benachrichtigungen verwendet werden.

.Bevor Sie beginnen
```

```
Die Adresse des Mail-Servers, den Sie ändern, muss verfügbar sein. Bei der
Adresse kann es sich um eine IPv4- oder IPv6-Adresse oder einen
vollqualifizierten Domänennamen handeln.

[NOTE]
====
Um einen vollständig qualifizierten Domänennamen zu verwenden, müssen Sie
auf beiden Controllern einen DNS-Server konfigurieren. Sie können einen
DNS-Server auf der Seite Hardware konfigurieren.

====
.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *E-Mail* aus.
. Wählen Sie *E-Mail-Server Konfigurieren*.
+
Das Dialogfeld Mailserver konfigurieren wird geöffnet.

. Bearbeiten Sie die Adresse des E-Mail-Servers, die Absenderinformationen
und die Kontaktinformationen.
+
** *Mail-Server-Adresse* -- Bearbeiten Sie den vollqualifizierten
Domainnamen, die IPv4-Adresse oder die IPv6-Adresse des Mailservers.
+
[NOTE]
====
Um einen vollständig qualifizierten Domänennamen zu verwenden, müssen Sie
auf beiden Controllern einen DNS-Server konfigurieren. Sie können einen
DNS-Server auf der Seite Hardware konfigurieren.

====
** *E-Mail-Absender-Adresse* -- Bearbeiten Sie die E-Mail-Adresse, die als
Absender der E-Mail verwendet werden soll. Diese Adresse wird im Feld
„von“ der E-Mail-Nachricht angezeigt.
** *Kontaktinformationen in E-Mail einfügen* -- um die Kontaktdaten des
Absenders zu bearbeiten, wählen Sie diese Option aus, und bearbeiten Sie
dann den Namen und die Telefonnummer.


. Klicken Sie Auf *Speichern*.




:leveloffset: -1
```

```
= Managen von SNMP-Warnmeldungen

:leveloffset: +1


[[IDec1e2a1bf540218d2d83217ad97f4f81]]
= Konfigurieren von SNMP-Warnmeldungen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um SNMP-Warnungen (Simple Network Management Protocol) zu konfigurieren,
müssen Sie mindestens einen Server identifizieren, auf dem der
Ereignismonitor des Speicherarrays SNMP-Traps senden kann. Die
Konfiguration erfordert einen Community-Namen oder Benutzernamen und eine
IP-Adresse für den Server.

.Bevor Sie beginnen
* Ein Netzwerkserver muss mit einer SNMP-Dienstanwendung konfiguriert
sein. Sie benötigen die Netzwerkadresse dieses Servers (entweder eine
IPv4- oder eine IPv6-Adresse), damit der Ereignismonitor Trap-Meldungen an
diese Adresse senden kann. Sie können mehrere Server verwenden (bis zu 10
Server sind zulässig).
* Die Management Information Base (MIB)-Datei wurde kopiert und mit der
SNMP-Dienst-Anwendung auf dem Server kompiliert. Diese MIB-Datei definiert
die Daten, die überwacht und verwaltet werden.
+
Wenn Sie nicht über die MIB-Datei, können Sie sie von der NetApp Support-
Website erhalten:

+
** Gehen Sie zu https://mysupport.netapp.com/site/global/dashboard["NetApp
Support"^].
** Klicken Sie auf die Registerkarte *Downloads* und wählen Sie dann
*Downloads*.
** Klicken Sie auf *E-Series SANtricity OS Controller Software*.
** Wählen Sie *Letzte Version Herunterladen*.
** Melden Sie sich an.
** Akzeptieren Sie die Vorsichtserklärung und die Lizenzvereinbarung.
** Scrollen Sie nach unten, bis Sie die MIB-Datei für Ihren Controller-Typ
sehen, und klicken Sie dann auf den Link, um die Datei herunterzuladen.
```

.Über diese Aufgabe
Diese Aufgabe beschreibt, wie Sie den SNMP-Server für Trap-Ziele identifizieren und anschließend Ihre Konfiguration testen.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *SNMP* aus.
+
Bei der Ersteinrichtung wird auf der Registerkarte SNMP „Configure Communities/Users“ angezeigt.

. Wählen Sie * Communities/Benutzer Konfigurieren*.
+
Das Dialogfeld SNMP-Version auswählen wird geöffnet.

. Wählen Sie die SNMP-Version für die Alarme aus, entweder *SNMPv2c* oder *SNMPv3*.
+
Je nach Auswahl wird das Dialogfeld „Communities konfigurieren“ oder das Dialogfeld „SNMPv3-Benutzer konfigurieren“ geöffnet.

. Befolgen Sie die entsprechenden Anweisungen für SNMPv2c (Communities) oder SNMPv3 (Benutzer):
+
** *SNMPv2c (Communities)* -- Geben Sie im Dialogfeld „Configure Communities“ eine oder mehrere Community-Strings für die Netzwerkserver ein. Ein Community-Name ist eine Zeichenfolge, die einen bekannten Satz von Management Stations identifiziert und in der Regel von einem Netzwerkadministrator erstellt wird. Es besteht nur aus druckbaren ASCII-Zeichen. Sie können bis zu 256 Communities hinzufügen. Wenn Sie fertig sind, klicken Sie auf *Speichern*.
** *SNMPv3 (Users)* -- Klicken Sie im Dialogfeld Configure SNMPv3 Users auf *Add*, und geben Sie anschließend die folgenden Informationen ein:
+
*** *Benutzername* -- Geben Sie einen Namen ein, um den Benutzer zu identifizieren, der bis zu 31 Zeichen lang sein kann.
*** *Engine ID* -- Wählen Sie die Engine-ID aus, die zur Generierung von Authentifizierungs- und Verschlüsselungsschlüsseln für Nachrichten verwendet wird, und müssen in der Verwaltungsdomäne eindeutig sein. In den meisten Fällen sollten Sie *Lokal* wählen. Wenn Sie eine nicht-Standardkonfiguration haben, wählen Sie *Benutzerdefiniert* aus. Ein weiteres Feld wird angezeigt, in dem Sie die autoritative Engine-ID als Hexadezimalstring eingeben müssen, wobei eine gerade Anzahl von Zeichen zwischen 10 und 32 Zeichen lang ist.

*** *Authentifizierungsdaten* -- Wählen Sie ein Authentifizierungsprotokoll, das die Identität der Benutzer sicherstellt. Geben Sie dann ein Authentifizierungspasswort ein, das erforderlich ist, wenn das Authentifizierungsprotokoll festgelegt oder geändert wird. Das Passwort muss zwischen 8 und 128 Zeichen lang sein.
*** *Datenschutzhinweise* -- Wählen Sie ein Datenschutzprotokoll, das zur Verschlüsselung der Inhalte von Nachrichten verwendet wird. Geben Sie dann ein Datenschutzkennwort ein, das erforderlich ist, wenn das Datenschutzprotokoll festgelegt oder geändert wird. Das Passwort muss zwischen 8 und 128 Zeichen lang sein. Wenn Sie fertig sind, klicken Sie auf *Hinzufügen*, und klicken Sie dann auf *Schließen*.

. Klicken Sie auf der Seite Warnungen auf der Registerkarte SNMP auf *Trap Destinations hinzufügen*.
+
Das Dialogfeld Trap-Ziele hinzufügen wird geöffnet.

. Geben Sie ein oder mehrere Trap-Ziele ein, wählen Sie die zugehörigen Community-Namen oder Benutzernamen aus, und klicken Sie dann auf *Hinzufügen*.
+
** *Trap-Ziel* -- Geben Sie eine IPv4- oder IPv6-Adresse des Servers ein, auf dem ein SNMP-Dienst ausgeführt wird.
** *Community-Name oder Benutzername* -- Wählen Sie in der Dropdown-Liste den Community-Namen (SNMPv2c) oder den Benutzernamen (SNMPv3) für dieses Trap-Ziel aus. (Wenn Sie nur einen definiert haben, wird der Name bereits in diesem Feld angezeigt.)
** *Authentifizierungsfehler senden Trap* -- Wählen Sie diese Option (das Kontrollkästchen) aus, wenn Sie das Trap-Ziel benachrichtigen möchten, wenn eine SNMP-Anfrage aufgrund eines nicht erkannten Community-Namens oder Benutzernamens abgelehnt wird. Nach dem Klicken auf *Hinzufügen* werden die Trap-Ziele und die zugehörigen Namen auf der Seite *SNMP* auf der Registerkarte *Alarme* angezeigt.

. Um sicherzustellen, dass ein Trap gültig ist, wählen Sie ein Trap-Ziel aus der Tabelle aus, und klicken Sie dann auf *Trap-Ziel testen*, um einen Test-Trap an die konfigurierte Adresse zu senden.

.Ergebnisse
Der Ereignismonitor sendet SNMP-Traps an den/die Server(s), wenn ein alertable Ereignis auftritt.

```
[[ID22a3674a0a4e236658503f3b2663a2f1]]
= Fügen Sie Trap-Ziele für SNMP-Warnungen hinzu
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können bis zu 10 Server zum Senden von SNMP-Traps hinzufügen.

.Bevor Sie beginnen
* Der Netzwerkserver, den Sie hinzufügen möchten, muss mit einer SNMP-
Serviceanwendung konfiguriert sein. Sie benötigen die Netzwerkadresse
dieses Servers (entweder eine IPv4- oder eine IPv6-Adresse), damit der
Ereignismonitor Trap-Meldungen an diese Adresse senden kann. Sie können
mehrere Server verwenden (bis zu 10 Server sind zulässig).
* Die Management Information Base (MIB)-Datei wurde kopiert und mit der
SNMP-Dienst-Anwendung auf dem Server kompiliert. Diese MIB-Datei definiert
die Daten, die überwacht und verwaltet werden.
+
Wenn Sie nicht über die MIB-Datei, können Sie sie von der NetApp Support-
Website erhalten:

+
** Gehen Sie zu https://mysupport.netapp.com/site/global/dashboard["NetApp
Support"^].
** Klicken Sie auf *Downloads* und wählen Sie dann *Downloads*.
** Klicken Sie auf *E-Series SANtricity OS Controller Software*.
** Wählen Sie *Letzte Version Herunterladen*.
** Melden Sie sich an.
** Akzeptieren Sie die Vorsichtserklärung und die Lizenzvereinbarung.
** Scrollen Sie nach unten, bis Sie die MIB-Datei für Ihren Controller-Typ
sehen, und klicken Sie dann auf den Link, um die Datei herunterzuladen.




.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *SNMP* aus.
+
Die aktuell definierten Trap-Ziele werden in der Tabelle angezeigt.
```

. Wählen Sie *Trap Desinations Hinzufügen*.
+
Das Dialogfeld Trap-Ziele hinzufügen wird geöffnet.

. Geben Sie ein oder mehrere Trap-Ziele ein, wählen Sie die zugehörigen Community-Namen oder Benutzernamen aus, und klicken Sie dann auf *Hinzufügen*.
+
** *Trap-Ziel* -- Geben Sie eine IPv4- oder IPv6-Adresse des Servers ein, auf dem ein SNMP-Dienst ausgeführt wird.
** *Community-Name oder Benutzername* -- Wählen Sie in der Dropdown-Liste den Community-Namen (SNMPv2c) oder den Benutzernamen (SNMPv3) für dieses Trap-Ziel aus. (Wenn Sie nur einen definiert haben, wird der Name bereits in diesem Feld angezeigt.)
** *Authentifizierungsfehler senden Trap* -- Wählen Sie diese Option (das Kontrollkästchen) aus, wenn Sie das Trap-Ziel benachrichtigen möchten, wenn eine SNMP-Anfrage aufgrund eines nicht erkannten Community-Namens oder Benutzernamens abgelehnt wird. Nach dem Klicken auf *Hinzufügen* werden die Trap-Ziele und die zugehörigen Community-Namen oder Benutzernamen in der Tabelle angezeigt.

. Um sicherzustellen, dass ein Trap gültig ist, wählen Sie ein Trap-Ziel aus der Tabelle aus, und klicken Sie dann auf *Trap-Ziel testen*, um einen Test-Trap an die konfigurierte Adresse zu senden.

.Ergebnisse
Der Ereignismonitor sendet SNMP-Traps an den/die Server(s), wenn ein alertable Ereignis auftritt.

[[ID2ac60d4102aec3b234333aefd4467dc2]]
= Konfigurieren Sie SNMP-MIB-Variablen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Für SNMP-Warnungen können Sie optional Management Information Base (MIB)-Variablen konfigurieren, die in SNMP-Traps angezeigt werden. Diese Variablen können den Namen des Speicher-Arrays, den Speicherort des Arrays und einen Ansprechpartner zurückgeben.

.Bevor Sie beginnen
Die MIB-Datei muss kopiert und mit der SNMP-Dienst-Anwendung auf dem Server kompiliert werden.

Wenn Sie keine MIB-Datei haben, können Sie es wie folgt erhalten:

* Gehen Sie zu https://mysupport.netapp.com/site/global/dashboard["NetApp Support"^].
* Klicken Sie auf *Downloads* und wählen Sie dann *Downloads*.
* Klicken Sie auf *E-Series SANtricity OS Controller Software*.
* Wählen Sie *Letzte Version Herunterladen*.
* Melden Sie sich an.
* Akzeptieren Sie die Vorsichtserklärung und die Lizenzvereinbarung.
* Scrollen Sie nach unten, bis Sie die MIB-Datei für Ihren Controller-Typ sehen, und klicken Sie dann auf den Link, um die Datei herunterzuladen.

.Über diese Aufgabe
In dieser Aufgabe wird beschrieben, wie MIB-Variablen für SNMP-Traps definiert werden. Diese Variablen können als Antwort auf SNMP GetRequests folgende Werte zurückgeben:

* `sysName` (Name für das Speicher-Array)
* `sysLocation` (Speicherort des Speicher-Arrays)
* `sysContact` (Name eines Administrators)

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *SNMP* aus.
. Wählen Sie *Konfigurieren von SNMP-MIB-Variablen*.
+
Das Dialogfeld SNMP-MIB-Variablen konfigurieren wird geöffnet.

. Geben Sie einen oder mehrere der folgenden Werte ein, und klicken Sie dann auf *Speichern*.
+
** *Name* -- der Wert für die MIB-Variable `sysName`. Geben Sie beispielsweise einen Namen für das Speicher-Array ein.
** *Lage* -- der Wert für die MIB Variable `sysLocation`. Geben Sie beispielsweise einen Speicherort des Speicher-Arrays ein.
** *Kontakt* -- der Wert für die MIB-Variable `sysContact`. Geben Sie beispielsweise einen Administrator ein, der für das Speicher-Array verantwortlich ist.

```
.Ergebnisse
Diese Werte werden in SNMP-Trap-Meldungen für Storage Array-Warnungen
angezeigt.



[[ID6e067766c529c5051597354dca7dc567]]
= Communities für SNMPv2c-Traps bearbeiten
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können Community-Namen für SNMPv2c-Traps bearbeiten.

.Bevor Sie beginnen
Ein Community-Name muss erstellt werden.

.Schritte
. Wählen Sie MENU:Einstellen von[Warnungen].
. Wählen Sie die Registerkarte *SNMP* aus.
+
Die Trap-Ziele und Community-Namen werden in der Tabelle angezeigt.

. Wählen Sie * Communities Konfigurieren*.
. Geben Sie den neuen Community-Namen ein und klicken Sie dann auf
*Speichern*. Community-Namen können nur aus druckbaren ASCII-Zeichen
bestehen.


.Ergebnisse
Auf der Registerkarte SNMP der Seite Meldungen wird der aktualisierte
Community-Name angezeigt.



[[ID92661cf755039ee7efde6f95621433eb]]
= Benutzereinstellungen für SNMPv3-Traps bearbeiten
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
```

```
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können Benutzerdefinitionen für SNMPv3-Traps bearbeiten.

.Bevor Sie beginnen
Für den SNMPv3-Trap muss ein Benutzer erstellt werden.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *SNMP* aus.
+
Die Trap-Ziele und Benutzernamen werden in der Tabelle angezeigt.

. Um eine Benutzerdefinition zu bearbeiten, wählen Sie den Benutzer in der
Tabelle aus und klicken dann auf *Benutzer konfigurieren*.
. Klicken Sie im Dialogfeld auf *Einstellungen anzeigen/bearbeiten*.
. Bearbeiten Sie folgende Informationen:
+
** *Benutzername* -- Ändern Sie den Namen, der den Benutzer identifiziert,
der bis zu 31 Zeichen lang sein kann.
** *Engine ID* -- Wählen Sie die Engine-ID aus, die zur Generierung von
Authentifizierungs- und Verschlüsselungsschlüsseln für Nachrichten
verwendet wird, und müssen in der Verwaltungsdomäne eindeutig sein. In den
meisten Fällen sollten Sie *Lokal* wählen. Wenn Sie eine nicht-
Standardkonfiguration haben, wählen Sie *Benutzerdefiniert* aus. Ein
weiteres Feld wird angezeigt, in dem Sie die autoritative Engine-ID als
Hexadezimalstring eingeben müssen, wobei eine gerade Anzahl von Zeichen
zwischen 10 und 32 Zeichen lang ist.
** *Authentifizierungsdaten* -- Wählen Sie ein
Authentifizierungsprotokoll, das die Identität der Benutzer sicherstellt.
Geben Sie dann ein Authentifizierungspasswort ein, das erforderlich ist,
wenn das Authentifizierungsprotokoll festgelegt oder geändert wird. Das
Passwort muss zwischen 8 und 128 Zeichen lang sein.
** *Datenschutzhinweise* -- Wählen Sie ein Datenschutzprotokoll, das zur
Verschlüsselung der Inhalte von Nachrichten verwendet wird. Geben Sie dann
ein Datenschutzkennwort ein, das erforderlich ist, wenn das
Datenschutzprotokoll festgelegt oder geändert wird. Das Passwort muss
zwischen 8 und 128 Zeichen lang sein.




.Ergebnisse
Auf der Registerkarte SNMP der Seite Meldungen werden die aktualisierten
```

```
Einstellungen angezeigt.



[[IDba7c31eb979f46020d2e8d6908c0848a]]
= Fügen Sie Communities für SNMPv2c-Traps hinzu
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können bis zu 256 Community-Namen für SNMPv2c-Traps hinzufügen.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *SNMP* aus.
+
Die Trap-Ziele und Community-Namen werden in der Tabelle angezeigt.

. Wählen Sie * Communities Konfigurieren*.
+
Das Dialogfeld „Communities konfigurieren“ wird geöffnet.

. Wählen Sie *Weitere Community hinzufügen*.
. Geben Sie den neuen Community-Namen ein und klicken Sie dann auf
*Speichern*.


.Ergebnisse
Der neue Community-Name wird auf der Registerkarte SNMP der Seite
Meldungen angezeigt.



[[ID8e785bee0475943eb45e3f03312fb2f0]]
= Benutzer für SNMPv3-Traps hinzufügen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

Sie können bis zu 256 Benutzer für SNMPv3-Traps hinzufügen.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *SNMP* aus.
+
Die Trap-Ziele und Benutzernamen werden in der Tabelle angezeigt.

. Wählen Sie *Benutzer Konfigurieren*.
+
Das Dialogfeld SNMPv3-Benutzer konfigurieren wird geöffnet.

. Wählen Sie *Hinzufügen*.
. Geben Sie die folgenden Informationen ein, und klicken Sie dann auf *Hinzufügen*.
+
** *Benutzername* -- Geben Sie einen Namen ein, um den Benutzer zu identifizieren, der bis zu 31 Zeichen lang sein kann.
** *Engine ID* -- Wählen Sie die Engine-ID aus, die zur Generierung von Authentifizierungs- und Verschlüsselungsschlüsseln für Nachrichten verwendet wird, und müssen in der Verwaltungsdomäne eindeutig sein. In den meisten Fällen sollten Sie *Lokal* wählen. Wenn Sie eine nicht-Standardkonfiguration haben, wählen Sie *Benutzerdefiniert* aus. Ein weiteres Feld wird angezeigt, in dem Sie die autoritative Engine-ID als Hexadezimalstring eingeben müssen, wobei eine gerade Anzahl von Zeichen zwischen 10 und 32 Zeichen lang ist.
** *Authentifizierungsdaten* -- Wählen Sie ein Authentifizierungsprotokoll, das die Identität der Benutzer sicherstellt. Geben Sie dann ein Authentifizierungspasswort ein, das erforderlich ist, wenn das Authentifizierungsprotokoll festgelegt oder geändert wird. Das Passwort muss zwischen 8 und 128 Zeichen lang sein.
** *Datenschutzhinweise* -- Wählen Sie ein Datenschutzprotokoll, das zur Verschlüsselung der Inhalte von Nachrichten verwendet wird. Geben Sie dann ein Datenschutzkennwort ein, das erforderlich ist, wenn das Datenschutzprotokoll festgelegt oder geändert wird. Das Passwort muss zwischen 8 und 128 Zeichen lang sein.

[[ID1d53e00103cf3d0b441b4e25f5f9f2ce]]
= Entfernen Sie Communities für SNMPv2c-Traps
:allow-uri-read:
:experimental:

```
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können einen Community-Namen für SNMPv2c-Traps entfernen.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *SNMP* aus.
+
Die Trap-Ziele und Community-Namen werden auf der Seite *Alerts*
angezeigt.

. Wählen Sie * Communities Konfigurieren*.
+
Das Dialogfeld „Communities konfigurieren“ wird geöffnet.

. Wählen Sie den Community-Namen aus, den Sie löschen möchten, und klicken
Sie auf das Symbol *Entfernen* (X) ganz rechts.
+
Wenn Trap-Ziele mit diesem Community-Namen verknüpft sind, werden im
Dialogfeld Community entfernen bestätigen die betroffenen Trap-
Zieladressen angezeigt.

. Bestätigen Sie den Vorgang, und klicken Sie dann auf *Entfernen*.


.Ergebnisse
Der Community-Name und das zugehörige Trap-Ziel werden von der Seite
Alerts entfernt.



[[ID6d796b4bb5b9ba812f9b73e0561d1781]]
= Benutzer für SNMPv3-Traps entfernen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können einen Benutzer für SNMPv3-Traps entfernen.
```

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *SNMP* aus.
+
Die Trap-Ziele und Benutzernamen werden auf der Seite Meldungen angezeigt.

. Wählen Sie *Benutzer Konfigurieren*.
+
Das Dialogfeld SNMPv3-Benutzer konfigurieren wird geöffnet.

. Wählen Sie den Benutzernamen aus, den Sie löschen möchten, und klicken Sie dann auf *Löschen*.
. Bestätigen Sie den Vorgang, und klicken Sie dann auf *Löschen*.

.Ergebnisse
Der Benutzername und das zugehörige Trap-Ziel werden von der Seite Warnungen entfernt.

[[ID55347416a87d1db17824bd55b6726a35]]
= Löschen von Trap-Zielen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können eine Trap-Zieladresse löschen, sodass der Event-Monitor des Speicherarrays keine SNMP-Traps mehr an diese Adresse sendet.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *SNMP* aus.
+
Die Trap-Zieladressen werden in der Tabelle angezeigt.

. Wählen Sie ein Trap-Ziel aus, und klicken Sie dann rechts oben auf der Seite auf *Löschen*.
. Bestätigen Sie den Vorgang, und klicken Sie dann auf *Löschen*.
+
Die Zieladresse wird nicht mehr auf der Seite „Meldungen“ angezeigt.

```
.Ergebnisse
Das gelöschte Trap-Ziel empfängt keine SNMP-Traps mehr vom Event-Monitor
des Speicherarrays.



:leveloffset: -1


= Managen von Syslog-Warnmeldungen

:leveloffset: +1


[[ID028cad55a01029596b6225ae96ea11b4]]
= Konfigurieren Sie den Syslog-Server für Warnmeldungen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um Syslog-Warnmeldungen zu konfigurieren, müssen Sie eine Syslog-
Serveradresse und einen UDP-Port eingeben. Es sind bis zu fünf Syslog-
Server zulässig.

.Bevor Sie beginnen
* Die Syslog-Serveradresse muss verfügbar sein. Bei dieser Adresse kann es
sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse
oder eine IPv6-Adresse handeln.
* UDP-Portnummer des Syslog-Servers muss verfügbar sein. Dieser Port ist
normalerweise 514.


.Über diese Aufgabe
Diese Aufgabe beschreibt, wie Sie die Adresse und den Port für den Syslog-
Server eingeben und anschließend die eingegebene Adresse testen.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *Syslog* aus.
+
Wenn noch kein Syslog-Server definiert ist, wird auf der Seite Warnungen
„Syslog-Server hinzufügen“ angezeigt.
```

```
. Klicken Sie Auf *Syslog-Server Hinzufügen*.
+
Das Dialogfeld Syslog Server hinzufügen wird geöffnet.

. Geben Sie Informationen für einen oder mehrere Syslog-Server ein
(maximal fünf), und klicken Sie dann auf *Hinzufügen*.
+
** *Server-Adresse* -- Geben Sie einen vollständig qualifizierten
Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
** *UDP Port* -- normalerweise ist der UDP Port für syslog 514. In der
Tabelle werden die konfigurierten Syslog-Server angezeigt.


. Um eine Testwarnung an die Serveradressen zu senden, wählen Sie *Alle
Syslog-Server testen*.


.Ergebnisse
Der Ereignismonitor sendet bei jedem Ereignis, das in einem Alarmtabellen
stattfindet, Warnmeldungen an den Syslog-Server. Weitere Informationen zum
Konfigurieren der Syslog-Einstellungen für Audit-Protokolle finden Sie
unter https://docs.netapp.com/us-en/e-series-santricity/sm-
settings/configure-syslog-server-for-audit-logs.html["Syslog-Server für
Audit-Protokolle konfigurieren"].


NOTE: Wenn mehrere Syslog-Server konfiguriert sind, erhalten alle
konfigurierten Syslog-Server ein Revisionsprotokoll.



[[IDab5987112607bc2fb18bf5d97287b1e9]]
= Bearbeiten Sie Syslog-Server für Warnmeldungen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die Serveradresse bearbeiten, die für den Empfang von Syslog-
Warnungen verwendet wird.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
```

. Wählen Sie die Registerkarte *Syslog* aus.
. Wählen Sie in der Tabelle eine Syslog-Serveradresse aus, und klicken Sie dann auf das Symbol *Bearbeiten* (Bleistift) von rechts.
+
Die Zeile wird zu einem bearbeitbaren Feld.

. Bearbeiten Sie die Serveradresse und die UDP-Portnummer und klicken Sie dann auf das Symbol *Speichern* (Häkchen).

.Ergebnisse
Die aktualisierte Serveradresse wird in der Tabelle angezeigt.

[[ID7fa96c17fe72250d162430bad2e3b0a6]]
= Fügen Sie Syslog-Server für Warnungen hinzu
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können maximal fünf Server für Syslog-Warnmeldungen hinzufügen.

.Bevor Sie beginnen
* Die Syslog-Serveradresse muss verfügbar sein. Bei dieser Adresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
* Die UDP-Portnummer des Syslog-Servers muss verfügbar sein. Dieser Port ist normalerweise 514.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *Syslog* aus.
. Wählen Sie *Syslog-Server Hinzufügen*.
+
Das Dialogfeld Syslog Server hinzufügen wird geöffnet.

. Wählen Sie *Weitere Syslog-Server hinzufügen*.
. Geben Sie Informationen für den Syslog-Server ein, und klicken Sie dann auf *Hinzufügen*.
+
** *Syslog Server Address* -- Geben Sie einen vollständig qualifizierten

```
Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
** *UDP Port* -- normalerweise ist der UDP Port für syslog 514.


+

NOTE: Sie können bis zu fünf Syslog-Server konfigurieren.



.Ergebnisse
Die Syslog-Server-Adressen werden in der Tabelle angezeigt.



[[ID1b91fc4d82d6dcfd1166d2d4619e7bb9]]
= Löschen von Syslog-Servern für Warnmeldungen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können einen Syslog-Server löschen, damit er keine Warnungen mehr
erhält.

.Schritte
. Wählen Sie Menü:Einstellungen[Alarme].
. Wählen Sie die Registerkarte *Syslog* aus.
. Wählen Sie eine Syslog-Serveradresse aus, und klicken Sie dann rechts
oben auf *Entfernen*.
+
Das Dialogfeld Löschen des Syslog-Servers bestätigen wird geöffnet.

. Bestätigen Sie den Vorgang, und klicken Sie dann auf *Löschen*.


.Ergebnisse
Der entfernte Server empfängt keine Warnmeldungen mehr von der
Ereignisüberwachung.



:leveloffset: -1
```

```
= FAQs

:leveloffset: +1


[[IDbbc1feb035f131025109281293d3c480]]
= Was ist, wenn Alarme deaktiviert sind?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Administratoren Benachrichtigungen über wichtige Ereignisse im
Speicher-Array erhalten sollen, müssen Sie eine Methode zur Alarmierung
konfigurieren.

Bei Storage Arrays, die mit SANtricity System Manager verwaltet werden,
konfigurieren Sie Warnmeldungen über die Seite „Meldungen“. Alert-
Benachrichtigungen können über E-Mail, SNMP-Traps oder Syslog-Nachrichten
gesendet werden. Zudem können E-Mail-Benachrichtigungen über den ersten
Setup-Assistenten konfiguriert werden.



[[IDb41f1fd0a20df74e90180eae06eecafd]]
= Wie konfiguriere ich SNMP- oder syslog-Alarme?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Neben E-Mail-Warnungen können Benachrichtigungen auch über SNMP-Traps
(Simple Network Management Protocol) oder Syslog-Nachrichten gesendet
werden.

Um SNMP- oder Syslog-Warnmeldungen zu konfigurieren, gehen Sie zu
MENU:Einstellungen[Warnungen].



[[ID54b86e3cf6d7e3653bb8da1541bc64a3]]
```

```
= Warum sind Zeitstempel zwischen dem Array und Warnungen uneinheitlich?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn das Speicher-Array Warnungen sendet, ist es für die Zeitzone des
Zielservers oder Hosts, der die Warnungen empfängt, nicht korrekt.
Stattdessen verwendet das Speicher-Array die lokale Zeit (GMT), um den
Zeitstempel zu erstellen, der für den Warnungsdatensatz verwendet wird.
Aufgrund dessen sind möglicherweise Inkonsistenzen zwischen den
Zeitstempel für das Storage-Array und dem Server oder Host, der eine
Meldung empfängt, zu erkennen.

Da das Speicherarray beim Senden von Warnungen nicht richtig für die
Zeitzone ist, ist der Zeitstempel für die Warnungen GMT-relative, der
einen Zeitzonenversatz von Null hat. Um einen Zeitstempel zu berechnen,
der Ihrer lokalen Zeitzone angemessen ist, sollten Sie Ihren
Stundenversatz von GMT bestimmen und diesen Wert dann von den Zeitstempel
hinzufügen oder abziehen.



:leveloffset: -1


:leveloffset: -1


= Array-Einstellungen

:leveloffset: +1


[[ID7001bc243d6b3763e077c1ec7ba79d62]]
= Einstellungsübersicht
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können SANtricity System Manager für einige allgemeine Array-
```

```
Einstellungen und Zusatzfunktionen konfigurieren.



== Welche Einstellungen kann ich konfigurieren?

Die Array-Einstellungen umfassen:

* xref:{relative_path}cache-settings-and-performance.html["Cache-
Einstellungen und Performance"]
* xref:{relative_path}automatic-load-balancing-
overview.html["Automatische Lastverteilung"]
* xref:{relative_path}how-add-on-features-work.html["Add-on-Funktionen"]
* xref:{relative_path}overview-drive-security.html["Laufwerkssicherheit"]




== Verwandte Aufgaben

Weitere Informationen zu Aufgaben im Zusammenhang mit Systemeinstellungen:

* xref:{relative_path}download-cli.html["Befehlszeilenschnittstelle (CLI)
herunterladen"]
* xref:{relative_path}create-internal-security-key.html["Interner
Sicherheitsschlüssel erstellen"]
* xref:{relative_path}create-external-security-key.html["Externen
Sicherheitsschlüssel erstellen"]
* xref:{relative_path}../sm-hardware/configure-iscsi-ports-
hardware.html["Konfigurieren Sie die iSCSI-Ports"]
* xref:{relative_path}../sm-hardware/configure-nvme-over-infiniband-ports-
hardware.html["KONFIGURIEREN SIE NVME over IB-Ports"]
* xref:{relative_path}../sm-hardware/configure-nvme-over-roce-ports-
hardware.html["Konfigurieren Sie NVMe over RoCE-Ports"]




= Konzepte

:leveloffset: +1


[[ID452fa512996d397bf87b45c864014cb8]]
= Cache-Einstellungen und Performance
:allow-uri-read:
:experimental:
```

```
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Der Cache-Speicher ist ein temporärer flüchtiger Speicher auf dem
Controller, der eine schnellere Zugriffszeit hat als das Laufwerk.

Durch Caching kann die I/O-Performance insgesamt wie folgt gesteigert
werden:

* Die vom Host für einen Lesevorgang angeforderten Daten befinden sich
möglicherweise bereits im Cache eines vorherigen Vorgangs, sodass ein
Laufwerkzugriff nicht erforderlich ist.
* Schreibdaten werden zunächst in den Cache geschrieben. Dadurch wird die
Anwendung wieder freigegeben, anstatt auf das Schreiben der Daten auf das
Laufwerk zu warten.


Die Standard-Cache-Einstellungen erfüllen die Anforderungen für die
meisten Umgebungen, Sie können sie jedoch bei Bedarf ändern.



== Cache-Einstellungen für Storage-Arrays

Für alle Volumes im Speicher-Array können Sie auf der Seite System die
folgenden Werte angeben:

* *Startwert für Spülung* -- der Prozentsatz der nicht geschriebenen Daten
im Cache, der einen Cache-Flush auslöst (auf Festplatte schreiben). Wenn
der Cache den angegebenen Startprozentsatz der nicht geschriebenen Daten
enthält, wird ein Flush ausgelöst. Standardmäßig wird der Cache vom
Controller bereinigt, wenn der Cache zu 80 % voll ist.
* *Cache Blockgröße* -- die maximale Größe jedes Cache Blocks, eine
Organisationseinheit für Cache Management. Die Cache-Blockgröße ist
standardmäßig 8 KiB, kann jedoch auf 4, 8, 16 oder 32 KiB eingestellt
werden. Idealerweise sollte die Cache-Blockgröße auf die vorwiegend
verwendete I/O-Größe Ihrer Applikationen eingestellt werden. Filesysteme
oder Datenbankapplikationen verwenden in der Regel kleinere Größen,
während eine größere Größe für Applikationen geeignet ist, die
umfangreiche Datentransfers oder sequenzielle I/O benötigen
```

```
== Volume-Cache-Einstellungen

Für einzelne Volumes in einem Speicher-Array können Sie auf der Seite
Volumes (Menü:Storage[Volumes]) die folgenden Werte angeben:

* *Lese-Cache* -- 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.
+
** *Dynamischer Lese-Cache Prefetch* -- der dynamische Cache-Lesevorfetch
ermöglicht dem Controller, zusätzliche sequenzielle Datenblöcke in den
Cache zu kopieren, während er Datenblöcke von einem Laufwerk in den Cache
liest. 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 basierend auf der Geschwindigkeit und der
Anfragegröße des Host-Lesevorgängen automatisch an. Ein wahlfreier Zugriff
bewirkt nicht, dass Daten im Cache abgerufen werden. Diese Funktion gilt
nicht, wenn das Lese-Caching deaktiviert ist.


* *Schreib-Cache* -- der Schreib-Cache ist ein Puffer, der Daten vom Host
speichert, der noch nicht auf die Laufwerke geschrieben wurde. Die Daten
bleiben im Schreib-Cache, bis sie auf die Laufwerke geschrieben werden.
Caching von Schreibzugriffen kann die I/O-Performance steigern.
+
[CAUTION]
====
*Möglicher Datenverlust* -- Wenn Sie die *Write Caching ohne Batterien*
Option aktivieren 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 Option *Write
Caching ohne Batterien* aktivieren.

====
+
** *Write Caching ohne Batterien* -- das Schreib-Caching ohne
Akkueinstellung lässt das Schreib-Caching auch dann fortgesetzt, 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.
** *Schreib-Cache mit Spiegelung* -- Schreib-Caching mit Spiegelung tritt auf, wenn die in den Cache-Speicher eines Controllers geschriebenen Daten 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.

[[ID284a2eba353bea30657854963f5597aa]]
= Automatischer Lastausgleich – Übersicht
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Der automatische Lastausgleich ermöglicht ein verbessertes I/O-Ressourcenmanagement, das dynamisch auf Laständerungen im Laufe der Zeit reagiert und die Eigentümerschaft der Volume-Controller automatisch angepasst wird, um Lastwucht-Ungleichgewicht zu beheben, wenn die Workloads zwischen den Controllern verschoben werden.

Die Auslastung jedes Controllers wird kontinuierlich überwacht und, zusammen mit den auf den Hosts installierten Multipath-Treibern, kann bei Bedarf automatisch ausgeglichen werden. Wenn die Workload automatisch auf die Controller umverteilt wird, entlastet der Storage-Administrator die manuelle Anpassung der Eigentümerschaft der Volume Controller, um Laständerungen am Storage Array zu bewältigen.

Wenn der automatische Lastenausgleich aktiviert ist, führt er folgende Funktionen aus:

* Automatische Überwachung und ausgewogene Nutzung von Controller-Ressourcen
* Bei Bedarf passt die Volume-Controller-Eigentümerschaft automatisch an, was die I/O-Bandbreite zwischen Hosts und Storage Array optimiert.

```
== Aktivieren und Deaktivieren des automatischen Lastauswuchtes

Der automatische Lastausgleich ist auf allen Speicherarrays standardmäßig
aktiviert.

Aus den folgenden Gründen möchten Sie den automatischen Lastausgleich auf
Ihrem Speicher-Array deaktivieren:

* Sie möchten die Controller-Eigentumsrechte eines bestimmten Volumes
nicht automatisch ändern, um einen Workload-Ausgleich zu schaffen.
* Sie arbeiten in einer hoch abgestimmten Umgebung, in der die
Lastverteilung gezielt eingerichtet ist, um eine bestimmte Verteilung
zwischen den Controllern zu erreichen.




== Hosttypen, die die Funktion Automatischer Lastenausgleich unterstützen

Obwohl der automatische Lastausgleich auf Speicherarray-Ebene aktiviert
ist, hat der für einen Host oder Host-Cluster ausgewählte Hosttyp direkten
Einfluss auf den Betrieb der Funktion.

Wenn Sie die Workloads des Speicher-Arrays auf Controller verteilen,
versucht die Funktion Automatischer Lastausgleich, Volumes zu verschieben,
auf die beide Controller zugreifen können und die nur einem Host oder
Host-Cluster zugewiesen sind, der die Funktion Automatischer Lastausgleich
unterstützt.

Dieses Verhalten verhindert, dass ein Host aufgrund des
Lastausgleichprozesses den Zugriff auf ein Volume verliert. Das
Vorhandensein von Volumes, die Hosts zugeordnet sind, die keinen
automatischen Lastausgleich unterstützen, wirkt sich jedoch auf die
Fähigkeit des Speicherarrays aus, den Workload auszugleichen. Damit der
automatische Lastausgleich den Workload ausgleichen kann, muss der
Multipath-Treiber TPGS unterstützen und der Hosttyp muss in der folgenden
Tabelle enthalten sein.

[NOTE]
====
Damit ein Hostcluster als für den automatischen Lastausgleich geeignet
angesehen werden kann, müssen alle Hosts in dieser Gruppe den
automatischen Lastausgleich unterstützen können.

====
[cols="1a,1a"]
```

```
|===
| Hosttyp unterstützt den automatischen Lastausgleich | Mit diesem
Multipath-Treiber


 a|
Windows oder Windows Cluster
 a|
MPIO mit NetApp E-Series DSM



 a|
Linux DM-MP (Kernel 3.10 oder höher)
 a|
DM-MP mit `scsi_dh_alua` Gerätehandler



 a|
VMware
 a|
Natives Multipathing-Plug-in (NMP) mit `VMW_SATP_ALUA Storage Array Type`
Plug-in

|===
[NOTE]
====
Bis auf kleinere Ausnahmen funktionieren Host-Typen, die den automatischen
Lastausgleich nicht unterstützen, weiterhin normal, unabhängig davon, ob
die Funktion aktiviert ist oder nicht. Eine Ausnahme besteht darin, dass
bei einem System ein Failover besteht, Storage-Arrays nicht zugewiesene
oder nicht zugewiesene Volumes zurück zum entsprechenden Controller
verschieben, wenn der Datenpfad wieder zurückkehrt. Alle Volumes, die
nicht-automatischen Load-Balancing-Hosts zugeordnet oder zugewiesen sind,
werden nicht verschoben.

====
Siehe https://mysupport.netapp.com/matrix["Interoperabilitäts-Matrix-
Tool"^] Informationen zur Kompatibilität für bestimmte Multipath-Treiber,
BS-Ebene und Controller-Laufwerksfachunterstützung



== Überprüfung der Betriebssystemkompatibilität mit der Funktion
Automatischer Lastenausgleich
```

Überprüfen Sie die Betriebssystemkompatibilität mit der Funktion Automatischer Lastausgleich, bevor Sie ein neues (oder ein vorhandenes) System einrichten.

. Wechseln Sie zum https://mysupport.netapp.com/matrix["Interoperabilitäts-Matrix-Tool"^] Um Ihre Lösung zu finden und den Support zu überprüfen.
+
Wenden Sie sich an den technischen Support, wenn auf Ihrem System Red hat Enterprise Linux 6 oder SUSE Linux Enterprise Server 11 ausgeführt wird.

. Aktualisieren und konfigurieren Sie den `/etc/multipath.conf file`.
. Stellen Sie das beide sicher `retain_attached_device_handler` Und `detect_prio` Sind auf festgelegt `yes` Für den jeweiligen Anbieter und das jeweilige Produkt oder Standardeinstellungen verwenden.

:leveloffset: -1

= Konfigurieren Sie Array-Einstellungen

:leveloffset: +1

[[IDffd941ce99356a15eb03891504037d2a]]
= Name des Speicher-Arrays bearbeiten
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können den Namen des Speicher-Arrays ändern, der in der Titelleiste des SANtricity-Systems Managers angezeigt wird.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Suchen Sie unter *Allgemein* das Feld *Name:*.
+
Wenn kein Name des Speicher-Arrays definiert wurde, wird in diesem Feld „Unbekannt“ angezeigt.

```
. Klicken Sie auf das Symbol *Bearbeiten* (Bleistift) neben dem Namen des
Speicherarrays.
+
Das Feld kann bearbeitet werden.

. Geben Sie einen neuen Namen ein.
+
Ein Name kann Buchstaben, Ziffern und die Sonderzeichen Unterstrich (_),
Strich (-) und Hash-Zeichen (#) enthalten. Ein Name darf keine Leerzeichen
enthalten. Ein Name kann maximal 30 Zeichen lang sein. Der Name muss
eindeutig sein.

. Klicken Sie auf das Symbol *Speichern* (Häkchen).
+
[NOTE]
====
Wenn Sie das bearbeitbare Feld schließen möchten, ohne Änderungen
vorzunehmen, klicken Sie auf das Symbol *Abbrechen* (X).

====


.Ergebnisse
Der neue Name wird in der Titelleiste des SANtricity System Managers
angezeigt.



[[ID20b8990a341c5f0d6bc4ce8bef0cd06b]]
= Schalten Sie die Speicher-Array Locator-Leuchten ein
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um den physischen Standort eines Speicherarrays in einem Schrank zu
finden, können Sie seine Locator-Leuchten (LED) einschalten.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Klicken Sie unter *Allgemein* auf *Storage Array Locator Lights*.
+
Das Dialogfeld Speicherarray Locator Lights einschalten wird geöffnet, und
die Locator-LEDs des entsprechenden Speicherarrays werden eingeschaltet.
```

. Wenn Sie das Speicher-Array physisch gefunden haben, kehren Sie zum Dialogfeld zurück und wählen Sie *aus*.

.Ergebnisse
Die Positionsleuchten werden ausgeschaltet, und das Dialogfeld wird geschlossen.

[[IDf00030ea33dbc52b890df1fe72c0ce37]]
= Speicherarray-Uhren synchronisieren
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Wenn das Network Time Protocol (NTP) nicht aktiviert ist, können Sie die Uhren auf den Controllern manuell so einstellen, dass sie mit dem Management-Client synchronisiert werden (das System, mit dem der Browser ausgeführt wird, der auf SANtricity System Manager zugreift).

.Über diese Aufgabe
Durch die Synchronisierung wird sichergestellt, dass Ereigniszeitstempel in den Zeitstempeln des Ereignisprotokolls in die Host-Log-Dateien geschrieben werden. Während der Synchronisierung bleiben die Controller verfügbar und betriebsbereit.

[NOTE]
====
Wenn NTP in System Manager aktiviert ist, verwenden Sie diese Option nicht, um Uhren zu synchronisieren. Stattdessen synchronisiert NTP die Uhren automatisch mit einem externen Host mithilfe von SNTP (Simple Network Time Protocol).

====
[NOTE]
====
Nach der Synchronisierung können Sie feststellen, dass Performance-Statistiken verloren gehen oder verzerrt sind, Zeitpläne betroffen sind (ASUP, Snapshots usw.), und Zeitstempel in den Log-Daten sind verzerrt. Die Verwendung von NTP verhindert dieses Problem.

```
====
.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Klicken Sie unter *Allgemein* auf *Speicherarray-Uhren synchronisieren*.
+
Das Dialogfeld Speicherarray-Uhren synchronisieren wird geöffnet. Es zeigt
das aktuelle Datum und die aktuelle Uhrzeit für die Controller und den
Computer an, der als Management-Client verwendet wird.

+
[NOTE]
====
Für Simplex-Speicher-Arrays wird nur ein Controller angezeigt.

====
. Wenn die im Dialogfeld angezeigten Zeiten nicht übereinstimmen, klicken
Sie auf *Synchronisieren*.


.Ergebnisse
Nach erfolgreicher Synchronisierung sind Ereigniszeitstempel für das
Ereignisprotokoll und die Host-Protokolle identisch.



[[ID8fff46a91ccfc412e856b88955a2c9c6]]
= Speicherarray-Konfiguration speichern
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die Konfigurationsinformationen eines Speicherarrays in einer
Skriptdatei speichern, um Zeit beim Einrichten zusätzlicher Speicher-
Arrays mit der gleichen Konfiguration zu sparen.

.Bevor Sie beginnen
Das Speicher-Array darf keinen Vorgang durchlaufen, der seine logischen
Konfigurationseinstellungen ändert. Beispiele für diese Vorgänge sind das
Erstellen oder Löschen von Volumes, das Herunterladen der Controller-
Firmware, das Zuweisen oder Ändern von Hot-Spare-Laufwerken oder das
Hinzufügen von Kapazität (Laufwerken) zu einer Volume-Gruppe.

.Über diese Aufgabe
```

Das Speichern der Speicherarray-Konfiguration generiert ein CLI-Skript (Command Line Interface), das Storage Array-Einstellungen, Volume-Konfiguration, Host-Konfiguration oder Host-to-Volume-Zuweisungen für ein Storage-Array enthält. Sie können dieses generierte CLI-Skript verwenden, um eine Konfiguration auf einem anderen Speicher-Array mit genau derselben Hardwarekonfiguration zu replizieren.

Sie sollten jedoch das erzeugte CLI-Skript nicht für die Disaster Recovery verwenden. Verwenden Sie stattdessen für eine Systemwiederherstellung die Sicherungsdatei der Konfigurationsdatenbank, die Sie manuell erstellen, oder wenden Sie sich an den technischen Support, um diese Daten von den neuesten Auto-Support-Daten zu erhalten.

Diese Operation _speichert diese Einstellungen nicht_:

* Die Lebensdauer des Akkus
* Die Tageszeit der Steuerung
* Die Einstellungen für den nichtflüchtigen statischen Random Access Memory (NVSRAM)
* Alle Premium-Funktionen
* Das Kennwort für das Speicher-Array
* Betriebsstatus und Status der Hardwarekomponenten
* Betriebsstatus (außer optimal) und Status der Volume-Gruppen
* Kopierservices wie Spiegelung und Volume-Kopien

[CAUTION]
====
Risiko von Anwendungsfehlern -- Verwenden Sie diese Option nicht, wenn das Speicher-Array einen Vorgang durchläuft, der jede logische Konfigurationseinstellung ändert. Beispiele für diese Vorgänge sind das Erstellen oder Löschen von Volumes, das Herunterladen der Controller-Firmware, das Zuweisen oder Ändern von Hot-Spare-Laufwerken oder das Hinzufügen von Kapazität (Laufwerken) zu einer Volume-Gruppe.

====
.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie *Speicherarray-Konfiguration Speichern*.
. Wählen Sie die Elemente der Konfiguration aus, die Sie speichern möchten:
+
** Storage Array-Einstellungen
** Konfiguration von Volumes
** Host-Konfiguration
** Zuweisung von Host zu Volume

```
+
[NOTE]
====
Wenn Sie das Element *Host-to-Volume Zuweisungen* auswählen, werden
standardmäßig auch das Element *Volume Configuration* und das Element
*Host Configuration* ausgewählt. Sie können keine „Host-to-Volume-
Zuweisungen“ speichern, ohne auch „Volume-Konfiguration“ und „Host-
Konfiguration“ zu speichern.

====
. Klicken Sie Auf *Speichern*.
+
Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen
gespeichert `storage-array-configuration.cfg`.



.Nachdem Sie fertig sind
Um die gespeicherte Speicher-Array-Konfiguration auf ein anderes Speicher-
Array zu laden, verwenden Sie die SANtricity-Befehlszeilenschnittstelle
(SMcli) mit dem `-f` Option zum Anwenden des `.cfg` Datei:

[NOTE]
====
Sie können eine Speicherarray-Konfiguration auch über die Unified Manager-
Oberfläche auf andere Speicher-Arrays laden (Menü wählen:Verwalten[Import-
Einstellungen]).

====



[[ID54097422df193d13beaa84f36fb90d7d]]
= Löschen Sie die Konfiguration des Speicherarrays
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Verwenden Sie den Vorgang Konfiguration löschen, wenn Sie alle Pools,
Volume-Gruppen, Volumes, Host-Definitionen und Host-Zuweisungen aus dem
Speicher-Array löschen möchten.
```

.Bevor Sie beginnen
Sichern Sie vor dem Löschen der Konfiguration des Speicherarrays die Daten.

.Über diese Aufgabe
Es gibt zwei Optionen für eine klare Speicherarray-Konfiguration:

* *Volume* -- normalerweise können Sie mit der Option Volume ein Test-Storage-Array als Produktions-Storage-Array neu konfigurieren. Beispielsweise können Sie ein Storage-Array für Tests konfigurieren und dann, wenn Sie die Testkonfiguration abgeschlossen haben, entfernen und das Storage-Array für eine Produktionsumgebung einrichten.
* *Speicher-Array* -- normalerweise können Sie die Option Speicher-Array verwenden, um ein Speicher-Array in eine andere Abteilung oder Gruppe zu verschieben. Beispielsweise können Sie ein Storage Array im Engineering verwenden, und jetzt erhält Engineering ein neues Storage Array, also möchten Sie das aktuelle Storage Array zu Administration verschieben, wo es neu konfiguriert wird.
+
Mit der Option Speicher-Array werden einige zusätzliche Einstellungen gelöscht.

[cols="1a,1a,1a"]
|===
| | Datenmenge | Storage Array Durchführt

 a|
Deaktiviert ARVM
 a|
X
 a|
X

 a|
Löscht Pools und Volume-Gruppen
 a|
X
 a|
X

```
 a|
Löscht Volumes
 a|
X
 a|
X



 a|
Löscht Hosts und Host-Cluster
 a|
X
 a|
X



 a|
Löscht Host-Zuweisungen
 a|
X
 a|
X



 a|
Löscht den Namen des Speicher-Arrays
 a|
 a|
X



 a|
Setzt die Cache-Einstellungen des Speicherarrays auf die
Standardeinstellung zurück
 a|
 a|
X

|===
[CAUTION]
====
*Risiko des Datenverlustes* -- dieser Vorgang löscht alle Daten aus Ihrem
Speicher-Array. (Es wird kein sicheres Löschen durchgeführt.) Sie können
```

```
diesen Vorgang nach dem Start nicht mehr abbrechen. Führen Sie diesen
Vorgang nur aus, wenn Sie vom technischen Support dazu aufgefordert
werden.

====
.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie *Speicherarray-Konfiguration Löschen*.
. Wählen Sie in der Dropdown-Liste entweder *Volume* oder *Storage Array*
aus.
. *Optional:* Wenn Sie die Konfiguration speichern möchten (nicht die
Daten), verwenden Sie die Links im Dialogfeld.
. Bestätigen Sie, dass Sie den Vorgang ausführen möchten.


.Ergebnisse
* Die aktuelle Konfiguration wird gelöscht und alle vorhandenen Daten auf
dem Speicher-Array zerstört.
* Zuweisung aller Laufwerke aufgehoben.




[[IDc294efb92bf312993cb65caf297f1bec]]
= Ändern Sie die Cache-Einstellungen für das Speicher-Array
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Für alle Volumes im Speicher-Array können Sie die Cache-
Speichereinstellungen für die Spülung und die Blockgröße anpassen.

.Über diese Aufgabe
Cache-Speicher ist ein temporärer flüchtiger Speicher auf dem Controller,
der eine schnellere Zugriffszeit als die Datenträger des Laufwerks hat. Um
die Cache-Performance zu optimieren, können Sie folgende Einstellungen
vornehmen:

[cols="25h,~"]
|===
| Cache-Einstellung | Beschreibung
```

```
 a|
Starten Sie die Spülung des Cache-Bedarfs
 a|
Die Cachetroscherung „Start Demand“ gibt den Prozentsatz der nicht
geschriebenen Daten im Cache an, die eine Cachetülung auslösen (auf die
Festplatte schreiben). Standardmäßig wird die Cache-Spülung gestartet,
wenn nicht geschriebene Daten eine Kapazität von 80 % erreichen. Ein
höherer Prozentsatz ist eine gute Wahl für Umgebungen, in denen in erster
Linie Schreibvorgänge ausgeführt werden. Neue Schreibanforderungen können
durch den Cache verarbeitet werden, ohne auf die Festplatte zugreifen zu
müssen. Niedrigere Einstellungen sind besser in Umgebungen, in denen der
I/O unzuverlässig ist (bei sprunghaften Datenanbrüchen), sodass das System
häufig zwischen Datenstoßweisen den Cache-Speicher aufschreibt. Ein
niedriger Startprozentsatz als 80 % kann jedoch zu einer
Leistungssteigerung führen.



 a|
Cache-Blockgröße
 a|
Die Cache-Blockgröße bestimmt die maximale Größe jedes Cache-Blocks. Diese
Einheit ist eine Organisationseinheit für das Cache Management.
Standardmäßig ist die Blockgröße 32 KiB. Das System ermöglicht die Cache-
Blockgröße von 4, 8, 16 oder 32 KiBs. Applikationen verwenden
unterschiedliche Blockgrößen, die sich auf die Storage-Performance
auswirken. Kleinere Größen sind eine gute Wahl für Dateisysteme oder
Datenbankanwendungen. Eine größere Größe eignet sich ideal für
Anwendungen, die sequenzielle I/O-Vorgänge wie Multimedia generieren.

|===
.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Scrollen Sie nach unten zu *zusätzliche Einstellungen* und klicken Sie
dann auf *Cache-Einstellungen ändern*.
+
Das Dialogfeld Cache-Einstellungen ändern wird geöffnet.

. Passen Sie die folgenden Werte an:
+
** *Starten Sie die Cachespülung der Nachfrage* -- Wählen Sie einen
Prozentsatz, der für die in Ihrer Umgebung verwendeten I/O-Vorgänge
geeignet ist. Wenn Sie sich für einen Wert unter 80 % entscheiden, können
Sie eine verminderte Leistung feststellen.
** **Cache Blockgröße -- **Wählen Sie eine Größe, die für Ihre Anwendungen
geeignet ist.
```

```
. Klicken Sie Auf *Speichern*.




[[ID121207dbb159d1fc002eaa52f49ee60a]]
= Automatische Lastverteilung festlegen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die Funktion Automatic Load Balancing stellt sicher, dass eingehender I/O-
Datenverkehr von den Hosts dynamisch verwaltet und auf beiden Controllern
ausgeglichen wird. Diese Funktion ist standardmäßig aktiviert, Sie können
sie jedoch aus dem SANtricity System Manager deaktivieren.

.Über diese Aufgabe
Wenn der automatische Lastenausgleich aktiviert ist, führt er folgende
Funktionen aus:

* Automatische Überwachung und ausgewogene Nutzung von Controller-
Ressourcen
* Bei Bedarf passt die Volume-Controller-Eigentümerschaft automatisch an,
was die I/O-Bandbreite zwischen Hosts und Storage Array optimiert.


Aus den folgenden Gründen möchten Sie den automatischen Lastausgleich auf
Ihrem Speicher-Array deaktivieren:

* Sie möchten die Controller-Eigentumsrechte eines bestimmten Volumes
nicht automatisch ändern, um einen Workload-Ausgleich zu schaffen.
* Sie arbeiten in einer hoch abgestimmten Umgebung, in der die
Lastverteilung gezielt eingerichtet ist, um eine bestimmte Verteilung
zwischen den Controllern zu erreichen.


.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Scrollen Sie nach unten zu *zusätzliche Einstellungen* und klicken Sie
dann auf *Automatischer Lastenausgleich aktivieren/deaktivieren*.
+
Der Text unter dieser Option gibt an, ob die Funktion derzeit aktiviert
```

```
oder deaktiviert ist.

+
Ein Bestätigungsdialogfeld wird geöffnet.

. Bestätigen Sie, indem Sie auf *Ja* klicken, um fortzufahren.
+
Wenn Sie diese Option auswählen, schalten Sie die Funktion zwischen
aktiviert/deaktiviert ein.

+
[NOTE]
====
Wenn diese Funktion von deaktiviert auf aktiviert verschoben wird, wird
auch die Funktion Host Connectivity Reporting automatisch aktiviert.

====




[[ID62eb0dbf1ad6b92040f84063c9e41982]]
= Aktivieren oder deaktivieren Sie die veraltete Managementoberfläche
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die Legacy-Managementoberfläche (Symbol) aktivieren oder
deaktivieren, eine Kommunikationsmethode zwischen dem Storage-Array und
dem Management-Client.

.Über diese Aufgabe
Standardmäßig ist die ältere Managementoberfläche auf aktiviert. Wenn die
Funktion deaktiviert wird, verwendet das Storage-Array und der Management-
Client eine sicherere Kommunikationsmethode (REST-API über HTTPS).
Bestimmte Tools und Aufgaben können jedoch beeinträchtigt werden, wenn die
Übertragung deaktiviert ist.

[NOTE]
====
Für das EF600 Storage-System ist diese Funktion standardmäßig deaktiviert.

====
```

Die Einstellung wirkt sich auf die Vorgänge wie folgt aus:

* *Ein* (Standard) -- erforderliche Einstellung zum Konfigurieren der Spiegelung mit der CLI und einigen anderen Tools, wie dem OCI-Adapter.
* *Aus* -- erforderliche Einstellung zur Durchsetzung von Vertraulichkeit bei der Kommunikation zwischen dem Speicher-Array und dem Management-Client und zum Zugriff auf externe Tools. Empfohlene Einstellung bei der Konfiguration eines Verzeichnisservers (LDAP).

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Blättern Sie nach unten zu *zusätzliche Einstellungen*, und klicken Sie dann auf *Verwaltungsschnittstelle ändern*.
. Klicken Sie im Dialogfeld auf *Ja*, um fortzufahren.

:leveloffset: -1

= Add-on-Funktionen konfigurieren

:leveloffset: +1

[[IDafdf035fae83be504026bfda93e3b1e7]]
= Funktionsweise der Add-on-Funktionen
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Bei Add-ons handelt es sich um Funktionen, die nicht in der Standardkonfiguration von SANtricity System Manager enthalten sind, und die möglicherweise eine Schlüsselfunktion erfordern. Eine Add-on-Funktion kann entweder eine einzelne Premium-Funktion oder ein im Paket enthaltene Features sein.

Die folgenden Schritte geben einen Überblick über die Aktivierung einer Premium-Funktion oder eines Features-Packs:

. Beziehen Sie sich auf folgende Informationen:
+

```
** Seriennummer des Gehäuses und Feature Enable Identifier, die das
Speicher-Array für das zu installierende Feature identifizieren. Diese
Elemente sind in System Manager verfügbar.
** Aktivierungscode für die Funktion, der bei Kauf der Funktion auf der
Support-Website verfügbar ist.


. Erhalten Sie den Funktionsschlüssel, indem Sie sich an Ihren Storage-
Provider wenden oder den Standort zur Aktivierung der Premium-Funktion
aufrufen. Geben Sie die Seriennummer des Gehäuses, aktivieren Sie den
Bezeichner und den Funktionscode für die Aktivierung an.
. Aktivieren Sie mit System Manager die Premium-Funktion oder das Feature
Pack mithilfe der Feature-Key-Datei.




[[ID3d0cadff2fc53c2e695f947f1c0af88e]]
= Terminologie der Add-on-Funktionen
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Erfahren Sie, welche Zusatzfunktionenbedingungen auf Ihr Storage Array
Anwendung finden.

[cols="25h,~"]
|===
| Laufzeit | Beschreibung


 a|
Kennzeichner Für Feature-Aktivierung
 a|
Eine Kennzeichenkennung für die Aktivierung einer Funktion ist eine
eindeutige Zeichenfolge, die das spezifische Speicherarray identifiziert.
Mit dieser Kennung wird sichergestellt, dass die Premium-Funktion nur mit
dem jeweiligen Speicherarray verknüpft ist. Dieser String wird unter Add-
ons auf der Systemseite angezeigt.



 a|
Feature-Schlüsseldatei
```

```
 a|
Eine Feature-Schlüsseldatei ist eine Datei, die Sie zum Entsperren und
Aktivieren einer Premium-Funktion oder eines Feature-Packs erhalten.



 a|
Funktionspaket
 a|
Ein Funktionspaket ist ein Bundle, das Attribute für Storage Arrays ändert
(zum Beispiel Ändern des Protokolls von Fibre Channel auf iSCSI). Für die
Aktivierung der Funktionen ist ein spezieller Schlüssel erforderlich.



 a|
Premiumfunktion
 a|
Eine Premium-Funktion ist eine zusätzliche Option, die einen Schlüssel
erfordert, um sie zu aktivieren. Dies ist nicht in der
Standardkonfiguration von System Manager enthalten.

|===



[[ID7b37a6b04367336124f4bdf779ca84b9]]
= Abrufen einer Feature-Schlüsseldatei
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um ein Premium Feature oder Feature Pack auf Ihrem Speicher-Array zu
aktivieren, müssen Sie zuerst eine Feature Key-Datei erhalten. Ein
Schlüssel ist nur einem Storage-Array zugeordnet.

.Über diese Aufgabe
In dieser Aufgabe wird beschrieben, wie die erforderlichen Informationen
für die Funktion gesammelt werden und anschließend eine Anforderung für
eine Feature Key-Datei gesendet wird. Erforderliche Informationen:

* Seriennummer des Chassis
* Kennzeichner Für Feature-Aktivierung
```

* Aktivierungscode Für Die Funktion

.Schritte
. Suchen Sie in System Manager die Seriennummer des Chassis und notieren Sie sie. Sie können sich diese Seriennummer anzeigen lassen, indem Sie den Mauszeiger über die Kachel Support Center bewegen.
. Suchen Sie in System Manager nach der Feature Enable Identifier. Gehen Sie zum Menü:Einstellungen[System], und scrollen Sie dann nach unten zu *Add-ons*. Suchen Sie nach der *Feature Enable Identifier*. Notieren Sie die Nummer für den Kennzeichner der Feature Enable.
. Suchen und notieren Sie den Code für die Aktivierung der Funktion. Für Features Packs wird dieser Code in den entsprechenden Anweisungen zur Durchführung der Konvertierung angegeben.
+
Bei Premium-Funktionen können Sie über die Support-Website auf den Aktivierungscode zugreifen:

+
.. Melden Sie sich bei an https://mysupport.netapp.com/site/global/dashboard["NetApp Support"^].
.. Gehen Sie zu *Software-Lizenzen* für Ihr Produkt.
.. Geben Sie die Seriennummer für das Speicher-Array-Chassis ein, und klicken Sie dann auf *Los*.
.. Suchen Sie in der Spalte *Lizenzschlüssel* nach den Aktivierungscodes für die Funktion.
.. Notieren Sie den Aktivierungscode der Funktion für die gewünschte Funktion.

. Fordern Sie eine Funktionsschlüsseldatei an, indem Sie eine E-Mail oder ein Textdokument an Ihren Speicheranbieter senden, und zwar mit folgenden Informationen: Chassis-Seriennummer, Enable-ID und Code zur Aktivierung der Funktion.
+
Sie können auch zu gehen http://partnerspfk.netapp.com["Aktivierung der NetApp Lizenz: Aktivierung der Premium-Funktionen von Storage Array"^] Und geben Sie die erforderlichen Informationen ein, um die Funktion oder das Funktionspaket zu erhalten. (Die Anweisungen auf dieser Website gelten für Premium-Funktionen, nicht für Funktionspakete.)

.Nachdem Sie fertig sind
Wenn Sie über eine Feature Key-Datei verfügen, können Sie das Premium Feature oder Feature Pack aktivieren.

```
[[ID225f593a9c0ef59ef865fce1206c0832]]
= Aktivieren Sie eine Premiumfunktion
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Eine Premium-Funktion ist eine zusätzliche Option, die einen Schlüssel zur
Aktivierung erfordert.

.Bevor Sie beginnen
* Sie haben einen Funktionschlüssel erhalten. Wenden Sie sich bei Bedarf
an den technischen Support, um einen Schlüssel zu erhalten.
* Sie haben die Schlüsseldatei auf den Management-Client geladen (das
System mit einem Browser zum Zugriff auf System Manager).


.Über diese Aufgabe
In dieser Aufgabe wird beschrieben, wie Sie mit System Manager eine
Premium-Funktion aktivieren.

[NOTE]
====
Wenn Sie eine Premium-Funktion deaktivieren möchten, müssen Sie den Befehl
„Speicher-Array-Funktion deaktivieren“ verwenden (`disable storageArray)
(featurePack | feature=featureAttributeList`) In der
Befehlszeilenschnittstelle (CLI).

====
.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter *Add-ons* die Option *Premium Feature aktivieren*.
+
Das Dialogfeld Premium-Funktion aktivieren wird geöffnet.

. Klicken Sie auf *Durchsuchen* und wählen Sie dann die Schlüsseldatei
aus.
+
Der Dateiname wird im Dialogfeld angezeigt.

. Klicken Sie Auf *Aktivieren*.
```

```
[[ID1f838c73ecb6a711c7074fb133b06e72]]
= Funktionspaket aktivieren
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Ein Funktionspaket ist ein Bundle, das Attribute für Storage Arrays ändert
(zum Beispiel Ändern des Protokolls von Fibre Channel auf iSCSI).
Funktionspakete erfordern einen speziellen Schlüssel für die
Unterstützung.

.Bevor Sie beginnen
* Sie haben die entsprechenden Anweisungen zur Konvertierung und zur
Vorbereitung der Attribute des neuen Speicherarrays befolgt. Eine
Anleitung zur Hostprotokollkonvertierung finden Sie im Hardware-
Wartungsleitfaden für Ihr Controller-Modell.
* Das Storage-Array ist offline, sodass keine Hosts oder Applikationen auf
das Array zugreifen können.
* Alle Daten werden gesichert.
* Sie haben eine Feature Pack-Datei erhalten.
+
Die Feature Pack-Datei wird auf den Management-Client geladen (das System
mit einem Browser für den Zugriff auf System Manager).



[NOTE]
====
Sie müssen ein Downtime-Wartungsfenster planen und alle I/O-Vorgänge
zwischen dem Host und den Controllern beenden. Beachten Sie außerdem, dass
Sie erst nach erfolgreichem Abschluss der Konvertierung auf Daten im
Speicher-Array zugreifen können.

====
.Über diese Aufgabe
In dieser Aufgabe wird beschrieben, wie Sie mit System Manager ein
Funktionspaket aktivieren. Wenn Sie fertig sind, müssen Sie das Speicher-
Array neu starten.

.Schritte
```

```
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter *Add-ons* die Option *Feature Pack ändern*.
. Klicken Sie auf *Durchsuchen* und wählen Sie dann die Schlüsseldatei
aus.
+
Der Dateiname wird im Dialogfeld angezeigt.

. Typ `change` Vor Ort.
. Klicken Sie Auf *Ändern*.
+
Die Funktionspaket-Migration beginnt und die Controller werden neu
gestartet. Nicht geschriebene Cache-Daten werden gelöscht, wodurch keine
I/O-Aktivität gewährleistet wird. Beide Controller werden automatisch neu
gestartet, damit das neue Feature Pack wirksam wird. Das Speicher-Array
kehrt nach Abschluss des Neubootens in einen reaktionsfähigen Zustand
zurück.




:leveloffset: -1


[[IDa7fbf6778481fc870033da0ccd387328]]
= Befehlszeilenschnittstelle (CLI) herunterladen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können das Paket für die Befehlszeilenschnittstelle (CLI) von
SANtricity System Manager herunterladen.

Die CLI bietet eine textbasierte Methode zur Konfiguration und Überwachung
von Speicher-Arrays. Es kommuniziert über HTTPS und verwendet dieselbe
Syntax wie die CLI, die im extern installierten Managementsoftwarepaket
verfügbar ist. Zum Herunterladen der CLI ist kein Schlüssel erforderlich.

.Bevor Sie beginnen
Eine Java Runtime Environment (JRE), Version 8 und höher, muss auf dem
Managementsystem verfügbar sein, auf dem Sie die CLI-Befehle ausführen
möchten.
```

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter *Add-ons* die Option *Command Line Interface*.
+
Das ZIP-Paket wird in den Browser heruntergeladen.

. Speichern Sie die ZIP-Datei im Verwaltungssystem, in dem Sie CLI-Befehle für das Speicher-Array ausführen möchten, und extrahieren Sie dann die Datei.
+
Sie können jetzt CLI-Befehle von einer Betriebssystemaufforderung ausführen, z. B. von der DOS C:-Eingabeaufforderung. Eine CLI-Befehlsreferenz steht im Menü Hilfe oben rechts in der System Manager-Benutzeroberfläche zur Verfügung.

= FAQs

:leveloffset: +1

[[ID2bcdfa1b1cb5ad737c9e80b9f36fd82a]]
= Was ist der automatische Lastausgleich?
:allow-uri-read:
:icons: font
:relative_path: ./sm-storage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Die Funktion „Automatischer Lastausgleich“ bietet einen automatischen I/O-Ausgleich und stellt sicher, dass eingehender I/O-Datenverkehr von den Hosts auf beiden Controllern dynamisch verwaltet und ausgeglichen wird.

Die Funktion Automatic Load Balancing bietet ein verbessertes I/O-Ressourcenmanagement, das dynamisch auf Laständerungen im Laufe der Zeit reagiert und die Eigentümerschaft der Volume-Controller automatisch angepasst wird, um Probleme bei der Lastverteilung, die zwischen den Controllern verschoben werden, zu beheben.

Die Auslastung jedes Controllers wird kontinuierlich überwacht und, zusammen mit den auf den Hosts installierten Multipath-Treibern, kann bei Bedarf automatisch ausgeglichen werden. Wenn die Workload automatisch auf die Controller umverteilt wird, entlastet der Storage-Administrator die

manuelle Anpassung der Eigentümerschaft der Volume Controller, um Laständerungen am Storage Array zu bewältigen.

Wenn der automatische Lastenausgleich aktiviert ist, führt er folgende Funktionen aus:

* Automatische Überwachung und ausgewogene Nutzung von Controller-Ressourcen
* Bei Bedarf passt die Volume-Controller-Eigentümerschaft automatisch an, was die I/O-Bandbreite zwischen Hosts und Storage Array optimiert.

[NOTE]
====
Jedes Volume, das der Nutzung des SSD-Caches eines Controllers zugewiesen ist, kann keine automatische Lastverteilung durchführen.

====

[[ID28eb964135e13c942fe0fd257a343adf]]
= Was ist der Controller Cache?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Der Controller-Cache ist ein physischer Speicherplatz, der zwei Arten von I/O-Vorgängen (Input/Output) vereinfacht: Zwischen den Controllern und Hosts sowie zwischen den Controllern und Festplatten.

Beim Lesen und Schreiben von Datentransfers kommunizieren die Hosts und Controller über High-Speed-Verbindungen. Die Kommunikation zwischen dem Backend des Controllers und den Festplatten ist jedoch langsamer, da die Festplatten relativ langsam sind.

Wenn der Controller-Cache Daten erhält, bestätigt der Controller den Host-Applikationen, dass er jetzt die Daten hält. Auf diese Weise müssen die Host-Applikationen nicht warten, bis der I/O auf die Festplatte geschrieben wird. Stattdessen können Applikationen den Betrieb fortsetzen. Auf die im Cache gespeicherten Daten können zudem von Server-Applikationen schnell zugegriffen werden, sodass kein zusätzliches Lesen von Festplatten erforderlich ist, um auf die Daten zuzugreifen.

Der Controller-Cache wirkt sich auf die Gesamt-Performance des Storage Arrays aus:

* Der Cache fungiert als Puffer, sodass die Übertragung von Host- und Festplattendaten nicht synchronisiert werden muss.
* Die Daten eines Lese- oder Schreibvorgangs vom Host befinden sich möglicherweise im Cache eines vorherigen Vorgangs, sodass kein Zugriff auf die Festplatte erforderlich ist.
* Bei Verwendung von Schreib-Caching kann der Host nachfolgende Schreibbefehle senden, bevor die Daten eines früheren Schreibvorgangs auf die Festplatte geschrieben werden.
* Wenn Cache-Prefetch aktiviert ist, wird der sequenzielle Lesezugriff optimiert. Cache Prefetch sorgt für einen Lesevorgang, bei dem die Daten im Cache gefunden werden, anstatt die Daten von der Festplatte zu lesen.

[CAUTION]
====
Möglicher Datenverlust -- Wenn Sie die *Write Caching ohne Batterien* Option aktivieren 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 Option *Write Caching ohne Batterien* aktivieren.

====

[[IDf9fa8542571d83fa6d8a6edaca9d564f]]
= Was wird Cachespülung?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Wenn die Menge der nicht geschriebenen Daten im Cache eine bestimmte Ebene erreicht, schreibt der Controller regelmäßig Cache-Daten auf ein Laufwerk. Dieser Schreibvorgang wird als „Spülen“ bezeichnet.

Der Controller verwendet zwei Algorithmen für das Spülen von Cache: Bedarfsbasiert und altersbasiert. Der Controller verwendet einen bedarfsorientierten Algorithmus, bis die Menge der im Cache gespeicherten Daten unter den Schwellenwert für die Cache-Spülung fällt. Standardmäßig beginnt ein Flush, wenn 80 Prozent des Caches verwendet werden.

In System Manager können Sie den Schwellenwert für „`Start Demand Cache Flush`“ festlegen, um den in Ihrer Umgebung verwendeten I/O-Typ optimal zu unterstützen. In einer Umgebung, in der hauptsächlich Schreibvorgänge ausgeführt werden, sollten Sie den „`Start Demand Cache Flush`“-Prozentsatz hoch einstellen, um die Wahrscheinlichkeit zu erhöhen, dass neue Schreibanforderungen durch den Cache verarbeitet werden können, ohne auf die Festplatte gehen zu müssen. Eine Einstellung mit hohem Prozentsatz begrenzt die Anzahl der Cache-Flushes, so dass mehr Daten im Cache verbleiben, was die Wahrscheinlichkeit von mehr Cache-Treffern erhöht.

In einer Umgebung, in der der I/O unregelmäßig ist (bei sprunghaften Datenanbrüchen), können Sie geringe Cache-Schreibvorgänge verwenden, sodass das System häufig zwischen Datenstoßweisen den Cache-Speicher stürzt. In einer vielfältigen I/O-Umgebung, die eine Vielzahl von Lasten verarbeitet, oder wenn die Lasttypen unbekannt sind, setzen Sie den Schwellenwert auf 50 Prozent als guter Mittelweg. Wenn Sie einen Startprozentsatz unter 80 Prozent wählen, können Sie eine verminderte Leistung feststellen, da die Daten für einen Host-Lesevorgang möglicherweise nicht verfügbar sind. Wird ein niedrigerer Prozentsatz ausgewählt, erhöht sich auch die Anzahl der Festplattenschreibvorgänge, die zur Aufrechterhaltung des Cache-Levels erforderlich sind, was den System-Overhead erhöht.

Der altersbasierte Algorithmus legt fest, wie lange die Schreibvorgänge im Cache verbleiben können, bevor sie auf die Festplatten gespeichert werden können. Die Controller verwenden den altersbasierten Algorithmus, bis der Schwellenwert für den Cache-Spülvorgang erreicht ist. Der Standardwert beträgt 10 Sekunden, dieser Zeitraum wird jedoch nur in Zeiten der Inaktivität gezählt. Sie können den Spülzeitpunkt in System Manager nicht ändern. Stattdessen müssen Sie den Befehl *Set Storage Array* in der Befehlszeilenschnittstelle (CLI) verwenden.

[CAUTION]
====
Möglicher Datenverlust -- Wenn Sie die *Write Caching ohne Batterien* Option aktivieren 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 Option *Write Caching ohne Batterien* aktivieren.

====

[[ID5ac2384a97e0ca29dc388f6950f5691b]]
= Was ist die Cache-Blockgröße?

```
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Der Controller des Storage Arrays ordnet den Cache in „Blöcke“ ein. Dabei handelt es sich um Speicherblöcke, die 8, 16 und 32 KiB groß sein können. Alle Volumes im Storage-System nutzen denselben Cache-Speicherplatz. Daher können die Volumes nur eine Cache-Blockgröße aufweisen.

Applikationen verwenden unterschiedliche Blockgrößen, die wiederum einen Einfluss auf die Storage-Performance haben können. Standardmäßig ist die Blockgröße in System Manager 32 KiB, Sie können den Wert jedoch auf 8, 16, 32 KiBs festlegen. Kleinere Größen sind eine gute Wahl für Dateisysteme oder Datenbankanwendungen. Eine größere Größe ist eine gute Wahl für Applikationen, die eine umfangreiche Datenübertragung, sequenziellen I/O oder eine hohe Bandbreite, wie z. B. Multimedia, erfordern.



[[ID5956f3c4e0886a0b26bac396e89be1d2]]
= Wann sollte ich Speicherarray-Uhren synchronisieren?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie sollten die Controller-Uhren im Speicher-Array manuell synchronisieren, wenn Sie bemerken, dass die in SANtricity System Manager angezeigten Zeitstempel nicht auf die im Management-Client angezeigten Zeitstempel ausgerichtet sind (der Computer, der über den Browser auf SANtricity System Manager zugreift). Diese Aufgabe ist nur erforderlich, wenn NTP (Network Time Protocol) im SANtricity-System-Manager nicht aktiviert ist.

[NOTE]
====
Es wird dringend empfohlen, einen NTP-Server zu verwenden, statt die Uhren manuell zu synchronisieren. NTP synchronisiert die Uhren automatisch mit einem externen Server mithilfe von SNTP (Simple Network Time Protocol).

====
Sie können den Synchronisierungsstatus über das Dialogfeld Speicherarray-
```

```
Uhren synchronisieren überprüfen, das auf der Seite System verfügbar ist.
Wenn die im Dialogfeld angezeigten Zeiten nicht übereinstimmen, führen Sie
eine Synchronisierung aus. Sie können dieses Dialogfeld in regelmäßigen
Abständen anzeigen, in dem angezeigt wird, ob die Zeitanzeigen der
Controller-Uhren auseinander getrieben wurden und nicht mehr
synchronisiert sind.



:leveloffset: -1


:leveloffset: -1


= Laufwerkssicherheit

:leveloffset: +1


[[ID08d61960f76d1eaa9bb0580b37e17e31]]
= Übersicht über die Laufwerkssicherheit
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die Laufwerksicherheit und die Schlüsselverwaltung über die
Seite Sicherheitsschlüsselverwaltung konfigurieren.



== Was ist Laufwerkssicherheit?

_Drive Security_ ist eine Funktion, die unberechtigten Zugriff auf Daten
auf sicheren Laufwerken verhindert, wenn sie aus dem Speicher-Array
entfernt werden. Dabei können es sich entweder um vollständige
Festplattenverschlüsselung (Full Disk Encryption, FDE)-Laufwerke oder um
FIPS-Laufwerke (Federal Information Processing Standard) handeln. Wenn
FDE- oder FIPS-Laufwerke physisch aus dem Array entfernt werden, kann
dieser erst betrieben werden, wenn sie in einem anderen Array installiert
sind. Dann befinden sich die Laufwerke erst dann in einem
sicherheitsrelevanten Zustand, wenn der richtige Sicherheitsschlüssel
bereitgestellt wird. Ein _Sicherheitsschlüssel_ ist eine Zeichenkette, die
```

von diesen Laufwerkstypen und den Controllern in einem Speicher-Array gemeinsam genutzt wird.

Weitere Informationen:

* xref:{relative_path}how-the-drive-security-feature-works.html["Funktionsweise der Laufwerkssicherheitsfunktion"]
* xref:{relative_path}how-security-key-management-works.html["Funktionsweise von Sicherheitsschlüsselmanagement"]
* xref:{relative_path}drive-security-terminology.html["Terminologie der Laufwerksicherheit"]

== Wie konfiguriere ich Verschlüsselungsmanagement?

Zur Implementierung von Laufwerkssicherheit müssen entweder FDE- oder FIPS-Laufwerke im Array installiert sein. Um die Schlüsselverwaltung für diese Laufwerke zu konfigurieren, gehen Sie zum Menü:Einstellungen[System > Sicherheitsschlüsselverwaltung], wo Sie entweder einen internen Schlüssel aus dem persistenten Speicher des Controllers oder einen externen Schlüssel von einem Schlüsselverwaltungsserver aus erstellen können. Schließlich aktivieren Sie die Laufwerksicherheit für Pools und Volume-Gruppen, indem Sie in den Volume-Einstellungen „sicher-fähig“ auswählen.

Weitere Informationen:

* xref:{relative_path}create-internal-security-key.html["Interner Sicherheitsschlüssel erstellen"]
* xref:{relative_path}create-external-security-key.html["Externen Sicherheitsschlüssel erstellen"]
* xref:{relative_path}../sm-storage/create-pool-manually.html["Pool manuell erstellen"]
* xref:{relative_path}../sm-storage/create-volume-group.html["Volume-Gruppen erstellen"]

== Wie entsperre ich Laufwerke?

Wenn Sie das Verschlüsselungsmanagement konfiguriert haben und später sichere Laufwerke von einem Speicher-Array auf ein anderes verschieben, müssen Sie den Sicherheitsschlüssel dem neuen Speicher-Array neu zuweisen, um Zugriff auf die verschlüsselten Daten auf den Laufwerken zu erhalten.

```
Weitere Informationen:

* xref:{relative_path}unlock-drives-using-an-internal-security-
key.html["Entsperren Sie Laufwerke bei Nutzung des internen
Verschlüsselungsmanagements"]
* xref:{relative_path}unlock-drives-using-an-external-security-
key.html["Entsperren von Laufwerken bei Verwendung von externer
Schlüsselverwaltung"]




== Verwandte Informationen

Weitere Informationen zu Aufgaben im Zusammenhang mit
Verschlüsselungsmanagement:

* xref:{relative_path}use-ca-signed-certificates-for-authentication-with-
a-key-management-server.html["Verwenden Sie CA-signierte Zertifikate zur
Authentifizierung mit einem Schlüsselverwaltungsserver"]
* xref:{relative_path}back-up-security-key.html["Sicherheitsschlüssel
sichern"]




= Konzepte

:leveloffset: +1


[[IDdc292993c8e6af96c8dcfefb87ba9f97]]
= Funktionsweise der Laufwerkssicherheitsfunktion
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Laufwerkssicherheit ist eine Funktion des Storage Arrays, die eine
zusätzliche Sicherheitsschicht bietet – entweder mit vollständigen
Festplatten-Verschlüsselung (FDE) oder FIPS-Laufwerken (Federal
Information Processing Standard).

Wenn diese Laufwerke zusammen mit der Sicherheitsfunktion des Laufwerks
```

verwendet werden, benötigen sie einen Sicherheitsschlüssel für den Zugriff auf ihre Daten. Wenn die Laufwerke physisch aus dem Array entfernt werden, können sie erst betrieben werden, wenn sie in einem anderen Array installiert sind. Zu diesem Zeitpunkt befinden sie sich in einem Sicherheitsstatus, bis der richtige Sicherheitsschlüssel bereitgestellt wird.

== So implementieren Sie Drive Security

Um die Laufwerkssicherheit zu implementieren, führen Sie die folgenden Schritte aus.

. Rüsten Sie Ihr Storage-Array mit sicheren Laufwerken aus – entweder mit FDE- oder mit FIPS-Laufwerken. (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.)
. Erstellen Sie einen Sicherheitsschlüssel, d. h. eine Zeichenkette, die vom Controller und den Laufwerken für Lese-/Schreibzugriff freigegeben wird. Sie können entweder einen internen Schlüssel aus dem persistenten Speicher des Controllers oder einen externen Schlüssel von einem Schlüsselmanagementserver erstellen. Für das externe Verschlüsselungsmanagement muss eine Authentifizierung mit dem Verschlüsselungsmanagement-Server eingerichtet werden.
. Aktivieren Sie die Laufwerkssicherheit für Pools und Volume-Gruppen:
+
** Erstellen Sie einen Pool oder eine Volume-Gruppe (suchen Sie in der Spalte *Secure-able* in der Tabelle Kandidaten nach *Ja*).
** Wählen Sie einen Pool oder eine Volume-Gruppe aus, wenn Sie ein neues Volume erstellen (suchen Sie nach *Ja* neben *sicher-fähig* in der Tabelle für Pool- und Volume-Gruppen Kandidaten).

== Wie Drive Security auf der Laufwerksebene funktioniert

Ein sicheres Laufwerk mit FDE oder FIPS verschlüsselt Daten beim Schreiben und entschlüsselt Daten beim Lesen. Diese Ver- und Entschlüsselung hat keine Auswirkungen auf die Leistung oder den Anwender-Workflow. Jedes Laufwerk verfügt über einen eigenen eindeutigen Verschlüsselungsschlüssel,

der nie vom Laufwerk übertragen werden kann.

Die Sicherheitsfunktion des Laufwerks bietet zusätzlichen Schutz durch sichere Laufwerke. Wenn auf diesen Laufwerken Volume-Gruppen oder -Pools zur Laufwerkssicherheit ausgewählt sind, suchen die Laufwerke nach einem Sicherheitsschlüssel, bevor sie den Zugriff auf die Daten zulassen. Die Laufwerkssicherheit für Pools und Volume-Gruppen kann jederzeit aktiviert werden, ohne dass bestehende Daten auf dem Laufwerk beeinträchtigt werden. Allerdings können Sie die Laufwerksicherheit nicht deaktivieren, ohne alle Daten auf dem Laufwerk zu löschen.

== So arbeitet Drive Security auf Ebene des Storage Arrays

Mit der Laufwerkssicherheitsfunktion erstellen Sie einen Sicherheitsschlüssel, der von den sicheren Laufwerken und Controllern in einem Speicher-Array gemeinsam genutzt wird. Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln die sicher-aktivierten Laufwerke in den Status Sicherheitsverriegelt, bis der Controller den Sicherheitsschlüssel anwendet.

Wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt und in einem anderen Speicher-Array neu installiert wird, befindet sich das Laufwerk in einem gesperrten Zustand. Das neu aufgelegene Laufwerk sucht nach dem Sicherheitsschlüssel, bevor es die Daten wieder zugänglich macht. Um die Daten zu entsperren, wenden Sie den Sicherheitsschlüssel aus dem Quell-Speicher-Array an. Nach erfolgreicher Entsperrung verwendet das neu aufgelegte Laufwerk dann den bereits im Ziel-Speicher-Array gespeicherten Sicherheitsschlüssel und die importierte Sicherheitsschlüsseldatei wird nicht mehr benötigt.

[NOTE]
====
Für das interne Verschlüsselungsmanagement wird der tatsächliche Sicherheitsschlüssel auf dem Controller an einem nicht zugänglichen Ort gespeichert. Sie ist weder in menschlich lesbarem Format, noch ist sie vom Benutzer zugänglich.

====

== So arbeitet Drive Security auf Volume-Ebene

Wenn Sie einen Pool oder eine Volume-Gruppe aus sicheren Laufwerken erstellen, können Sie auch die Laufwerksicherheit für diese Pools oder Volume-Gruppen aktivieren. Mit der Option Laufwerkssicherheit können die

Laufwerke und damit verbundene Volume-Gruppen und Pools sicher-_enabled_ erstellt werden.

Beachten Sie die folgenden Richtlinien, bevor Sie Volume-Gruppen und -Pools mit sicheren Aktivierung erstellen:

* Volume-Gruppen und Pools müssen vollständig aus sicheren Laufwerken bestehen. (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.)
* Volume-Gruppen und Pools müssen sich im optimalen Zustand befinden.

[[ID1b47d9661d152212f74dbb350fc206fd]]
= Funktionsweise von Sicherheitsschlüsselmanagement
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Bei der Implementierung der Laufwerkssicherheitsfunktion benötigen die sicheren Laufwerke (FIPS oder FDE) einen Sicherheitsschlüssel für den Datenzugriff. Ein Sicherheitsschlüssel ist eine Zeichenkette, die zwischen diesen Laufwerkstypen und den Controllern in einem Speicher-Array gemeinsam verwendet wird.

Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln die sicher-aktivierten Laufwerke in den Status Sicherheitsverriegelt, bis der Controller den Sicherheitsschlüssel anwendet. Wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt wird, sind die Daten des Laufwerks gesperrt. Wenn das Laufwerk in einem anderen Speicher-Array neu installiert wird, sucht es nach dem Sicherheitsschlüssel, bevor es die Daten wieder zugänglich macht. Um die Daten zu entsperren, müssen Sie den ursprünglichen Sicherheitsschlüssel anwenden.

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 gepflegt und „`hidden`“ in einem nicht zugänglichen Ort im persistenten Speicher des Controllers gespeichert. Führen Sie folgende Schritte durch, um das interne Verschlüsselungsmanagement zu implementieren:

. 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.
. 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.
. Erstellen Sie einen internen Sicherheitsschlüssel, der das Definieren 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. Um einen internen Schlüssel zu erstellen, gehen Sie zu Menü:Einstellungen[System > Sicherheitsschlüsselverwaltung > Internen Schlüssel erstellen].

Der Sicherheitsschlüssel wird auf dem Controller an einem verborgenen, 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. Um externes Verschlüsselungsmanagement zu implementieren, führen Sie die folgenden Schritte aus:

. 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.
. 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.
. Abrufen einer signierten Client-Zertifikatdatei. Ein Client-Zertifikat
validiert die Controller des Storage-Arrays, damit der
Verschlüsselungsmanagement-Server ihren KMIP-Anforderungen vertrauen kann.
+
.. Zunächst haben Sie eine Client Certificate Signing Request (CSR)
abgeschlossen und heruntergeladen. Wechseln Sie zum
Menü:Einstellungen[Zertifikate > Schlüsselverwaltung > CSR abschließen].
.. Als Nächstes fordern Sie ein signiertes Clientzertifikat von einer
Zertifizierungsstelle an, die vom Schlüsselverwaltungsserver
vertrauenswürdig ist. (Sie können auch mithilfe der CSR-Datei ein Client-
Zertifikat vom Schlüsselverwaltungsserver erstellen und herunterladen.)
.. Sobald Sie über eine Clientzertifikatdatei verfügen, kopieren Sie diese
Datei auf den Host, auf dem Sie auf System Manager zugreifen.
.. Alternativ können Sie eine Zertifikatsignierungsanforderung extern mit
einem privaten und öffentlichen Schlüsselpaar erstellen.


. 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.
. Erstellen eines externen Schlüssels, der die IP-Adresse des
Verschlüsselungsmanagement-Servers und die Port-Nummer, die für die KMIP-
Kommunikation verwendet wird, definiert. Während dieses Prozesses laden
Sie auch Zertifikatdateien. Um einen externen Schlüssel zu erstellen,
gehen Sie zu Menü:Einstellungen[System > Sicherheitsschlüsselverwaltung >
External Key erstellen].


Das System stellt mit den eingegebenen Anmeldedaten eine Verbindung zum
Schlüsselverwaltungsserver her. Anschließend können sichere Volume-Gruppen
und -Pools erstellt oder die Sicherheit für vorhandene Volume-Gruppen und
-Pools aktiviert werden.



[[ID576ff58c4bb044fdf946b10b21d1220a]]
= Terminologie der Laufwerksicherheit
```

```
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Erfahren Sie, wie die Bedingungen für die Laufwerksicherheit auf Ihr
Speicherarray angewendet werden.

[cols="25h,~"]
|===
| Laufzeit | Beschreibung


 a|
Laufwerkssicherheit
 a|
Laufwerkssicherheit ist eine Funktion des Storage Arrays, die eine
zusätzliche Sicherheitsschicht bietet – entweder mit vollständigen
Festplatten-Verschlüsselung (FDE) oder FIPS-Laufwerken (Federal
Information Processing Standard). Wenn diese Laufwerke zusammen mit der
Sicherheitsfunktion des Laufwerks verwendet werden, benötigen sie einen
Sicherheitsschlüssel für den Zugriff auf ihre Daten. Wenn die Laufwerke
physisch aus dem Array entfernt werden, können sie erst betrieben werden,
wenn sie in einem anderen Array installiert sind. Zu diesem Zeitpunkt
befinden sie sich in einem Sicherheitsstatus, bis der richtige
Sicherheitsschlüssel bereitgestellt wird.



 a|
FDE-Laufwerke
 a|
Vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE)
ermöglicht die Verschlüsselung auf Festplattenlaufwerken auf Hardware-
Ebene. Die Festplatte enthält einen ASIC-Chip, der Daten während des
Schreibvorgangs verschlüsselt und die Daten beim Lesen entschlüsselt.



 a|
FIPS-Laufwerke
 a|
FIPS-Laufwerke verwenden Federal Information Processing Standards (FIPS)
140-2 Level 2. Es handelt sich im Wesentlichen um FDE-Laufwerke, die den
Standards der US-Regierung entsprechen, um solide
```

Verschlüsselungsalgorithmen und -Methoden sicherzustellen. FIPS-Laufwerke haben höhere Sicherheitsstandards als FDE-Laufwerke.

 a|
Management- Client
 a|
Ein lokales System (Computer, Tablet usw.), das einen Browser für den Zugriff auf System Manager enthält.

 a|
Ausdruck übergeben
 a|
Der Passphrase wird verwendet, um den Sicherheitsschlüssel für Sicherungszwecke zu verschlüsseln. Der gleiche Passphrase, der für die Verschlüsselung des Sicherheitsschlüssels verwendet wird, muss angegeben werden, wenn der gesicherte Sicherheitsschlüssel als Ergebnis einer Laufwerksmigration oder eines Kopftauschens importiert wird. Ein Passphrase kann zwischen 8 und 32 Zeichen lang sein.

[NOTE]
====
Der Passphrase für die Laufwerksicherheit ist unabhängig vom Administratorkennwort des Speicherarrays.

====

 a|
Secure-fähige Laufwerke
 a|
Sichere Laufwerke können entweder vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) sein, die Daten während des Schreibvorgangs verschlüsseln und Daten während Lesevorgängen entschlüsseln. Diese Laufwerke gelten als sicher-_fähig_, da sie mit der Sicherheitsfunktion des Laufwerks für zusätzliche Sicherheit verwendet werden können. Wenn die Laufwerkssicherheitsfunktion für Volume-Gruppen und -Pools aktiviert ist, die mit diesen Laufwerken verwendet werden, werden die Laufwerke sicher-_Enabled_.

 a|

Secure-Enabled Laufwerke
 a|
Secure-Enabled-Laufwerke werden mit der Drive Security-Funktion verwendet. Wenn Sie die Laufwerkssicherheitsfunktion aktivieren und dann Laufwerksicherheit auf einem Pool oder einer Volume-Gruppe auf Secure-_fähigen_-Laufwerken anwenden, werden die Laufwerke sicher___-aktiviert____. Lese- und Schreibzugriff ist nur über einen Controller verfügbar, der mit dem korrekten Sicherheitsschlüssel konfiguriert ist. Diese zusätzliche Sicherheit verhindert einen nicht autorisierten Zugriff auf die Daten auf einem Laufwerk, das physisch vom Storage-Array entfernt wird.

 a|
Sicherheitsschlüssel
 a|
Ein Sicherheitsschlüssel ist eine Zeichenkette, die von den sicheren Laufwerken und Controllern in einem Speicher-Array gemeinsam genutzt wird. Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln die sicher-aktivierten Laufwerke in den Status Sicherheitsverriegelt, bis der Controller den Sicherheitsschlüssel anwendet. Wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt wird, sind die Daten des Laufwerks gesperrt. Wenn das Laufwerk in einem anderen Speicher-Array neu installiert wird, sucht es nach dem Sicherheitsschlüssel, bevor es die Daten wieder zugänglich macht. Um die Daten zu entsperren, müssen Sie den ursprünglichen Sicherheitsschlüssel anwenden. Sie können Sicherheitsschlüssel mit einer der folgenden Methoden erstellen und verwalten:

* Internes Verschlüsselungsmanagement – Erstellen und Warten von Sicherheitsschlüsseln im persistenten Speicher des Controllers
* Externes Verschlüsselungsmanagement -- Erstellen und Verwalten von Sicherheitsschlüsseln auf einem externen Schlüsselverwaltungsserver.

 a|
Kennung des Sicherheitsschlüssels
 a|
Die Security Key-ID ist eine Zeichenfolge, die dem Sicherheitsschlüssel bei der Schlüsselerstellung zugeordnet ist. Die Kennung wird auf dem Controller und auf allen Laufwerken gespeichert, die mit dem Sicherheitsschlüssel verbunden sind.

```
|===



:leveloffset: -1


= Konfigurieren Sie die Sicherheitsschlüssel

:leveloffset: +1


[[IDade9909206fda29a488b5440b61b74e5]]
= Interner Sicherheitsschlüssel erstellen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Zur Verwendung der Laufwerkssicherheitsfunktion können Sie einen internen
Sicherheitsschlüssel erstellen, der von den Controllern und sicheren
Laufwerken im Speicher-Array gemeinsam genutzt wird. Interne Schlüssel
befinden sich im persistenten Speicher des Controllers.

.Bevor Sie beginnen
* Sichere Laufwerke müssen im Speicher-Array installiert sein. Es können
sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung
(Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information
Processing Standard) handelt.
* Die Laufwerkssicherheitsfunktion muss aktiviert sein. Andernfalls wird
während dieser Aufgabe ein Dialogfeld „Sicherheitsschlüssel nicht
erstellen“ geöffnet. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter,
um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu
erhalten.


[NOTE]
====
Wenn sowohl FDE- als auch FIPS-Laufwerke im Storage Array installiert
werden, nutzen sie alle denselben Sicherheitsschlüssel.

====
.Über diese Aufgabe
In dieser Aufgabe definieren Sie eine Kennung und eine Passphrase, die dem
```

internen Sicherheitsschlüssel zugeordnet werden sollen.

[NOTE]
====
Der Passphrase für die Laufwerksicherheit ist unabhängig vom Administratorkennwort des Speicherarrays.

====
.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter *Security Key Management* die Option *Interner Schlüssel erstellen*.
+
Wenn Sie noch keinen Sicherheitsschlüssel generiert haben, wird das Dialogfeld Sicherheitsschlüssel erstellen geöffnet.

. Geben Sie Informationen in die folgenden Felder ein:
+
** *Einen Sicherheitsschlüssel-Identifier definieren* -- Sie können entweder den Standardwert akzeptieren (Speicherarray-Name und Zeitstempel, der von der Controller-Firmware generiert wird) oder Ihren eigenen Wert eingeben. Sie können bis zu 189 alphanumerische Zeichen ohne Leerzeichen, Satzzeichen oder Symbole eingeben.
+
[NOTE]
====
Zusätzliche Zeichen werden automatisch generiert und an beide Enden der eingegebenen Zeichenfolge angehängt. Die generierten Zeichen stellen sicher, dass die Kennung eindeutig ist.

====
** *Passphrase definieren/Passphrase erneut eingeben* -- Geben Sie eine Passphrase ein und bestätigen Sie diese. Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:
+
*** Ein Großbuchstabe (einer oder mehrere). Beachten Sie, dass die Passphrase Groß- und Kleinschreibung beachtet.
*** Eine Nummer (eine oder mehrere).
*** Ein nicht-alphanumerisches Zeichen wie !, *, @ (eines oder mehrere).

+
[CAUTION]
====

Beachten Sie, Ihre Einträge zur späteren Verwendung aufzuzeichnen. Wenn Sie ein sicheres Laufwerk aus dem Speicher-Array verschieben müssen, müssen Sie die Kennung kennen und den Ausdruck übergeben, um Laufwerkdaten zu entsperren.

====
. Klicken Sie Auf *Erstellen*.
+
Der Sicherheitsschlüssel wird auf dem Controller an einem nicht zugänglichen Ort gespeichert. Zusammen mit dem eigentlichen Schlüssel gibt es eine verschlüsselte Schlüsseldatei, die von Ihrem Browser heruntergeladen wird.

+
[NOTE]
====
Der Pfad für die heruntergeladene Datei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.

====
. Notieren Sie sich die Schlüsselkennung, den Passphrase und den Speicherort der heruntergeladenen Schlüsseldatei, und klicken Sie dann auf *Schließen*.

.Ergebnisse
Sie können jetzt sichere Volume-Gruppen oder -Pools erstellen oder die Sicherheit bei vorhandenen Volume-Gruppen und -Pools aktivieren.

[NOTE]
====
Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln alle sicheren Laufwerke in den Status Sicherheitsverriegelt. In diesem Zustand sind die Daten nicht zugänglich, bis der Controller den korrekten Sicherheitsschlüssel während der Laufwerkinitialisierung anwendet. Wenn ein gesperrtes Laufwerk physisch entfernt und in einem anderen System installiert wird, verhindert der Status „Sicherheitsgesperrt“ unbefugten Zugriff auf seine Daten.

====
.Nachdem Sie fertig sind
Sie sollten den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass die Schlüsseldatei nicht beschädigt ist.

[[ID5dda48e8c5f73c14128a822c244f7dca]]

```
= Externen Sicherheitsschlüssel erstellen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um die Laufwerkssicherheitsfunktion mit einem Schlüsselverwaltungsserver
verwenden zu können, müssen Sie einen externen Schlüssel erstellen, der
vom Schlüsselverwaltungsserver und den sicheren Laufwerken im Speicher-
Array gemeinsam genutzt wird.

.Bevor Sie beginnen
* Sichere Laufwerke müssen im Array installiert werden. Es können sich bei
diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk
Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing
Standard) handelt.
+
[NOTE]
====
Wenn sowohl FDE- als auch FIPS-Laufwerke im Storage Array installiert
werden, nutzen sie alle denselben Sicherheitsschlüssel.

====
* Die Laufwerkssicherheitsfunktion muss aktiviert sein. Andernfalls wird
während dieser Aufgabe ein Dialogfeld „Sicherheitsschlüssel nicht
erstellen“ geöffnet. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter,
um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu
erhalten.
* Sie haben eine signierte Client-Zertifikatdatei für die Controller des
Speicher-Arrays und haben diese Datei auf den Host kopiert, auf dem Sie
auf System Manager zugreifen. Ein Client-Zertifikat validiert die
Controller des Storage-Arrays, damit der wichtige Management-Server seine
KMIP-Anforderungen (Key Management Interoperability Protocol) anvertrauen
kann.
* Sie müssen eine Zertifikatdatei vom Schlüsselverwaltungsserver abrufen
und diese Datei anschließend auf den Host kopieren, auf den 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.
+
[NOTE]
====
```

Weitere Informationen zum Serverzertifikat finden Sie in der Dokumentation für Ihren Schlüsselverwaltungsserver.

====

.Über diese Aufgabe
In dieser Aufgabe definieren Sie die IP-Adresse des Schlüsselverwaltungsservers und die verwendete Portnummer und laden dann Zertifikate für die externe Schlüsselverwaltung.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter * Security Key Management* die Option *External Key erstellen* aus.
+
[NOTE]
====
Wenn derzeit die interne Schlüsselverwaltung konfiguriert ist, wird ein Dialogfeld geöffnet, in dem Sie aufgefordert werden, zu bestätigen, dass Sie zur externen Schlüsselverwaltung wechseln möchten.

====
+
Das Dialogfeld External Security Key erstellen wird geöffnet.

. Geben Sie unter *Verbinden mit Key Server* Informationen in die folgenden Felder ein.
+
** *Key Management Server-Adresse* -- Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein, der für die Schlüsselverwaltung verwendet wird.
** *Nummer des Key Management-Ports* -- Geben Sie die Portnummer ein, die für die KMIP-Kommunikation verwendet wird. Die am häufigsten für die Kommunikation mit dem Verschlüsselungsmanagement-Server verwendete Portnummer ist 5696.
+
Optional: Wenn Sie einen Backup Key Server konfigurieren möchten, klicken Sie auf *Add Key Server* und geben Sie dann die Informationen dieses Servers ein. Der zweite Schlüsselserver wird verwendet, wenn der primäre Schlüsselserver nicht erreicht werden kann. Stellen Sie sicher, dass jeder Schlüsselserver Zugriff auf dieselbe Schlüsseldatenbank hat. Andernfalls wird das Array Fehler senden und kann den Backup-Server nicht verwenden.

+

NOTE: Es wird immer nur ein einziger Schlüsselserver verwendet. Wenn das Speicher-Array den primären Schlüsselserver nicht erreichen kann, kontaktiert das Array den Backup-Schlüsselserver. Beachten Sie, dass die Parität zwischen beiden Servern beibehalten werden muss. Andernfalls kann es zu Fehlern kommen.

** *Client-Zertifikat auswählen* -- Klicken Sie auf die erste *Durchsuchen*-Schaltfläche, um die Zertifikatdatei für die Speicher-Array-Controller auszuwählen.
** *Select private key file* -- Klicken Sie bei Bedarf auf die zweite *Browse*-Schaltfläche, um eine private Schlüsseldatei für die Controller des Speicherarrays auszuwählen.
** *Serverzertifikat des Schlüsselverwaltungsservers auswählen* -- Klicken Sie auf die dritte Schaltfläche *Durchsuchen*, um die Zertifikatdatei für den Schlüsselverwaltungsserver auszuwählen. Sie können für den Schlüsselverwaltungsserver ein Stammzertifikat, ein Zwischenzertifikat oder ein Serverzertifikat auswählen.

. Klicken Sie Auf *Weiter*.
. Unter *Create/Backup Key* können Sie einen Sicherungsschlüssel für Sicherheitszwecke erstellen.
+
** (Empfohlen) um einen Sicherungsschlüssel zu erstellen, lassen Sie das Kontrollkästchen aktiviert, und geben Sie dann einen Passphrase ein und bestätigen Sie ihn. Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:
+
*** Ein Großbuchstabe (einer oder mehrere). Beachten Sie, dass die Passphrase Groß- und Kleinschreibung beachtet.
*** Eine Nummer (eine oder mehrere).
*** Ein nicht-alphanumerisches Zeichen wie !, *, @ (eines oder mehrere).

+
[CAUTION]
====
Beachten Sie, Ihre Einträge zur späteren Verwendung aufzuzeichnen. Wenn Sie ein sicheres Laufwerk aus dem Speicher-Array verschieben möchten, müssen Sie den Passphrase kennen, um die Laufwerkdaten zu entsperren.

====
+
** Wenn Sie keinen Sicherungsschlüssel erstellen möchten, deaktivieren Sie

das Kontrollkästchen.
+
[CAUTION]
====
Beachten Sie, dass bei einem Verlust des Zugriffs auf den externen Schlüsselserver und ohne Backup-Schlüssel der Zugriff auf die Daten auf den Laufwerken verloren geht, wenn sie zu einem anderen Storage-Array migriert werden. Diese Option ist die einzige Methode zum Erstellen eines Sicherungsschlüssels in System Manager.

====

. Klicken Sie Auf *Fertig Stellen*.
+
Das System stellt mit den eingegebenen Anmeldedaten eine Verbindung zum Schlüsselverwaltungsserver her. Anschließend wird eine Kopie des Sicherheitsschlüssels auf Ihrem lokalen System gespeichert.

+
[NOTE]
====
Der Pfad für die heruntergeladene Datei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.

====
. Notieren Sie Ihren Passphrase und den Speicherort der heruntergeladenen Schlüsseldatei und klicken Sie dann auf *Schließen*.
+
Auf der Seite wird die folgende Meldung mit zusätzlichen Links zur externen Schlüsselverwaltung angezeigt:

+
`Current key management method: External`

. Testen Sie die Verbindung zwischen dem Speicher-Array und dem Schlüsselverwaltungsserver, indem Sie *Testkommunikation* wählen.
+
Die Testergebnisse werden im Dialogfeld angezeigt.

.Ergebnisse
Wenn das externe Verschlüsselungsmanagement aktiviert ist, können Sie sicher aktivierte Volume-Gruppen oder -Pools erstellen oder die Sicherheit für vorhandene Volume-Gruppen und -Pools aktivieren.

```
[NOTE]
====
Wenn die Stromversorgung der Laufwerke aus- und wieder eingeschaltet wird, wechseln alle sicheren Laufwerke in den Status Sicherheitsverriegelt. In diesem Zustand sind die Daten nicht zugänglich, bis der Controller den korrekten Sicherheitsschlüssel während der Laufwerkinitialisierung anwendet. Wenn ein gesperrtes Laufwerk physisch entfernt und in einem anderen System installiert wird, verhindert der Status „Sicherheitsgesperrt“ unbefugten Zugriff auf seine Daten.

====
.Nachdem Sie fertig sind
Sie sollten den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass die Schlüsseldatei nicht beschädigt ist.



:leveloffset: -1


= Management von Sicherheitsschlüsseln

:leveloffset: +1


[[ID7e690baecbd300afdfa01fd215507504]]
= Sicherheitsschlüssel ändern
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können jederzeit einen Sicherheitsschlüssel durch einen neuen Schlüssel ersetzen. Möglicherweise müssen Sie einen Sicherheitsschlüssel ändern, wenn Ihr Unternehmen eine potenzielle Sicherheitsverletzung hat und sicherstellen möchte, dass nicht autorisierte Mitarbeiter nicht auf die Daten zugreifen können.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter * Security Key Management* die Option *Change Key*.
+
Das Dialogfeld Sicherheitsschlüssel ändern wird geöffnet.
```

. Geben Sie die folgenden Felder ein.
+
** *Definieren Sie einen Sicherheitsschlüssel-Identifier* -- (nur für interne Sicherheitsschlüssel.) Akzeptieren Sie den Standardwert (Storage Array-Name und Zeitstempel, der von der Controller-Firmware generiert wird) oder geben Sie Ihren eigenen Wert ein. Sie können bis zu 189 alphanumerische Zeichen ohne Leerzeichen, Satzzeichen oder Symbole eingeben.
+
[NOTE]
====
Zusätzliche Zeichen werden automatisch generiert und an beide Enden der eingegebenen Zeichenfolge angehängt. Die generierten Zeichen tragen dazu bei, dass die Kennung eindeutig ist.

====
** *Passphrase definieren/Passphrase erneut eingeben* -- Geben Sie in jedes dieser Felder Ihren Passphrase ein. Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:
+
*** Ein Großbuchstabe (einer oder mehrere). Beachten Sie, dass die Passphrase Groß- und Kleinschreibung beachtet.
*** Eine Nummer (eine oder mehrere).
*** Ein nicht-alphanumerisches Zeichen wie !, *, @ (eines oder mehrere).

. Wenn Sie bei externen Sicherheitsschlüsseln den alten Sicherheitsschlüssel löschen möchten, wenn der neue Schlüssel erstellt wird, aktivieren Sie unten im Dialogfeld das Kontrollkästchen „aktuellen Sicherheitsschlüssel löschen...“.
+
[CAUTION]
====
Vergewissern Sie sich, Ihre Einträge für eine spätere Verwendung aufzuzeichnen -- Wenn Sie ein sicheres Laufwerk aus dem Speicher-Array verschieben müssen, müssen Sie die Kennung kennen und den Ausdruck übergeben, um die Laufwerkdaten zu entsperren.

====
. Klicken Sie Auf *Ändern*.
+
Der neue Sicherheitsschlüssel überschreibt den vorherigen Schlüssel, der nicht mehr gültig ist.

```
+
[NOTE]
====
Der Pfad für die heruntergeladene Datei hängt möglicherweise vom Standard-
Download-Speicherort Ihres Browsers ab.

====
. Notieren Sie sich die Schlüsselkennung, den Passphrase und den
Speicherort der heruntergeladenen Schlüsseldatei, und klicken Sie dann auf
*Schließen*.


.Nachdem Sie fertig sind
Sie sollten den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass
die Schlüsseldatei nicht beschädigt ist.



[[IDa25652e4ff638f4cbacf3578106f3e66]]
= Wechsel von externem zu internem Verschlüsselungsmanagement
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die Verwaltungsmethode für die Laufwerksicherheit von einem
externen Schlüsselserver in die interne Methode ändern, die vom Speicher-
Array verwendet wird. Der zuvor für das externe Verschlüsselungsmanagement
definierte Sicherheitsschlüssel wird dann für das interne
Verschlüsselungsmanagement verwendet.

.Über diese Aufgabe
In dieser Aufgabe deaktivieren Sie die externe Schlüsselverwaltung und
laden eine neue Sicherungskopie auf Ihren lokalen Host herunter. Der
vorhandene Schlüssel wird weiterhin für die Laufwerksicherheit verwendet,
wird aber intern im Speicher-Array verwaltet.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter * Security Key Management* die Option *External Key
Management deaktivieren* aus.
+
Das Dialogfeld External Key Management deaktivieren wird geöffnet.
```

. Geben Sie unter *Passphrase definieren/Passphrase erneut eingeben* einen Passphrase für die Sicherung des Schlüssels ein und bestätigen Sie diesen. Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:
+
** Ein Großbuchstabe (einer oder mehrere). Beachten Sie, dass die Passphrase Groß- und Kleinschreibung beachtet.
** Eine Nummer (eine oder mehrere).
** Ein nicht-alphanumerisches Zeichen wie !, *, @ (eines oder mehrere).

+
[CAUTION]
====
Notieren Sie sich Ihre Einträge für die spätere Verwendung. Wenn Sie ein sicheres Laufwerk aus dem Speicher-Array verschieben müssen, müssen Sie die Kennung kennen und den Ausdruck übergeben, um Laufwerkdaten zu entsperren.

====
. Klicken Sie Auf *Deaktivieren*.
+
Der Backup-Schlüssel wird auf Ihren lokalen Host heruntergeladen.

. Notieren Sie sich die Schlüsselkennung, den Passphrase und den Speicherort der heruntergeladenen Schlüsseldatei, und klicken Sie dann auf *Schließen*.

.Ergebnisse
Die Laufwerksicherheit wird jetzt intern über das Speicher-Array verwaltet.

.Nachdem Sie fertig sind
Sie sollten den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass die Schlüsseldatei nicht beschädigt ist.

[[IDc35c9fd28f3d3b641cfea12b7df1147e]]
= Bearbeiten der Einstellungen des Verschlüsselungsmanagementservers
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Wenn Sie die externe Schlüsselverwaltung konfiguriert haben, können Sie die Einstellungen des Verschlüsselungsmanagementservers jederzeit anzeigen und bearbeiten.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter *Security Key Management* die Option *Key Management Server-Einstellungen anzeigen/bearbeiten* aus.
. Bearbeiten Sie die Informationen in den folgenden Feldern:
+
** *Key Management Server-Adresse* -- Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein, der für die Schlüsselverwaltung verwendet wird.
** *Nummer des Key Management-Ports* -- Geben Sie die Portnummer ein, die für die Kommunikation mit dem Key Management Interoperability Protocol (KMIP) verwendet wird.
+
Optional: Sie können einen anderen Schlüsselserver hinzufügen, indem Sie auf *Schlüsselserver hinzufügen* klicken.

. Klicken Sie Auf *Speichern*.

[[IDbc553efe3267000770d17b08464b60d4]]
= Sicherheitsschlüssel sichern
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Nach dem Erstellen oder Ändern eines Sicherheitsschlüssels können Sie eine Sicherungskopie der Schlüsseldatei erstellen, falls das Original beschädigt wird.

.Über diese Aufgabe
In dieser Aufgabe wird beschrieben, wie Sie einen zuvor erstellten Sicherheitsschlüssel sichern. Während dieses Verfahrens erstellen Sie einen neuen Passphrase für das Backup. Diese Passphrase muss nicht mit der Passphrase übereinstimmen, die bei der Erstellung des ursprünglichen

```
Schlüssels oder der letzten Änderung verwendet wurde. Der Passphrase wird
nur auf das Backup angewendet, das Sie erstellen.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter * Security Key Management* die Option *Back Up Key*.
+
Das Dialogfeld Sicherheitsschlüssel sichern wird geöffnet.

. Geben Sie in den Feldern *Passphrase definieren/Passphrase erneut
eingeben* einen Passphrase für dieses Backup ein und bestätigen Sie
diesen.
+
Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:

+
** Ein Großbuchstabe (einer oder mehrere)
** Eine Nummer (eine oder mehrere)
** Ein nicht-alphanumerisches Zeichen wie !, *, @ (ein oder mehrere)


+
[CAUTION]
====
*Bitte notieren Sie Ihren Eintrag für den späteren Gebrauch*. Sie
benötigen den Passphrase, um auf die Sicherung dieses
Sicherheitsschlüssels zuzugreifen.

====
. Klicken Sie Auf *Sichern*.
+
Ein Backup des Sicherheitsschlüssels wird auf Ihren lokalen Host
heruntergeladen, und dann wird das Dialogfeld *Sicherheitsschlüssel
sichern/aufzeichnen* geöffnet.

+
[NOTE]
====
Der Pfad für die heruntergeladene Sicherheitsschlüsseldatei hängt
möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.

====
. Zeichnen Sie Ihren Passphrase an einem sicheren Ort auf, und klicken Sie
dann auf *Schließen*.


.Nachdem Sie fertig sind
```

```
Sie sollten den Sicherungsschlüssel überprüfen.



[[ID73f1c0135d50cb1c6ff1a553bcc1d9e2]]
= Validierung des Sicherheitsschlüssels
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass
er nicht beschädigt wurde, und um sicherzustellen, dass Sie über einen
korrekten Passphrase verfügen.

.Über diese Aufgabe
In dieser Aufgabe wird beschrieben, wie Sie den zuvor erstellten
Sicherheitsschlüssel validieren. Dies ist ein wichtiger Schritt, um
sicherzustellen, dass die Schlüsseldatei nicht beschädigt ist und der
Passphrase korrekt ist, wodurch sichergestellt wird, dass Sie später auf
die Laufwerkdaten zugreifen können, wenn Sie ein sicheres Laufwerk von
einem Speicher-Array in ein anderes verschieben.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter * Security Key Management* die Option *Validate Key*
aus.
+
Das Dialogfeld Sicherheitsschlüssel validieren wird geöffnet.

. Klicken Sie auf *Durchsuchen* und wählen Sie dann die Schlüsseldatei aus
(z. B. `drivesecurity.slk`).
. Geben Sie die Passphrase ein, die mit der ausgewählten Taste verknüpft
ist.
+
Wenn Sie eine gültige Schlüsseldatei auswählen und den Ausdruck übergeben,
steht die Schaltfläche *Validieren* zur Verfügung.

. Klicken Sie Auf *Validieren*.
+
Die Ergebnisse der Validierung werden im Dialogfeld angezeigt.

. Wenn in den Ergebnissen „der Sicherheitsschlüssel erfolgreich validiert
wurde“ angezeigt wird, klicken Sie auf *Schließen*. Wenn eine
```

```
Fehlermeldung angezeigt wird, befolgen Sie die im Dialogfeld angezeigten
Anweisungen.




[[ID569622803c92021f7706cc3e694caae2]]
= Entsperren Sie Laufwerke bei Nutzung des internen
Verschlüsselungsmanagements
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie das interne Verschlüsselungsmanagement konfiguriert haben und
später sichere Laufwerke von einem Speicher-Array auf ein anderes
verschieben, müssen Sie den Sicherheitsschlüssel dem neuen Speicher-Array
neu zuweisen, um Zugriff auf die verschlüsselten Daten auf den Laufwerken
zu erhalten.

.Bevor Sie beginnen
* Auf dem Quell-Array (dem Array, in dem Sie die Laufwerke entfernen)
haben Sie Volume-Gruppen exportiert und die Laufwerke entfernt. Auf dem
Ziel-Array haben Sie die Laufwerke neu installiert.
+

NOTE: Die Funktion „Exportieren/Importieren“ wird in der
Benutzeroberfläche von System Manager nicht unterstützt. Sie müssen die
Befehlszeilenschnittstelle (CLI) verwenden, um eine Volume-Gruppe in ein
anderes Storage-Array zu exportieren bzw. zu importieren.

+
Detaillierte Anweisungen für die Migration einer Volume-Gruppe finden Sie
in https://kb.netapp.com/["NetApp Knowledge Base"^]. Befolgen Sie die
entsprechenden Anweisungen für neuere Arrays, die von System Manager oder
für ältere Systeme gemanagt werden.

* Die Laufwerkssicherheitsfunktion muss aktiviert sein. Andernfalls wird
während dieser Aufgabe ein Dialogfeld „Sicherheitsschlüssel nicht
erstellen“ geöffnet. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter,
um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu
erhalten.
* Sie müssen den Sicherheitsschlüssel kennen, der mit den Laufwerken
verknüpft ist, die Sie entsperren möchten.
```

* Die Sicherheitsschlüsseldatei steht auf dem Management-Client zur Verfügung (das System mit einem Browser, der zum Zugriff auf System Manager verwendet wird). Wenn Sie die Laufwerke in ein Storage-Array verschieben, das von einem anderen System gemanagt wird, müssen Sie die Sicherheitsschlüsseldatei auf diesen Management-Client verschieben.

.Über diese Aufgabe
Wenn Sie die interne Schlüsselverwaltung verwenden, wird der Sicherheitsschlüssel lokal auf dem Speicher-Array gespeichert. Ein Sicherheitsschlüssel ist eine Zeichenkette, die vom Controller und den Laufwerken für Lese-/Schreibzugriff freigegeben wird. Wenn die Laufwerke physisch aus dem Array entfernt und in einem anderen installiert werden, können sie erst betrieben werden, wenn Sie den richtigen Sicherheitsschlüssel angeben.

[NOTE]
====
Sie können entweder einen internen Schlüssel aus dem persistenten Speicher des Controllers oder einen externen Schlüssel von einem Schlüsselmanagementserver erstellen. In diesem Thema wird das Entsperren von Daten beschrieben, wenn das _interne_ Verschlüsselungsmanagement verwendet wird. Wenn Sie _External_ Key Management verwendet haben, lesen Sie xref:{relative_path}unlock-drives-using-an-external-security-key.html["Entsperren von Laufwerken bei Verwendung von externer Schlüsselverwaltung"]. Wenn Sie ein Controller-Upgrade durchführen und alle Controller gegen die neueste Hardware austauschen, müssen Sie die verschiedenen Schritte ausführen, wie im E-Series und SANtricity Dokumentationszentrum in beschrieben link:https://docs.netapp.com/us-en/e-series/upgrade-controllers/upgrade-unlock-drives-task.html["Entsperren von Laufwerken"].

====
Nach der Neuinstallation von Secure-Enabled-Laufwerken in einem anderen Array erkennt das Array die Laufwerke und zeigt den Zustand „Need Attention“ sowie den Status „Security Key needed“ an. Um die Laufwerkdaten zu entsperren, wählen Sie die Sicherheitsschlüsseldatei aus und geben den Passphrase für den Schlüssel ein. (Dieser Passphrase entspricht nicht dem Administratorkennwort des Speicherarrays.)

Wenn andere sichere Laufwerke im neuen Speicher-Array installiert sind, verwenden sie möglicherweise einen anderen Sicherheitsschlüssel als den, den Sie importieren. Während des Importvorgangs wird der alte Sicherheitsschlüssel nur verwendet, um die Daten für die zu installierenden Laufwerke freizuschalten. Wenn die Entsperrung erfolgreich ist, werden die neu installierten Laufwerke erneut auf den

Sicherheitsschlüssel des Ziel-Speicher-Arrays codiert.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter * Security Key Management* * * Secure Drives entsperren* aus.
+
Das Dialogfeld Sichere Laufwerke entsperren wird geöffnet. Alle Laufwerke, für die ein Sicherheitsschlüssel erforderlich ist, sind in der Tabelle aufgeführt.

. *Optional:* bewegen Sie die Maus über eine Laufwerksnummer, um die Position des Laufwerks zu sehen (Regalnummer und Einschubnummer).
. Klicken Sie auf *Durchsuchen* und wählen Sie dann die Sicherheitsschlüsseldatei aus, die dem Laufwerk entspricht, das Sie entsperren möchten.
+
Die ausgewählte Schlüsseldatei wird im Dialogfeld angezeigt.

. Geben Sie den Passphrase ein, der dieser Schlüsseldatei zugeordnet ist.
+
Die eingegebenen Zeichen sind maskiert.

. Klicken Sie Auf *Entsperren*.
+
Wenn der Entsperrvorgang erfolgreich ist, wird im Dialogfeld „die zugeordneten sicheren Laufwerke wurden entsperrt“ angezeigt.

.Ergebnisse
Wenn alle Laufwerke gesperrt und dann entsperrt sind, wird jeder Controller im Speicher-Array neu gestartet. Wenn sich jedoch bereits einige nicht freigeschaltete Laufwerke im Ziel-Speicher-Array befinden, werden die Controller nicht neu gestartet.

.Nachdem Sie fertig sind
Auf dem Ziel-Array (dem Array mit den neu installierten Laufwerken) können Sie nun Volume-Gruppen importieren.

NOTE: Die Funktion „Exportieren/Importieren“ wird in der Benutzeroberfläche von System Manager nicht unterstützt. Sie müssen die Befehlszeilenschnittstelle (CLI) verwenden, um eine Volume-Gruppe in ein anderes Storage-Array zu exportieren bzw. zu importieren.

Detaillierte Anweisungen für die Migration einer Volume-Gruppe finden Sie

```
in https://kb.netapp.com/["NetApp Knowledge Base"^].



[[ID6aea74152277da1142682deecd03c3ec]]
= Entsperren von Laufwerken bei Verwendung von externer
Schlüsselverwaltung
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie die externe Schlüsselverwaltung konfiguriert haben und später
sichere Laufwerke von einem Speicher-Array auf ein anderes verschieben,
müssen Sie den Sicherheitsschlüssel dem neuen Speicher-Array neu zuweisen,
um Zugriff auf die verschlüsselten Daten auf den Laufwerken zu erhalten.

.Bevor Sie beginnen
* Auf dem Quell-Array (dem Array, in dem Sie die Laufwerke entfernen)
haben Sie Volume-Gruppen exportiert und die Laufwerke entfernt. Auf dem
Ziel-Array haben Sie die Laufwerke neu installiert.
+

NOTE: Die Funktion „Exportieren/Importieren“ wird in der
Benutzeroberfläche von System Manager nicht unterstützt. Sie müssen die
Befehlszeilenschnittstelle (CLI) verwenden, um eine Volume-Gruppe in ein
anderes Storage-Array zu exportieren bzw. zu importieren.

+
Detaillierte Anweisungen für die Migration einer Volume-Gruppe finden Sie
in https://kb.netapp.com/["NetApp Knowledge Base"^]. Befolgen Sie die
entsprechenden Anweisungen für neuere Arrays, die von System Manager oder
für ältere Systeme gemanagt werden.

* Die Laufwerkssicherheitsfunktion muss aktiviert sein. Andernfalls wird
während dieser Aufgabe ein Dialogfeld „Sicherheitsschlüssel nicht
erstellen“ geöffnet. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter,
um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu
erhalten.
* Sie müssen die IP-Adresse und die Port-Nummer des
Verschlüsselungsmanagementservers kennen.
* Sie haben eine signierte Client-Zertifikatdatei für die Controller des
Speicher-Arrays und haben diese Datei auf den Host kopiert, auf dem Sie
```

auf System Manager zugreifen. Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit der wichtige Management-Server seine KMIP-Anforderungen (Key Management Interoperability Protocol) anvertrauen kann.
* Sie müssen eine Zertifikatdatei vom Schlüsselverwaltungsserver abrufen und diese Datei anschließend auf den Host kopieren, auf den 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.

[NOTE]
====
Weitere Informationen zum Serverzertifikat finden Sie in der Dokumentation für Ihren Schlüsselverwaltungsserver.

====
.Über diese Aufgabe
Wenn Sie die externe Schlüsselverwaltung verwenden, wird der Sicherheitsschlüssel extern auf einem Server gespeichert, der zum sicheren Schutz von Sicherheitsschlüsseln entwickelt wurde. Ein Sicherheitsschlüssel ist eine Zeichenkette, die vom Controller und den Laufwerken für Lese-/Schreibzugriff freigegeben wird. Wenn die Laufwerke physisch aus dem Array entfernt und in einem anderen installiert werden, können sie erst betrieben werden, wenn Sie den richtigen Sicherheitsschlüssel angeben.

[NOTE]
====
Sie können entweder einen internen Schlüssel aus dem persistenten Speicher des Controllers oder einen externen Schlüssel von einem Schlüsselmanagementserver erstellen. In diesem Thema wird das Entsperren von Daten beschrieben, wenn _External_ Verschlüsselungsmanagement verwendet wird. Wenn Sie _interne Schlüsselverwaltung verwendet haben, lesen Sie xref:{relative_path}unlock-drives-using-an-internal-security-key.html["Entsperren Sie Laufwerke bei Nutzung des internen Verschlüsselungsmanagements"]. Wenn Sie ein Controller-Upgrade durchführen und alle Controller gegen die neueste Hardware austauschen, müssen Sie die verschiedenen Schritte ausführen, wie im E-Series und SANtricity Dokumentationszentrum in beschrieben link:https://docs.netapp.com/us-en/e-series/upgrade-controllers/upgrade-unlock-drives-task.html["Entsperren von Laufwerken"].

====
Nach der Neuinstallation von Secure-Enabled-Laufwerken in einem anderen

Array erkennt das Array die Laufwerke und zeigt den Zustand „Need Attention“ sowie den Status „Security Key needed“ an. Um die Laufwerkdaten zu entsperren, importieren Sie die Sicherheitsschlüsseldatei und geben den Passphrase für den Schlüssel ein. (Dieser Passphrase entspricht nicht dem Administratorkennwort des Speicherarrays.) Während dieses Prozesses konfigurieren Sie das Speicher-Array so, dass ein externer Schlüsselverwaltungsserver verwendet wird, und der sichere Schlüssel kann dann aufgerufen werden. Sie müssen die Kontaktinformationen des Servers angeben, damit das Speicherarray eine Verbindung herstellen und den Sicherheitsschlüssel abrufen kann.

Wenn andere sichere Laufwerke im neuen Speicher-Array installiert sind, verwenden sie möglicherweise einen anderen Sicherheitsschlüssel als den, den Sie importieren. Während des Importvorgangs wird der alte Sicherheitsschlüssel nur verwendet, um die Daten für die zu installierenden Laufwerke freizuschalten. Wenn die Entsperrung erfolgreich ist, werden die neu installierten Laufwerke erneut auf den Sicherheitsschlüssel des Ziel-Speicher-Arrays codiert.

.Schritte
. Wählen Sie Menü:Einstellungen[System].
. Wählen Sie unter * Security Key Management* die Option *External Key erstellen* aus.
. Schließen Sie den Assistenten mit den erforderlichen Verbindungsinformationen und Zertifikaten ab.
. Klicken Sie auf *Kommunikation testen*, um den Zugriff auf den externen Schlüsselverwaltungsserver zu gewährleisten.
. Wählen Sie * Sichere Laufwerke Entsperren*.
+
Das Dialogfeld Sichere Laufwerke entsperren wird geöffnet. Alle Laufwerke, für die ein Sicherheitsschlüssel erforderlich ist, sind in der Tabelle aufgeführt.

. *Optional:* bewegen Sie die Maus über eine Laufwerksnummer, um die Position des Laufwerks zu sehen (Regalnummer und Einschubnummer).
. Klicken Sie auf *Durchsuchen* und wählen Sie dann die Sicherheitsschlüsseldatei aus, die dem Laufwerk entspricht, das Sie entsperren möchten.
+
Die ausgewählte Schlüsseldatei wird im Dialogfeld angezeigt.

. Geben Sie den Passphrase ein, der dieser Schlüsseldatei zugeordnet ist.
+
Die eingegebenen Zeichen sind maskiert.

. Klicken Sie Auf *Entsperren*.

```
+
Wenn der Entsperrvorgang erfolgreich ist, wird im Dialogfeld „die
zugeordneten sicheren Laufwerke wurden entsperrt“ angezeigt.



.Ergebnisse
Wenn alle Laufwerke gesperrt und dann entsperrt sind, wird jeder
Controller im Speicher-Array neu gestartet. Wenn sich jedoch bereits
einige nicht freigeschaltete Laufwerke im Ziel-Speicher-Array befinden,
werden die Controller nicht neu gestartet.

.Nachdem Sie fertig sind
Auf dem Ziel-Array (dem Array mit den neu installierten Laufwerken) können
Sie nun Volume-Gruppen importieren.


NOTE: Die Funktion „Exportieren/Importieren“ wird in der
Benutzeroberfläche von System Manager nicht unterstützt. Sie müssen die
Befehlszeilenschnittstelle (CLI) verwenden, um eine Volume-Gruppe in ein
anderes Storage-Array zu exportieren bzw. zu importieren.

Detaillierte Anweisungen für die Migration einer Volume-Gruppe finden Sie
in https://kb.netapp.com/["NetApp Knowledge Base"^].



:leveloffset: -1


= FAQs

:leveloffset: +1


[[IDbd09673541ebc59d3d26913f686c0712]]
= Was muss ich vor der Erstellung eines Sicherheitsschlüssels wissen?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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 gepflegt und „`hidden`“ in einem nicht zugänglichen Ort im persistenten Speicher des Controllers gespeichert. Bevor Sie einen internen Sicherheitsschlüssel erstellen, müssen Sie Folgendes tun:

. 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.
. 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:

. 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.
. 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.
. Abrufen einer signierten Client-Zertifikatdatei. Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit der Verschlüsselungsmanagement-Server ihren KMIP-Anforderungen vertrauen kann.
+
.. Zunächst haben Sie eine Client Certificate Signing Request (CSR) abgeschlossen und heruntergeladen. Wechseln Sie zum Menü:Einstellungen[Zertifikate > Schlüsselverwaltung > CSR abschließen].
.. 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.)
.. Sobald Sie über eine Clientzertifikatdatei verfügen, kopieren Sie diese Datei auf den Host, auf dem Sie auf System Manager zugreifen.

. 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.

[[IDcee79465850030c149b445f62084cb53]]

```
= Warum muss ich eine Passphrase definieren?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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.



[[IDba671f564e6951ddacb79d8f662a9089]]
= Warum sind Sicherheitsinformationen wichtig?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie die Informationen über die Sicherheitsschlüssel verlieren und
kein Backup haben, können Sie Daten verlieren, wenn Sie sichere Laufwerke
verschieben oder ein Controller-Upgrade durchführen. Sie benötigen einen
Sicherheitsschlüssel, um die Daten auf den Laufwerken zu entsperren.

Achten Sie darauf, die Sicherheitsschlüsselkennung, den zugehörigen
Passphrase und den Speicherort auf dem lokalen Host, auf dem die
Sicherheitsschlüsseldatei gespeichert wurde, zu notieren.



[[IDa00024bbafd260ef25941d0b935aa7b8]]
= Was muss ich vor dem Sichern eines Sicherheitsschlüssels beachten?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Ihr ursprünglicher Sicherheitsschlüssel beschädigt wird und Sie kein
```

```
Backup haben, verlieren Sie den Zugriff auf die Daten auf den Laufwerken,
wenn sie von einem Speicher-Array zu einem anderen migriert werden.

Vor dem Sichern eines Sicherheitsschlüssels sollten Sie folgende
Richtlinien beachten:

* Stellen Sie sicher, dass Sie die Kennung des Sicherheitsschlüssels
kennen und den Satz der ursprünglichen Schlüsseldatei übergeben.
+
[NOTE]
====
Nur interne Schlüssel verwenden Kennungen. Beim Erstellen der Kennung
wurden automatisch zusätzliche Zeichen generiert und an beide Enden der
Identifikationszeichenfolge angehängt. Die generierten Zeichen stellen
sicher, dass die Kennung eindeutig ist.

====
* Sie erstellen einen neuen Passphrase für das Backup. Diese Passphrase
muss nicht mit der Passphrase übereinstimmen, die bei der Erstellung des
ursprünglichen Schlüssels oder der letzten Änderung verwendet wurde. Der
Passphrase wird nur auf das Backup angewendet, das Sie erstellen.
+
[NOTE]
====
Der Passphrase für die Laufwerksicherheit sollte nicht mit dem
Administratorkennwort des Speicherarrays verwechselt werden. Der
Passphrase für die Laufwerksicherheit schützt Backups eines
Sicherheitsschlüssels. Das Administratorpasswort schützt das gesamte
Speicherarray vor unberechtigtem Zugriff.

====
* Die Backup-Sicherheitsschlüsseldatei wird auf den Management-Client
heruntergeladen. Der Pfad für die heruntergeladene Datei hängt
möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.
Stellen Sie sicher, dass Sie den Speicherort Ihrer Sicherheitsschlüssel-
Informationen notieren.




[[ID10ac66288f6f89e04152c0a772701b72]]
= Was muss ich wissen, bevor sichere Laufwerke entsperrt werden?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Um die Daten von einem sicheren Laufwerk zu entsperren, müssen Sie seinen
Sicherheitsschlüssel importieren.

Beachten Sie vor dem Entsperren von sicheren Laufwerken die folgenden
Richtlinien:

* Das Speicherarray muss bereits einen Sicherheitsschlüssel haben. Die
migrierten Laufwerke werden erneut auf das Ziel-Storage-Array übertragen.
* Bei den zu migrierenden Laufwerken müssen Sie die
Sicherheitsschlüsselkennung und den Passphrase kennen, der der
Sicherheitsschlüsseldatei entspricht.
* Die Sicherheitsschlüsseldatei muss auf dem Management-Client verfügbar
sein (das System mit einem Browser, der zum Zugriff auf System Manager
verwendet wird).
* Wenn Sie ein gesperrtes NVMe-Laufwerk zurücksetzen, müssen Sie die
Sicherheits-ID des Laufwerks eingeben. Um die Sicherheits-ID zu finden,
müssen Sie das Laufwerk physisch entfernen und die PSID-Zeichenfolge
(maximal 32 Zeichen) auf dem Laufwerketikett suchen. Stellen Sie sicher,
dass das Laufwerk neu installiert ist, bevor Sie den Vorgang starten.




[[ID0b7a181a8e32f125cf11fd51bb8eae95]]
= Zugriff auf Lese-/Schreibzugriffe
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Das Fenster Laufwerkseinstellungen enthält Informationen zu den
Laufwerksicherheitsattributen. „Read/Write Accessible“ ist eines der
Attribute, das anzeigt, ob Daten eines Laufwerks gesperrt wurden.

Um die Attribute der Laufwerksicherheit anzuzeigen, gehen Sie zur Seite
Hardware. Wählen Sie ein Laufwerk aus, klicken Sie auf *Einstellungen
anzeigen* und dann auf *Weitere Einstellungen anzeigen*. Unten auf der
Seite ist der Wert für das Attribut Lesen/Schreiben, auf das zugegriffen
werden kann, *Ja*, wenn das Laufwerk entsperrt ist. Der Wert für das
Attribut Read/Write, das auf die Zugriffsberechtigung zugegriffen werden
kann, lautet *Nein, ungültiger Sicherheitsschlüssel*, wenn das Laufwerk
```

```
gesperrt ist. Sie können ein sicheres Laufwerk entsperren, indem Sie einen
Sicherheitsschlüssel importieren (gehen Sie zu Menü:Einstellungen[System >
Sichere Laufwerke entsperren]).



[[IDb1972e9ea4f0d385039051e095227a05]]
= Was muss ich über die Validierung des Sicherheitsschlüssels wissen?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Nachdem Sie einen Sicherheitsschlüssel erstellt haben, sollten Sie die
Schlüsseldatei überprüfen, um sicherzustellen, dass sie nicht beschädigt
ist.

Wenn die Validierung fehlschlägt, gehen Sie wie folgt vor:

* Wenn die Sicherheitsschlüsselkennung nicht mit der Kennung auf dem
Controller übereinstimmt, suchen Sie die richtige
Sicherheitsschlüsseldatei, und versuchen Sie die Validierung erneut.
* Wenn der Controller den Sicherheitsschlüssel nicht zur Validierung
entschlüsseln kann, haben Sie möglicherweise den Passphrase falsch
eingegeben. Überprüfen Sie den Passphrase, geben Sie ihn ggf. erneut ein,
und versuchen Sie dann erneut die Validierung. Wenn die Fehlermeldung
erneut angezeigt wird, wählen Sie eine Sicherungskopie der Schlüsseldatei
(falls verfügbar) aus, und versuchen Sie die Validierung erneut.
* Wenn Sie den Sicherheitsschlüssel immer noch nicht validieren können,
ist die Originaldatei möglicherweise beschädigt. Erstellen Sie ein neues
Backup des Schlüssels und validieren Sie diese Kopie.



[[IDa1151fa8ef987b8eb91d7d351fe723b3]]
= Worin besteht der Unterschied zwischen internem Sicherheitsschlüssel und
externem Sicherheitsschlüsselmanagement?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

```
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.



:leveloffset: -1


:leveloffset: -1


= Zugriffsmanagement

:leveloffset: +1


[[IDef4454929565cc9e890e8a19cf4c2666]]
= Zugriffsmanagement – Überblick
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die Zugriffsverwaltung ist eine Methode zur Einrichtung der
Benutzerauthentifizierung in SANtricity System Manager.



== Welche Authentifizierungsmethoden sind verfügbar?

Zu den Authentifizierungsmethoden zählen RBAC (rollenbasierte
Zugriffssteuerung), Directory Services und Security Assertion Markup
Language (SAML):

* *RBAC/Lokale Benutzerrollen* -- Authentifizierung wird über im Storage
```

```
Array erzwungene RBAC-Funktionen gemanagt. Lokale Benutzerrollen umfassen
vordefinierte Benutzerprofile und Rollen mit spezifischen
Zugriffsberechtigungen.
* *Directory Services* -- die Authentifizierung wird über einen LDAP-
Server (Lightweight Directory Access Protocol) und Verzeichnisdienste, wie
z. B. Microsoft Active Directory, verwaltet.
* *SAML* -- Authentifizierung wird über einen Identitäts-Provider (IdP)
mit SAML 2.0 verwaltet.


Weitere Informationen:

* xref:{relative_path}how-access-management-works.html["Funktionsweise von
Access Management"]
* xref:{relative_path}access-management-terminology.html["Terminologie für
das Zugriffsmanagement"]
* xref:{relative_path}permissions-for-mapped-roles.html["Berechtigungen
für zugeordnete Rollen"]
* xref:{relative_path}access-management-with-local-user-roles.html["Lokale
Benutzerrollen"]
* xref:{relative_path}access-management-with-directory-
services.html["Verzeichnisdienste"]
* xref:{relative_path}access-management-with-saml.html["SAML"]




== Wie konfiguriere ich die Authentifizierung?

Das Storage Array ist vorkonfiguriert zur Nutzung von lokalen
Benutzerrollen, eine Implementierung von RBAC-Funktionen. Wenn Sie eine
andere Methode konfigurieren möchten, gehen Sie zu menu:Settings[Access
Management].

Weitere Informationen:

* xref:{relative_path}add-directory-server.html["Fügen Sie einen LDAP-
Verzeichnisserver hinzu"]
* xref:{relative_path}configure-saml.html["Konfigurieren Sie SAML"]




== Verwandte Informationen

Weitere Informationen zu Aufgaben im Zusammenhang mit Zugriffsmanagement:
```

```
* xref:{relative_path}change-passwords.html["Passwörter ändern"]
* xref:{relative_path}view-audit-log-activity.html["Zeigen Sie die
Aktivität des Prüfprotokolls an"]
* xref:{relative_path}configure-syslog-server-for-audit-logs.html["Syslog-
Server für Audit-Protokolle konfigurieren"]




= Konzepte

:leveloffset: +1


[[ID2af9f6c8e6fd51f93da7353ef8de36ae]]
= Funktionsweise von Access Management
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die Zugriffsverwaltung ist eine Methode zur Einrichtung der
Benutzerauthentifizierung in SANtricity System Manager.

Konfiguration und Benutzerauthentifizierung:

. Ein Administrator meldet sich bei System Manager mit einem
Benutzerprofil an, das die Berechtigungen für Sicherheitsadministrator
enthält.
+
[NOTE]
====
Bei der ersten Anmeldung wird der Benutzername verwendet `admin` Wird
automatisch angezeigt und kann nicht geändert werden. Der `admin` Der
Benutzer hat vollen Zugriff auf alle Funktionen im System.

====
. Der Administrator navigiert in der Benutzeroberfläche zur
Zugriffsverwaltung. Das Storage Array ist vorkonfiguriert zur Verwendung
von lokalen Benutzerrollen, bei denen es sich um die Implementierung von
RBAC-Funktionen (rollenbasierte Zugriffssteuerung) handelt.
. Der Administrator konfiguriert eine oder mehrere der folgenden
Authentifizierungsmethoden:
+
** *Lokale Benutzerrollen* -- Authentifizierung wird über im Storage Array
```

erzwungene RBAC-Funktionen gemanagt. Lokale Benutzerrollen umfassen vordefinierte Benutzerprofile und Rollen mit spezifischen Zugriffsberechtigungen. Administratoren können diese lokalen Benutzerrollen als einzige Authentifizierungsmethode verwenden oder in Kombination mit einem Verzeichnisdienst verwenden. Es ist keine Konfiguration erforderlich – abgesehen von der Festlegung von Passwörtern für die Benutzer.
** *Directory Services* -- die Authentifizierung wird über einen LDAP-Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst verwaltet, z. B. über Microsoft Active Directory. Ein Administrator stellt eine Verbindung zum LDAP-Server her und ordnet die LDAP-Benutzer den im Speicher-Array eingebetteten lokalen Benutzerrollen zu.
** *SAML* -- Authentifizierung wird über einen Identitäts-Provider (IdP) mit der Security Assertion Markup Language (SAML) 2.0 verwaltet. Ein Administrator stellt die Verbindung zwischen dem IdP-System und dem Storage-Array her und ordnet anschließend die IdP-Benutzer den im Storage-Array eingebetteten lokalen Benutzerrollen zu.

. Der Administrator stellt Benutzern die Anmeldeinformationen für System Manager zur Verfügung.
. Benutzer melden sich beim System an, indem sie ihre Anmeldedaten eingeben.
+
[NOTE]
====
Wenn die Authentifizierung mit SAML und einem SSO (Single Sign On) verwaltet wird, umgehen das System möglicherweise das Anmeldedialogfeld von System Manager.

====
+
Während der Anmeldung führt das System die folgenden Hintergrundaufgaben aus:

+
** Authentifiziert Benutzernamen und Kennwort anhand des Benutzerkontos.
** Legt die Berechtigungen des Benutzers basierend auf den zugewiesenen Rollen fest.
** Ermöglicht dem Benutzer den Zugriff auf Aufgaben in der Benutzeroberfläche.
** Zeigt den Benutzernamen oben rechts in der Schnittstelle an.

== In System Manager verfügbare Aufgaben

Der Zugriff auf Aufgaben hängt von den zugewiesenen Rollen eines Benutzers ab. Dazu gehören:

* *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
* *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access Management, Zertifikatverwaltung, Audit Log Management und die Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder auszuschalten.
* *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-Upgrades. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
* *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

Eine nicht verfügbare Aufgabe ist entweder ausgegraut oder wird in der Benutzeroberfläche nicht angezeigt. Beispielsweise kann ein Benutzer mit der Rolle „Monitor" alle Informationen zu Volumes anzeigen, jedoch keinen Zugriff auf Funktionen zum Ändern des Volumes haben. Die Registerkarten für Funktionen wie *Kopierdienste* und *zum Workload hinzufügen* werden ausgegraut; es sind nur *Einstellungen anzeigen/bearbeiten* verfügbar.

== Einschränkungen bei Unified Manager und Storage Manager

Wenn SAML für ein Storage-Array konfiguriert ist, können Benutzer den Speicher für dieses Array nicht über Unified Manager oder die alten Storage Manager-Schnittstellen erkennen oder managen.

Wenn lokale Benutzerrollen und Verzeichnisdienste konfiguriert sind, müssen Benutzer Anmeldeinformationen eingeben, bevor eine der folgenden Funktionen ausgeführt wird:

* Umbenennen des Speicher-Arrays
* Aktualisieren der Controller-Firmware
* Laden einer Speicherarray-Konfiguration
* Ausführen eines Skripts
* Es wird versucht, einen aktiven Vorgang auszuführen, wenn eine nicht verwendete Sitzung abgelaufen ist

```
[[ID2873eab4a9d934f5c02998e3fcaa388b]]
= Terminologie für das Zugriffsmanagement
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Erfahren Sie, wie die Bedingungen für das Zugriffsmanagement auf Ihr
Storage Array Anwendung finden.

[cols="25h,~"]
|===
| Laufzeit | Beschreibung


 a|
Access Token
 a|
Access Tokens werden verwendet, um sich anstelle von Benutzernamen und
Passwort mit DER REST-API oder der Befehlszeilenschnittstelle (CLI) zu
authentifizieren. Token sind einem bestimmten Benutzer (einschließlich
LDAP-Benutzer) zugeordnet und enthalten eine Reihe von Berechtigungen und
eine Ablauffrist.



 a|
Active Directory
 a|
Active Directory (AD) ist ein Microsoft-Verzeichnisdienst, der LDAP für
Windows-Domänennetzwerke verwendet.



 a|
Verbindlich
 a|
Bindevorgänge werden zur Authentifizierung von Clients auf dem
Verzeichnisserver verwendet. Binding erfordert in der Regel Konto- und
Kennwortanmeldeinformationen, aber einige Server erlauben anonyme
Bindevorgänge.
```

a|
CA
a|
Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer, die sichere Verbindungen zwischen Clients und Servern ermöglichen.

a|
Zertifikat
a|
Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).

a|
IDP
a|
Ein Identitäts-Provider (IdP) ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert und festgestellt werden können, ob dieser Benutzer erfolgreich authentifiziert wurde. Der IdP kann so konfiguriert werden, dass er Multi-Faktor-Authentifizierung bietet und eine beliebige Benutzerdatenbank, wie z. B. Active Directory, verwendet. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich.

a|
LDAP
a|
Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll für den Zugriff auf verteilte Verzeichnisinformationsdienste und die Wartung. Mit diesem Protokoll können viele verschiedene Anwendungen und Dienste eine Verbindung zum LDAP-Server zur Überprüfung von Benutzern herstellen.

a|

```
RBAC
 a|
Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) ist
eine Methode zur Regulierung des Zugriffs auf Computer- oder
Netzwerkressourcen, basierend auf den Rollen einzelner Benutzer. RBAC-
Kontrollen werden auf dem Storage Array durchgesetzt und umfassen
vordefinierte Rollen.



 a|
SAML
 a|
Security Assertion Markup Language (SAML) ist ein XML-basierter Standard
für die Authentifizierung und Autorisierung zwischen zwei Einheiten. SAML
ermöglicht Multi-Faktor-Authentifizierung, bei der Benutzer zwei oder mehr
Elemente zur Identitätsnachweise bereitstellen müssen (z. B. ein Passwort
und ein Fingerabdruck). Die integrierte SAML-Funktion des Speicherarrays
ist SAML2.0-konform für Identitätsbehauptung, Authentifizierung und
Autorisierung.



 a|
SP
 a|
Ein Service-Provider (SP) ist ein System, das die
Benutzerauthentifizierung und den Zugriff steuert. Wenn Access Management
mit SAML konfiguriert ist, fungiert das Storage-Array als Dienstanbieter
für die Anforderung der Authentifizierung vom Identity Provider.



 a|
SSO
 a|
Bei Single Sign On (SSO) handelt es sich um einen
Authentifizierungsservice, mit dem ein Satz an Anmeldeinformationen auf
mehrere Anwendungen zugreifen kann.

|===



[[IDdeac70e586dfe3b2bc41ca2695b4312b]]
= Berechtigungen für zugeordnete Rollen
:allow-uri-read:
```

```
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die auf dem Storage-Array erzwungenen RBAC-Funktionen (rollenbasierte
Zugriffssteuerung) umfassen vordefinierte Benutzerprofile, die mit einer
oder mehreren zugewiesenen Rollen ausgestattet sind. Jede Rolle umfasst
Berechtigungen für den Zugriff auf Aufgaben in SANtricity System Manager.

Auf Benutzerprofile und zugeordnete Rollen kann über das
Menü:Einstellungen[Zugriffsmanagement > Lokale Benutzerrollen] in der
Benutzeroberfläche eines System Managers zugegriffen werden.

Die Rollen ermöglichen Benutzern den Zugriff auf Aufgaben wie folgt:

* *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes
und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
* *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management, Zertifikatverwaltung, Audit Log Management und die
Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder
auszuschalten.
* *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem
Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-
Upgrades. Kein Zugriff auf Speicherobjekte oder die
Sicherheitskonfiguration.
* *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


Wenn ein Benutzer über keine Berechtigungen für eine bestimmte Aufgabe
verfügt, ist diese Aufgabe entweder ausgegraut oder wird nicht in der
Benutzeroberfläche angezeigt.



[[ID8a71be84a1789255a54577f3089a0e03]]
= Zugriffsverwaltung mit lokalen Benutzerrollen
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

```
Administratoren können für das Zugriffsmanagement die im Storage Array
erzwungenen RBAC-Funktionen (rollenbasierte Zugriffssteuerung) nutzen.
Diese Funktionen werden als „lokale Benutzerrollen“ bezeichnet.



== Konfigurationsworkflow

Lokale Benutzerrollen sind für das Speicher-Array vorkonfiguriert. Um
lokale Benutzerrollen für die Authentifizierung zu verwenden, können
Administratoren Folgendes tun:

. Ein Administrator meldet sich bei System Manager mit einem
Benutzerprofil an, das die Berechtigungen für Sicherheitsadministrator
enthält.
+
[NOTE]
====
Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

====
. Ein Administrator überprüft die Benutzerprofile, die vordefiniert sind
und nicht geändert werden können.
. Optional weist der Administrator jedem Benutzerprofil neue Passwörter
zu.
. Benutzer melden sich mit ihren zugewiesenen Anmeldedaten am System an.



== Vereinfachtes

Bei der Verwendung von nur lokalen Benutzerrollen für die
Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben
ausführen:

* Passwörter ändern.
* Legen Sie eine Mindestlänge für Passwörter fest.
* Benutzern erlauben, sich ohne Passwörter anzumelden.



[[IDc03657dd2ef3a0e94ef342281cca66a3]]
= Zugriffsmanagement mit Verzeichnisdiensten
:allow-uri-read:
:icons: font
```

```
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Für die Zugriffsverwaltung können Administratoren einen LDAP-Server
(Lightweight Directory Access Protocol) und einen Verzeichnisdienst wie
Microsoft Active Directory verwenden.



== Konfigurationsworkflow

Wenn ein LDAP-Server und ein Verzeichnisdienst im Netzwerk verwendet
werden, funktioniert die Konfiguration wie folgt:

. Ein Administrator meldet sich bei System Manager mit einem
Benutzerprofil an, das die Berechtigungen für Sicherheitsadministrator
enthält.
+
[NOTE]
====
Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

====
. Der Administrator gibt die Konfigurationseinstellungen für den LDAP-
Server ein. Zu den Einstellungen gehören der Domain-Name, die URL und die
Bind-Kontoinformationen.
. Wenn der LDAP-Server ein sicheres Protokoll (LDAPS) verwendet, lädt der
Administrator eine Zertifikatskette für die Authentifizierung zwischen dem
LDAP-Server und dem Speicher-Array hoch.
. Nachdem die Serververbindung hergestellt wurde, ordnet der Administrator
die Benutzergruppen den Rollen des Speicherarrays zu. Diese Rollen sind
vordefiniert und können nicht geändert werden.
. Der Administrator testet die Verbindung zwischen dem LDAP-Server und dem
Speicher-Array.
. Benutzer melden sich mit ihren zugewiesenen LDAP/Directory Services-
Anmeldedaten am System an.



== Vereinfachtes

Bei der Verwendung von Verzeichnisdiensten zur Authentifizierung können
Administratoren die folgenden Verwaltungsaufgaben ausführen:
```

```
* Fügen Sie einen Verzeichnisserver hinzu.
* Bearbeiten der Einstellungen des Verzeichnisservers.
* Zuordnen von LDAP-Benutzern zu lokalen Benutzerrollen.
* Entfernen Sie einen Verzeichnisserver.




[[IDaf2a059efc5a5029d39bb8096f05f19a]]
= Zugriffsmanagement mit SAML
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Für die Zugriffsverwaltung können Administratoren die in das Array
integrierten Funktionen der Security Assertion Markup Language (SAML) 2.0
verwenden.



== Konfigurationsworkflow

Die SAML-Konfiguration funktioniert wie folgt:

. Ein Administrator meldet sich bei System Manager mit einem
Benutzerprofil an, das die Berechtigungen für Sicherheitsadministrator
enthält.
+
[NOTE]
====
Der `admin` Der Benutzer hat vollständigen Zugriff auf alle Funktionen in
System Manager.

====
. Der Administrator wechselt zur Registerkarte *SAML* unter
Zugriffsverwaltung.
. Ein Administrator konfiguriert die Kommunikation mit dem Identity
Provider (IdP). Ein IdP ist ein externes System, mit dem
Anmeldeinformationen von einem Benutzer angefordert werden und
festgestellt wird, ob der Benutzer erfolgreich authentifiziert wurde. Zum
Konfigurieren der Kommunikation mit dem Storage-Array lädt der
Administrator die IdP-Metadatendatei aus dem IdP-System herunter und lädt
die Datei anschließend mit System Manager zum Hochladen auf das Storage-
Array ein.
```

. Ein Administrator stellt eine Vertrauensbeziehung zwischen dem Dienstanbieter und dem IdP her. Ein Dienstanbieter steuert die Benutzerautorisierung. In diesem Fall fungiert der Controller im Speicher-Array als Service Provider. Zum Konfigurieren der Kommunikation verwendet der Administrator System Manager zum Exportieren einer Service-Provider-Metadatendatei für jeden Controller. Aus dem IdP-System importiert der Administrator diese Metadatendateien in das IdP.
+
[NOTE]
====
Administratoren sollten außerdem sicherstellen, dass das IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.

====
. Der Administrator ordnet die Rollen des Storage-Arrays den in IdP definierten Benutzerattributen zu. Dazu verwendet der Administrator System Manager zum Erstellen der Zuordnungen.
. Der Administrator testet die SSO-Anmeldung an der IdP-URL. Dieser Test stellt sicher, dass das Storage-Array und das IdP kommunizieren können.
+
[CAUTION]
====
Sobald SAML aktiviert ist, können Sie sie über die Benutzeroberfläche nicht deaktivieren oder die IdP-Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an den technischen Support, um Hilfe zu erhalten.

====
. In System Manager aktiviert der Administrator SAML für das Storage-Array.
. Benutzer melden sich mit ihren SSO-Anmeldedaten am System an.

== Vereinfachtes

Bei der Verwendung von SAML zur Authentifizierung können Administratoren die folgenden Managementaufgaben ausführen:

* Neue Rollenzuordnungen ändern oder erstellen
* Exportieren Sie die Dateien von Dienstanbietern

```
== Zugriffsbeschränkungen

Wenn SAML aktiviert ist, können Benutzer Speicher für dieses Array nicht
über Unified Manager oder die alte Storage Manager-Schnittstelle ermitteln
oder managen.

Außerdem können die folgenden Clients nicht auf Services und Ressourcen
des Speicherarrays zugreifen:

* Enterprise Management-Fenster (EMW)
* Befehlszeilenschnittstelle (CLI)
* Software Developer Kits (SDK)-Clients
* In-Band-Clients
* REST-API-Clients für die HTTP-Standardauthentifizierung
* Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an




[[ID643b28d16d5e7e9b2f2eba1181562e94]]
= Auf Token zugreifen
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Access Tokens bieten eine Authentifizierungsmethode mit DER REST-API oder
der Befehlszeilenschnittstelle (CLI), ohne Benutzernamen und Kennwörter
offenzulegen. Ein Token ist einem bestimmten Benutzer (einschließlich
LDAP-Benutzer) zugeordnet und umfasst eine Reihe von Berechtigungen und
eine Ablauffrist.



== Zugriff auf SAML- und JSON-Webtoken

Standardmäßig ist ein System mit aktivierter SAML nicht für den Zugriff
auf herkömmliche Befehlszeilentools verfügbar. DIE REST-API und die CLI
funktionieren wirkungslos, da der MFA-Workflow zur Authentifizierung eine
Umleitung zu einem Identity Provider-Server erfordert. Deshalb müssen Sie
Token in System Manager generieren, die die Authentifizierung eines
Benutzers über MFA vorgeben.


NOTE: Für die Verwendung von Webtoken ist SAML nicht erforderlich, aber
```

```
SAML wird für die höchste Sicherheitsstufe empfohlen.



== Workflow zum Erstellen und Verwenden von Token

. Erstellen Sie in System Manager ein Token, und bestimmen Sie dessen
Ablauf.
. Kopieren Sie den Token-Text in die Zwischenablage, oder laden Sie ihn in
eine Datei herunter, und speichern Sie den Token-Text an einem sicheren
Ort.
. Verwenden Sie das Token wie folgt:
+
** *Rest API*: Um ein Token in einer REST-API-Anforderung zu verwenden,
fügen Sie einen HTTP-Header zu Ihren Anforderungen hinzu. Beispiel:
`Authorization: Bearer _<access-token-value>_`
** *Secure CLI*: Um ein Token in der CLI zu verwenden, fügen Sie den
Token-Wert in die Befehlszeile ein oder verwenden Sie den Pfad zu einer
Datei, die den Token-Wert enthält. Beispiel:
+
*** Token-Wert in der Befehlszeile: `-t _access-token-value_`
*** Pfad zu einer Datei mit dem Token-Wert: `-T _access-token-file_`







Weitere Informationen:

* xref:{relative_path}access-management-tokens-create.html["Erstellen von
Zugriffs-Tokens"]
* xref:{relative_path}access-management-tokens-edit.html["Bearbeiten Sie
Access Tokens"]
* xref:{relative_path}access-management-tokens-revoke.html["Access Token
widerrufen"]




:leveloffset: -1


= Lokale Benutzerrollen verwenden

:leveloffset: +1
```

```
[[ID7d1b9aab287ce36063585ec97ad89131]]
= Zeigen Sie lokale Benutzerrollen an
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Auf der Registerkarte Lokale Benutzerrollen können Sie die Zuordnungen der
Benutzerprofile zu den Standardrollen anzeigen. Diese Zuordnungen sind
Teil der RBAC (rollenbasierte Zugriffssteuerung), die im Storage Array
durchgesetzt wird.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.

.Über diese Aufgabe
Die Benutzerprofile und Zuordnungen können nicht geändert werden. Es
können nur Passwörter geändert werden.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
+
Die Benutzerprofile sind in der Tabelle aufgeführt:

+
** *Root Admin* (admin) -- Super-Administrator, der Zugriff auf alle
Funktionen im System hat. Dieses Benutzerprofil enthält alle Rollen.
** *Storage Admin* (Storage) -- der Administrator für die gesamte Storage-
Bereitstellung verantwortlich. Dieses Benutzerprofil umfasst die folgenden
Rollen: Storage-Administrator, Support-Administrator und Monitor.
** *Security Admin* (Security) -- der für die Sicherheitskonfiguration
verantwortliche Benutzer, einschließlich Zugriffsverwaltung,
Zertifikatverwaltung und Secure-Enabled Drive-Funktionen. Dieses
Benutzerprofil umfasst die folgenden Rollen: Security Admin und Monitor.
** *Support Admin* (Support) -- der Benutzer ist verantwortlich für
Hardware-Ressourcen, Ausfalldaten und Firmware-Upgrades. Dieses
Benutzerprofil umfasst die folgenden Rollen: Unterstützen Sie Admin und
Monitor.
** *Monitor* (Monitor) -- Ein Benutzer mit schreibgeschütztem Zugriff auf
```

```
das System. Dieses Benutzerprofil enthält nur die Rolle Monitor.




[[IDbf2658164522c7e7afef43db88389694]]
= Passwörter ändern
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die Benutzerpasswörter für jedes Benutzerprofil in Access
Management ändern.

.Bevor Sie beginnen
* Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-
Berechtigungen enthält.
* Sie müssen das lokale Administratorkennwort kennen.


.Über diese Aufgabe
Beachten Sie bei der Auswahl eines Passworts die folgenden Richtlinien:

* Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Einstellung
für ein Mindestpasswort erfüllen oder überschreiten (unter „Einstellungen
anzeigen/bearbeiten“).
* Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt.
* Nachgestellte Leerzeichen werden nicht von Kennwörtern entfernt, wenn
sie eingestellt sind. Achten Sie darauf, Leerzeichen einzugeben, wenn
diese im Passwort enthalten waren.
* Um die Sicherheit zu erhöhen, verwenden Sie mindestens 15
alphanumerische Zeichen, und ändern Sie das Passwort häufig.


[NOTE]
====
Durch Ändern des Passworts in System Manager wird es auch in der
Befehlszeilenschnittstelle (CLI) geändert. Außerdem führen
Kennwortänderungen dazu, dass die aktive Sitzung des Benutzers beendet
wird.
```

```
====
.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
. Wählen Sie einen Benutzer aus der Tabelle aus.
+
Die Schaltfläche Kennwort ändern steht zur Verfügung.

. Wählen Sie *Passwort Ändern*.
+
Das Dialogfeld Kennwort ändern wird geöffnet.

. Wenn für lokale Benutzerpasswörter keine Mindestkennwortlänge festgelegt
ist, können Sie das Kontrollkästchen aktivieren, damit der ausgewählte
Benutzer ein Kennwort für den Zugriff auf das Speicher-Array eingeben
muss. Anschließend können Sie das neue Passwort für den ausgewählten
Benutzer eingeben.
. Geben Sie Ihr lokales Administratorpasswort ein und klicken Sie dann auf
*Ändern*.


.Ergebnisse
Wenn der Benutzer derzeit angemeldet ist, wird die aktive Sitzung des
Benutzers durch die Kennwortänderung beendet.



[[IDe7052bb7c597207f7b1235382d9e4381]]
= Ändern Sie die Einstellungen für das lokale Benutzerpasswort
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die erforderliche Mindestlänge für alle neuen oder
aktualisierten lokalen Benutzerpasswörter im Speicher-Array festlegen. Sie
können lokalen Benutzern auch ohne Eingabe eines Kennworts den Zugriff auf
das Speicher-Array erlauben.

.Bevor Sie beginnen
Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-
Berechtigungen enthält.

.Über diese Aufgabe
```

Beachten Sie die folgenden Richtlinien, wenn Sie die Mindestlänge für lokale Benutzerpasswörter festlegen:

* Die Einstellung von Änderungen wirkt sich nicht auf vorhandene lokale Benutzerpasswörter aus.
* Die Mindestlänge für lokale Benutzerpasswörter muss zwischen 0 und 30 Zeichen liegen.
* Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Mindestlängeneinstellung erfüllen oder überschreiten.
* Legen Sie keine Mindestlänge für das Passwort fest, wenn lokale Benutzer ohne Eingabe eines Kennworts auf das Speicher-Array zugreifen möchten.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
. Wählen Sie die Schaltfläche *Einstellungen anzeigen/bearbeiten*.
+
Das Dialogfeld Einstellungen für das lokale Benutzerpasswort wird geöffnet.

. Führen Sie einen der folgenden Schritte aus:
+
** Um lokalen Benutzern den Zugriff auf das Speicher-Array zu ermöglichen, ohne ein Passwort einzugeben, deaktivieren Sie das Kontrollkästchen „Alle lokalen Benutzerpasswörter müssen mindestens sein“.
** Um eine Mindestkennwortlänge für alle lokalen Benutzerpasswörter festzulegen, aktivieren Sie das Kontrollkästchen „Alle lokalen Benutzerpasswörter müssen mindestens sein“ und verwenden Sie dann das Spinner-Feld, um die erforderliche Mindestlänge für alle lokalen Benutzerpasswörter festzulegen.
+
Neue lokale Benutzerpasswörter müssen die aktuelle Einstellung erfüllen oder überschreiten.

. Klicken Sie Auf *Speichern*.

:leveloffset: -1

= Verzeichnisdienste verwenden

```
:leveloffset: +1


[[IDc323c46c69b83fee52a57c66d48b677a]]
= Fügen Sie einen LDAP-Verzeichnisserver hinzu
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um die Authentifizierung für die Zugriffsverwaltung zu konfigurieren,
können Sie die Kommunikation zwischen dem Speicher-Array und einem LDAP-
Server herstellen und die LDAP-Benutzergruppen den vordefinierten Rollen
des Arrays zuordnen.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
* LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich
Domänenname, Server-URL und optional Benutzername und Kennwort für das
Bindekonto.
* Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette
des LDAP-Servers auf Ihrem lokalen Computer installiert sein.


.Über diese Aufgabe
Das Hinzufügen eines Verzeichnisservers ist ein zweistufiger Prozess.
Geben Sie zuerst den Domain-Namen und die URL ein. Wenn Ihr Server ein
sicheres Protokoll verwendet, müssen Sie auch ein CA-Zertifikat zur
Authentifizierung hochladen, wenn es von einer nicht standardmäßigen
Signierungsbehörde signiert ist. Wenn Sie über Anmeldedaten für ein
Bindekonto verfügen, können Sie auch Ihren Benutzernamen und Ihr Kennwort
eingeben. Als Nächstes werden die Benutzergruppen des LDAP-Servers den
vordefinierten Rollen des Speicher-Arrays zugeordnet.

[NOTE]
====
Während des Verfahrens zum Hinzufügen eines LDAP-Servers wird die alte
Verwaltungsschnittstelle deaktiviert. Die alte Managementoberfläche
(Symbol) ist eine Methode der Kommunikation zwischen dem Storage-Array und
dem Management-Client. Wenn die Option deaktiviert ist, nutzen das
```

```
Storage-Array und der Management-Client eine sicherere
Kommunikationsmethode (REST-API über HTTPS).

====
.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie auf der Registerkarte Verzeichnisdienste die Option
*Verzeichnisserver hinzufügen* aus.
+
Das Dialogfeld Add Directory Server wird geöffnet.

. Geben Sie auf der Registerkarte Servereinstellungen die
Anmeldeinformationen für den LDAP-Server ein.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Konfigurationseinstellungen*



 a|
Domäne(en)
 a|
Geben Sie den Domänennamen des LDAP-Servers ein. Geben Sie für mehrere
Domänen die Domänen in eine kommagetrennte Liste ein. Der Domänenname wird
in der Anmeldung (_username_@_Domain_) verwendet, um anzugeben, gegen
welchen Verzeichnisserver sich authentifizieren soll.



 a|
Server-URL
 a|
Geben Sie die URL für den Zugriff auf den LDAP-Server in Form von ein
`ldap[s]://*host*:*port*`.



 a|
Zertifikat hochladen (optional)
```

a|

NOTE: Dieses Feld wird nur angezeigt, wenn ein LDAPS-Protokoll im obigen Feld Server-URL angegeben wird.

Klicken Sie auf *Durchsuchen* und wählen Sie ein CA-Zertifikat zum Hochladen aus. Dies ist das vertrauenswürdige Zertifikat oder die Zertifikatskette, die für die Authentifizierung des LDAP-Servers verwendet wird.

a|
Konto binden (optional)
a|
Geben Sie ein schreibgeschütztes Benutzerkonto ein, um Suchanfragen auf dem LDAP-Server und für die Suche in den Gruppen durchzuführen. Geben Sie den Kontonamen im LDAP-Format ein. Wenn der Bindebenutzer beispielsweise „bind-Benutzer" heißt, können Sie einen Wert wie „CN=bindact,CN=users,DC=cpoc,DC=local" eingeben.

a|
Bindepasswort (optional)
a|

NOTE: Dieses Feld wird angezeigt, wenn Sie oben ein Bindungskonto eingeben.

Geben Sie das Passwort für das Bindekonto ein.

a|
Testen Sie die Serververbindung, bevor Sie sie hinzufügen
a|
Aktivieren Sie dieses Kontrollkästchen, wenn Sie sicherstellen möchten, dass das Speicher-Array mit der eingegebenen LDAP-Serverkonfiguration kommunizieren kann. Der Test erfolgt, nachdem Sie unten im Dialogfeld auf *Hinzufügen* geklickt haben. Wenn dieses Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die Konfiguration nicht hinzugefügt. Sie müssen den Fehler beheben oder das Kontrollkästchen deaktivieren, um den Test zu überspringen und die Konfiguration hinzuzufügen.

```
 a|
**Berechtigungs-Einstellungen**



 a|
Basis-DN suchen
 a|
Geben Sie den LDAP-Kontext ein, um nach Benutzern zu suchen, normalerweise
in Form von `CN=Users, DC=cpoc, DC=local`.



 a|
Attribut Benutzername
 a|
Geben Sie das Attribut ein, das zur Authentifizierung an die Benutzer-ID
gebunden ist. Beispiel: `sAMAccountName`.



 a|
Gruppenattribut\(s\)
 a|
Geben Sie eine Liste der Gruppenattribute für den Benutzer ein, die für
die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: `memberOf,
managedObjects`.

|===
====
. Klicken Sie auf die Registerkarte **Rollenzuordnung**.
. Weisen Sie den vordefinierten Rollen LDAP-Gruppen zu. Einer Gruppe
können mehrere Rollen zugewiesen sein.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*
```

```
 a|
Gruppen-DN
 a|
Geben Sie den Group Distinguished Name (DN) für die zu zugeordnete LDAP-
Benutzergruppe an. Reguläre Ausdrücke werden unterstützt. Diese speziellen
regulären Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich
entgangen werden (`\`Wenn sie nicht Teil eines regulären Ausdrucksmusters
sind: \.[]{}()<>*+-=!?^



 a|
Rollen
 a|
Klicken Sie in das Feld, und wählen Sie eine der Rollen des Speicherarrays
aus, die dem Gruppen-DN zugeordnet werden sollen. Sie müssen jede Rolle,
die Sie für diese Gruppe aufnehmen möchten, einzeln auswählen. Die Rolle
„Überwachen“ ist erforderlich, wenn Sie sich mit den anderen Rollen bei
SANtricity-System-Manager anmelden. Die zugeordneten Rollen umfassen die
folgenden Berechtigungen:

** *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes
und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management, Zertifikatverwaltung, Audit Log Management und die
Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder
auszuschalten.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem
Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-
Upgrades. Kein Zugriff auf Speicherobjekte oder die
Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


|===
====
+
[NOTE]
====
Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Der System Manager funktioniert ohne die
vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

====
. Klicken Sie auf *Weitere Zuordnungen hinzufügen*, um weitere Gruppen-zu-
```

Rolle-Zuordnungen einzugeben.
. Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf *Hinzufügen*.
+
Das System führt eine Validierung durch und stellt sicher, dass das Speicher-Array und der LDAP-Server kommunizieren können. Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die im Dialogfeld eingegebenen Anmeldeinformationen, und geben Sie die Informationen ggf. erneut ein.

[[ID8dfc9eca5bf19b245ee4170cea7138f1]]
= Bearbeiten Sie die Einstellungen des Verzeichnisservers und die Rollenzuordnungen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Wenn Sie zuvor einen Verzeichnisserver in der Zugriffsverwaltung konfiguriert haben, können Sie dessen Einstellungen jederzeit ändern. Zu den Einstellungen gehören die Informationen zur Serververbindung und die Zuordnungen von Gruppen zu Rollen.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
* Ein Verzeichnisserver muss definiert werden.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *Directory Services* aus.
. Wenn mehr als ein Server definiert ist, wählen Sie den Server aus der Tabelle aus, den Sie bearbeiten möchten.
. Wählen Sie *Einstellungen Anzeigen/Bearbeiten*.
+
Das Dialogfeld Verzeichnisservereinstellungen wird geöffnet.

. Ändern Sie auf der Registerkarte Servereinstellungen die gewünschten Einstellungen.

```
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Konfigurationseinstellungen*



 a|
Domäne(en)
 a|
Der/die Domänenname(n) des/der LDAP-Server(e). Geben Sie für mehrere
Domänen die Domänen in eine kommagetrennte Liste ein. Der Domänenname wird
in der Anmeldung (_username_@_Domain_) verwendet, um anzugeben, gegen
welchen Verzeichnisserver sich authentifizieren soll.



 a|
Server-URL
 a|
Die URL für den Zugriff auf den LDAP-Server in Form von
`ldap[s]://host:port`.



 a|
Konto binden (optional)
 a|
Das schreibgeschützte Benutzerkonto für Suchabfragen am LDAP-Server und
für die Suche in den Gruppen.



 a|
Bindepasswort (optional)
 a|
Das Kennwort für das Bindekonto. (Dieses Feld wird angezeigt, wenn ein
Bindekonto eingegeben wird.)
```

```
 a|
Testen Sie vor dem Speichern die Serververbindung
 a|
Überprüft, ob das Speicher-Array mit der LDAP-Serverkonfiguration
kommunizieren kann. Der Test erfolgt, nachdem Sie unten im Dialogfeld auf
*Speichern* geklickt haben. Wenn dieses Kontrollkästchen aktiviert ist und
der Test fehlschlägt, wird die Konfiguration nicht geändert. Sie müssen
den Fehler beheben oder das Kontrollkästchen deaktivieren, um den Test zu
überspringen und die Konfiguration erneut zu bearbeiten.



 a|
*Berechtigungseinstellungen*



 a|
Basis-DN suchen
 a|
Der LDAP-Kontext für die Suche nach Benutzern, in der Regel in Form von
`CN=Users, DC=cpoc, DC=local`.



 a|
Attribut Benutzername
 a|
Das Attribut, das zur Authentifizierung an die Benutzer-ID gebunden ist.
Beispiel: `sAMAccountName`.



 a|
Gruppenattribut(e)
 a|
Eine Liste der Gruppenattribute für den Benutzer, die für die Zuordnung
von Gruppen zu Rollen verwendet werden. Beispiel: `memberOf,
managedObjects`.

|===
====
. Ändern Sie auf der Registerkarte Rollenzuordnung die gewünschte
Zuordnung.
+
.Felddetails
```

```
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Gruppen-DN
 a|
Der Domain-Name für die LDAP-Benutzergruppe, die zugeordnet werden soll. Reguläre Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich entgangen werden (`\`Wenn sie nicht Teil eines regulären Ausdrucksmusters sind: \.[]{}()<>*+-=!?^



 a|
Rollen
 a|
Die Rollen des Speicherarrays, die dem Gruppen-DN zugeordnet werden sollen. Sie müssen jede Rolle, die Sie für diese Gruppe aufnehmen möchten, einzeln auswählen. Die Rolle „Überwachen“ ist erforderlich, wenn Sie sich mit den anderen Rollen bei SANtricity-System-Manager anmelden. Die Rollen des Speicher-Arrays umfassen:

** *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access Management, Zertifikatverwaltung, Audit Log Management und die Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder auszuschalten.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-Upgrades. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.


|===
```

```
====
+
[NOTE]
====
Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Der System Manager funktioniert ohne die
vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

====
. Klicken Sie auf *Weitere Zuordnungen hinzufügen*, um weitere Gruppen-zu-
Rolle-Zuordnungen einzugeben.
. Klicken Sie Auf *Speichern*.


.Ergebnisse
Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen
beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.



[[ID9646defd774d640d679ae3af659604fb]]
= Verzeichnisserver entfernen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um die Verbindung zwischen einem Verzeichnisserver und dem Speicher-Array
zu unterbrechen, können Sie die Serverinformationen von der Seite
Zugriffsverwaltung entfernen. Sie möchten diese Aufgabe möglicherweise
ausführen, wenn Sie einen neuen Server konfiguriert haben und den alten
dann entfernen möchten.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.

.Über diese Aufgabe
Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen
beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
```

```
. Wählen Sie die Registerkarte *Directory Services* aus.
. Wählen Sie in der Liste den Verzeichnisserver aus, den Sie löschen
möchten.
. Klicken Sie Auf *Entfernen*.
+
Das Dialogfeld Verzeichnisserver entfernen wird geöffnet.

. Typ `remove` Klicken Sie im Feld auf *Entfernen*.
+
Die Konfigurationseinstellungen des Verzeichnisservers, die
Berechtigungseinstellungen und Rollenzuordnungen werden entfernt. Benutzer
können sich nicht mehr mit Anmeldeinformationen von diesem Server
anmelden.




:leveloffset: -1


= Verwenden Sie SAML

:leveloffset: +1


[[ID86ad05afd3f1e6ad003540e01a71e007]]
= Konfigurieren Sie SAML
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Zum Konfigurieren der Authentifizierung für das Zugriffsmanagement können
Sie die im Speicher-Array integrierten SAML-Funktionen (Security Assertion
Markup Language) verwenden. Mit dieser Konfiguration wird eine Verbindung
zwischen einem Identitätsanbieter und dem Speicheranbieter hergestellt.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* Sie müssen die IP-Adresse oder den Domänennamen jedes Controllers im
Speicher-Array kennen.
```

* Ein IdP-Administrator hat ein IdP-System konfiguriert.
* Ein IdP-Administrator hat sichergestellt, dass der IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.
* Ein Administrator hat sichergestellt, dass die IdP-Server- und -Controller-Uhren synchronisiert werden (entweder über einen NTP-Server oder durch Anpassen der Controller-Uhreinstellungen).
* Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, das für den Zugriff auf System Manager verwendet wird.

.Über diese Aufgabe
Ein Identitäts-Provider (IdP) ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert und festgestellt werden können, ob dieser Benutzer erfolgreich authentifiziert wurde. Der IdP kann so konfiguriert werden, dass er Multi-Faktor-Authentifizierung bietet und eine beliebige Benutzerdatenbank, wie z. B. Active Directory, verwendet. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich. Ein Service-Provider (SP) ist ein System, das die Benutzerauthentifizierung und den Zugriff steuert. Wenn Access Management mit SAML konfiguriert ist, fungiert das Storage-Array als Dienstanbieter für die Anforderung der Authentifizierung vom Identity Provider. Um eine Verbindung zwischen dem IdP und dem Storage-Array herzustellen, teilen Sie Metadatendateien zwischen diesen beiden Einheiten gemeinsam. Als Nächstes ordnen Sie die IdP-Benutzereinheiten den Storage-Array-Rollen zu. Und schließlich testen Sie die Verbindung und SSO-Anmeldedaten, bevor Sie SAML aktivieren.

[NOTE]
====
SAML und Directory Services. Wenn Sie SAML aktivieren, wenn Directory Services als Authentifizierungsmethode konfiguriert sind, ersetzt SAML die Directory Services in System Manager. Wenn Sie SAML später deaktivieren, wird die Konfiguration der Verzeichnisdienste wieder in die vorherige Konfiguration zurückgeführt.

====
[CAUTION]
====
Bearbeiten und Deaktivieren. Sobald SAML aktiviert ist, können Sie es nicht über die Benutzeroberfläche deaktivieren, noch können Sie die IdP-Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an den technischen Support, um Hilfe zu erhalten.

====

Die Konfiguration der SAML-Authentifizierung erfolgt in mehreren Schritten.

== Schritt 1: Laden Sie die IdP-Metadatendatei hoch

Um das Storage-Array mit IdP-Verbindungsinformationen bereitzustellen, importieren Sie IdP-Metadaten in System Manager. Das IdP-System benötigt diese Metadaten, um Authentifizierungsanforderungen an die richtige URL weiterzuleiten und die erhaltenen Antworten zu validieren. Sie müssen nur eine Metadatendatei für das Storage-Array hochladen, selbst wenn es zwei Controller gibt.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *SAML* aus.
+
Auf der Seite wird eine Übersicht der Konfigurationsschritte angezeigt.

. Klicken Sie auf den Link * Import Identity Provider (IdP) file*.
+
Das Dialogfeld „Datei des Identitätsanbieters importieren“ wird geöffnet.

. Klicken Sie auf *Durchsuchen*, um die IdP-Metadatendatei auszuwählen und auf Ihr lokales System hochzuladen.
+
Nach der Auswahl der Datei wird die IdP-Entity-ID angezeigt.

. Klicken Sie Auf *Import*.

== Schritt 2: Exportieren Sie die Dateien des Dienstanbieters

Um eine Vertrauensbeziehung zwischen dem IdP und dem Storage-Array herzustellen, importieren Sie die Metadaten des Service-Providers in das IdP. Die IdP benötigt diese Metadaten, um eine Vertrauensbeziehung zu den Controllern aufzubauen und Autorisierungsanforderungen zu bearbeiten. Die Datei enthält Informationen wie den Domänennamen oder die IP-Adresse des Controllers, sodass das IdP mit den Service-Providern kommunizieren kann.

.Schritte
. Klicken Sie auf den Link *Export Service Provider Files*.
+
Das Dialogfeld Dateien des Dienstanbieters exportieren wird geöffnet.

. Geben Sie die Controller-IP-Adresse oder den DNS-Namen in das Feld *Controller A* ein, und klicken Sie dann auf *Exportieren*, um die Metadatendatei auf Ihrem lokalen System zu speichern. Wenn das Speicher-Array zwei Controller enthält, wiederholen Sie diesen Schritt für den zweiten Controller im Feld *Controller B*.
+
Nachdem Sie auf *Export* geklickt haben, werden die Metadaten des Dienstanbieters auf Ihr lokales System heruntergeladen. Notieren Sie sich, wo die Datei gespeichert ist.

. Suchen Sie im lokalen System die Metadatendatei(en) des Serviceanbieters, die Sie exportiert haben.
+
Es gibt eine XML-formatierte Datei für jeden Controller.

. Importieren Sie vom IdP-Server die Metadatendatei(en) des Dienstanbieters, um die Vertrauensbeziehung herzustellen. Sie können die Dateien entweder direkt importieren oder manuell die Controller-Informationen aus den Dateien eingeben.

== Schritt 3: Rollen zuordnen

Um Benutzern Autorisierung und Zugriff auf System Manager zu ermöglichen, müssen Sie die IdP-Benutzerattribute und Gruppenmitgliedschaften den vordefinierten Rollen des Speicherarrays zuordnen.

.Bevor Sie beginnen
* Ein IdP-Administrator hat Benutzerattribute und Gruppenmitgliedschaften im IdP-System konfiguriert.
* Die IdP-Metadatendatei wird in System Manager importiert.
* Für die Vertrauensbeziehung wird für jeden Controller eine Metadatendatei des Dienstanbieters in das IdP-System importiert.

.Schritte
. Klicken Sie auf den Link für *Mapping System Manager* Rollen.
+
Das Dialogfeld Rollenzuordnung wird geöffnet.

. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.
+
.Felddetails

```
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Benutzerattribut
 a|
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-Gruppe an.



 a|
Attributwert
 a|
Geben Sie den Attributwert für die zu zugeordnete Gruppe an. Reguläre Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich entgangen werden (`\`Wenn sie nicht Teil eines regulären Ausdrucksmusters sind: \.[]{}()<>*+-=!?^



 a|
Rollen
 a|
Klicken Sie in das Feld, und wählen Sie eine der Rollen des Speicherarrays aus, die dem Attribut zugeordnet werden sollen. Sie müssen jede Rolle einzeln auswählen, die Sie einschließen möchten. Die Rolle „Monitor“ ist erforderlich, wenn Sie sich mit den anderen Rollen bei System Manager anmelden. Die Sicherheitsadministratorrolle ist auch für mindestens eine Gruppe erforderlich.

Die zugeordneten Rollen umfassen die folgenden Berechtigungen:

** *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access Management, Zertifikatverwaltung, Audit Log Management und die Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder
```

```
auszuschalten.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem
Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-
Upgrades. Kein Zugriff auf Speicherobjekte oder die
Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


|===
====
+
[NOTE]
====
Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Der System Manager funktioniert ohne die
vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

====
. Klicken Sie auf *Weitere Zuordnungen hinzufügen*, um weitere Gruppen-zu-
Rolle-Zuordnungen einzugeben.
+
[NOTE]
====
Rollenzuordnungen können geändert werden, nachdem SAML aktiviert ist.

====
. Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf *Speichern*.




== Schritt 4: SSO-Anmeldung testen

Um sicherzustellen, dass das IdP-System und das Speicherarray
kommunizieren können, können Sie optional eine SSO-Anmeldung testen.
Dieser Test wird auch während des letzten Schritts zur Aktivierung von
SAML durchgeführt.

.Bevor Sie beginnen
* Die IdP-Metadatendatei wird in System Manager importiert.
* Für die Vertrauensbeziehung wird für jeden Controller eine
Metadatendatei des Dienstanbieters in das IdP-System importiert.


.Schritte
. Klicken Sie auf den Link *SSO-Login testen*.
```

```
+
Zum Eingeben von SSO-Anmeldedaten wird ein Dialogfeld geöffnet.

. Geben Sie die Anmeldeinformationen für einen Benutzer mit
Sicherheitsadministratorrechten und Überwachungsberechtigungen ein.
+
Ein Dialogfeld wird geöffnet, während das System die Anmeldung testet.

. Suchen Sie nach einer Meldung für den erfolgreichen Test. Wenn der Test
erfolgreich abgeschlossen wurde, fahren Sie mit dem nächsten Schritt zur
Aktivierung von SAML fort.
+
Wenn der Test nicht erfolgreich abgeschlossen wird, wird eine
Fehlermeldung mit weiteren Informationen angezeigt. Stellen Sie sicher,
dass:

+
** Der Benutzer gehört zu einer Gruppe mit Berechtigungen für Security
Admin und Monitor.
** Die Metadaten, die Sie für den IdP-Server hochgeladen haben, sind
korrekt.
** Die Controller-Adressen in den SP-Metadatendateien sind korrekt.




== Schritt 5: SAML aktivieren

Der letzte Schritt besteht darin, die SAML-Konfiguration für die
Benutzerauthentifizierung abzuschließen. Während dieses Prozesses werden
Sie vom System auch aufgefordert, eine SSO-Anmeldung zu testen. Der SSO-
Anmelde-Test wird im vorherigen Schritt beschrieben.

.Bevor Sie beginnen
* Die IdP-Metadatendatei wird in System Manager importiert.
* Für die Vertrauensbeziehung wird für jeden Controller eine
Metadatendatei des Dienstanbieters in das IdP-System importiert.
* Mindestens ein Monitor und eine Sicherheitsadministratorzuordnung sind
konfiguriert.


[CAUTION]
====
*Bearbeiten und Deaktivieren.* Sobald SAML aktiviert ist, können Sie es
nicht über die Benutzeroberfläche deaktivieren, noch können Sie die IdP-
```

```
Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren
oder bearbeiten müssen, wenden Sie sich an den technischen Support, um
Hilfe zu erhalten.

====
.Schritte
. Wählen Sie auf der Registerkarte *SAML* den Link *SAML* aktivieren.
+
Das Dialogfeld SAML aktivieren bestätigen wird geöffnet.

. Typ `enable`, Und klicken Sie dann auf *Aktivieren*.
. Geben Sie die Benutzeranmeldeinformationen für einen SSO-Anmeldetest
ein.


.Ergebnisse
Nachdem das System SAML aktiviert hat, werden alle aktiven Sitzungen
beendet und die Authentifizierung von Benutzern über SAML beginnt.



[[ID40179a014562980881366eb8e6a401ad]]
= SAML-Rollenzuordnungen ändern
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie zuvor SAML für Access Management konfiguriert haben, können Sie
die Rollenzuordnungen zwischen den IdP-Gruppen und den vordefinierten
Rollen des Speicherarrays ändern.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* Ein IdP-Administrator hat Benutzerattribute und Gruppenmitgliedschaften
im IdP-System konfiguriert.
* SAML wurde konfiguriert und aktiviert.


.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *SAML* aus.
```

```
. Wählen Sie *Rollenzuordnung*.
+
Das Dialogfeld Rollenzuordnung wird geöffnet.

. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen
zu. Einer Gruppe können mehrere Rollen zugewiesen sein.
+
[CAUTION]
====
Achten Sie darauf, dass Sie Ihre Berechtigungen nicht entfernen, während
SAML aktiviert ist, oder Sie verlieren den Zugriff auf System Manager.

====
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Benutzerattribut
 a|
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-
Gruppe an.



 a|
Attributwert
 a|
Geben Sie den Attributwert für die zu zugeordnete Gruppe an.



 a|
Rollen
 a|
Klicken Sie in das Feld, und wählen Sie eine der Rollen des Speicherarrays
aus, die dem Attribut zugeordnet werden sollen. Sie müssen jede Rolle, die
```

```
Sie für diese Gruppe aufnehmen möchten, einzeln auswählen. Die Rolle
„Monitor“ ist erforderlich, wenn Sie sich mit den anderen Rollen bei
System Manager anmelden. Eine Sicherheitsadministratorrolle muss
mindestens einer Gruppe zugewiesen werden. Die zugeordneten Rollen
umfassen die folgenden Berechtigungen:

** *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes
und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management, Zertifikatverwaltung, Audit Log Management und die
Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder
auszuschalten.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem
Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-
Upgrades. Kein Zugriff auf Speicherobjekte oder die
Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


|===
====
+

NOTE: Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Der System Manager funktioniert ohne die
vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

. Klicken Sie optional auf *Weitere Zuordnungen hinzufügen*, um weitere
Gruppen-zu-Rolle-Zuordnungen einzugeben.
. Klicken Sie Auf *Speichern*.


.Ergebnisse
Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen
beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.



[[ID268744c0d61e852591eaee7280e15210]]
= Exportieren Sie SAML-Dienstanbieter-Dateien
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Bei Bedarf können die Metadaten von Service-Providern für das Storage-
Array exportiert und die Datei(en) in das IdP-System (Identity Provider)
importiert werden.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* SAML wurde konfiguriert und aktiviert.


.Über diese Aufgabe
In dieser Aufgabe exportieren Sie Metadaten aus den Controllern (eine
Datei für jeden Controller). Die IdP benötigt diese Metadaten, um eine
Vertrauensbeziehung zu den Controllern aufzubauen und
Authentifizierungsanforderungen zu verarbeiten. Die Datei enthält
Informationen wie den Domänennamen des Controllers oder die IP-Adresse,
die das IdP zum Senden von Anforderungen verwenden kann.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *SAML* aus.
. Wählen Sie *Export*.
+
Das Dialogfeld Dateien des Dienstanbieters exportieren wird geöffnet.

. Klicken Sie für jeden Controller auf *Exportieren*, um die
Metadatendatei auf Ihrem lokalen System zu speichern.
+
[NOTE]
====
Die Domain-Name-Felder für jeden Controller sind schreibgeschützt.

====
+
Notieren Sie sich, wo die Datei gespeichert ist.

. Suchen Sie im lokalen System die Metadatendatei(en) des
Serviceanbieters, die Sie exportiert haben.
+
Es gibt eine XML-formatierte Datei für jeden Controller.

. Importieren Sie vom IdP-Server die Metadatendatei(en) des
Dienstanbieters. Sie können die Dateien entweder direkt importieren oder
```

```
manuell die Controller-Informationen von ihnen eingeben.
. Klicken Sie Auf *Schließen*.




:leveloffset: -1


= Verwenden Sie Access Tokens

:leveloffset: +1


[[IDdb74e0f75f7d88f1330a56f53274a179]]
= Erstellen von Zugriffs-Tokens
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können ein Zugriffstoken erstellen, um sich anstelle eines
Benutzernamens und Passworts mit der REST-API oder der
Befehlszeilenschnittstelle (CLI) zu authentifizieren.


NOTE: Token haben keine Passwörter, daher müssen Sie sie sorgfältig
verwalten.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *Access Token* aus.
. Wählen Sie *Access Token Settings Anzeigen/Bearbeiten* Aus. Stellen Sie
im Dialogfeld sicher, dass das Kontrollkästchen *Access Token* aktivieren
aktiviert ist. Klicken Sie auf *Speichern*, um das Dialogfeld zu
schließen.
. Wählen Sie *Zugriffstoken Erstellen*.
. Wählen Sie im Dialogfeld die Dauer für das zu gültige Token aus.
+

NOTE: Nach Ablauf des Tokens werden die Authentifizierungsversuche des
Benutzers fehlschlagen.

. Klicken Sie Auf *Erstellen.*
```

```
. Wählen Sie im Dialogfeld eine der folgenden Optionen aus:
+
** *Kopieren* um den Token-Text in die Zwischenablage zu speichern.
** *Download* um den Token-Text in einer Datei zu speichern.
+

NOTE: Speichern Sie den Token-Text unbedingt. Dies ist Ihre einzige
Möglichkeit, den Text anzuzeigen, bevor Sie den Dialog schließen.



. Klicken Sie Auf *Schließen*.
. Verwenden Sie das Token wie folgt:
+
** *Rest API*: Um ein Token in einer REST-API-Anforderung zu verwenden,
fügen Sie einen HTTP-Header zu Ihren Anforderungen hinzu. Beispiel:
`Authorization: Bearer _<access-token-value>_`
** *Secure CLI*: Um ein Token in der CLI zu verwenden, fügen Sie den
Token-Wert in die Befehlszeile ein oder verwenden Sie den Pfad zu einer
Datei, die den Token-Wert enthält. Beispiel:
+
*** Token-Wert in der Befehlszeile: `-t _access-token-value_`
*** Pfad zu einer Datei mit dem Token-Wert: `-T _access-token-file_`
+

NOTE: Die CLI fordert den Benutzer auf, in der Befehlszeile einen Access-
Token-Wert anzugeben, wenn kein Benutzername, kein Passwort oder Token
angegeben wird.









[[ID91a40d71f1941e238684833e572962dc]]
= Bearbeiten Sie die Einstellungen für das Zugriffstoken
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

```
Sie können Einstellungen für Access Token bearbeiten, die die Ablaufzeit
und die Fähigkeit zum Erstellen neuer Token umfassen.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *Access Token* aus.
. Wählen Sie *Access Token Settings Anzeigen/Bearbeiten* Aus.
. Im Dialogfeld können Sie eine oder beide Aufgaben ausführen:
+
** Aktivieren oder Deaktivieren der Token-Erstellung
** Ändern Sie den Ablauf der vorhandenen Token.
+

NOTE: Wenn Sie die Einstellung *Access Token* aktivieren dewählen, wird
sowohl die Token-Erstellung als auch die Token-Authentifizierung
verhindert. Wenn Sie diese Einstellung später wieder aktivieren, können
nicht abgelaufene Token erneut verwendet werden. Wenn Sie alle vorhandenen
Token dauerhaft widerrufen möchten, lesen Sie xref:{relative_path}access-
management-tokens-revoke.html["Access Token widerrufen"].



. Klicken Sie Auf *Speichern*.




[[IDdc04ca1a8839c2198f15caa9716d5e62]]
= Access Token widerrufen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können alle Zugriffstoken aufheben, wenn Sie feststellen, dass ein
Token kompromittiert wurde oder wenn Sie eine manuelle Schlüsselrotation
für die kryptografischen Schlüssel durchführen möchten, die zum Signieren
und Validieren der Access Tokens verwendet werden.

Mit diesem Vorgang werden die zum Signieren der Token verwendeten
Schlüssel neu generiert. Sobald die Schlüssel zurückgesetzt wurden, werden
_all_ emittierte Token sofort ungültig. Da das Speicherarray keine Token
verfolgt, können einzelne Token nicht entzogen werden.
```

```
.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *Access Token* aus.
. Wählen Sie *Alle Zugriffstoken Aufheben*.
. Klicken Sie im Dialogfeld auf *Ja*.


Nachdem Sie alle Token entsorgt haben, können Sie neue Token erstellen und
diese sofort verwenden.



:leveloffset: -1


= Syslog managen

:leveloffset: +1


[[ID38cbcfedc1bfc9dada92dbd303f10ae3]]
= Zeigen Sie die Aktivität des Prüfprotokolls an
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Durch die Anzeige von Prüfprotokollen können Benutzer mit
Sicherheitsadministratorberechtigungen Benutzeraktionen,
Authentifizierungsfehler, ungültige Anmeldeversuche und die Lebensdauer
der Benutzersitzung überwachen.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte **Überwachungsprotokoll** aus.
+
Die Aktivität des Überwachungsprotokolls wird im Tabellenformat angezeigt,
das die folgenden Informationspalten enthält:
```

```
+
** *Datum/Uhrzeit* -- Zeitstempel, wann das Speicherarray das Ereignis
erkannt hat (in GMT).
** *Benutzername* -- der Benutzername, der dem Ereignis zugeordnet ist.
Bei nicht authentifizierten Aktionen im Speicher-Array wird „N/A“ als
Benutzername angezeigt. Nicht authentifizierte Aktionen können vom
internen Proxy oder einem anderen Mechanismus ausgelöst werden.
** *Statuscode* -- HTTP-Statuscode der Operation (200, 400 usw.) und
beschreibenden Text, der dem Ereignis zugeordnet ist.
** *URL abgerufen* -- vollständige URL (einschließlich Host) und
Abfragezeichenfolge.
** *Client-IP-Adresse* -- IP-Adresse des Clients, der dem Ereignis
zugeordnet ist.
** *Quelle* -- Logging-Quelle, die mit dem Ereignis verknüpft ist, kann
System Manager, CLI, Web Services oder Support Shell sein.
** *Beschreibung* -- zusätzliche Informationen über die Veranstaltung,
falls zutreffend.


. Verwenden Sie die Auswahl auf der Seite „Überwachungsprotokoll“, um
Ereignisse anzuzeigen und zu verwalten.
+
.Auswahldetails
[%collapsible]
====
[cols="25h,~"]
|===
| Auswahl | Beschreibung


 a|
Zeigt Ereignisse aus dem...
 a|
Grenzwerte für Ereignisse, die nach Datumsbereich angezeigt werden (letzte
24 Stunden, letzte 7 Tage, letzte 30 Tage oder ein benutzerdefinierter
Datumsbereich).



 a|
Filtern
 a|
Begrenzungsereignisse, die durch die in das Feld eingegebenen Zeichen
angezeigt werden. Verwenden Sie Anführungszeichen (") für eine genaue
Wortabgleiche, geben Sie ein `OR` Um ein oder mehrere Wörter
zurückzugeben, oder geben Sie einen Strich ( -- ) ein, um Wörter
```

```
auszulassen.



 a|
Aktualisierung
 a|
Wählen Sie *Aktualisieren*, um die Seite auf die aktuellen Ereignisse zu
aktualisieren.



 a|
Einstellungen Anzeigen/Bearbeiten
 a|
Wählen Sie *Einstellungen anzeigen/bearbeiten* aus, um ein Dialogfeld zu
öffnen, in dem Sie eine vollständige Protokollrichtlinie und eine Ebene
der zu protokollierenden Aktionen festlegen können.



 a|
Löschen von Ereignissen
 a|
Wählen Sie *Löschen* aus, um ein Dialogfeld zu öffnen, in dem Sie alte
Ereignisse von der Seite entfernen können.



 a|
Spalten ein-/ausblenden
 a|
Klicken Sie auf das Spaltensymbol *ein/Ausblenden*image:../media/sam-1140-
ss-access-columns.gif["Spalte ein-/ausblenden"], um zusätzliche Spalten
für die Anzeige in der Tabelle auszuwählen. Weitere Spalten sind:

** *Methode* -- die HTTP-Methode (z. B. POST, GET, DELETE usw.).
** *CLI Befehl ausgeführt* -- der CLI-Befehl (Grammatik) ausgeführt für
Secure CLI Anfragen.
** *CLI Rückgabestatus* -- Ein CLI-Statuscode oder eine Anforderung für
Eingabedateien vom Client.
** *Symbol-Verfahren* -- das Symbol-Verfahren ausgeführt.
** *SSH Event Type* -- Secure Shell (SSH) Ereignistyp, wie Login, Logout
und Login_fail.
** *SSH Session PID* -- Prozess-ID-Nummer der SSH-Sitzung.
** *SSH Sitzungsdauer(en)* -- die Anzahl der Sekunden, die der Benutzer
angemeldet war.
```

```
** *Authentifizierungstyp* -- Typen können lokalen Benutzer, LDAP, SAML
und Access Token enthalten.
** *Authentifizierungs-ID* -- ID der authentifizierten Sitzung.




 a|
Spaltenfilter ein- oder ausschalten
 a|
Klicken Sie auf das Symbol *Umschalten*image:../media/sam-1140-ss-access-
toggle.gif["Umschalten"], um Filterfelder für jede Spalte zu öffnen. Geben
Sie in ein Spaltenfeld Zeichen ein, um die durch diese Zeichen angezeigten
Ereignisse einzuschränken. Klicken Sie erneut auf das Symbol, um die
Filterfelder zu schließen.



 a|
Änderungen rückgängig machen
 a|
Klicken Sie auf das Symbol *Rückgängig*image:../media/sam-1140-ss-access-
undo.gif["Rückgängig Machen"], um die Tabelle auf die
Standardkonfiguration zurückzusenden.



 a|
Exportieren
 a|
Klicken Sie auf *Exportieren*, um die Tabellendaten in einer
kommagetrennten Datei (CSV) zu speichern.

|===
====




[[IDc50b73e81240316a438ae65b9cbb0c3a]]
= Richtlinien für Prüfprotokolle definieren
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Sie können die Überschreibungsrichtlinie und die im Audit-Protokoll
aufgezeichneten Ereignistypen ändern.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.

.Über diese Aufgabe
Dieser Task beschreibt, wie die Einstellungen für das
Überwachungsprotokoll geändert werden, einschließlich der Richtlinie zum
Überschreiben alter Ereignisse und der Richtlinie für die Aufzeichnung von
Ereignistypen.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *Prüfprotokoll* aus.
. Wählen Sie *Einstellungen Anzeigen/Bearbeiten*.
+
Das Dialogfeld Einstellungen für das Überwachungsprotokoll wird geöffnet.

. Ändern Sie die Überschreibungsrichtlinie oder die Arten der
aufgezeichneten Ereignisse.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
Überschreibungsrichtlinie
 a|
Legt die Richtlinie zum Überschreiben alter Ereignisse fest, wenn die
maximale Kapazität erreicht ist:

** *Die ältesten Ereignisse im Audit-Protokoll können überschrieben
werden, wenn das Audit-Protokoll voll ist* -- überschreibt die alten
Ereignisse, wenn das Audit-Protokoll 50,000 Datensätze erreicht.
** *Das manuelle Löschen von Audit-Protokollereignissen ist erforderlich*
-- gibt an, dass Ereignisse nicht automatisch gelöscht werden; stattdessen
erscheint eine Schwellenwertwarnung im festgelegten Prozentsatz.
```

```
Ereignisse müssen manuell gelöscht werden.
+

NOTE: Wenn die Überschreibungsrichtlinie deaktiviert ist und die Einträge
des Prüfprotokolls die maximale Grenze erreichen, wird Benutzern der
Zugriff auf System Manager ohne die Berechtigung des
Sicherheitsadministrators verweigert. Um den Systemzugriff für Benutzer
ohne Sicherheitsadministrator-Berechtigungen wiederherzustellen, muss ein
Benutzer, der der Rolle Sicherheitsadministrator zugewiesen ist, die alten
Ereignisdatensätze löschen.

+

NOTE: Überschreibungsrichtlinien gelten nicht, wenn ein Syslog-Server für
die Archivierung von Audit-Protokollen konfiguriert ist.




 a|
Level der zu protokollierenden Aktionen
 a|
Legt die Arten von zu protokollierenden Ereignissen fest:

** *Änderungsereignisse aufzeichnen* -- zeigt nur Ereignisse an, bei denen
eine Benutzeraktion eine Systemänderung beinhaltet.
** *Alle Änderungen und schreibgeschützten Ereignisse* -- zeigt alle
Ereignisse an, einschließlich einer Benutzeraktion, die das Lesen oder
Herunterladen von Informationen beinhaltet.


|===
====
. Klicken Sie Auf *Speichern*.




[[ID4f8ed31430f801ebe35a3fbf250beb24]]
= Löschen von Ereignissen aus dem Auditprotokoll
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Sie können das Audit-Protokoll von alten Ereignissen löschen, wodurch das
Suchen durch Ereignisse leichter zu verwalten ist. Sie haben die
Möglichkeit, alte Ereignisse beim Löschen in einer CSV-Datei
(kommagetrennte Werte) zu speichern.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *Prüfprotokoll* aus.
. Wählen Sie *Löschen*.
+
Das Dialogfeld Prüfprotokoll löschen wird geöffnet.

. Wählen Sie oder geben Sie die Anzahl der ältesten Ereignisse ein, die
Sie löschen möchten.
. Wenn Sie die gelöschten Ereignisse in eine CSV-Datei exportieren möchten
(empfohlen), lassen Sie das Kontrollkästchen aktiviert. Sie werden
aufgefordert, einen Dateinamen und Speicherort einzugeben, wenn Sie im
nächsten Schritt auf *Löschen* klicken. Wenn Sie keine Ereignisse in einer
CSV-Datei speichern möchten, aktivieren Sie das Kontrollkästchen, um die
Auswahl aufzuheben.
. Klicken Sie Auf *Löschen*.
+
Ein Bestätigungsdialogfeld wird geöffnet.

. Typ `delete` Klicken Sie im Feld auf *Löschen*.
+
Die ältesten Ereignisse werden von der Seite „Überwachungsprotokoll“
entfernt.




[[ID460398bb9a14571548fa10b9d8337c6c]]
= Syslog-Server für Audit-Protokolle konfigurieren
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
```

```
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie Auditprotokolle auf einem externen Syslog-Server archivieren
möchten, können Sie die Kommunikation zwischen diesem Server und dem
Speicher-Array konfigurieren. Nach der Verbindungsherstellung werden
Audit-Protokolle automatisch auf dem Syslog-Server gespeichert.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* Die Syslog-Serveradresse, das Protokoll und die Portnummer müssen
verfügbar sein. Bei der Serveradresse kann es sich um einen vollständig
qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse
handeln.
* Wenn Ihr Server ein sicheres Protokoll verwendet (z. B. TLS), muss auf
Ihrem lokalen System ein Zertifikat für Zertifizierungsstellen (CA)
verfügbar sein. CA-Zertifikate identifizieren Website-Eigentümer für
sichere Verbindungen zwischen Servern und Clients.


.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie auf der Registerkarte Audit Log die Option *Configure Syslog
Servers* aus.
+
Das Dialogfeld Configure Syslog Servers wird geöffnet.

. Klicken Sie Auf *Hinzufügen*.
+
Das Dialogfeld Syslog Server hinzufügen wird geöffnet.

. Geben Sie Informationen für den Server ein, und klicken Sie dann auf
*Hinzufügen*.
+
** *Server-Adresse* -- Geben Sie einen vollständig qualifizierten
Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
** *Protokoll* -- Wählen Sie aus der Dropdown-Liste ein Protokoll aus (z.
B. TLS, UDP oder TCP).
** *Zertifikat hochladen (optional)* -- Wenn Sie das TLS-Protokoll
ausgewählt haben und noch kein signiertes CA-Zertifikat hochgeladen haben,
klicken Sie auf *Durchsuchen*, um eine Zertifikatdatei hochzuladen. Audit-
Protokolle werden nicht ohne vertrauenswürdiges Zertifikat auf einem
Syslog-Server archiviert.
```

```
+
[NOTE]
====
Wenn das Zertifikat später ungültig wird, schlägt der TLS-Handshake fehl.
Als Ergebnis wird eine Fehlermeldung in das Auditprotokoll geschrieben und
Meldungen werden nicht mehr an den Syslog-Server gesendet. Um dieses
Problem zu lösen, müssen Sie das Zertifikat auf dem Syslog-Server beheben
und dann zum Menü:Einstellungen[Audit-Protokoll > Syslog-Server
konfigurieren > Alle testen] wechseln.

====
** *Port* -- Geben Sie die Portnummer für den Syslog-Empfänger ein.
Nachdem Sie auf *Hinzufügen* geklickt haben, wird das Dialogfeld Configure
Syslog Servers geöffnet und der konfigurierte Syslog Server auf der Seite
angezeigt.


. Um die Serververbindung mit dem Speicher-Array zu testen, wählen Sie
*Alle testen*.


.Ergebnisse
Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-
Server gesendet. Frühere Protokolle werden nicht übertragen. Weitere
Informationen zur Konfiguration von Syslog-Einstellungen für Warnmeldungen
finden Sie unter https://docs.netapp.com/us-en/e-series-santricity/sm-
settings/configure-syslog-server-for-alerts.html["Konfigurieren Sie den
Syslog-Server für Warnmeldungen"].

 NOTE: If multiple syslog servers are configured, all configured syslog
servers will receive an audit log.



[[ID64f4450d1c1a4c5c7f0a343af4de0ff3]]
= Bearbeiten Sie die Syslog-Servereinstellungen für Audit-
Protokolldatensätze
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die Einstellungen für den Syslog-Server ändern, der für die
Archivierung von Audit-Protokollen verwendet wird, und auch ein neues
```

Zertifikat für die Zertifizierungsstelle (Certificate Authority, CA) für den Server hochladen.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
* Die Syslog-Serveradresse, das Protokoll und die Portnummer müssen verfügbar sein. Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
* Wenn Sie ein neues CA-Zertifikat hochladen, muss das Zertifikat auf Ihrem lokalen System verfügbar sein.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie auf der Registerkarte Audit Log die Option *Configure Syslog Servers* aus.
+
Konfigurierte Syslog-Server werden auf der Seite angezeigt.

. Um die Serverinformationen zu bearbeiten, wählen Sie rechts neben dem Servernamen das Symbol *Bearbeiten* (Bleistift) aus und nehmen Sie die gewünschten Änderungen in den folgenden Feldern vor:
+
** *Server-Adresse* -- Geben Sie einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
** *Protokoll* -- Wählen Sie aus der Dropdown-Liste ein Protokoll aus (z. B. TLS, UDP oder TCP).
** *Port* -- Geben Sie die Portnummer für den Syslog-Empfänger ein.

. Wenn Sie das Protokoll in das sichere TLS-Protokoll (entweder von UDP oder TCP) geändert haben, klicken Sie auf *Vertrautes Zertifikat importieren*, um ein CA-Zertifikat hochzuladen.
. Um die neue Verbindung mit dem Speicher-Array zu testen, wählen Sie *Alle testen*.

.Ergebnisse
Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-Server gesendet. Frühere Protokolle werden nicht übertragen.

:leveloffset: -1

```
= FAQs

:leveloffset: +1


[[IDe1823dca246f3cb948002f4ced4dc244]]
= Warum kann ich mich nicht anmelden?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn bei der Anmeldung bei SANtricity System Manager ein Fehler angezeigt
wird, prüfen Sie die folgenden möglichen Ursachen.

Fehler beim Anmelden bei System Manager können aus einem der folgenden
Gründe auftreten:

* Sie haben einen falschen Benutzernamen oder ein falsches Passwort
eingegeben.
* Sie verfügen über unzureichende Berechtigungen.
* Der Verzeichnisserver (falls konfiguriert) ist möglicherweise nicht
verfügbar. Wenn dies der Fall ist, melden Sie sich mit einer lokalen
Benutzerrolle an.
* Sie haben mehrmals versucht, sich erfolglos anzumelden, was den
Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, bis Sie sich erneut
anmelden können.
* Eine Sperrbedingung wurde ausgelöst und Ihr Prüfprotokoll ist
möglicherweise voll. Wechseln Sie zu Zugriffsmanagement und löschen Sie
alte Ereignisse aus dem Revisionsprotokoll.
* SAML-Authentifizierung ist aktiviert. Aktualisieren Sie Ihren Browser,
um sich anzumelden.


Aus einem der folgenden Gründe können Anmeldefehler bei einem Remote-
Speicher-Array auftreten:

* Sie haben ein falsches Kennwort eingegeben.
* Sie haben mehrmals versucht, sich erfolglos anzumelden, was den
Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, um sich erneut
anzumelden.
* Die maximale Anzahl an Client-Verbindungen, die auf dem Controller
verwendet werden, wurde erreicht. Suchen Sie nach mehreren Benutzern oder
```

```
Clients.




[[ID6bac31b66cb7b503194535a30dc34546]]
= Was muss ich vor dem Hinzufügen eines Verzeichnisservers wissen?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Stellen Sie vor dem Hinzufügen eines Verzeichnisservers in der
Zugriffsverwaltung sicher, dass Sie die folgenden Anforderungen erfüllen.

* Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
* LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich
Domänenname, Server-URL und optional Benutzername und Kennwort für das
Bindekonto.
* Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette
des LDAP-Servers auf Ihrem lokalen Computer installiert sein.




[[ID7d88df0222e7522ab89333d12784d54a]]
= Was muss ich über die Zuordnung von Speicher-Array-Rollen wissen?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Bevor Sie Gruppen zu Rollen zuordnen, lesen Sie die folgenden Richtlinien
durch.

Die integrierten RBAC-Funktionen (rollenbasierte Zugriffssteuerung) des
Storage-Arrays umfassen folgende Rollen:

* *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes
und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
* *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management, Zertifikatverwaltung, Audit Log Management und die
Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder
```

```
auszuschalten.
* *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem
Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-
Upgrades. Kein Zugriff auf Speicherobjekte oder die
Sicherheitskonfiguration.
* *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.




== Verzeichnisdienste

Wenn Sie einen LDAP-Server (Lightweight Directory Access Protocol) und
Verzeichnisdienste verwenden, stellen Sie sicher, dass:

* Ein Administrator hat im Verzeichnisdienst Benutzergruppen definiert.
* Sie kennen die Gruppen-Domain-Namen für die LDAP-Benutzergruppen.
Reguläre Ausdrücke werden unterstützt. Diese speziellen regulären
Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich entgangen
werden (`\`) Wenn sie nicht Teil eines regulären Ausdrucksmusters sind:
+
[listing]
----
\.[]{}()<>*+-=!?^$|
----
* Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Der System Manager funktioniert ohne die
vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.




== SAML

Wenn Sie die im Speicher-Array integrierten SAML-Funktionen (Security
Assertion Markup Language) verwenden, stellen Sie sicher, dass:

* Ein IdP-Administrator (Identity Provider) hat im IdP-System
Benutzerattribute und Gruppenmitgliedschaften konfiguriert.
* Sie kennen die Namen der Gruppenmitgliedschaft.
* Sie kennen den Attributwert für die zu zugeordnete Gruppe. Reguläre
Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen
müssen mit einem umgekehrten Schrägstrich entgangen werden (`\`) Wenn sie
nicht Teil eines regulären Ausdrucksmusters sind:
+
[listing]
```

```
----
\.[]{}()<>*+-=!?^$|
----
* Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Der System Manager funktioniert ohne die
vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.




[[ID6be62eaf39ab64327e90033e97ac46f4]]
= Welche externen Verwaltungstools können von dieser Änderung betroffen
sein?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie bestimmte Änderungen in SANtricity System Manager vornehmen, wie
z. B. das Wechseln der Managementoberfläche oder die Verwendung von SAML
für eine Authentifizierungsmethode, sind die Verwendung einiger externer
Tools und Funktionen möglicherweise eingeschränkt.



== Managementoberfläche

Tools, die direkt mit der älteren Managementoberfläche (Symbol), z. B.
SANtricity SMI-S Provider oder OnCommand Insight (OCI), kommunizieren,
funktionieren nur, wenn die Einstellung für die ältere
Managementoberfläche aktiviert ist. Darüber hinaus können Sie keine alten
CLI-Befehle verwenden oder Spiegelungsvorgänge durchführen, wenn diese
Einstellung deaktiviert ist.

Weitere Informationen erhalten Sie vom technischen Support.



== SAML-Authentifizierung

Wenn SAML aktiviert ist, können die folgenden Clients nicht auf Storage-
Array-Services und -Ressourcen zugreifen:

* Enterprise Management-Fenster (EMW)
* Befehlszeilenschnittstelle (CLI)
```

```
* Software Developer Kits (SDK)-Clients
* In-Band-Clients
* REST-API-Clients für die HTTP-Standardauthentifizierung
* Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an


Weitere Informationen erhalten Sie vom technischen Support.



[[ID4050d32214aa0579ca69ba3601fd9393]]
= Was muss ich vor der Konfiguration und Aktivierung von SAML wissen?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Bevor Sie die SAML-Funktionen (Security Assertion Markup Language) für die
Authentifizierung konfigurieren und aktivieren, müssen Sie sicherstellen,
dass Sie die folgenden Anforderungen erfüllen und SAML-Einschränkungen
verstehen.



== Anforderungen

Bevor Sie beginnen, stellen Sie sicher, dass:

* Ein Identitäts-Provider (IdP) ist in Ihrem Netzwerk konfiguriert. Ein
IdP ist ein externes System, mit dem Anmeldeinformationen von einem
Benutzer angefordert werden und festgestellt wird, ob der Benutzer
erfolgreich authentifiziert wurde. Ihr Sicherheitsteam ist für die
Instandhaltung des IdP verantwortlich.
* Ein IdP-Administrator hat Benutzerattribute und Gruppen im IdP-System
konfiguriert.
* Ein IdP-Administrator hat sichergestellt, dass der IdP die Möglichkeit
unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.
* Ein Administrator hat sichergestellt, dass die IdP-Server- und
-Controller-Uhren synchronisiert werden (entweder über einen NTP-Server
oder durch Anpassen der Controller-Uhreinstellungen).
* Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf
dem lokalen System verfügbar, das für den Zugriff auf System Manager
verwendet wird.
* Sie kennen die IP-Adresse oder den Domain-Namen der einzelnen Controller
im Storage-Array.
```

```
== Einschränkungen

Zusätzlich zu den oben genannten Anforderungen sollten Sie sich mit den
folgenden Einschränkungen vertraut machen:

* Sobald SAML aktiviert ist, können Sie sie über die Benutzeroberfläche
nicht deaktivieren oder die IdP-Einstellungen bearbeiten. Wenn Sie die
SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an
den technischen Support, um Hilfe zu erhalten. Es wird empfohlen, die SSO-
Anmeldungen zu testen, bevor Sie SAML im letzten Konfigurationsschritt
aktivieren. (Das System führt auch einen SSO-Anmeldetest vor Aktivierung
von SAML durch.)
* Wenn Sie SAML zukünftig deaktivieren, stellt das System automatisch die
vorherige Konfiguration wieder her (lokale Benutzerrollen und/oder
Verzeichnisdienste).
* Wenn Verzeichnisdienste derzeit für die Benutzerauthentifizierung
konfiguriert sind, überschreibt SAML diese Konfiguration.
* Wenn SAML konfiguriert ist, können die folgenden Clients nicht auf
Speicher-Array-Ressourcen zugreifen:
+
** Enterprise Management-Fenster (EMW)
** Befehlszeilenschnittstelle (CLI)
** Software Developer Kits (SDK)-Clients
** In-Band-Clients
** REST-API-Clients für die HTTP-Standardauthentifizierung
** Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an




[[IDc80d528b6951ac00da0e3185dccb4da1]]
= Welche Arten von Ereignissen werden im Auditprotokoll aufgezeichnet?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Das Revisionsprotokoll kann Änderungsereignisse oder sowohl Änderungs- als
auch schreibgeschützte Ereignisse aufzeichnen.
```

Abhängig von den Richtlinieneinstellungen werden die folgenden Ereignistypen angezeigt:

* *Änderungsereignisse* -- Benutzeraktionen aus System Manager heraus, die Änderungen am System, z. B. die Bereitstellung von Speicher, mit sich bringen.
* *Modifizierung und schreibgeschützte Ereignisse* -- Benutzeraktionen, die Änderungen am System beinhalten, sowie Ereignisse, die Informationen anzeigen oder herunterladen, wie zum Beispiel die Anzeige von Volume-Zuweisungen.

[[ID0029c56ea34db4eae88ff31fc9fedb2c]]
= Was muss ich vor der Konfiguration eines Syslog-Servers wissen?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können Audit-Protokolle auf einem externen Syslog-Server archivieren.

Beachten Sie vor der Konfiguration eines Syslog-Servers die folgenden Richtlinien.

* Stellen Sie sicher, dass Sie die Serveradresse, das Protokoll und die Portnummer kennen. Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
* Wenn Ihr Server ein sicheres Protokoll verwendet (z. B. TLS), muss auf Ihrem lokalen System ein Zertifikat für Zertifizierungsstellen (CA) verfügbar sein. CA-Zertifikate identifizieren Website-Eigentümer für sichere Verbindungen zwischen Servern und Clients.
* Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-Server gesendet. Frühere Protokolle werden nicht übertragen.
* Die Einstellungen der Überschreibrichtlinie (verfügbar unter *Ansicht/Einstellungen bearbeiten*) haben keinen Einfluss auf das Management von Protokollen mit einer Syslog-Serverkonfiguration.
* Auditprotokolle folgen dem Nachrichtenformat RFC 5424.

```
[[ID3743f9cad1777d9711fcbd0bb6110f20]]
= Der Syslog-Server empfängt keine Audit-Protokolle mehr. Was mache ich?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie einen Syslog-Server mit einem TLS-Protokoll konfiguriert haben,
kann der Server keine Meldungen empfangen, wenn das Zertifikat aus
irgendeinem Grund ungültig wird. Eine Fehlermeldung über das ungültige
Zertifikat wird im Auditprotokoll veröffentlicht.

Um dieses Problem zu lösen, müssen Sie zuerst das Zertifikat für den
Syslog-Server reparieren. Wenn eine gültige Zertifikatskette vorhanden
ist, gehen Sie zu Menü:Einstellungen[Audit Log > Syslog-Server
konfigurieren > Alle testen].



:leveloffset: -1


:leveloffset: -1


= Zertifikate

:leveloffset: +1


[[ID22c2292d8bf8925d5a5fe6110a8a6e87]]
= Zertifikatübersicht
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können SANtricity System Manager verwenden, um
Zertifikatsignierungsanforderungen (CSRs) zu erstellen, Zertifikate zu
importieren und vorhandene Zertifikate zu verwalten.
```

== Was sind Zertifikate?

Zertifikate sind digitale Dateien, die Online-Einheiten wie Websites und Server für eine sichere Kommunikation im Internet identifizieren. Es gibt zwei Arten von Zertifikaten: Ein _signiertes Zertifikat_ wird von einer Zertifizierungsstelle (CA) validiert und ein _selbst-signiertes Zertifikat_ wird vom Eigentümer des Unternehmens anstelle eines Dritten validiert.

Weitere Informationen:

* xref:{relative_path}how-certificates-work-sam.html["Funktionsweise von Zertifikaten"]
* xref:{relative_path}certificate-terminology.html["Terminologie des Zertifikats"]

== Wie konfiguriere ich signierte Zertifikate?

Sie können eine Signaturanforderung von System Manager oder extern mit einem privaten und öffentlichen Schlüsselpaar generieren. Die Signaturanforderung wird an eine Zertifizierungsstelle gesendet, um die Zertifikatdateien zu generieren. Sobald die Zertifizierungsstelle die Zertifikatdateien zurückgibt, importieren Sie diese mit System Manager.

Weitere Informationen:

* xref:{relative_path}use-ca-signed-certificates-for-controllers.html["Verwenden Sie CA-signierte Zertifikate für Controller"]
* xref:{relative_path}use-ca-signed-certificates-for-authentication-with-a-key-management-server.html["Verwenden Sie CA-signierte Zertifikate zur Authentifizierung mit einem Schlüsselverwaltungsserver"]

== Verwandte Informationen

Weitere Informationen zu Zertifikataufgaben:

* xref:{relative_path}view-imported-certificates.html["Anzeigen importierter Zertifikatinformationen"]
* xref:{relative_path}enable-certificate-revocation-checking.html["Überprüfung des Zertifikatsannuls aktivieren"]

```
= Konzepte

:leveloffset: +1


[[ID4218b988a2d72ee120f71ec44215a615]]
= Funktionsweise von Zertifikaten
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Zertifikate sind digitale Dateien, die Online-Einheiten wie Websites und
Server für eine sichere Kommunikation im Internet identifizieren.

Zertifikate stellen sicher, dass die Webkommunikation in verschlüsselter
Form, privat und unverändert, nur zwischen dem angegebenen Server und dem
angegebenen Client übertragen wird. Mit System Manager können Sie
Zertifikate zwischen dem Browser auf einem Host-Managementsystem (als
Client fungieren) und den Controllern in einem Storage-System (als Server
fungieren) verwalten.

Ein Zertifikat kann von einer vertrauenswürdigen Behörde signiert werden,
oder es kann selbst signiert werden. „Unterzeichnen“ bedeutet einfach,
dass jemand die Identität des Eigentümers validiert 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.

[NOTE]
====
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. Ein selbst signiertes Zertifikat verwendet jedoch nicht die
gleiche Vertrauenskette wie ein CA-signiertes Zertifikat.

Selbstsignierte Zertifikate werden von Browsern nicht „`Trusted`“. 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.



== Zertifikate, die für den Schlüsselverwaltungsserver verwendet werden

Wenn Sie einen externen Schlüsselverwaltungsserver mit der
Laufwerkssicherheitsfunktion verwenden, können Sie auch Zertifikate zur
Authentifizierung zwischen diesem Server und den Controllern verwalten.



[[IDbf342fe88c1c956db75aaa1edafd5edd]]
= Terminologie des Zertifikats
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die folgenden Begriffe gelten für das Zertifikatmanagement.

[cols="25h,~"]
|===
| Laufzeit | Beschreibung


 a|
CA
```

a|
Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer, die sichere Verbindungen zwischen Clients und Servern ermöglichen.

a|
CSR
a|
Eine Zertifikatsignierungsanforderung (CSR) ist eine Nachricht, die von einem Antragsteller an eine Zertifizierungsstelle (CA) gesendet wird. Der CSR überprüft die Informationen, die die Zertifizierungsstelle zum ausstellen eines Zertifikats benötigt.

a|
Zertifikat
a|
Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).

a|
Zertifikatskette
a|
Eine Dateihierarchie, die den Zertifikaten eine Sicherheitsschicht hinzufügt. In der Regel umfasst die Kette ein Stammzertifikat oben in der Hierarchie, ein oder mehrere Zwischenzertifikate und die Serverzertifikate, die die Entitäten identifizieren.

a|
Client-Zertifikat
a|
Für das Management von Sicherheitsschlüssel validiert ein Client-Zertifikat die Controller des Speicherarrays, damit der Schlüsselverwaltungsserver ihre IP-Adressen anvertrauen kann.

```
 a|
Zwischenzertifikat
 a|
Ein oder mehrere Zwischenzertifikate verzweigen von der Root in der
Zertifikatkette. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die
als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten
fungieren sollen.



 a|
Zertifikat für Schlüsselmanagement-Server
 a|
Für das Sicherheitsschlüsselmanagement validiert ein Zertifikat für den
Schlüsselmanagement-Server den Server, damit das Storage-Array seiner IP-
Adresse vertrauen kann.



 a|
Schlüsselspeicher
 a|
Ein Schlüsselspeicher ist ein Repository auf Ihrem Host-Managementsystem,
das private Schlüssel enthält, zusammen mit ihren entsprechenden
öffentlichen Schlüsseln und Zertifikaten. Diese Schlüssel und Zertifikate
identifizieren Ihre eigenen Einheiten, z. B. die Controller.



 a|
OCSP-Server
 a|
Der OCSP-Server (Online Certificate Status Protocol) ermittelt, ob die
Zertifizierungsstelle vor ihrem geplanten Ablaufdatum Zertifikate
widerrufen hat und blockiert dann den Zugriff des Benutzers auf einen
Server, wenn das Zertifikat widerrufen wird.



 a|
Stammzertifikat
 a|
Das Stammzertifikat befindet sich oben in der Hierarchie in der
Zertifikatskette und enthält einen privaten Schlüssel, 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.



 a|
Signiertes Zertifikat
 a|
Ein Zertifikat, das von einer Zertifizierungsstelle (CA) validiert wird.
Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass
Daten verschlüsselt zwischen einem Server und einem Client über eine
HTTPS-Verbindung gesendet werden. Darüber hinaus enthält ein signiertes
Zertifikat Details über den Eigentümer des Unternehmens (in der Regel ein
Server oder eine Website) und eine digitale Signatur bestehend aus
Buchstaben und Zahlen. Ein signiertes Zertifikat nutzt eine
Vertrauenskette und wird daher am häufigsten in Produktionsumgebungen
verwendet. Auch als „CA-signiertes Zertifikat“ oder als
„Managementzertifikat“ bezeichnet.



 a|
Selbstsigniertes Zertifikat
 a|
Ein selbstsigniertes Zertifikat wird vom Eigentümer des Unternehmens
validiert. Diese Datendatei enthält einen privaten Schlüssel und stellt
sicher, dass Daten verschlüsselt zwischen einem Server und einem Client
über eine HTTPS-Verbindung gesendet werden. Es enthält auch eine digitale
Signatur, die aus Buchstaben und Zahlen besteht. Ein selbstsigniertes
Zertifikat verwendet nicht dieselbe Vertrauenskette wie ein CA-signiertes
Zertifikat und wird daher am häufigsten in Testumgebungen eingesetzt. Auch
als vorinstalliertes Zertifikat bezeichnet.



 a|
Serverzertifikat
 a|
Das Server-Zertifikat befindet sich unten in der Zertifikatskette. Es
identifiziert Ihre spezifische Einheit, z. B. eine Website oder ein
anderes Gerät. Jeder Controller in einem Storage-System benötigt ein
separates Serverzertifikat.

|===



:leveloffset: -1
```

```
= Zertifikate verwenden

:leveloffset: +1


[[ID2a046962823537d1d6758a8618ec3215]]
= Verwenden Sie CA-signierte Zertifikate für Controller
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können von einer Zertifizierungsstelle signierte Zertifikate für die
sichere Kommunikation zwischen den Controllern und dem für den Zugriff auf
SANtricity System Manager verwendeten Browser erhalten.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.
* Sie müssen die IP-Adresse oder DNS-Namen jedes Controllers kennen.


.Über diese Aufgabe
Die Verwendung von CA-signierten Zertifikaten ist ein dreistufiges
Verfahren.



== Schritt 1: Schließen Sie CSRs für die Controller ab

Sie müssen zuerst eine CSR-Datei (Certificate Signing Request) für jeden
Controller im Speicher-Array generieren.

.Über diese Aufgabe
In dieser Aufgabe wird beschrieben, wie eine CSR-Datei aus System Manager
generiert wird. Der CSR stellt Informationen über Ihr Unternehmen und
entweder die IP-Adresse oder den DNS-Namen des Controllers zur Verfügung.
Während dieser Aufgabe wird eine CSR-Datei erzeugt, wenn das Speicher-
Array einen Controller und zwei CSR-Dateien hat, wenn es zwei Controller
hat.
```

```
[NOTE]
====
Alternativ können Sie eine CSR-Datei mit einem Tool wie OpenSSL generieren
und zu überspringen <<Schritt 2: Senden Sie die CSR-Dateien>>.

====
.Schritte
. Wählen Sie Menü:Einstellungen[Zertifikate].
. Wählen Sie auf der Registerkarte Array Management die Option *Complete
CSR* aus.
+
[NOTE]
====
Wenn ein Dialogfeld angezeigt wird, in dem Sie aufgefordert werden, ein
selbstsigniertes Zertifikat für den zweiten Controller anzunehmen, klicken
Sie zum Fortfahren auf *Selbstsigniertes Zertifikat akzeptieren*.

====
. 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 Speicher-Array oder Geschäft
befindet.
** *Bundesland/Region (optional)* -- der Staat oder die Region, in der
sich Ihr Speicher-Array oder Ihr Geschäft befindet.
** *Land ISO Code* -- der zweistellige ISO-Code Ihres Landes
(International Organization for Standardization), wie z. B. die USA.


+
[CAUTION]
====
Einige Felder sind möglicherweise bereits mit den entsprechenden
Informationen ausgefüllt, z. B. mit der IP-Adresse des Controllers. Ändern
Sie die vorausgefüllten Werte nur, wenn Sie sich sicher sind, dass sie
nicht korrekt sind. Wenn Sie zum Beispiel noch keinen CSR-Vorgang
abgeschlossen haben, wird die Controller-IP-Adresse auf „`localhost.`“
gesetzt. In diesem Fall müssen Sie „`localhost`“ in den DNS-Namen oder die
IP-Adresse des Controllers ändern.

====
. Überprüfen oder geben Sie die folgenden Informationen über Controller A
```

in Ihrem Speicher-Array ein:
+
** *Controller Ein gemeinsamer Name* -- die IP-Adresse oder der DNS-Name von Controller A wird standardmäßig angezeigt. Stellen Sie sicher, dass diese Adresse korrekt ist. Sie muss mit den Angaben übereinstimmen, die Sie für den Zugriff auf System Manager im Browser eingeben. Der DNS-Name kann nicht mit einem Platzhalter beginnen.
** *Controller Eine alternative IP-Adresse* -- Wenn der gemeinsame Name eine IP-Adresse ist, können Sie optional weitere IP-Adressen oder Aliase für Controller A eingeben Verwenden Sie für mehrere Einträge ein kommagetrenntes Format.
** *Controller Ein alternativer DNS-Name* -- Wenn der gemeinsame Name ein DNS-Name ist, geben Sie weitere DNS-Namen für Controller A. 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. Wenn das Speicher-Array nur über einen Controller verfügt, steht die *Finish*-Taste zur Verfügung.
+
Wenn das Speicher-Array über zwei Controller verfügt, steht die Schaltfläche *Weiter* zur Verfügung.

+
[NOTE]
====
Klicken Sie nicht auf den Link *Skip this Step*, wenn Sie eine CSR-Anfrage erstellen. Dieser Link wird in Fehlerwiederherstellungssituationen bereitgestellt. In seltenen Fällen kann eine CSR-Anfrage auf einem Controller fehlschlagen, aber nicht auf dem anderen. Über diesen Link können Sie den Schritt zum Erstellen einer CSR-Anfrage für Controller A überspringen, wenn er bereits definiert ist, und mit dem nächsten Schritt zum erneuten Erstellen einer CSR-Anfrage auf Controller B fortfahren

====
. Wenn nur ein Controller vorhanden ist, klicken Sie auf *Fertig stellen*. Wenn zwei Controller vorhanden sind, klicken Sie auf *Weiter*, um die Daten für Controller B einzugeben (wie oben), und klicken Sie dann auf *Fertig stellen*.
+
Für einen einzelnen Controller wird eine CSR-Datei auf Ihr lokales System heruntergeladen. Für Dual Controller werden zwei CSR-Dateien heruntergeladen. Der Speicherort des Downloads hängt von Ihrem Browser ab.

. Gehen Sie zu <<Schritt 2: Senden Sie die CSR-Dateien>>.

== Schritt 2: Senden Sie die CSR-Dateien

Nachdem Sie die CSR-Dateien (Certificate Signing Request) erstellt haben, senden Sie die Dateien an eine Zertifizierungsstelle (CA). 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
. Suchen Sie die heruntergeladenen CSR-Dateien.
. Senden Sie die CSR-Dateien an eine CA (z. B. Verisign oder DigiCert), und fordern Sie signierte Zertifikate im PEM-Format an.
+
[CAUTION]
====
Nachdem Sie eine CSR-Datei an die CA gesendet haben, generieren SIE keine andere CSR-Datei. Wenn Sie eine CSR generieren, 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.

====
. Wenn die Zertifizierungsstelle die signierten Zertifikate zurückgibt, gehen Sie zu <<Schritt 3: Importieren Sie signierte Zertifikate für Controller>>.

== Schritt 3: Importieren Sie signierte Zertifikate für Controller

Nachdem Sie von der Zertifizierungsstelle (CA) signierte Zertifikate erhalten haben, importieren Sie die Dateien für die Controller.

.Bevor Sie beginnen
* Die CA hat signierte Zertifikatdateien zurückgegeben. Diese Dateien enthalten das Stammzertifikat, ein oder mehrere Zwischenzertifikate und die Serverzertifikate.
* 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 die Serverzertifikate, die die Controller identifizieren. Sie können die Windows verwenden `certmgr` Dienstprogramm zum Auspacken der Dateien (Rechtsklick und wählen Sie Menü: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 haben die Zertifikatdateien auf das Hostsystem kopiert, auf das Sie auf System Manager zugreifen.

.Schritte
. Menü auswählen:Einstellungen[Zertifikate]
. Wählen Sie auf der Registerkarte Array Management die Option *Import* aus.
+
Es wird ein Dialogfeld zum Importieren der Zertifikatdatei(en) geöffnet.

. Klicken Sie auf die Schaltflächen *Durchsuchen*, um zuerst die Stamm- und Zwischenzertifikatdateien auszuwählen, und wählen Sie dann jedes Serverzertifikat für die Controller aus. Die Root- und Zwischendateien sind für beide Controller gleich. Nur die Serverzertifikate sind für jeden Controller eindeutig. 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.

. Klicken Sie Auf *Import*.
+
Die Dateien werden hochgeladen und validiert.

.Ergebnis
Die Sitzung wird automatisch beendet. Sie müssen sich erneut anmelden, damit die Zertifikate wirksam werden. Wenn Sie sich erneut anmelden, werden die neuen CA-signierten Zertifikate für Ihre Sitzung verwendet.

[[IDda273d5685005b3667ba4867eda9c26a]]
= Managementzertifikate zurücksetzen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können die Zertifikate auf den Controllern von der Verwendung von CA-signierten Zertifikaten zurück auf die werkseitig eingestellten, selbstsignierten Zertifikate zurücksetzen.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
* CA-signierte Zertifikate müssen bereits importiert werden.

.Über diese Aufgabe
Mit der Funktion Reset werden die aktuellen CA-signierten Zertifikatdateien von jedem Controller gelöscht. Die Controller werden dann mithilfe selbstsignierter Zertifikate wiederhergestellt.

.Schritte
. Wählen Sie Menü:Einstellungen[Zertifikate].
. Wählen Sie auf der Registerkarte Array Management die Option *Zurücksetzen*.
+
Es wird ein Dialogfeld zum Zurücksetzen der Managementzertifikate bestätigen geöffnet.

. Typ `reset` Klicken Sie im Feld 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.

.Ergebnisse
Die Controller werden mithilfe von selbstsignierten Zertifikaten wiederhergestellt. Das System fordert Benutzer daher auf, das selbstsignierte Zertifikat für ihre Sitzungen manuell anzunehmen.

[[ID3fe8666e8d9c98245a90dd70f80523e5]]
= Anzeigen importierter Zertifikatinformationen

```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Auf der Seite Zertifikate können Sie den Zertifikatstyp, die ausstellende
Behörde und den gültigen Datumsbereich der Zertifikate für das Speicher-
Array anzeigen.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.

.Schritte
. Wählen Sie Menü:Einstellungen[Zertifikate].
. Wählen Sie eine der Registerkarten aus, um Informationen zu den
Zertifikaten anzuzeigen.
+
[cols="25h,~"]
|===
| Registerkarte | Beschreibung


 a|
Array-Management
 a|
Zeigen Sie Informationen zu den für jeden Controller importierten CA-
signierten Zertifikaten an, einschließlich der Root-Datei, der
Zwischendatei(en) und der Serverdatei(en).



 a|
Bewährt
 a|
Informationen über alle anderen Arten von Zertifikaten anzeigen, die für
die Controller importiert wurden. Verwenden Sie das Filterfeld unter
*Zertifikate anzeigen, die...* sind, um entweder vom Benutzer installierte
oder vorinstallierte Zertifikate anzuzeigen.

** *Vom Benutzer installiertes* -- Zertifikate, die ein Benutzer in das
Speicher-Array hochgeladen hat, die vertrauenswürdige Zertifikate
enthalten können, wenn der Controller als Client (anstelle eines Servers),
```

```
LDAPS-Zertifikate und Identity Federation-Zertifikate fungiert.
** *Vorinstalliert* -- im Speicher-Array enthaltene selbstsignierte
Zertifikate.




 a|
Verschlüsselungs-Management
 a|
Zeigen Sie Informationen zu den für einen externen
Schlüsselverwaltungsserver importierten CA-signierten Zertifikaten an.

|===




[[ID52f95c4567d6cf2fcc4dc64e3d23d26e]]
= Importieren Sie Zertifikate für Controller, wenn Sie als Clients
fungieren
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn der Controller eine Verbindung zurückweist, weil er die
Vertrauenskette für einen Netzwerkserver nicht validieren kann, können Sie
ein Zertifikat über die Registerkarte „Trusted“ importieren, auf der der
Controller (als Client agiert) die Kommunikation von diesem Server
akzeptieren kann.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.
* Die Zertifikatdateien werden auf Ihrem lokalen System installiert.


.Über diese Aufgabe
Das Importieren von Zertifikaten aus der Registerkarte „Trusted“ ist
möglicherweise erforderlich, wenn Sie zulassen möchten, dass andere Server
die Controller kontaktieren (z. B. ein LDAP-Server oder ein Syslog-Server,
der TLS verwendet).
```

.Schritte
. Wählen Sie Menü:Einstellungen[Zertifikate].
. Wählen Sie auf der Registerkarte Trusted die Option *Import* aus.
+
Es wird ein Dialogfeld zum Importieren der vertrauenswürdigen Zertifikatdateien geöffnet.

. Klicken Sie auf *Durchsuchen*, um die Zertifikatdateien für die Controller auszuwählen.
+
Die Dateinamen werden im Dialogfeld angezeigt.

. Klicken Sie Auf *Import*.

.Ergebnisse
Die Dateien werden hochgeladen und validiert.

[[ID596ce7648fffed5fa526fb7ce2ff49e1]]
= Überprüfung des Zertifikatsannuls aktivieren
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können automatische Überprüfungen auf widerrief Zertifikate aktivieren, sodass ein OCSP-Server (Online Certificate Status Protocol) Benutzer daran blockiert, nicht sichere Verbindungen zu machen.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
* Auf beiden Controllern wird ein DNS-Server konfiguriert, wodurch ein vollständig qualifizierter Domain-Name für den OCSP-Server verwendet werden kann. Diese Aufgabe ist auf der Seite Hardware verfügbar.
* Wenn Sie Ihren eigenen OCSP-Server angeben möchten, müssen Sie die URL dieses Servers kennen.

.Über diese Aufgabe

Die automatische Überprüfung des Widerrufs ist hilfreich, wenn die CA ein Zertifikat falsch ausgestellt hat oder ein privater Schlüssel gefährdet ist.

Während dieser Aufgabe können Sie einen OCSP-Server konfigurieren oder den in der Zertifikatdatei angegebenen Server verwenden. Der OCSP-Server prüft, ob die CA Zertifikate vor ihrem geplanten Ablaufdatum widerrufen hat, und blockiert dann den Zugriff des Benutzers auf einen Standort, wenn das Zertifikat widerrufen wird.

.Schritte
. Wählen Sie Menü:Einstellungen[Zertifikate].
. Wählen Sie die Registerkarte * Trusted* aus.
+
[NOTE]
====
Sie können auch die Überprüfung des Widerrufs über die Registerkarte * Key Management* aktivieren.

====
. Klicken Sie auf *Sonstige Aufgaben*, und wählen Sie im Dropdown-Menü die Option *Überprüfung der Widerruherstellung aktivieren* aus.
. Wählen Sie *Ich möchte die Sperrprüfung aktivieren* aus, damit im Kontrollkästchen ein Häkchen angezeigt wird und im Dialogfeld zusätzliche Felder angezeigt werden.
. Im Feld *OCSP Responder Address* können Sie optional eine URL für einen OCSP Responder-Server eingeben. Wenn Sie keine Adresse eingeben, verwendet das System die URL des OCSP-Servers aus der Zertifikatsdatei.
. Klicken Sie auf *Testadresse*, um sicherzustellen, dass das System eine Verbindung zur angegebenen URL öffnen kann.
. Klicken Sie Auf *Speichern*.

.Ergebnisse
Wenn das Speicher-Array versucht, eine Verbindung mit einem Server mit einem widerrufenen Zertifikat herzustellen, wird die Verbindung verweigert und ein Ereignis protokolliert.

[[ID87f8a40a9e34f75b604dc914f3cb07a2]]
= Vertrauenswürdige Zertifikate löschen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/

```
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die vom Benutzer installierten Zertifikate löschen, die zuvor
über die Registerkarte „Vertrauenswürdig“ importiert wurden.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.
* Wenn Sie ein vertrauenswürdiges Zertifikat mit einer neuen Version
aktualisieren, muss das aktualisierte Zertifikat importiert werden, bevor
Sie das alte Zertifikat löschen.


[CAUTION]
====
Möglicherweise verlieren Sie den Zugriff auf ein System, wenn Sie ein
Zertifikat löschen, das zur Authentifizierung der Controller und eines
anderen Servers, z. B. eines LDAP-Servers verwendet wird, bevor Sie ein
Ersatzzertifikat importieren.

====
.Über diese Aufgabe
Diese Aufgabe beschreibt das Löschen von vom Benutzer installierten
Zertifikaten. Die vorinstallierten, selbstsignierten Zertifikate können
nicht gelöscht werden.

.Schritte
. Wählen Sie Menü:Einstellungen[Zertifikate].
. Wählen Sie die Registerkarte * Trusted* aus.
+
In der Tabelle sind die vertrauenswürdigen Zertifikate des Speicher-Arrays
aufgeführt.

. Wählen Sie in der Tabelle das Zertifikat aus, das Sie entfernen möchten.
. Klicken Sie auf Menü:Sonstige Aufgaben[Löschen].
+
Das Dialogfeld Vertrauenswürdiges Zertifikat bestätigen wird geöffnet.

. Typ `delete` Klicken Sie im Feld auf *Löschen*.




[[IDbcbef14a43ce332abeee027059246536]]
```

```
= Verwenden Sie CA-signierte Zertifikate zur Authentifizierung mit einem
Schlüsselverwaltungsserver
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Für die sichere Kommunikation zwischen einem Schlüsselverwaltungsserver
und den Speicher-Array-Controllern müssen Sie die entsprechenden
Zertifikatssätze konfigurieren.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.

.Über diese Aufgabe
Die Authentifizierung zwischen den Controllern und einem
Schlüsselverwaltungsserver ist ein zweistufiges Verfahren.



== Schritt 1: CSR für die Authentifizierung mit einem
Schlüsselverwaltungsserver abschließen und einreichen

Sie müssen zuerst eine CSR-Datei (Certificate Signing Request) generieren
und dann mithilfe des CSR ein signiertes Clientzertifikat von einer
Zertifizierungsstelle (CA) anfordern, die vom Schlüsselverwaltungsserver
vertrauenswürdig ist. Sie können auch mithilfe der heruntergeladenen CSR-
Datei ein Client-Zertifikat vom Schlüsselverwaltungsserver erstellen und
herunterladen. Ein Client-Zertifikat validiert die Controller des Storage-
Arrays, damit der wichtige Management-Server seine KMIP-Anforderungen (Key
Management Interoperability Protocol) anvertrauen kann.


NOTE: CSR-Dateien, die extern über private und öffentliche Schlüsselpaare
generiert werden, können über das Dialogfeld „externen
Sicherheitsschlüssel erstellen“ importiert werden. Weitere Informationen
zum Importieren einer extern generierten CSR-Datei finden Sie unter
https://docs.netapp.com/us-en/e-series-santricity/sm-settings/use-ca-
signed-certificates-for-authentication-with-a-key-management-
server.html#step-2-import-certificates-for-the-key-management-
server["Schritt 2: Importieren Sie Zertifikate für den
Schlüsselverwaltungsserver"].
```

.Schritte
. Wählen Sie Menü:Einstellungen[Zertifikate].
. Wählen Sie auf der Registerkarte Key Management die Option *Complete CSR* aus.
. Geben Sie die folgenden Informationen ein:
+
** *Gemeinsamer Name* -- Ein Name, der den Client identifiziert. Es ist gängige Praxis, die im gemeinsamen Namen vorhandenen Anforderungen an die Namenskonventionen für Clientzertifikate mit den Anforderungen des KMS-Servers zu vergleichen. Der gemeinsame Name hilft dem KMS normalerweise, das Clientzertifikat zu identifizieren, wenn es während eines Handshake präsentiert wird.
** *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 oder der Ort, in dem sich Ihre Organisation befindet.
** *Bundesland/Region (optional)* -- der Staat oder die Region, in der sich Ihre Organisation befindet.
** *Land ISO Code* -- der zweistellige ISO-Code (International Organization for Standardization), wie die USA, wo sich Ihre Organisation befindet.

. Klicken Sie Auf *Download*.
+
Eine CSR-Datei wird auf Ihrem lokalen System gespeichert.

. Fordern Sie ein signiertes Clientzertifikat von der Zertifizierungsstelle an, die vom Schlüsselverwaltungsserver vertrauenswürdig ist.
+

NOTE: Es ist üblich, dass der Schlüsselverwaltungsserver über eine Funktion verfügt, die signierte Zertifikate direkt generiert, da er als eigene Zertifizierungsstelle fungiert.

. Wenn Sie ein Clientzertifikat besitzen, gehen Sie zu <<Schritt 2: Importieren Sie Zertifikate für den Schlüsselverwaltungsserver>>.

== Schritt 2: Importieren Sie Zertifikate für den

```
Schlüsselverwaltungsserver

Im nächsten Schritt importieren Sie Zertifikate zur Authentifizierung
zwischen dem Storage-Array und dem Schlüsselverwaltungsserver. Es gibt
zwei Arten von Zertifikaten: Das Clientzertifikat überprüft die Controller
des Speicherarrays, während das Zertifikat für den
Schlüsselverwaltungsserver den Server validiert. Sie müssen sowohl die
Client-Zertifikatdatei für die Controller als auch die
Serverzertifikatdatei für den Schlüsselverwaltungsserver laden.

.Bevor Sie beginnen
* Sie haben eine signierte Client-Zertifikatdatei (siehe <<Schritt 1: CSR
für die Authentifizierung mit einem Schlüsselverwaltungsserver abschließen
und einreichen>>), und Sie haben diese Datei auf den Host kopiert, auf den
Sie auf System Manager zugreifen. Ein Client-Zertifikat validiert die
Controller des Storage-Arrays, damit der wichtige Management-Server seine
KMIP-Anforderungen (Key Management Interoperability Protocol) anvertrauen
kann.
* Sie müssen eine Zertifikatdatei vom Schlüsselverwaltungsserver abrufen
und diese Datei anschließend auf den Host kopieren, auf den 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.
+
[NOTE]
====
Weitere Informationen zum Serverzertifikat finden Sie in der Dokumentation
für Ihren Schlüsselverwaltungsserver.

====


.Schritte
. Wählen Sie Menü:Einstellungen[Zertifikate].
. Wählen Sie auf der Registerkarte Schlüsselverwaltung die Option *Import*
aus.
+
Es wird ein Dialogfeld zum Importieren der Zertifikatdateien geöffnet.

. Klicken Sie neben *Select Client Certificate* auf die Schaltfläche
*Browse*, um die Clientzertifikatdatei für die Controller des
Speicherarrays auszuwählen.
+
Der Dateiname wird im Dialogfeld angezeigt.
```

```
. Wenn Sie eine Zertifikatdatei extern mit einem privaten und öffentlichen
Schlüsselpaar erzeugt haben, klicken Sie auf die Schaltfläche
*Durchsuchen* neben *Private Schlüsseldatei auswählen*, um die
Zertifikatdatei für die Controller des Speicherarrays auszuwählen.
+
Der Dateiname wird im Dialogfeld angezeigt.

. Neben *Wählen Sie das Serverzertifikat des Schlüsselverwaltungsservers*,
klicken Sie auf die Schaltfläche *Durchsuchen*, um die
Serverzertifikatdatei für Ihren Schlüsselverwaltungsserver auszuwählen.
Sie können für den Schlüsselverwaltungsserver ein Stammzertifikat, ein
Zwischenzertifikat oder ein Serverzertifikat auswählen.
+
Der Dateiname wird im Dialogfeld angezeigt.

. Klicken Sie Auf *Import*.
+
Die Dateien werden hochgeladen und validiert.




[[ID5708b419ffd3fc8a3cd8316d6c1dbb36]]
= Export von Zertifikaten für den Schlüsselverwaltungsserver
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können ein Zertifikat für einen Schlüsselverwaltungsserver auf Ihrem
lokalen Computer speichern.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.
* Zertifikate müssen bereits importiert werden.


.Schritte
. Wählen Sie Menü:Einstellungen[Zertifikate].
. Wählen Sie die Registerkarte * Key Management* aus.
. Wählen Sie in der Tabelle das Zertifikat aus, das Sie exportieren
```

```
möchten, und klicken Sie dann auf *Exportieren*.
+
Ein Dialogfeld „Speichern“ wird geöffnet.

. Geben Sie einen Dateinamen ein und klicken Sie auf *Speichern*.




:leveloffset: -1


= FAQs

:leveloffset: +1


[[ID4fa2fa5fc06ce296940598d566f3a865]]
= Warum wird das Dialogfeld „Zugriff auf anderen Controller nicht möglich“
angezeigt?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie bestimmte Vorgänge im Zusammenhang mit CA-Zertifikaten ausführen
(z. B. ein Zertifikat importieren), wird möglicherweise ein Dialogfeld
angezeigt, in dem Sie aufgefordert werden, ein selbstsigniertes Zertifikat
für den zweiten Controller anzunehmen.

In Speicher-Arrays mit zwei Controllern (Duplexkonfigurationen) wird
dieses Dialogfeld manchmal angezeigt, wenn SANtricity System Manager nicht
mit dem zweiten Controller kommunizieren kann oder wenn Ihr Browser das
Zertifikat während eines bestimmten Punktes nicht akzeptieren kann.

Wenn dieses Dialogfeld geöffnet wird, klicken Sie auf *Selbstsigniertes
Zertifikat akzeptieren*, um fortzufahren. Wenn Sie in einem anderen
Dialogfeld zur Eingabe eines Passworts aufgefordert werden, geben Sie Ihr
Administratorpasswort ein, das zum Zugriff auf System Manager verwendet
wird.

Wenn dieses Dialogfeld erneut angezeigt wird und Sie keine
Zertifikataufgabe abschließen können, führen Sie einen der folgenden
Schritte aus:
```

```
* Verwenden Sie einen anderen Browsertyp, um auf diesen Controller
zuzugreifen, das Zertifikat zu akzeptieren und fortzufahren.
* Greifen Sie mit System Manager auf den zweiten Controller zu,
akzeptieren Sie das selbstsignierte Zertifikat, kehren Sie dann zum ersten
Controller zurück und fahren Sie fort.



[[IDb03453a9f4f012d81a7f7073acfd3968]]
= Wie weiß ich, welche Zertifikate zum externen Schlüsselmanagement in den
SANtricity System Manager hochgeladen werden müssen?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Für das externe Verschlüsselungsmanagement importieren Sie zwei Arten von
Zertifikaten zur Authentifizierung zwischen dem Storage-Array und dem
Schlüsselverwaltungsserver, damit sich die beiden Entitäten gegenseitig
vertrauen können.

Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit
der wichtige Management-Server seine KMIP-Anforderungen (Key Management
Interoperability Protocol) anvertrauen kann.

Um ein Client-Zertifikat zu erhalten, verwenden Sie System Manager, um
eine CSR für das Speicher-Array abzuschließen. Sie können eine CSR auch
extern mit einem privaten und öffentlichen Schlüsselpaar erstellen.

Anschließend können Sie die CSR auf einen Schlüsselverwaltungsserver
hochladen und von dort aus ein Clientzertifikat generieren. Wenn Sie über
ein Clientzertifikat verfügen, kopieren Sie diese Datei auf den Host, auf
den Sie auf System Manager zugreifen.

Ein Zertifikat für den Schlüsselmanagementserver validiert den
Schlüsselmanagementserver, damit das Storage-Array seiner IP-Adresse
vertrauen kann. Rufen Sie die Serverzertifikatdatei vom
Schlüsselverwaltungsserver ab, und kopieren Sie diese Datei dann auf den
Host, auf dem Sie auf System Manager zugreifen.



[[ID6ac783601958d3fbdab09cf1054129e9]]
= Was muss ich über die Überprüfung des Annullierung von Zertifikaten
```

```
wissen?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Mit SANtricity System Manager können Sie mithilfe eines OCSP-Servers
(Online Certificate Status Protocol) nach gesperrten Zertifikaten suchen,
anstatt Zertifikatsperrlisten (Certificate Revocation Lists, CRLs)
hochzuladen.

Zurückwiderrufen Zertifikate sollten nicht mehr vertrauenswürdig sein. Ein
Zertifikat kann aus mehreren Gründen widerrufen werden; beispielsweise
wenn die Zertifizierungsstelle (CA) das Zertifikat nicht ordnungsgemäß
ausgestellt hat, ein privater Schlüssel kompromittiert wurde oder die
identifizierte Entität nicht den Richtlinienanforderungen entspricht.

Nachdem Sie in System Manager eine Verbindung zu einem OCSP-Server
hergestellt haben, führt das Speicherarray eine Widerrufs-Prüfung durch,
wenn es eine Verbindung zu einem AutoSupport-Server, einem externen
Schlüsselverwaltungsserver (EKMS), einem Lightweight Directory Access
Protocol over SSL (LDAPS)-Server oder einem Syslog-Server herstellt. Das
Speicher-Array versucht, die Zertifikate dieser Server zu validieren, um
sicherzustellen, dass sie nicht widerrufen wurden. Der Server gibt dann
für dieses Zertifikat einen Wert von „gut“, „gesperrt“ oder „unbekannt“
zurück. Wenn das Zertifikat widerrufen wird oder das Array nicht den OCSP-
Server kontaktieren kann, wird die Verbindung abgelehnt.

[NOTE]
====
Wenn Sie eine OCSP-Antwortadresse in System Manager oder in der
Befehlszeilenschnittstelle (CLI) angeben, wird die OCSP-Adresse, die in
der Zertifikatsdatei gefunden wurde, überschrieben.

====



[[IDf1c5e0e9f6bed974360caaba8b423d38]]
= Für welche Servertypen wird die Überprüfung des Widerrufs aktiviert?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Das Speicher-Array führt Sperrprüfungen durch, wenn es eine Verbindung zu
einem AutoSupport-Server, einem externen Schlüsselverwaltungsserver
(EKMS), einem Lightweight Directory Access Protocol over SSL (LDAPS)-
Server oder einem Syslog-Server herstellt.



:leveloffset: -1


:leveloffset: -1


= Unterstützung

:leveloffset: +1


[[ID929874beea0aec942a4f46d0a60df2c8]]
= Support-Übersicht
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Auf der Seite Support erhalten Sie Zugriff auf die Ressourcen für den
technischen Support.



== Welche Support-Aufgaben stehen zur Verfügung?

In Support können Sie Kontakte für den technischen Support anzeigen,
Diagnosen durchführen, AutoSupport konfigurieren, das Ereignisprotokoll
anzeigen und Software-Upgrades durchführen.

Weitere Informationen:

* xref:{relative_path}autosupport-feature-overview.html["Übersicht über
die Funktionen von AutoSupport"]
* xref:{relative_path}overview-event-log.html["Übersicht über das
Ereignisprotokoll"]
```

```
* xref:{relative_path}overview-upgrade-center.html["Übersicht zum Upgrade
Center"]




== Wie kann ich mich an den technischen Support wenden?

Klicken Sie auf der Hauptseite auf MENU:Support[Support Center >
Registerkarte Support Resources]. Die Kontaktinformationen für den
technischen Support finden Sie oben rechts auf der Schnittstelle.



= Informationen und Diagnosen anzeigen

:leveloffset: +1


[[IDbe1e039696456241e70f94e9fb0a146a]]
= Anzeigen des Speicher-Array-Profils
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Das Speicherarrayprofil enthält eine Beschreibung aller Komponenten und
Eigenschaften des Speicherarrays.

.Über diese Aufgabe
Sie können das Speicher-Array-Profil als Hilfe bei der Wiederherstellung
oder als Übersicht über die aktuelle Konfiguration des Speicher-Arrays
verwenden. Möglicherweise möchten Sie eine Kopie des Speicher-Array-
Profils auf dem Management-Client speichern und eine Papierkopie des
Speicher-Array-Profils mit dem Speicher-Array aufbewahren. Erstellen Sie
eine neue Kopie des Speicher-Array-Profils, wenn sich Ihre Konfiguration
ändert.

.Schritte
. Wählen Sie Menü:Registerkarte Support[Support Center > Support-
Ressourcen].
. Scrollen Sie nach unten zu *Detaillierte Speicher-Array-Informationen*
und wählen Sie dann *Storage-Array-Profil*.
+
```

```
Der Bericht wird auf Ihrem Bildschirm angezeigt.

+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Abschnitt | Beschreibung


 a|
Storage Array Durchführt
 a|
Zeigt alle Optionen an, die Sie konfigurieren können, und die statischen
Optionen des Speicherarrays. Zu diesen Optionen gehören die Anzahl an
Controllern, Festplatten-Shelfs, Laufwerken, Festplatten-Pools, Volume-
Gruppen, Volumes und Hot Spare-Laufwerke; maximale Anzahl von Laufwerk-
Shelfs, Laufwerken, Solid State Disks (SSDs) und Volumes zulässig; Anzahl
der Snapshot-Gruppen, Snapshot Images, Snapshot Volumes und
Konsistenzgruppen; Informationen über Funktionen; Informationen über
Firmware-Versionen; Informationen zur Seriennummer des Chassis,
AutoSupport-Status und Informationen zu AutoSupport-Zeitplan; Die
Einstellungen für die automatische Unterstützung von Datenerfassung und
geplante Support-Datenerfassung, das Speicher-Array World-Wide Identifier
(WWID) sowie die Medien-Scan- und Cache-Einstellungen.



 a|
Storage
 a|
Zeigt eine Liste aller Speichergeräte im Speicher-Array an. Je nach
Konfiguration Ihres Speicher-Arrays können im Abschnitt Speicher diese
Unterabschnitte angezeigt werden.

** *Disk Pools* -- zeigt eine Liste aller Disk Pools im Speicher-Array an.
** *Volume Groups* -- zeigt eine Liste aller Volume-Gruppen im Speicher-
Array an. Volumes und freie Kapazität sind in der Reihenfolge ihrer
Erstellung aufgeführt.
** *Volumes* -- zeigt eine Liste aller Volumes im Speicher-Array an. Die
aufgeführten Informationen umfassen Volume-Namen, Volume-Status,
Kapazität, RAID-Level, Volume-Gruppe oder Festplatten-Pool, den
Laufwerkstyp und weitere Details.
** *Fehlende Volumes* -- zeigt eine Liste aller Volumes im Speicher-Array
an, die derzeit einen fehlenden Status aufweisen. Die aufgeführten
```

```
Informationen enthalten den World Wide Identifier (WWID) für jedes
fehlende Volume.




 a|
Kopierdienste
 a|
Zeigt eine Liste aller Kopierdienste an, die für das Speicher-Array
verwendet werden. Je nach Konfiguration des Speicher-Arrays können im
Abschnitt Kopierdienste folgende Unterabschnitte angezeigt werden:

** *Volume Copies* -- zeigt eine Liste aller Kopierpaare im Speicher-Array
an. Die aufgeführten Informationen umfassen die Anzahl der Kopien, die
Namen der Kopiepaare, den Status, den Start-Zeitstempel und weitere
Details.
** *Snapshot Groups* -- zeigt eine Liste aller Snapshot-Gruppen im
Speicher-Array an.
** *Snapshot Images* -- zeigt eine Liste aller Snapshots im Speicher-Array
an.
** *Snapshot Volumes* -- zeigt eine Liste aller Snapshot-Volumen im
Speicher-Array an.
** *Consistency Groups* -- zeigt eine Liste aller Consistency Groups im
Speicher-Array an.
** *Mitgliedsvolumes* -- zeigt eine Liste aller Mitgliedsvolumes der
Consistency Group im Speicher-Array an.
** *Mirror Groups* -- zeigt eine Liste aller gespiegelten Volumes an.
** *Reservierte Kapazität* -- zeigt eine Liste aller reservierten
Kapazitäts-Volumes im Speicher-Array an.




 a|
Host-Zuweisungen
 a|
Zeigt eine Liste der Host-Zuweisungen im Speicher-Array an. Die
aufgeführten Informationen umfassen den Volume-Namen, die Logical Unit
Number (LUN), die Controller-ID, den Host-Namen oder den Host-Cluster-
Namen und den Volume-Status. Weitere Informationen sind aufgeführt, unter
anderem Topologiedefinitionen und Hosttypdefinitionen.



 a|
Trennt
```

a|
Zeigt eine Liste der gesamten Hardware im Storage Array an. Je nach Konfiguration des Speicherarrays werden diese Unterabschnitte im Abschnitt Hardware angezeigt.

** *Controller* -- zeigt eine Liste aller Controller im Speicher-Array an und enthält den Controller-Standort, -Status und -Konfiguration. Darüber hinaus sind Informationen zu Laufwerkskanälen, Informationen zu Host-Kanälen und Informationen zu Ethernet-Ports enthalten.
** *Drives* -- zeigt eine Liste aller Laufwerke im Speicher-Array an. Die Laufwerke werden in der Reihenfolge der Shelf-ID, der Fach-ID und der Steckplatz-ID aufgelistet. Die aufgeführten Informationen umfassen die Shelf-ID, die Fach-ID, die Steckplatz-ID, den Status, die Rohkapazität, Der Medientyp, der Schnittstellentyp, die aktuelle Datenrate, die Produkt-ID und die Firmware-Version für jedes Laufwerk. Der Abschnitt zu Laufwerken enthält außerdem Channel-Informationen, Informationen zur Hot-Spare-Abdeckung und Informationen zum Verschleiß (nur für SSD-Laufwerke). Die Verschleißinformationen umfassen den Prozentsatz der verwendeten Haltbarkeit. Dies ist die Menge der Daten, die auf die bisherigen SSD-Laufwerke geschrieben wurden, geteilt durch die theoretische Gesamtschreibgrenze der Laufwerke.
** *Drive Channels* -- zeigt Informationen zu allen Laufwerkskanälen im Speicher-Array an. Die aufgeführten Informationen umfassen den Kanalstatus, den Verbindungsstatus (falls zutreffend), die Anzahl der Laufwerke und die Anzahl der kumulativen Fehler.
** *Shelves* -- zeigt Informationen zu allen Regalen im Speicher-Array an. Die aufgeführten Informationen umfassen Laufwerktypen und Statusinformationen für jede Komponente des Shelf. Zu den Shelf-Komponenten gehören u. a. Akku-Pakete, SFP-Transceiver (Small Form-factor Pluggable), Behälter mit Stromversorgung und Lüfter sowie EAM-Behälter (Input/Output Module). Im Abschnitt Hardware wird auch die Sicherheitsschlüsselkennung angezeigt, wenn ein Sicherheitsschlüssel vom Speicher-Array verwendet wird.

a|
Funktionen
a|
Zeigt eine Liste der installierten Funktionspakete sowie eine maximal zulässige Anzahl von Snapshot-Gruppen, Snapshots (alt) und Volumes pro Host oder Host-Cluster an. Die Informationen im Abschnitt Funktionen umfassen auch die Laufwerksicherheit, d. h., ob das Speicher-Array aktiviert ist oder die Sicherheit deaktiviert ist.

```
|===
====
. Um das Speicher-Array-Profil zu durchsuchen, geben Sie einen Suchbegriff
in das Textfeld *Suchen* ein, und klicken Sie dann auf *Suchen*.
+
Alle übereinstimmenden Begriffe werden hervorgehoben. Um alle Ergebnisse
nacheinander durchzublättern, klicken Sie mit * Suchen*.

. Klicken Sie zum Speichern des Speicher-Array-Profils auf *Speichern*.
+
Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen
gespeichert `storage-array-profile.txt`.




[[ID9bf1b7a7f6ec5ebc35775f1051d40565]]
= Anzeige des Software- und Firmware-Inventars
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Im Software- und Firmwarebestand sind die Firmware-Versionen für jede
Komponente im Speicher-Array aufgeführt.

.Über diese Aufgabe
Ein Storage Array besteht aus vielen Komponenten, darunter Controller,
Laufwerke, Schubladen und Input/Output-Module (IOMs). Jede dieser
Komponenten enthält Firmware. Einige Firmware-Versionen hängen von anderen
Firmware-Versionen ab. Um Informationen über alle Firmware-Versionen in
Ihrem Speicher-Array zu erfassen, lesen Sie den Software- und Firmware-
Bestand. Der technische Support kann die Software- und Firmware-
Bestandsaufnahme analysieren, um falsche Firmware-Zuordnungen zu erkennen.

.Schritte
. Wählen Sie Menü:Registerkarte Support[Support Center > Support-
Ressourcen].
. Scrollen Sie nach unten zu *Ausführliche Speicher-Array-Informationen
starten* und wählen Sie dann *Software- und Firmware-Bestandsaufnahme*
aus.
+
Der Bericht „Software- und Firmware-Bestandsaufnahme“ wird auf dem
```

```
Bildschirm angezeigt.

. Klicken Sie zum Speichern der Software- und Firmware-Bestandsliste auf
*Speichern*.
+
Die Datei wird im Ordner Downloads für Ihren Browser mit dem Dateinamen
gespeichert `firmware-inventory.txt`.

. Folgen Sie den Anweisungen des technischen Supports, um die Datei an sie
zu senden.




:leveloffset: -1


= Erfassen von Diagnosedaten

:leveloffset: +1


[[ID3ef38839210d17f3fe16104e7d6c1fce]]
= Manuelles Sammeln von Support-Daten
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können verschiedene Arten von Inventar-, Status- und Performance-Daten
zu Ihrem Storage-Array in einer einzelnen Datei sammeln. Der technische
Support kann die Datei zur Fehlerbehebung und weiteren Analyse verwenden.

.Über diese Aufgabe
```

Wenn die AutoSupport-Funktion aktiviert ist, können Sie diese Daten auch sammeln, indem Sie auf die Registerkarte **AutoSupport** gehen und **AutoSupport senden** wählen.

Sie können jeweils nur einen Erfassungsvorgang ausführen. Wenn Sie versuchen, einen anderen Vorgang zu starten, erhalten Sie eine Fehlermeldung.

Führen Sie diesen Vorgang nur aus, wenn Sie vom technischen Support dazu aufgefordert werden.

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Support-Daten Erfassen** Aus.
3. Klicken Sie Auf **Collect**.

   Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `support-data.7z`. Wenn Ihr Regal Schubladen enthält, werden die Diagnosedaten für dieses Shelf in einer separaten Datei mit dem Namen gezippt archiviert `tray-component-state-capture.7z`.

4. Folgen Sie den Anweisungen des technischen Supports, um die Datei an sie zu senden.

Erfassen von Konfigurationsdaten

Sie können RAID-Konfigurationsdaten vom Controller speichern. Dieser enthält alle Daten für Volume-Gruppen und Festplatten-Pools. Anschließend können Sie sich an den technischen Support wenden, um Hilfe beim Wiederherstellen der Daten zu erhalten.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie der aktuelle Status der RAID-Konfigurationsdatenbank gespeichert wird. Diese Daten werden vom RPA-Speicherort des Controllers abgerufen.

> Die Funktion Konfigurationsdaten erfassen speichert die gleichen Informationen wie der CLI-Befehl für `save storageArray dbmDatabase`.

Sie sollten diese Aufgabe nur ausführen, wenn Sie von einer Recovery Guru-Operation oder technischem Support dazu aufgefordert werden.

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Konfigurationsdaten Erfassen**.
3. Klicken Sie im Dialogfeld auf **Collect**.

   Die Datei, `configurationData-<arrayName>-<dateTime>.7z`, Wird im Ordner Downloads für Ihren Browser gespeichert.

4. Wenden Sie sich an den technischen Support, um weitere Informationen zum Senden der Datei an sie und zum Laden der Daten zurück in das System zu erhalten.

Rufen Sie Recovery Support-Dateien

Der technische Support kann Dateien zum Recovery Support verwenden, um Probleme zu beheben. Diese Dateien werden von SANtricity System Manager automatisch gespeichert.

Bevor Sie beginnen

Der technische Support hat angefordert, dass Sie ihnen zusätzliche Dateien zur Fehlerbehebung senden.

Über diese Aufgabe

Recovery-Support-Dateien enthalten die folgenden Arten von Dateien:

- Unterstützen von Datendateien
- AutoSupport-Geschichte
- AutoSupport-Log
- SAS/RLS-Diagnosedateien
- Recovery-Profildaten
- Datenbankeinfassungsdateien

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Wiederherstellungs-Support-Dateien Abrufen**.

   In einem Dialogfeld werden alle Dateien für die Recovery-Unterstützung aufgeführt, die Ihr Speicher-Array erfasst hat. Um bestimmte Dateien zu finden, können Sie eine der Spalten sortieren oder Zeichen in das Feld **Filter** eingeben.

3. Wählen Sie eine Datei aus und klicken Sie dann auf **Download**.

   Die Datei wird im Ordner Downloads für Ihren Browser gespeichert.

4. Wenn Sie weitere Dateien speichern müssen, wiederholen Sie den vorherigen Schritt.
5. Klicken Sie Auf **Schließen**.
6. Folgen Sie den Anweisungen des technischen Supports, um die Datei an sie zu senden.

Trace-Puffer abrufen

Sie können die Trace-Puffer von den Controllern abrufen und die Datei zur Analyse an den technischen Support senden.

Über diese Aufgabe

Die Firmware verwendet die Trace-Puffer, um die Verarbeitung, insbesondere Ausnahmebedingungen, aufzuzeichnen, die für das Debuggen von Daten hilfreich sein können. Sie können Trace-Puffer abrufen, ohne den Betrieb des Storage Array zu unterbrechen und mit minimalen Auswirkungen auf die Performance.

Führen Sie diesen Vorgang nur aus, wenn Sie vom technischen Support dazu aufgefordert werden.

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Trace Buffers Abrufen**.
3. Aktivieren Sie das Kontrollkästchen neben jedem Controller, für den Trace-Puffer abgerufen werden sollen.

   Sie können einen oder beide Controller auswählen. Wenn die Statusmeldung des Controllers rechts von einem Kontrollkästchen fehlgeschlagen oder deaktiviert ist, ist das Kontrollkästchen deaktiviert.

4. Klicken Sie Auf **Ja**.

   Die Datei wird im Ordner Downloads für Ihren Browser mit dem Dateinamen gespeichert `trace-buffers.7z`.

5. Folgen Sie den Anweisungen des technischen Supports, um die Datei an sie zu senden.

Erstellen von Statistiken zu I/O-Pfaden

Sie können die Statistikdatei für den I/O-Pfad speichern und sie dem technischen Support zur Analyse senden.

Über diese Aufgabe

Der technische Support verwendet die Statistiken des I/O-Pfads, um die Diagnose von Performance-Problemen zu erleichtern. Probleme mit der Applikations-Performance können durch Arbeitsspeicherauslastung, CPU-Auslastung, Netzwerklatenz, I/O-Latenz oder andere Probleme verursacht werden. Die Statistiken des I/O-Pfads werden während der Support-Datenerfassung automatisch erfasst oder manuell erfasst. Wenn AutoSupport aktiviert ist, werden zudem automatisch die I/O-Pfadstatistiken erfasst und an den technischen Support gesendet.

Die Zähler für die I/O-Pfadstatistiken werden zurückgesetzt, nachdem Sie bestätigt haben, dass Sie die Statistiken für den I/O-Pfad sammeln möchten. Die Zähler werden zurückgesetzt, auch wenn Sie den Vorgang anschließend abbrechen. Die Zähler werden auch zurückgesetzt, wenn der Controller zurückgesetzt wird (neu startet).

Führen Sie diesen Vorgang nur aus, wenn Sie vom technischen Support dazu aufgefordert werden.

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **E/A-Pfadstatistik sammeln**.
3. Bestätigen Sie, dass Sie den Vorgang durchführen möchten, indem Sie eingeben `collect`, Und klicken Sie dann auf **Collect**.

   Die Datei wird im Ordner Downloads für Ihren Browser mit dem Dateinamen gespeichert `io-path-statistics.7z`.

4. Folgen Sie den Anweisungen des technischen Supports, um die Datei an sie zu senden.

Abrufen des Integritätsabbilds

Sie können ein Zustandsabbild für den Controller überprüfen. Ein Systemzustand-Image ist ein Rohdaten-Dump des Prozessorspeichers des Controllers, mit dem der technische Support ein Problem mit einem Controller diagnostizieren kann.

Über diese Aufgabe

Die Firmware generiert automatisch ein Systemzustand-Image, wenn bestimmte Fehler erkannt werden. Nachdem ein Systemzustand-Image generiert wurde, wird der Controller, bei dem der Fehler neu gebootet wurde und ein Ereignis im Ereignisprotokoll protokolliert.

Wenn AutoSupport aktiviert ist, wird das Systemzustand-Image automatisch an den technischen Support gesendet. Wenn Sie AutoSupport nicht aktiviert haben, müssen Sie sich an den technischen Support wenden, um Anweisungen zum Abrufen des Zustands-Images zu erhalten und dieses zur Analyse zu senden.

Führen Sie diesen Vorgang nur aus, wenn Sie vom technischen Support dazu aufgefordert werden.

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Integritätsbild Abrufen**.

   Sie können sich im Abschnitt Details die Größe des Integritätsabbilds anzeigen lassen, bevor Sie die Datei herunterladen.

3. Klicken Sie Auf **Collect**.

   Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `health-image.7z`.

4. Folgen Sie den Anweisungen des technischen Supports, um die Datei an sie zu senden.

Führen Sie Wiederherstellungsmaßnahmen durch

Unlesbare Sektoren-Log anzeigen

Sie können das unlesbare Sektoren-Log speichern und die Datei zur Analyse an den technischen Support senden.

Über diese Aufgabe

Das unlesbare Sektoren-Log enthält detaillierte Aufzeichnungen von unlesbaren Sektoren, die durch Laufwerke verursacht werden, die unwiederherstellbare Medienfehler melden. Unlesbare Sektoren werden während der normalen I/O und bei Modifizierungsvorgängen, wie z.B. Rekonstruktionen, erkannt. Wenn unlesbare Sektoren auf einem Speicher-Array erkannt werden, wird für das Speicher-Array eine Warnmeldung erforderlich angezeigt. Der Recovery Guru unterscheidet, welche unlesbare Sektorbedingung Aufmerksamkeit benötigt. Daten, die in einem unlesbaren Sektor enthalten sind, können nicht wiederhergestellt werden und sollten als verloren betrachtet werden.

Das unlesbare Sektoren-Log kann bis zu 1,000 unlesbare Sektoren speichern. Wenn das unlesbare Sektoren-Protokoll 1,000 Einträge erreicht, gelten die folgenden Bedingungen:

- Wenn während der Rekonstruktion neue unlesbare Sektoren erkannt werden, schlägt die Rekonstruktion fehl, und es wird kein Eintrag protokolliert.
- Bei neuen unlesbaren Sektoren, die während der E/A erkannt werden, schlägt die E/A fehl, und es wird kein Eintrag protokolliert.

  Dazu gehören RAID 5-Schreibvorgänge und RAID 6-Schreibvorgänge, die vor dem Überlauf erfolgreich waren.

Möglicher Datenverlust — Wiederherstellung aus unlesbaren Sektoren ist ein kompliziertes Verfahren, das mehrere verschiedene Methoden beinhalten kann. Führen Sie diesen Vorgang nur aus, wenn Sie vom technischen Support dazu aufgefordert werden.

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].

2. Wählen Sie **Unlesbare Sektoren Anzeigen/Löschen**.
3. So speichern Sie das Protokoll der unlesbaren Sektoren:

   a. In der ersten Spalte der Tabelle können Sie entweder einzelne Volumes auswählen, für die Sie das unlesbare Sektoren-Protokoll speichern möchten (klicken Sie auf das Kontrollkästchen neben jedem Volume), oder wählen Sie alle Volumes aus (aktivieren Sie das Kontrollkästchen in der Tabellenüberschrift).

      Um bestimmte Volumes zu finden, können Sie eine der Spalten sortieren oder Zeichen in das Feld **Filter** eingeben.

   b. Klicken Sie Auf **Speichern**.

   Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `unreadable-sectors.txt`.

4. Wenn Sie vom technischen Support aufgefordert werden, das unlesbare Sektoren-Protokoll zu löschen, führen Sie die folgenden Schritte aus:

   a. In der ersten Spalte der Tabelle können Sie entweder einzelne Volumes auswählen, für die Sie das unlesbare Sektoren-Protokoll löschen möchten (klicken Sie auf das Kontrollkästchen neben jedem Volume) oder alle Volumes auswählen (aktivieren Sie das Kontrollkästchen in der Tabellenüberschrift).

   b. Klicken Sie auf **Löschen** und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

Aktivieren Sie die Laufwerksanschlüsse neu

Sie können dem Controller anzeigen, dass zur Wiederherstellung einer Fehldrahtbedingung Korrekturmaßnahmen ergriffen wurden.

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Laufwerksanschlüsse wieder aktivieren** aus, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

   Diese Option wird nur angezeigt, wenn im Speicher-Array Laufwerkanschlüsse deaktiviert sind.

   Der Controller aktiviert alle SAS-Ports, die bei Erkennung einer Fehlleitung deaktiviert wurden.

Löschen Sie den Wiederherstellungsmodus

Verwenden Sie nach dem Wiederherstellen einer Speicherarray-Konfiguration den Vorgang „Clear Recovery Mode“, um die I/O-Vorgänge auf dem Speicher-Array fortzusetzen und in den normalen Betrieb zurückzukehren.

Bevor Sie beginnen

- Wenn Sie das Speicher-Array in eine frühere Konfiguration zurückversetzen möchten, müssen Sie die Konfiguration aus dem Backup wiederherstellen, bevor Sie den Wiederherstellungsmodus beenden.
- Sie müssen Validierungsprüfungen oder technischen Support durchführen, um sicherzustellen, dass die Wiederherstellung erfolgreich war. Nachdem festgestellt wurde, dass die Wiederherstellung erfolgreich war, kann der Wiederherstellungsmodus gelöscht werden.

Über diese Aufgabe

Das Storage-Array enthält eine Konfigurationsdatenbank mit einem Datensatz seiner logischen Konfiguration (Pools, Volume-Gruppen, Volumes usw.). Wenn Sie die Speicherarray-Konfiguration absichtlich löschen oder die Konfigurationsdatenbank beschädigt wird, wechselt das Speicher-Array in den Recovery-Modus. Der Recovery-Modus stoppt den I/O und friert die Konfigurationsdatenbank an, sodass Sie eine der folgenden Aufgaben ausführen können:

- Stellen Sie die Konfiguration aus dem automatischen Backup wieder her, das auf den Flash-Geräten des Controllers gespeichert ist. Hierfür müssen Sie sich an den technischen Support wenden.
- Stellen Sie die Konfiguration aus einem früheren Vorgang „Konfigurationsdatenbank speichern“ wieder her. Vorgänge der Konfigurationsdatenbank speichern werden über die Befehlszeilenschnittstelle (CLI) ausgeführt.
- Konfigurieren Sie das Storage-Array von Grund auf neu.

Nachdem die Konfiguration des Speicherarrays wiederhergestellt oder neu definiert wurde und Sie überprüft haben, dass alles gut ist, müssen Sie den Wiederherstellungsmodus manuell deaktivieren.

> Sie können den Vorgang „Wiederherstellung löschen“ nach dem Start nicht mehr abbrechen. Der Wiederherstellungsmodus kann lange dauern. Führen Sie diesen Vorgang nur aus, wenn Sie vom technischen Support dazu aufgefordert werden.

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Wiederherstellungsmodus löschen**, und bestätigen Sie, dass Sie diesen Vorgang ausführen möchten.

   Diese Option wird nur angezeigt, wenn sich das Speicher-Array im Wiederherstellungsmodus befindet.

Managen Sie AutoSupport

Übersicht über die Funktionen von AutoSupport

Die AutoSupport Funktion überwacht den Zustand eines Storage Arrays und sendet automatische Aussendungen an den technischen Support.

Der technische Support nutzt die AutoSupport-Daten aktiv, um die Diagnose und Lösung von Kundenproblemen zu beschleunigen und proaktiv potenzielle Probleme zu erkennen und zu vermeiden.

AutoSupport-Daten enthalten Informationen zu Konfiguration, Status, Performance- und Systemereignissen eines Storage-Arrays. Die AutoSupport-Daten enthalten keine Benutzerdaten. Dispatches können sofort oder nach Zeitplan (täglich und wöchentlich) versendet werden.

Die wichtigsten Vorteile

Zu den wichtigsten Vorteilen der AutoSupport Funktion zählen:

- Schnellere Fallbearbeitung
- Schnelleres Management von Zwischenfällen durch ausgereiftes Monitoring
- Automatisierte Berichterstellung nach Zeitplan sowie automatisierte Berichterstellung zu kritischen Ereignissen
- Automatische Anforderungen zum Austausch von Hardware für ausgewählte Komponenten, z. B.

Laufwerke

- Nicht in das System eingreifende Warnungen, die Sie über Probleme informieren und Informationen für technischen Support bereitstellen, damit diese Korrekturmaßnahmen ergreifen können
- AutoSupport Analyse-Tools, die Patches überwachen, um bekannte Konfigurationsprobleme zu erkennen

Einzelne AutoSupport Funktionen

Die AutoSupport Funktion besteht aus drei separaten Funktionen, die separat aktiviert werden können.

- **Basic AutoSupport** — ermöglicht Ihrem Speicherarray die automatische Erfassung und Übermittlung von Daten an den technischen Support.
- **AutoSupport OnDemand** — ermöglicht technischen Support, bei Bedarf eine erneute Übertragung eines früheren AutoSupport Dispatch zur Fehlerbehebung anzufordern. Sämtliche Übertragungen werden vom Storage Array aus initiiert, nicht vom AutoSupport Server. Das Storage Array überprüft in regelmäßigen Abständen mit dem AutoSupport Server, um zu ermitteln, ob es noch ausstehende Neuübertragungsanfragen gibt und entsprechend darauf reagiert.
- **Ferndiagnose** — ermöglicht technischen Support, bei Bedarf einen neuen, aktuellen AutoSupport-Dispatch zur Fehlerbehebung anzufordern. Sämtliche Übertragungen werden vom Storage Array aus initiiert, nicht vom AutoSupport Server. Das Storage-Array überprüft in regelmäßigen Abständen mit dem AutoSupport Server, um zu ermitteln, ob ausstehende neue Anfragen zu bestehen und entsprechend darauf zu reagieren.

Unterschied zwischen AutoSupport und Erfassung von Supportdaten

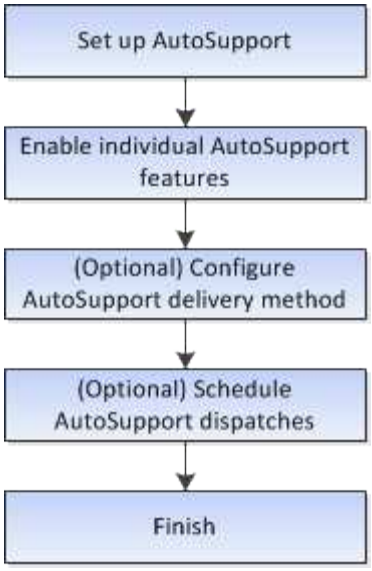
Im Speicher-Array gibt es zwei Methoden zum Erfassen von Supportdaten:

- **AutoSupport Feature** — Daten werden automatisch erfasst.
- **Support-Datenoption sammeln** — Daten müssen gesammelt und manuell gesendet werden.

Die AutoSupport Funktion ist benutzerfreundlicher, da Daten automatisch erfasst und gesendet werden. AutoSupport Daten können proaktiv eingesetzt werden, um Probleme vorzubeugen, bevor sie entstehen. Die AutoSupport Funktion beschleunigt die Fehlerbehebung, da der technische Support bereits auf die Daten zugreifen kann. Aus diesen Gründen ist die AutoSupport-Funktion die bevorzugte Datenerfassungsmethode.

Workflow für die AutoSupport Funktion

Konfigurieren Sie in SANtricity System Manager die AutoSupport-Funktion, indem Sie die folgenden Schritte ausführen.



Aktivieren oder Deaktivieren von AutoSupport Funktionen

Sie aktivieren die AutoSupport-Funktion und die einzelnen AutoSupport-Funktionen während der Ersteinrichtung oder Sie können sie später aktivieren oder deaktivieren.

Bevor Sie beginnen

Wenn Sie AutoSupport OnDemand oder Remote-Diagnose aktivieren möchten, muss die AutoSupport-Bereitstellungsmethode auf HTTPS gesetzt werden.

Über diese Aufgabe

Sie können die AutoSupport-Funktion jederzeit deaktivieren, jedoch wird dringend empfohlen, sie aktiviert zu lassen. Wenn Sie die AutoSupport-Funktion aktivieren, kann die Problembestimmung und -Behebung bei Problemen mit Ihrem Storage Array erheblich beschleunigt werden.

Die AutoSupport Funktion besteht aus drei separaten Funktionen, die separat aktiviert werden können.

- **Basic AutoSupport** — ermöglicht Ihrem Speicherarray die automatische Erfassung und Übermittlung von Daten an den technischen Support.
- **AutoSupport OnDemand** — ermöglicht technischen Support, bei Bedarf eine erneute Übertragung eines früheren AutoSupport Dispatch zur Fehlerbehebung anzufordern. Sämtliche Übertragungen werden vom Storage Array aus initiiert, nicht vom AutoSupport Server. Das Storage Array überprüft in regelmäßigen Abständen mit dem AutoSupport Server, um zu ermitteln, ob es noch ausstehende Neuübertragungsanfragen gibt und entsprechend darauf reagiert.
- **Ferndiagnose** — ermöglicht technischen Support, bei Bedarf einen neuen, aktuellen AutoSupport-Dispatch zur Fehlerbehebung anzufordern. Sämtliche Übertragungen werden vom Storage Array aus initiiert, nicht vom AutoSupport Server. Das Storage-Array überprüft in regelmäßigen Abständen mit dem AutoSupport Server, um zu ermitteln, ob ausstehende neue Anfragen zu bestehen und entsprechend darauf zu reagieren.

Schritte

1. Wählen Sie MENU:Support[Support Center > AutoSupport].
2. Wählen Sie **AutoSupport-Funktionen aktivieren/deaktivieren**.
3. Aktivieren Sie die Kontrollkästchen neben den AutoSupport-Funktionen, die Sie aktivieren möchten.

Die Features hängen voneinander ab, wie durch die Einzüge der Elemente im Dialogfeld angegeben. Beispielsweise müssen Sie AutoSupport OnDemand aktivieren, bevor Sie die Remote-Diagnose aktivieren können.

4. Klicken Sie Auf **Speichern**.

   Wenn Sie AutoSupport deaktivieren, wird auf der Startseite eine Benachrichtigung angezeigt. Sie können die Benachrichtigung verwerfen, indem Sie auf **Ignorieren** klicken.

Konfigurieren der AutoSupport-Bereitstellungsmethode

Die AutoSupport-Funktion unterstützt die HTTPS- und SMTP-Protokolle für die Bereitstellung von Dispatches an den technischen Support.

Bevor Sie beginnen

- Die AutoSupport-Funktion muss aktiviert sein. Sie sehen, ob die Funktion auf der Seite AutoSupport aktiviert ist.
- Ein DNS-Server muss in Ihrem Netzwerk installiert und konfiguriert sein. Die DNS-Server-Adresse muss in System Manager konfiguriert sein (diese Aufgabe ist auf der Seite Hardware verfügbar).

Über diese Aufgabe

Überprüfen Sie die verschiedenen Protokolle:

- **HTTPS** — ermöglicht es Ihnen, sich direkt mit dem Ziel-Server des technischen Supports über HTTPS zu verbinden. Wenn Sie AutoSupport OnDemand oder Remote-Diagnose aktivieren möchten, muss die AutoSupport-Bereitstellungsmethode auf HTTPS gesetzt werden.
- **E-Mail** — ermöglicht Ihnen, einen E-Mail-Server als Liefermethode für das Senden von AutoSupport-Entsendungen zu verwenden.

> **Unterschiede zwischen den Methoden HTTPS und Email**. Die E-Mail-Versandmethode, die SMTP verwendet, weist einige wichtige Unterschiede zur HTTPS-Bereitstellungsmethode auf. Erstens ist die Größe der Dispatches für die E-Mail-Methode auf 5 MB begrenzt, was bedeutet, dass einige ASUP Datensammlungen nicht versendet werden. Zweitens ist die AutoSupport OnDemand-Funktion nur für die HTTPS-Bereitstellungsmethode verfügbar.

Schritte

1. Wählen Sie MENU:Support[Support Center > AutoSupport].
2. Wählen Sie **AutoSupport-Bereitstellungsmethode konfigurieren**.

   Es wird ein Dialogfeld angezeigt, in dem die Versandmethoden aufgeführt sind.

3. Wählen Sie die gewünschte Liefermethode aus, und wählen Sie dann die Parameter für diese Bereitstellungsmethode aus. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie HTTPS ausgewählt haben, wählen Sie einen der folgenden Bereitstellungsparameter aus:
     - **Direkt** — dieser Lieferparameter ist die Standardauswahl. Wenn Sie diese Option wählen, können Sie mithilfe des HTTPS-Protokolls eine direkte Verbindung zum technischen Supportsystem des Ziels herstellen.
     - **Über Proxy Server** — mit dieser Option können Sie die HTTP Proxy-Serverdetails angeben, die für die Verbindung mit dem technischen Zielunterstützungssystem erforderlich sind. Sie müssen die Host-Adresse und die Portnummer angeben. Sie müssen jedoch nur die Details zur Host-

Authentifizierung (Benutzername und Passwort) eingeben, falls erforderlich.

- **Über Proxy Auto-Configuration Script (PAC)** — Geben Sie den Speicherort einer PAC-Skriptdatei (Proxy Auto-Configuration) an. Mit einer PAC-Datei kann das System automatisch den entsprechenden Proxyserver auswählen, um eine Verbindung mit dem technischen Zielunterstützungssystem herzustellen.

◦ Wenn Sie E-Mail ausgewählt haben, geben Sie die folgenden Informationen ein:

- Die E-Mail-Server-Adresse als vollständig qualifizierter Domain-Name, IPv4-Adresse oder IPv6-Adresse.
- Die E-Mail-Adresse, die im Feld „von“ der AutoSupport-Entsendmail angezeigt wird.
- **Optional; wenn Sie einen Konfigurationstest durchführen möchten**: Die E-Mail-Adresse, an der eine Bestätigung gesendet wird, wenn das AutoSupport-System den Testversand erhält.
- Wenn Sie Nachrichten verschlüsseln möchten, wählen Sie **SMTPS** oder **STARTTLS** für den Verschlüsselungstyp aus, und wählen Sie dann die Portnummer für verschlüsselte Nachrichten aus. Wählen Sie andernfalls * Keine*.
- Geben Sie bei Bedarf einen Benutzernamen und ein Kennwort für die Authentifizierung mit dem ausgehenden Absender und dem E-Mail-Server ein.

4. Wenn Sie eine Firewall haben, die die Bereitstellung dieser ASUP-Einsendungen blockiert, fügen Sie der Whitelist die folgende URL hinzu: `https://support.netapp.com/put/AsupPut/`
5. Klicken Sie auf **Testkonfiguration**, um die Verbindung zum Server des technischen Supports mit den angegebenen Lieferparametern zu testen. Wenn Sie die AutoSupport On-Demand-Funktion aktiviert haben, testet das System auch die Verbindung für die AutoSupport OnDemand-Entsendungsbereitstellung.

   Wenn der Konfigurationstest fehlschlägt, überprüfen Sie Ihre Konfigurationseinstellungen, und führen Sie den Test erneut aus. Wenden Sie sich an den technischen Support, wenn der Test weiterhin fehlschlägt.

6. Klicken Sie Auf **Speichern**.

Planen Sie AutoSupport-Entsendungen

SANtricity System Manager erstellt automatisch einen Standardzeitplan für AutoSupport-Entsendungen. Wenn Sie es bevorzugen, können Sie Ihren eigenen Zeitplan angeben.

Bevor Sie beginnen

Die AutoSupport-Funktion muss aktiviert sein. Sie sehen, ob die Funktion auf der Seite AutoSupport aktiviert ist.

Über diese Aufgabe

- **Tageszeit** — tägliche Dispatches werden täglich im von Ihnen angegebenen Zeitraum gesammelt und gesendet. System Manager wählt eine Zufallszeit während des Bereichs aus. Alle Zeiten werden in Coordinated Universal Time (UTC) angegeben, was sich von der lokalen Zeit des Speicherarrays unterscheiden kann. Sie müssen die lokale Zeit Ihres Speicher-Arrays in UTC konvertieren.
- **Wochentag** — wöchentliche Entsendungen werden gesammelt und einmal pro Woche versendet. System Manager wählt einen Tag nach dem Zufallsprinzip aus den von Ihnen angegebenen Tagen aus. Deaktivieren Sie alle Tage, an denen keine wöchentliche Entsendung erfolgen soll. System Manager wählt einen Tag nach dem Zulassen aus.
- **Wöchentliche Zeit** — wöchentliche Entsendungen werden einmal pro Woche in dem von Ihnen angegebenen Zeitraum gesammelt und versendet. System Manager wählt eine Zufallszeit während des Bereichs aus. Alle Zeiten werden in Coordinated Universal Time (UTC) angegeben, was sich von der lokalen Zeit des Speicherarrays unterscheiden kann. Sie müssen die lokale Zeit Ihres Speicher-Arrays in

UTC konvertieren.

Schritte

1. Wählen Sie MENU:Support[Support Center > AutoSupport].
2. Wählen Sie **AutoSupport-Entsendungen planen**.

   Der Assistent AutoSupport-Entsendungen planen wird angezeigt.

3. Befolgen Sie die Schritte im Assistenten.

Senden Sie AutoSupport-Patches

Mit SANtricity System Manager können Sie AutoSupport Entsendungen an den technischen Support senden, ohne auf einen geplanten Versand warten zu müssen.

Bevor Sie beginnen

Die AutoSupport-Funktion muss aktiviert sein. Sie sehen, ob die Funktion auf der Seite AutoSupport aktiviert ist.

Über diese Aufgabe

Dieser Vorgang erfasst Support-Daten und sendet sie automatisch an den technischen Support, damit Probleme behoben werden können.

Schritte

1. Wählen Sie MENU:Support[Support Center > AutoSupport].
2. Wählen Sie **AutoSupport Entsendung senden**.

   Das Dialogfeld Entsendung von AutoSupport senden wird angezeigt.

3. Bestätigen Sie den Vorgang, indem Sie **Senden** wählen.

Anzeigen des AutoSupport-Status

Auf der Seite AutoSupport erfahren Sie, ob die AutoSupport-Funktion und die einzelnen AutoSupport-Funktionen derzeit aktiviert sind.

Schritte

1. Wählen Sie MENU:Support[Support Center > AutoSupport].
2. Sehen Sie sich rechts auf der Seite unterhalb der Registerkarten an, um zu erfahren, ob die AutoSupport-Basisfunktion aktiviert ist.
3. Bewegen Sie den Mauszeiger über das Fragezeichen, um zu sehen, ob einzelne AutoSupport-Funktionen aktiviert sind.

Zeigen Sie das AutoSupport-Protokoll an

Das AutoSupport-Protokoll enthält Informationen zum Status, zum Versandverlauf und zu Fehlern, die bei der Lieferung von AutoSupport-Entsendungen auftreten.

Über diese Aufgabe

Es können mehrere Protokolldateien vorhanden sein. Wenn die aktuelle Protokolldatei 200 KB erreicht, wird

sie archiviert und eine neue Protokolldatei erstellt. Der Name der archivierten Protokolldatei lautet `ASUPMessages.n`, Wobei *n* eine Ganzzahl zwischen 1 und 9 ist. Wenn mehrere Protokolldateien vorhanden sind, können Sie das aktuellste Protokoll oder ein vorheriges Protokoll anzeigen.

- **Aktueller Log** — zeigt eine Liste der neuesten aufgezeichneten Ereignisse an.
- **Archived Log** — zeigt eine Liste früherer Ereignisse an.

Schritte

1. Wählen Sie MENU:Support[Support Center > AutoSupport].
2. Wählen Sie **AutoSupport-Protokoll anzeigen**.

   Es wird ein Dialogfeld angezeigt, in dem das aktuelle AutoSupport-Protokoll aufgelistet wird.

3. Wenn Sie frühere AutoSupport-Protokolle sehen möchten, wählen Sie das Optionsfeld **archiviert** und wählen Sie dann ein Protokoll aus der Dropdown-Liste **AutoSupport-Protokoll auswählen** aus.

   Die Option „archiviert“ wird nur angezeigt, wenn auf dem Speicher-Array archivierte Protokolle vorhanden sind.

   Das ausgewählte AutoSupport-Protokoll wird im Dialogfeld angezeigt.

4. **Optional:** um das AutoSupport-Protokoll zu durchsuchen, geben Sie einen Begriff in das Feld **Suchen** ein und klicken auf **Suchen**.

   Klicken Sie erneut auf **Suchen**, um nach weiteren Vorkommen des Begriffs zu suchen.

Fenster AutoSupport-Wartung aktivieren

Aktivieren Sie das AutoSupport-Wartungsfenster, um die automatische Ticketerstellung bei Fehlerereignissen zu unterdrücken. Im normalen Betriebsmodus eröffnet das Storage Array über AutoSupport einen Support-Fall, wenn ein Problem auftritt.

Schritte

1. Wählen Sie MENU:Support[Support Center > AutoSupport].
2. Wählen Sie **Fenster AutoSupport-Wartung aktivieren**.
3. Geben Sie die E-Mail-Adresse ein, um eine Bestätigung zu erhalten, dass das Wartungsfenster bearbeitet wurde.

   Je nach Konfiguration können Sie bis zu fünf E-Mail-Adressen eingeben. Wenn Sie mehr als eine Adresse hinzufügen möchten, wählen Sie **Weitere E-Mail hinzufügen**, um ein anderes Feld zu öffnen.

4. Geben Sie die Dauer (in Stunden) an, um das Wartungsfenster zu aktivieren.

   Die maximal unterstützte Dauer beträgt 72 Stunden.

5. Klicken Sie Auf **Ja**.

   Die automatische Erstellung von AutoSupport-Tickets bei Fehlerereignissen wird vorübergehend für das angegebene Zeitfenster unterbunden.

Nachdem Sie fertig sind

Das Wartungsfenster beginnt erst, wenn die Anfrage des Storage-Arrays von den AutoSupport-Servern verarbeitet wird. Warten Sie, bis Sie eine Bestätigungs-E-Mail erhalten haben, bevor Sie Wartungsarbeiten an Ihrem Speicher-Array durchführen.

Deaktivieren Sie das AutoSupport-Wartungsfenster

Deaktivieren Sie das AutoSupport-Wartungsfenster, um die automatische Erstellung von Tickets bei Fehlerereignissen zu ermöglichen. Wenn das AutoSupport-Wartungsfenster deaktiviert ist, öffnet das Storage-Array AutoSupport im Falle eines Problems einen Support-Fall.

Schritte

1. Wählen Sie MENU:Support[Support Center > AutoSupport].
2. Wählen Sie * Fenster AutoSupport-Wartung deaktivieren*.
3. Geben Sie die E-Mail-Adresse ein, um eine Bestätigung zu erhalten, dass die Anfrage zum Deaktivieren des Wartungsfensters bearbeitet wurde.

   Je nach Konfiguration können Sie bis zu fünf E-Mail-Adressen eingeben. Wenn Sie mehr als eine Adresse hinzufügen möchten, wählen Sie **Weitere E-Mail hinzufügen**, um ein anderes Feld zu öffnen.

4. Klicken Sie Auf **Ja**.

   Die automatische Erstellung von AutoSupport Tickets bei Fehlerereignissen ist aktiviert.

Nachdem Sie fertig sind

Das Wartungsfenster wird erst enden, wenn die Anfrage des Storage-Arrays von den AutoSupport-Servern bearbeitet wurde. Warten Sie, bis Sie eine Bestätigungs-E-Mail erhalten haben, bevor Sie fortfahren.

Veranstaltungen anzeigen

Übersicht über das Ereignisprotokoll

Das Ereignisprotokoll liefert eine Verlaufsliste zu Ereignissen, die im Storage-Array aufgetreten sind. Dies hilft dem technischen Support bei der Behebung von Ereignissen, die zu Ausfällen führen.

Sie können das Ereignisprotokoll als zusätzliches Diagnose-Tool für den Recovery Guru zur Verfolgung von Storage Array-Ereignissen verwenden. Greifen Sie stets zuerst auf den Recovery Guru zu, wenn Sie versuchen, eine Wiederherstellung nach Komponentenausfällen im Storage Array durchzuführen.

Ereigniskategorien

Die Ereignisse im Ereignisprotokoll werden mit unterschiedlichen Status kategorisiert. Ereignisse, für die Sie Maßnahmen ergreifen müssen, haben die folgenden Status:

- Kritisch
- Warnung

Ereignisse, die informativ sind und keine sofortigen Maßnahmen erfordern, sind die folgenden:

- Informativ

Kritische Ereignisse

Kritische Ereignisse weisen auf ein Problem mit dem Speicher-Array hin. Wenn das kritische Ereignis sofort behoben wird, kann der Verlust des Datenzugriffs verhindert werden.

Wenn ein kritisches Ereignis eintritt, wird es im Ereignisprotokoll protokolliert. Alle kritischen Ereignisse werden an die SNMP-Verwaltungskonsole oder an den E-Mail-Empfänger gesendet, den Sie so konfiguriert haben, dass Sie Benachrichtigungen erhalten. Wenn die Shelf-ID zum Zeitpunkt des Ereignisses nicht bekannt ist, wird die Shelf-ID als „Shelf unbekannt“ aufgeführt.

Bei Erhalt eines kritischen Ereignisses finden Sie im Recovery Guru Procedure eine detaillierte Beschreibung des kritischen Ereignisses. Schließen Sie das Verfahren des Recovery Guru zur Korrektur des kritischen Ereignisses ab. Zur Korrektur bestimmter kritischer Ereignisse müssen Sie sich möglicherweise an den technischen Support wenden.

Zeigen Sie mithilfe des Ereignisprotokolls Ereignisse an

Sie können das Ereignisprotokoll anzeigen, das einen historischen Datensatz von Ereignissen enthält, die auf dem Speicher-Array aufgetreten sind.

Schritte

1. Wählen Sie Menü:Support[Ereignisprotokoll].

   Die Seite Ereignisprotokoll wird angezeigt.

Seitendetails

Element	Beschreibung
Feld „Alle anzeigen“	Wechselt zwischen allen Ereignissen und nur den kritischen und den Warnungsereignissen.
Filterfeld	Filtert die Ereignisse. Nützlich, um nur Ereignisse anzuzeigen, die sich auf eine bestimmte Komponente, ein bestimmtes Ereignis usw. beziehen
Wählen Sie das Spaltensymbol.	Ermöglicht Ihnen die Auswahl weiterer Spalten, die angezeigt werden sollen. In anderen Spalten erhalten Sie zusätzliche Informationen über das Ereignis.
Kontrollkästchen	Ermöglicht die Auswahl der zu speicherenden Ereignisse. Das Kontrollkästchen in der Tabellenüberschrift wählt alle Ereignisse aus.
Spalte „Datum/Uhrzeit“	Der Datums- und Zeitstempel des Ereignisses, entsprechend der Steuerungsuhr. Das Ereignisprotokoll sortiert anfänglich Ereignisse auf der Grundlage der Sequenznummer. In der Regel entspricht diese Sequenz dem Datum und der Uhrzeit. Die beiden Controller-Uhren im Speicher-Array konnten jedoch nicht synchronisiert werden. In diesem Fall könnten im Ereignisprotokoll einige vermeintliche Inkonsistenzen bezüglich der Ereignisse und des angezeigten Datums und der angezeigten Zeit angezeigt werden.
Spalte „Priorität“	Es gibt diese Prioritätswerte: • **Kritisch** — beim Speicher-Array ist ein Problem vorhanden. Wenn Sie jedoch sofortige Maßnahmen ergreifen, können Sie den Zugriff auf die Daten unter Umständen verhindern. Kritische Ereignisse werden für Warnmeldungen verwendet. Alle kritischen Ereignisse werden an jeden Netzwerk-Management-Client (über SNMP-Traps) oder an den von Ihnen konfigurierten E-Mail-Empfänger gesendet. • **Warnung** — ein Fehler ist aufgetreten, der die Leistung und die Fähigkeit des Speicherarrays beeinträchtigt hat, nach einem anderen Fehler wiederherzustellen. • **Informativ** — nicht kritische Informationen im Zusammenhang mit dem Speicher-Array.
Spalte Komponententyp	Die vom Ereignis betroffene Komponente. Bei der Komponente kann es sich um Hardware, z. B. ein Laufwerk oder ein Controller, oder um Software, z. B. Controller-Firmware, handeln.
Spalte „Komponentenposition“	Der physische Speicherort der Komponente im Speicher-Array.

Element	Beschreibung
Spalte Beschreibung	Eine Beschreibung des Ereignisses. • Beispiel* — `Drive write failure - retries exhausted`
Spalte Sequenznummer	Eine 64-Bit-Nummer, die einen bestimmten Protokolleintrag für ein Speicher-Array eindeutig identifiziert. Diese Zahl erhöht sich bei jedem neuen Ereignisprotokolleintrag um eins. Um diese Informationen anzuzeigen, klicken Sie auf das Symbol **Spalten auswählen**.
Spalte Ereignistyp	Eine 4-stellige Zahl, die jeden Typ des protokollierten Ereignisses identifiziert. Um diese Informationen anzuzeigen, klicken Sie auf das Symbol **Spalten auswählen**.
Spalte Ereignisspezifische Codes	Diese Informationen werden vom technischen Support verwendet. Um diese Informationen anzuzeigen, klicken Sie auf das Symbol **Spalten auswählen**.
Spalte Ereigniskategorie	• **Fehler** – Eine Komponente im Speicher-Array ist ausgefallen, z. B. ein Laufwerkausfall oder ein Batteriefehler. • **Statusänderung** – ein Element des Speicherarrays, das den Status geändert hat; beispielsweise ist ein Volume in den Status „optimal“ übergegangen oder ein Controller in den Status „Offline“ übergegangen. • **Intern** – interne Controller-Operationen, für die keine Benutzeraktion erforderlich ist; zum Beispiel hat der Controller den Tagesbeginn abgeschlossen. • **Befehl** – ein Befehl, der dem Speicher-Array ausgegeben wurde; zum Beispiel wurde ein Hot Spare zugewiesen. • **Fehler** – auf dem Speicher-Array wurde eine Fehlerbedingung erkannt, z. B. kann ein Controller den Cache nicht synchronisieren und bereinigen oder auf dem Speicher-Array wird ein Redundanzfehler erkannt. • **Allgemein** – jedes Ereignis, das nicht gut in eine andere Kategorie passt. Um diese Informationen anzuzeigen, klicken Sie auf das Symbol „ **Spalten auswählen “.
Angemeldet durch Spalte	Der Name des Controllers, der das Ereignis protokolliert hat. Um diese Informationen anzuzeigen, klicken Sie auf das Symbol „ **Spalten auswählen “.

2. Um neue Ereignisse aus dem Speicher-Array abzurufen, klicken Sie auf **Aktualisieren**.

   Es kann einige Minuten dauern, bis ein Ereignis protokolliert und auf der Seite Ereignisprotokoll angezeigt wird.

3. So speichern Sie das Ereignisprotokoll in einer Datei:

a. Aktivieren Sie das Kontrollkästchen neben jedem Ereignis, das Sie speichern möchten.
b. Klicken Sie Auf **Speichern**.

   Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `major-event-log-timestamp.log`.

4. So löschen Sie Ereignisse aus dem Ereignisprotokoll:

   Das Ereignisprotokoll speichert ca. 8,000 Ereignisse, bevor ein Ereignis durch ein neues Ereignis ersetzt wird. Wenn Sie die Ereignisse beibehalten möchten, können Sie sie speichern und aus dem Ereignisprotokoll löschen.

   a. Speichern Sie zuerst das Ereignisprotokoll.
   b. Klicken Sie auf **alles löschen**, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

Management von Upgrades

Übersicht zum Upgrade Center

Nutzen Sie das Upgrade Center, um die neueste Software und Firmware herunterzuladen und Ihre Controller und Laufwerke zu aktualisieren.

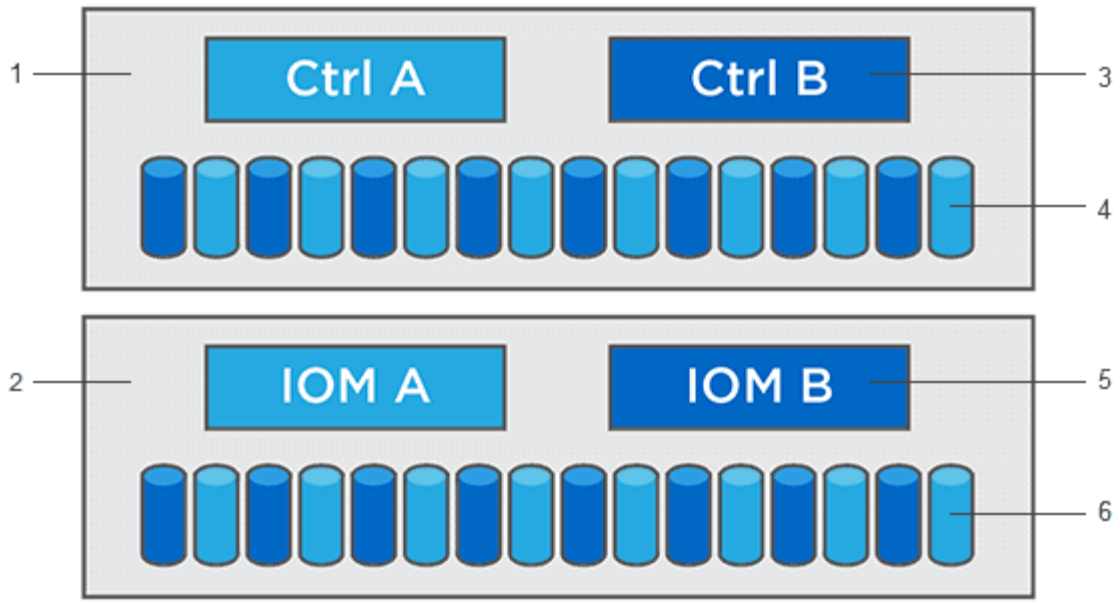
Controller-Upgrade – Übersicht

Sie können die Software und die Firmware Ihres Speicherarrays für alle neuesten Funktionen und Fehlerbehebungen aktualisieren.

Im Betriebssystem-Controller-Upgrade enthaltene Komponenten

Mehrere Storage-Array-Komponenten enthalten Software oder Hardware, die ein gelegentlich Upgrade durchgeführt werden soll.

- **Management Software** — System Manager ist die Software, die das Speicher-Array verwaltet.
- **Controller-Firmware** — Controller-Firmware verwaltet den I/O zwischen Hosts und Volumes.
- **Controller NVSRAM** — Controller NVSRAM ist eine Controller-Datei, die die Standardeinstellungen für die Controller angibt.
- **IOM-Firmware** — die I/O-Modul-Firmware (IOM) verwaltet die Verbindung zwischen einem Controller und einem Festplatten-Shelf. Es überwacht auch den Status der Komponenten.
- **Supervisor Software** — Supervisor Software ist die virtuelle Maschine auf einem Controller, in dem die Software ausgeführt wird.



[1] Controller-Shelf; [2] Festplatten-Shelf; [3] Software, Controller-Firmware, Controller NVSRAM Supervisor-Software; [4] Laufwerk-Firmware; [5] IOM-Firmware; [6] Laufwerk-Firmware

Sie können Ihre aktuellen Software- und Firmware-Versionen im Dialogfeld „Software- und Firmware-Bestandsaufnahme“ anzeigen. Gehen Sie zu **Support › Upgrade Center** und klicken Sie dann auf den Link für **Software- und Firmware-Bestandsaufnahme**.

Im Rahmen des Upgrades muss möglicherweise auch der Multipath-/Failover-Treiber und/oder der HBA-Treiber des Hosts aktualisiert werden, damit der Host mit den Controllern korrekt interagieren kann. Informationen zum ermitteln, ob dies der Fall ist, finden Sie im "Netapp Interoperabilitäts-Matrix-Tool".

Wann I/O gestoppt werden soll

Wenn Ihr Storage Array zwei Controller enthält und Sie einen Multipath-Treiber installiert haben, kann das Storage Array die I/O-Verarbeitung während des Upgrades fortsetzen. Während des Upgrades führt Controller A alle seine Volumes an Controller B durch, aktualisiert seine Volumes und alle Volumes von Controller B und führt dann ein Upgrade für Controller B durch

Zustandsprüfung vor dem Upgrade

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. Die folgenden Bedingungen können das Upgrade verhindern:

- Ausgefallene zugewiesene Laufwerke
- Hot Spares werden verwendet
- Unvollständige Volume-Gruppen
- Exklusive Vorgänge ausgeführt
- Fehlende Volumes
- Controller befindet sich im Status „nicht optimal“
- Übermäßige Anzahl von Ereignisprotokollereignissen
- Fehler bei der Validierung der Konfigurationsdatenbank

- Laufwerke mit alten Versionen von DACstore

Sie können die Integritätsprüfung vor dem Upgrade auch separat durchführen, ohne ein Upgrade durchführen zu müssen.

Überblick über das Laufwerk-Upgrade

Die Laufwerk-Firmware steuert die betrieblichen Eigenschaften eines Laufwerks auf niedriger Ebene. Die Hersteller der Laufwerke veröffentlichen regelmäßig Updates zu Laufwerk-Firmware, um neue Funktionen hinzuzufügen, die Performance zu verbessern und Fehler zu beheben.

Upgrades der Online- und Offline-Laufwerk-Firmware

Es gibt zwei Arten von Upgrade-Methoden für die Festplatten-Firmware: Online und offline.

Online

Während eines Online-Upgrades werden Festplatten nacheinander aktualisiert. Das Storage-Array verarbeitet die I/O-Verarbeitung während des Upgrades weiter. Sie müssen keine I/O-Vorgänge beenden Wenn ein Laufwerk eine Online-Aktualisierung durchführen kann, wird die Online-Methode automatisch verwendet.

Laufwerke, die ein Online-Upgrade durchführen können, umfassen Folgendes:

- Laufwerke in einem optimalen Pool
- Laufwerke in einer optimalen redundanten Volume-Gruppe (RAID 1, RAID 5 und RAID 6)
- Nicht zugewiesene Laufwerke
- Standby-Hot-Spare-Laufwerke

Ein Online-Upgrade der Laufwerk-Firmware kann mehrere Stunden in Anspruch nehmen, sodass dem Storage Array potenzielle Volume-Ausfälle zur Verfügung stehen. In folgenden Fällen kann es zu einem Volumenausfall kommen:

- In einer RAID 1- oder RAID 5-Volume-Gruppe fällt ein Laufwerk aus, während ein anderes Laufwerk in der Volume-Gruppe aktualisiert wird.
- In einem RAID 6 Pool oder einer Volume-Gruppe fallen zwei Laufwerke aus, während ein anderes Laufwerk im Pool oder in der Volume-Gruppe aktualisiert wird.

Offline (parallel)

Bei einem Offline-Upgrade werden alle Laufwerke desselben Laufwerktyps gleichzeitig aktualisiert. Diese Methode erfordert das Stoppen der I/O-Aktivität zu den Volumes, die mit den ausgewählten Laufwerken verknüpft sind. Da mehrere Laufwerke gleichzeitig aktualisiert werden können (parallel), wird die Ausfallzeit insgesamt deutlich reduziert. Wenn ein Laufwerk nur eine Offline-Aktualisierung durchführen kann, wird die Offline-Methode automatisch verwendet.

Die folgenden Laufwerke MÜSSEN die Offline-Methode verwenden:

- Laufwerke in einer nicht redundanten Volume-Gruppe (RAID 0)
- Laufwerke in einem nicht optimalen Pool oder einer Volume-Gruppe
- Laufwerke im SSD-Cache

Kompatibilität

Jede Laufwerk-Firmware-Datei enthält Informationen über den Laufwerkstyp, auf dem die Firmware ausgeführt wird. Sie können die angegebene Firmware-Datei nur auf ein kompatibles Laufwerk herunterladen. System Manager überprüft während des Upgrades die Kompatibilität automatisch.

Upgrades von Controller-Software und Firmware

Sie können die Software des Storage-Arrays und optional die IOM-Firmware und den nichtflüchtigen statischen Random-Access-Speicher (NVSRAM) aktualisieren, um sicherzustellen, dass Sie über alle neuesten Funktionen und Fehlerbehebungen verfügen.

Bevor Sie beginnen

- Sie wissen, ob Sie Ihre IOM-Firmware aktualisieren möchten.

  In der Regel sollten Sie alle Komponenten gleichzeitig aktualisieren. Sie können jedoch entscheiden, die IOM-Firmware nicht zu aktualisieren, wenn Sie sie nicht als Teil des Upgrades der SANtricity OS Software aktualisieren möchten oder wenn Sie vom technischen Support aufgefordert wurden, Ihre IOM-Firmware herunterzustufen (Sie können nur die Firmware über die Befehlszeilenschnittstelle herunterstufen).

- Sie wissen, ob Sie die NVSRAM-Controller-Datei aktualisieren möchten.

  In der Regel sollten Sie alle Komponenten gleichzeitig aktualisieren. Sie entscheiden sich jedoch möglicherweise nicht, die NVSRAM-Controller-Datei zu aktualisieren, wenn Ihre Datei entweder gepatcht wurde oder eine benutzerdefinierte Version ist und Sie sie nicht überschreiben möchten.

- Sie wissen, ob Sie Ihr Betriebssystem-Upgrade jetzt oder später aktivieren möchten.

  Gründe für eine spätere Aktivierung sind u. a.:

  - **Tageszeit** — die Aktivierung der Software und Firmware kann eine lange Zeit dauern, so dass Sie möglicherweise warten möchten, bis I/O-Lasten leichter sind. Der Controller-Failover während der Aktivierung, sodass die Performance möglicherweise niedriger ist als üblich, bis das Upgrade abgeschlossen ist.
  - **Paketyp** — möglicherweise möchten Sie die neue Software und Firmware auf einem Speicher-Array testen, bevor Sie die Dateien auf anderen Speicher-Arrays aktualisieren.

- Sie wissen, ob Sie von ungesicherten Laufwerken oder intern gesicherten Laufwerken wechseln möchten, um einen externen Schlüsselverwaltungsserver (KMS) für die Laufwerkssicherheit zu verwenden.
- Sie wissen, ob Sie eine rollenbasierte Zugriffssteuerung in Ihrem Storage-Array nutzen möchten.

Über diese Aufgabe

Sie können nur die Betriebssystemsoftware oder nur die NVSRAM-Controller-Datei aktualisieren oder Sie können beide Dateien aktualisieren.

Führen Sie diesen Vorgang nur aus, wenn Sie vom technischen Support dazu aufgefordert werden.

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 enthält oder kein Multipath-Treiber installiert ist, beenden Sie die I/O-Aktivität 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 Menü:Support[Upgrade Center].
3. Laden Sie die neue Datei von der Support-Website auf Ihren Management-Client herunter.

   a. Klicken Sie auf **NetApp Support**, um die Support Website zu starten.
   b. Klicken Sie auf der Support-Website auf die Registerkarte **Downloads** und wählen Sie dann **Downloads** aus.
   c. Wählen Sie **E-Series SANtricity OS Controller Software**.
   d. Befolgen Sie die restlichen Anweisungen.

   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.

4. Wenn Sie die IOM-Firmware derzeit NICHT aktualisieren möchten, klicken Sie auf **EAM-Auto-Synchronisierung unterbrechen**.

   Wenn Sie über ein Speicher-Array mit einem einzelnen Controller verfügen, wird die IOM-Firmware nicht aktualisiert.

5. Klicken Sie unter SANtricity OS Software Upgrade auf **Upgrade starten**.

   Das Dialogfeld SANtricity OS-Software aktualisieren wird angezeigt.

6. Wählen Sie eine oder mehrere Dateien aus, um den Upgrade-Prozess zu starten:

   a. Wählen Sie die SANtricity OS-Softwaredatei aus, indem Sie auf **Durchsuchen** klicken und zur Betriebssystemsoftware navigieren, die Sie von der Support-Website heruntergeladen haben.
   b. Wählen Sie die NVSRAM-Controller-Datei aus, indem Sie auf **Durchsuchen** klicken und zur NVSRAM-Datei navigieren, die Sie von der Support-Website heruntergeladen haben. Controller-NVSRAM-Dateien haben einen ähnlichen Dateinamen wie `N2800-830000-000.dlp`.

      Diese Aktionen treten auf:

      - Standardmäßig werden nur die Dateien angezeigt, die mit der aktuellen Speicherarray-Konfiguration kompatibel sind.
      - Wenn Sie eine Datei für die Aktualisierung auswählen, werden Name und Größe der Datei angezeigt.

7. **Optional:** Wenn Sie eine SANtricity OS Software-Datei für ein Upgrade ausgewählt haben, können Sie die Dateien auf den Controller übertragen, ohne sie zu aktivieren, indem Sie das Kontrollkästchen **Dateien übertragen, aber nicht aktualisieren (Upgrade später aktivieren)** aktivieren.
8. Klicken Sie auf **Start** und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

   Sie können den Vorgang während der Integritätsprüfung vor dem Upgrade abbrechen, jedoch nicht während der Übertragung oder Aktivierung.

9. **Optional:** um eine Liste der aktualisierten Versionen anzuzeigen, klicken Sie auf **Log speichern**.

Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `drive_upgrade_log-timestamp.txt`.

Nachdem Sie fertig sind

- Vergewissern Sie sich, dass alle Komponenten auf der Seite Hardware angezeigt werden.
- Überprüfen Sie die neuen Software- und Firmware-Versionen, indem Sie das Dialogfeld Software- und Firmware-Bestandsaufnahme aktivieren (gehen Sie zu Menü:Support[Upgrade Center] und klicken Sie dann auf den Link für **Software- und Firmware-Bestandsaufnahme**).
- Wenn Sie den Controller NVSRAM aktualisiert haben, gehen während der Aktivierung alle benutzerdefinierten Einstellungen, die Sie auf den vorhandenen NVSRAM angewendet haben, verloren. Sie müssen die benutzerdefinierten Einstellungen erneut auf den NVSRAM anwenden, nachdem der Aktivierungsvorgang abgeschlossen ist.

Aktivieren von Controller-Software und -Firmware

Sie können die Upgrade-Dateien sofort aktivieren oder bis zu einem angenehmeren Zeitpunkt warten.

Über diese Aufgabe

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

- **Tageszeit** — die Aktivierung der Software und Firmware kann eine lange Zeit dauern, so dass Sie möglicherweise warten möchten, bis I/O-Lasten leichter sind. Der Controller-Failover während der Aktivierung, sodass die Performance möglicherweise niedriger ist als üblich, bis das Upgrade abgeschlossen ist.
- **Paketyp** — möglicherweise möchten Sie die neue Software und Firmware auf einem Speicher-Array testen, bevor Sie die Dateien auf anderen Speicher-Arrays aktualisieren.

Wenn Sie über Software oder Firmware verfügen, die übertragen, aber nicht aktiviert wurde, wird im Bereich Benachrichtigungen der System Manager Startseite und auch auf der Seite Upgrade Center eine Benachrichtigung angezeigt.

Sie können den Aktivierungsvorgang nach dem Start nicht beenden.

Schritte

1. Wählen Sie Menü:Support[Upgrade Center].
2. Klicken Sie im Bereich SANtricity OS-Software-Upgrade auf **Aktivieren** und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

   Sie können den Vorgang während der Integritätsprüfung vor dem Upgrade abbrechen, jedoch nicht während der Aktivierung.

   Die Integritätsprüfung vor dem Upgrade beginnt. Wenn die Integritätsprüfung vor dem Upgrade erfolgreich besteht, wird die Aktivierung der Dateien fortgesetzt. Sollte die vor-Upgrade-Systemprüfung fehlschlagen, nutzen Sie den Recovery Guru oder wenden Sie sich an den technischen Support, um das Problem zu lösen. Bei einigen Bedingungen empfiehlt Ihnen der technische Support, trotz der Fehler mit dem Upgrade fortzufahren, indem Sie das Kontrollkästchen **Upgrade zulassen** aktivieren.

   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:** um eine Liste der aktualisierten Versionen anzuzeigen, klicken Sie auf **Log speichern**.

   Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `drive_upgrade_log-timestamp.txt`.

Nachdem Sie fertig sind

- Vergewissern Sie sich, dass alle Komponenten auf der Seite Hardware angezeigt werden.
- Überprüfen Sie die neuen Software- und Firmware-Versionen, indem Sie das Dialogfeld Software- und Firmware-Bestandsaufnahme aktivieren (gehen Sie zu Menü:Support[Upgrade Center] und klicken Sie dann auf den Link für **Software- und Firmware-Bestandsaufnahme**).
- Wenn Sie den Controller NVSRAM aktualisiert haben, gehen während der Aktivierung alle benutzerdefinierten Einstellungen, die Sie auf den vorhandenen NVSRAM angewendet haben, verloren. Sie müssen die benutzerdefinierten Einstellungen erneut auf den NVSRAM anwenden, nachdem der Aktivierungsvorgang abgeschlossen ist.

Aktualisieren Sie die Laufwerk-Firmware

Sie können Ihre Festplatten-Firmware aktualisieren, um sicherzustellen, dass Sie über alle neuesten Funktionen und Fehlerbehebungen verfügen.

Bevor Sie beginnen

- Sie haben Ihre Daten mithilfe von Disk-to-Disk Backups, Volume-Kopien (in einer Volume-Gruppe, die nicht von der geplanten Firmware-Aktualisierung betroffen ist) oder einer Remote-Spiegelung gesichert.
- Das Speicherarray hat einen optimalen Status.
- Alle Laufwerke haben einen optimalen Status.
- Auf dem Speicher-Array werden keine Konfigurationsänderungen ausgeführt.
- Wenn die Laufwerke nur offline aktualisieren können, werden die I/O-Aktivitäten aller Volumes, die mit den Laufwerken verbunden sind, angehalten.

Schritte

1. Wählen Sie Menü:Support[Upgrade Center].
2. Laden Sie die neuen Dateien von der Support-Website auf Ihren Management-Client herunter.
3. Klicken Sie unter Laufwerk-Firmware-Upgrade auf **Upgrade starten**.

   Es wird ein Dialogfeld angezeigt, in dem die aktuell verwendeten Laufwerk-Firmware-Dateien aufgelistet werden.

4. Extrahieren Sie die Dateien, die Sie von der Support-Website heruntergeladen haben (entpacken).
5. Klicken Sie auf **Durchsuchen** und wählen Sie die neuen Laufwerk-Firmware-Dateien aus, die Sie von der Support-Website heruntergeladen haben.

   Die Firmware-Dateien des Laufwerks haben einen ähnlichen Dateinamen wie `D_HUC101212CSS600_30602291_MS01_2800_0002` Mit der Erweiterung von `.dlp`.

   Sie können bis zu vier Laufwerk-Firmware-Dateien auswählen, jeweils eine. Wenn mehrere Firmware-Dateien eines Laufwerks mit demselben Laufwerk kompatibel sind, wird ein Dateikonflikt angezeigt. Legen Sie fest, welche Laufwerk-Firmware-Datei Sie für das Upgrade verwenden möchten, und entfernen Sie die

andere.

6. Klicken Sie Auf **Weiter**.

   Das Dialogfeld **Select Drives** wird angezeigt, in dem die Laufwerke aufgeführt werden, die Sie mit den ausgewählten Dateien aktualisieren können.

   Es werden nur kompatible Laufwerke angezeigt.

   Die ausgewählte Firmware für das Laufwerk wird im Bereich der vorgeschlagenen Firmware-Informationen angezeigt. Wenn Sie die Firmware ändern müssen, klicken Sie auf **Zurück**, um zum vorherigen Dialogfeld zurückzukehren.

7. Wählen Sie die Art des Upgrades aus, die Sie durchführen möchten:
   - **Online (Standard)** — zeigt die Laufwerke, die einen Firmware-Download unterstützen können *während das Speicher-Array I/O* verarbeitet. Bei Auswahl dieser Upgrade-Methode müssen Sie die I/O-Vorgänge der zugehörigen Volumes, die diese Laufwerke verwenden, nicht anhalten. Diese Laufwerke werden nacheinander aktualisiert, während das Storage-Array I/O-Operationen zu diesen Laufwerken verarbeitet.
   - **Offline (parallel)** — zeigt die Laufwerke an, die einen Firmware-Download unterstützen können *nur während alle I/O-Aktivitäten angehalten sind* auf beliebigen Volumes, die die Laufwerke verwenden. Bei Auswahl dieser Upgrade-Methode müssen Sie alle I/O-Aktivitäten auf Volumes anhalten, die die Laufwerke verwenden, die Sie aktualisieren. Laufwerke, die keine Redundanz aufweisen, müssen als Offline-Betrieb verarbeitet werden. Diese Anforderung umfasst alle Laufwerke, die mit SSD-Cache, eine RAID 0-Volume-Gruppe oder einen beliebigen Pool oder eine herabgestuften Volume-Gruppe verbunden sind. Das Offline-Upgrade (parallel) ist in der Regel schneller als die Online-Methode (Standard).
8. Wählen Sie in der ersten Spalte der Tabelle das Laufwerk oder die Laufwerke aus, die aktualisiert werden sollen.
9. Klicken Sie auf **Start** und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

   Wenn Sie das Upgrade beenden möchten, klicken Sie auf **Stop**. Alle derzeit ausgeführten Firmware-Downloads abgeschlossen. Alle nicht gestarteten Firmware-Downloads werden abgebrochen.

   > Das Anhalten der Laufwerk-Firmware-Aktualisierung kann zu Datenverlust oder nicht verfügbaren Laufwerken führen.

10. **Optional:** um eine Liste der aktualisierten Versionen anzuzeigen, klicken Sie auf **Log speichern**.

    Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `drive_upgrade_log-timestamp.txt`.

11. Wenn während des Aktualisierungsvorgangs eines der folgenden Fehler auftritt, ergreifen Sie die entsprechende empfohlene Maßnahme.

Fehler und empfohlene Aktionen

Wenn dieser Fehler beim Herunterladen der Firmware auftritt…	Führen Sie dann folgende Schritte aus…
Ausgefallene zugewiesene Laufwerke	Ein Grund für den Fehler könnte sein, dass das Laufwerk nicht über die entsprechende Signatur verfügt. Stellen Sie sicher, dass es sich bei dem betroffenen Laufwerk um ein autorisiertes Laufwerk handelt. Weitere Informationen erhalten Sie vom technischen Support. Stellen Sie beim Austausch eines Laufwerks sicher, dass das Ersatzlaufwerk eine Kapazität hat, die der des ausgefallenen Laufwerks entspricht oder größer ist als das ausgefallene Laufwerk, das Sie ersetzen. Sie können das ausgefallene Laufwerk ersetzen, während das Speicher-Array I/O-Vorgänge erhält
Prüfen Sie das Speicher-Array	• Stellen Sie sicher, dass jedem Controller eine IP-Adresse zugewiesen wurde. • Stellen Sie sicher, dass alle an den Controller angeschlossenen Kabel nicht beschädigt sind. • Stellen Sie sicher, dass alle Kabel fest angeschlossen sind.
Integrierte Hot-Spare-Laufwerke	Diese Fehlerbedingung muss korrigiert werden, bevor Sie die Firmware aktualisieren können. Starten Sie System Manager und beheben Sie das Problem mit dem Recovery Guru.
Unvollständige Volume-Gruppen	Wenn eine oder mehrere Volume-Gruppen oder Disk Pools unvollständig sind, müssen Sie diese Fehlerbedingung korrigieren, bevor Sie die Firmware aktualisieren können. Starten Sie System Manager und beheben Sie das Problem mit dem Recovery Guru.
Exklusive Vorgänge \ (außer Hintergrund-Medien/Paritäts-Scan\), die derzeit auf Volume-Gruppen ausgeführt werden	Wenn ein oder mehrere exklusive Vorgänge ausgeführt werden, müssen die Vorgänge abgeschlossen sein, bevor die Firmware aktualisiert werden kann. Überwachen Sie den Fortschritt des Betriebs mit System Manager.
Fehlende Volumes	Sie müssen den fehlenden Datenträgerzustand korrigieren, bevor die Firmware aktualisiert werden kann. Starten Sie System Manager und beheben Sie das Problem mit dem Recovery Guru.

Wenn dieser Fehler beim Herunterladen der Firmware auftritt…	Führen Sie dann folgende Schritte aus…
Beide Controller befinden sich in einem anderen Zustand als optimal	Einer der Controller des Storage Arrays muss Aufmerksamkeit schenken. Diese Bedingung muss korrigiert werden, bevor die Firmware aktualisiert werden kann. Starten Sie System Manager und beheben Sie das Problem mit dem Recovery Guru.
Falsche Informationen zur Speicherpartition zwischen Controller-Objektgrafiken	Beim Validieren der Daten auf den Controllern ist ein Fehler aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
Die SPM-Überprüfung des Datenbank-Controllers schlägt fehl	Auf einem Controller ist ein Fehler bei der Zuordnung von Speicherpartitionen zur Datenbank aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
Überprüfung der Konfigurationsdatenbank \(Wenn vom Speicher-Array unterstützte Controller-Version\)	Auf einem Controller ist ein Fehler in der Konfigurationsdatenbank aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
MEL-bezogene Prüfungen	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
In den letzten 7 Tagen wurden mehr als 10 DDE-Informations- oder kritische MEL-Ereignisse gemeldet	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
In den letzten 7 Tagen wurden mehr als 2 Seiten 2C kritische MEL-Ereignisse gemeldet	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
In den letzten 7 Tagen wurden mehr als 2 heruntergestuften Drive Channel-kritische MEL-Ereignisse gemeldet	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
Mehr als 4 kritische MEL-Einträge in den letzten 7 Tagen	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

Nachdem Sie fertig sind

Die Aktualisierung der Laufwerk-Firmware ist abgeschlossen. Sie können den normalen Betrieb fortsetzen.

Überprüfen Sie die möglichen Software- und Firmware-Upgrade-Fehler

Fehler können während des Upgrades der Controller-Software oder der Aktualisierung der Laufwerk-Firmware auftreten.

Fehler beim Herunterladen der Firmware	Beschreibung	Empfohlene Maßnahmen
Ausgefallene zugewiesene Laufwerke	Fehler beim Aktualisieren eines zugewiesenen Laufwerks im Speicher-Array.	Ein Grund für den Fehler könnte sein, dass das Laufwerk nicht über die entsprechende Signatur verfügt. Stellen Sie sicher, dass es sich bei dem betroffenen Laufwerk um ein autorisiertes Laufwerk handelt. Weitere Informationen erhalten Sie vom technischen Support. Stellen Sie beim Austausch eines Laufwerks sicher, dass das Ersatzlaufwerk eine Kapazität hat, die der des ausgefallenen Laufwerks entspricht oder größer ist als das ausgefallene Laufwerk, das Sie ersetzen. Sie können das ausgefallene Laufwerk ersetzen, während das Speicher-Array I/O-Vorgänge erhält
Integrierte Hot-Spare-Laufwerke	Wenn das Laufwerk als Hot Spare gekennzeichnet ist und für eine Volume-Gruppe verwendet wird, schlägt der Firmware-Upgrade-Prozess fehl.	Diese Fehlerbedingung muss korrigiert werden, bevor Sie die Firmware aktualisieren können. Starten Sie System Manager und beheben Sie das Problem mit dem Recovery Guru.
Unvollständige Volume-Gruppen	Wenn ein Laufwerk, das Teil einer Volume-Gruppe ist, umgangen, entfernt oder nicht reagiert wird, wird es als unvollständige Volume-Gruppe betrachtet. Eine unvollständige Volume-Gruppe verhindert Firmware-Upgrades.	Wenn eine oder mehrere Volume-Gruppen oder Disk Pools unvollständig sind, müssen Sie diese Fehlerbedingung korrigieren, bevor Sie die Firmware aktualisieren können. Starten Sie System Manager und beheben Sie das Problem mit dem Recovery Guru.
Exklusive Vorgänge (nicht für Medien-/Paritäts-Scan im Hintergrund), die derzeit auf Volume-Gruppen ausgeführt werden	Die Firmware kann nicht aktualisiert werden, wenn exklusive Vorgänge auf einem Volume ausgeführt werden.	Wenn ein oder mehrere exklusive Vorgänge ausgeführt werden, müssen die Vorgänge abgeschlossen sein, bevor die Firmware aktualisiert werden kann. Überwachen Sie den Fortschritt des Betriebs mit System Manager.

Fehler beim Herunterladen der Firmware	Beschreibung	Empfohlene Maßnahmen
Fehlende Volumes	Die Firmware kann nicht aktualisiert werden, wenn ein Volume fehlt.	Sie müssen den fehlenden Datenträgerzustand korrigieren, bevor die Firmware aktualisiert werden kann. Starten Sie System Manager und beheben Sie das Problem mit dem Recovery Guru.
Beide Controller befinden sich in einem anderen Zustand als optimal	Die Firmware kann nicht aktualisiert werden, wenn sich beide Controller in einem anderen Zustand als optimal befinden.	Einer der Controller des Storage Arrays muss Aufmerksamkeit schenken. Diese Bedingung muss korrigiert werden, bevor die Firmware aktualisiert werden kann. Starten Sie System Manager und beheben Sie das Problem mit dem Recovery Guru.
Die SPM-Überprüfung des Datenbank-Controllers schlägt fehl	Firmware kann nicht aktualisiert werden, da die Datenbank für die Speicherpartitionen-Zuordnungen beschädigt ist.	Auf einem Controller ist ein Fehler bei der Zuordnung von Speicherpartitionen zur Datenbank aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
Überprüfung der Konfigurationsdatenbank (sofern von der Controller-Version des Speicherarrays unterstützt)	Firmware kann nicht aktualisiert werden, da die Konfigurationsdatenbank beschädigt ist.	Auf einem Controller ist ein Fehler in der Konfigurationsdatenbank aufgetreten. Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
MEL-bezogene Prüfungen	Die Firmware kann nicht aktualisiert werden, da das Ereignisprotokoll Fehler enthält.	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
In den letzten 7 Tagen wurden mehr als 10 DDE-Informations- oder kritische MEL-Ereignisse gemeldet	Die Firmware kann nicht aktualisiert werden, da in den letzten sieben Tagen mehr als 10 DDE-Informations- oder kritische MEL-Ereignisse gemeldet wurden.	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
In den letzten 7 Tagen wurden mehr als 2 Seiten 2C kritische MEL-Ereignisse gemeldet	Die Firmware kann nicht aktualisiert werden, da in den letzten sieben Tagen mehr als zwei Seiten kritische MEL-Ereignisse auf 2C gemeldet wurden.	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.

Fehler beim Herunterladen der Firmware	Beschreibung	Empfohlene Maßnahmen
In den letzten 7 Tagen wurden mehr als 2 heruntergestuften Drive Channel-kritische MEL-Ereignisse gemeldet	Die Firmware kann nicht aktualisiert werden, da in den letzten sieben Tagen mehr als zwei heruntergestuften wichtigen MEL-Ereignisse im Laufwerkskanal gemeldet wurden.	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
Mehr als 4 kritische MEL-Einträge in den letzten 7 Tagen	Die Firmware kann nicht aktualisiert werden, da in den letzten sieben Tagen mehr als vier kritische Ereignisprotokolleinträge gemeldet werden.	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
Eine gültige Management-IP-Adresse ist erforderlich.	Für diesen Vorgang ist eine gültige Controller-IP-Adresse erforderlich.	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
Der Befehl erfordert eine aktive Management-IP-Adresse für jeden Controller.	Für diesen Vorgang ist für jeden mit dem Speicher-Array verbundenen Controller eine Controller-IP-Adresse erforderlich.	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
Nicht bearbeiteten Download-Dateityp zurückgegeben.	Die angegebene Download-Datei wird nicht unterstützt.	Wenden Sie sich an den technischen Support, um dieses Problem zu lösen.
Beim Hochladen der Firmware ist ein Fehler aufgetreten.	Fehler beim Herunterladen der Firmware, da der Controller die Anforderung nicht verarbeiten kann. Überprüfen Sie, ob das Speicher-Array optimal ist, und wiederholen Sie den Vorgang.	Falls dieser Fehler erneut auftritt, nachdem überprüft wurde, ob das Speicher-Array optimal ist, wenden Sie sich an den technischen Support, um dieses Problem zu beheben.
Während der Firmware-Aktivierung ist ein Fehler aufgetreten.	Die Firmware-Aktivierung ist fehlgeschlagen, da der Controller die Anforderung nicht verarbeiten kann. Überprüfen Sie, ob das Speicher-Array optimal ist, und wiederholen Sie den Vorgang.	Falls dieser Fehler erneut auftritt, nachdem überprüft wurde, ob das Speicher-Array optimal ist, wenden Sie sich an den technischen Support, um dieses Problem zu beheben.
Zeitüberschreitung beim Warten auf Neustart des Controllers {0} erreicht.	Die Managementsoftware kann nach einem Neubooten keine Verbindung mit dem Controller {0} herstellen. Überprüfen Sie, ob ein einsatzbereiter Verbindungspfad zum Speicher-Array vorhanden ist, und versuchen Sie den Vorgang erneut, falls der Vorgang nicht erfolgreich abgeschlossen wurde.	Falls dieser Fehler erneut auftritt, nachdem überprüft wurde, ob das Speicher-Array optimal ist, wenden Sie sich an den technischen Support, um dieses Problem zu beheben.

Einige dieser Bedingungen können Sie mit dem Recovery Guru in System Manager korrigieren. Unter bestimmten Bedingungen müssen Sie sich jedoch unter Umständen an den technischen Support wenden. Die Informationen zum Herunterladen der neuesten Controller-Firmware finden Sie im Speicher-Array. Diese Information hilft dem technischen Support, die Fehlerbedingungen zu verstehen, die ein Firmware-Upgrade und -Download verhindern.

FAQs

Welche Daten sammle ich?

Die AutoSupport-Funktion und die manuelle Support-Datenerfassung bieten Möglichkeiten zum Erfassen von Daten in einem Kunden-Support Bundle zur Remote-Fehlerbehebung und Problemanalyse durch den technischen Support.

Das Customer Support Bundle sammelt alle Arten von Informationen zum Storage Array in einer einzigen komprimierten Datei. Die erfassten Informationen umfassen physische Konfiguration, logische Konfiguration, Versionsinformationen, Ereignisse, Log-Dateien, Und Performance-Daten. Die Informationen werden nur vom technischen Support verwendet, um Probleme mit dem Storage-Array zu lösen.

Was zeigt mir unlesbare Sektoren Daten?

Sie können detaillierte Daten über unlesbare Sektoren anzeigen, die auf den Laufwerken in Ihrem Speicher-Array erkannt wurden.

Das unlesbare Sektoren-Log zeigt zuerst den zuletzt unlesbaren Sektor an. Das Protokoll enthält die folgenden Informationen zu den Volumes, die die unlesbaren Sektoren enthalten. Die Felder sind sortischbar.

Feld	Beschreibung
Betroffenes Volume	Zeigt die Beschriftung des Volumens an. Wenn ein fehlendes Volume unlesbare Sektoren enthält, wird für das fehlende Volume die World Wide Identifier angezeigt.
Logical Unit Number (LUN)	Zeigt die LUN für das Volume. Wenn auf dem Volume keine LUN vorhanden ist, wird im Dialogfeld „NA“ angezeigt.
Zugewiesen Zu	Zeigt die Hosts oder Host-Cluster, die Zugriff auf das Volume haben. Wenn ein Host, Host-Cluster oder sogar ein Standardcluster auf das Volume nicht zugreifen kann, wird im Dialogfeld „NA“ angezeigt.

Um weitere Informationen zu den unlesbaren Sektoren zu erhalten, klicken Sie auf das Pluszeichen (+) neben einem Volume.

Feld	Beschreibung
Datum/Uhrzeit	Zeigt das Datum und die Uhrzeit an, zu der der unlesbare Sektor erkannt wurde.
Logische Block-Adresse Des Volume	Zeigt die logische Blockadresse (LBA) des Volumes an.

Feld	Beschreibung
Position Des Laufwerks	Zeigt das Festplatten-Shelf, die Schublade (wenn Ihr Festplatten-Shelf Schubladen aufweist) und den Auflageort des Laufwerks an.
Logische Blockadresse Des Laufwerks	Zeigt die LBA des Laufwerks an.
Fehlertyp	Zeigt einen der folgenden Fehlertypen an: • **Physical** — Ein Fehler beim physischen Medium. • **Logisch** — Ein Lesefehler an anderer Stelle im Stripe, der unlesbare Daten verursacht. Zum Beispiel ein unlesbarer Sektor aufgrund von Medienfehlern an anderer Stelle im Volumen. • * Inkonsistente* — inkonsistente Redundanzdaten. • **Data Assurance** — Ein Data Assurance-Fehler.

Was ist ein Gesundheitsbild?

Ein Systemzustand-Image ist ein Rohdaten-Dump des Prozessorspeichers des Controllers, mit dem der technische Support ein Problem mit einem Controller diagnostizieren kann.

Die Firmware generiert automatisch ein Systemzustand-Image, wenn bestimmte Fehler erkannt werden. Bei bestimmten Fehlerbehebungsszenarios kann der technische Support anfordern, dass Sie die Datei für das Systemzustand abrufen und an sie senden.

Was tun die AutoSupport-Funktionen?

Die AutoSupport Funktion besteht aus drei separaten Funktionen, die separat aktiviert werden können.

- **Basic AutoSupport** — ermöglicht Ihrem Speicherarray die automatische Erfassung und Übermittlung von Daten an den technischen Support.
- **AutoSupport OnDemand** — ermöglicht technischen Support, bei Bedarf eine erneute Übertragung eines früheren AutoSupport Dispatch zur Fehlerbehebung anzufordern. Sämtliche Übertragungen werden vom Storage Array aus initiiert, nicht vom AutoSupport Server. Das Storage Array überprüft in regelmäßigen Abständen mit dem AutoSupport Server, um zu ermitteln, ob es noch ausstehende Neuübertragungsanfragen gibt und entsprechend darauf reagiert.
- **Ferndiagnose** — ermöglicht technischen Support, bei Bedarf einen neuen, aktuellen AutoSupport-Dispatch zur Fehlerbehebung anzufordern. Sämtliche Übertragungen werden vom Storage Array aus initiiert, nicht vom AutoSupport Server. Das Storage-Array überprüft in regelmäßigen Abständen mit dem AutoSupport Server, um zu ermitteln, ob ausstehende neue Anfragen zu bestehen und entsprechend darauf zu reagieren.

Welche Datentypen werden über die AutoSupport Funktion erfasst?

Die AutoSupport-Funktion enthält drei standardmäßige Entsendungstypen: Ereignispatches, geplante Dispatches sowie On-Demand- und Remote-Diagnose-

Patches.

Die AutoSupport-Daten enthalten keine Benutzerdaten.

- **Event-Entsendungen**

  Wenn Ereignisse auf dem System auftreten, die über proaktive Benachrichtigungen an den technischen Support verfügen, sendet die AutoSupport Funktion automatisch einen Event-ausgelösten Dispatch.

  - Wird gesendet, wenn ein Support-Ereignis auf dem verwalteten Speicher-Array auftritt.
  - In diesem Service wird eine umfassende Übersicht über die Ereignisse zum Zeitpunkt des Ereignisses des Storage-Arrays erstellt.

- **Geplante Entsendungen**

  Die AutoSupport-Funktion sendet automatisch mehrere Entsendungen nach einem regelmäßigen Zeitplan.

  - **Tägliche Dispatches** — wird in einem vom Benutzer konfigurierbaren Zeitintervall einmal täglich gesendet. Enthält die aktuellen Systemereignisprotokolle und Performance-Daten.
  - **Wöchentlich Dispatches** — wird einmal wöchentlich in einem vom Benutzer konfigurierbaren Zeitintervall und Tag gesendet. Einschließlich Konfigurations- und Systemstatus-Informationen.

- **AutoSupport OnDemand und Remote Diagnostics Dispatches**
  - **AutoSupport OnDemand** — ermöglicht technischen Support, bei Bedarf eine erneute Übertragung eines früheren AutoSupport Dispatch zur Fehlerbehebung anzufordern. Sämtliche Übertragungen werden vom Storage Array aus initiiert, nicht vom AutoSupport Server. Das Storage Array überprüft in regelmäßigen Abständen mit dem AutoSupport Server, um zu ermitteln, ob es noch ausstehende Neuübertragungsanfragen gibt und entsprechend darauf reagiert.
  - **Ferndiagnose** — ermöglicht technischen Support, bei Bedarf einen neuen, aktuellen AutoSupport-Dispatch zur Fehlerbehebung anzufordern. Sämtliche Übertragungen werden vom Storage Array aus initiiert, nicht vom AutoSupport Server. Das Storage-Array überprüft in regelmäßigen Abständen mit dem AutoSupport Server, um zu ermitteln, ob ausstehende neue Anfragen zu bestehen und entsprechend darauf zu reagieren.

Wie konfiguriere ich die Bereitstellungsmethode für die AutoSupport-Funktion?

Die AutoSupport-Funktion unterstützt die Protokolle HTTPS und SMTP zur Bereitstellung von AutoSupport-Dispatches an den technischen Support.

Bevor Sie beginnen

- Die AutoSupport-Funktion muss aktiviert sein. Sie sehen, ob die Funktion auf der Seite AutoSupport aktiviert ist.
- Ein DNS-Server muss in Ihrem Netzwerk installiert und konfiguriert sein. Die DNS-Server-Adresse muss in System Manager konfiguriert sein (diese Aufgabe ist auf der Seite Hardware verfügbar).

Über diese Aufgabe

Überprüfen Sie die verschiedenen Protokolle:

- **HTTPS** — ermöglicht es Ihnen, sich direkt mit dem Ziel-Server des technischen Supports über HTTPS zu verbinden. Wenn Sie AutoSupport OnDemand oder Remote-Diagnose aktivieren möchten, muss die AutoSupport-Bereitstellungsmethode auf HTTPS gesetzt werden.
- **E-Mail** — ermöglicht Ihnen, einen E-Mail-Server als Liefermethode für das Senden von AutoSupport-

Entsendungen zu verwenden.

Unterschiede zwischen den Methoden HTTPS und Email. Die E-Mail-Versandmethode, die SMTP verwendet, weist einige wichtige Unterschiede zur HTTPS-Bereitstellungsmethode auf. Erstens ist die Größe der Dispatches für die E-Mail-Methode auf 5 MB begrenzt, was bedeutet, dass einige ASUP Datensammlungen nicht versendet werden. Zweitens ist die AutoSupport OnDemand-Funktion nur für die HTTPS-Bereitstellungsmethode verfügbar.

Schritte

1. Wählen Sie MENU:Support[Support Center > AutoSupport].
2. Wählen Sie **AutoSupport-Bereitstellungsmethode konfigurieren**.

   Es wird ein Dialogfeld angezeigt, in dem die Versandmethoden aufgeführt sind.

3. Wählen Sie die gewünschte Liefermethode aus, und wählen Sie dann die Parameter für diese Bereitstellungsmethode aus. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie HTTPS ausgewählt haben, wählen Sie einen der folgenden Bereitstellungsparameter aus:
     - **Direkt** — dieser Lieferparameter ist die Standardauswahl. Wenn Sie diese Option wählen, können Sie mithilfe des HTTPS-Protokolls eine direkte Verbindung zum technischen Supportsystem des Ziels herstellen.
     - **Über Proxy Server** — mit dieser Option können Sie die HTTP Proxy-Serverdetails angeben, die für die Verbindung mit dem technischen Zielunterstützungssystem erforderlich sind. Sie müssen die Host-Adresse und die Portnummer angeben. Sie müssen jedoch nur die Details zur Host-Authentifizierung (Benutzername und Passwort) eingeben, falls erforderlich.
     - **Über Proxy Auto-Configuration Script (PAC)** — Geben Sie den Speicherort einer PAC-Skriptdatei (Proxy Auto-Configuration) an. Mit einer PAC-Datei kann das System automatisch den entsprechenden Proxyserver auswählen, um eine Verbindung mit dem technischen Zielunterstützungssystem herzustellen.
   - Wenn Sie E-Mail ausgewählt haben, geben Sie die folgenden Informationen ein:
     - Die E-Mail-Server-Adresse als vollständig qualifizierter Domain-Name, IPv4-Adresse oder IPv6-Adresse.
     - Die E-Mail-Adresse, die im Feld „von“ der AutoSupport-Entsendmail angezeigt wird.
     - **Optional; wenn Sie einen Konfigurationstest durchführen möchten.** die E-Mail-Adresse, an die eine Bestätigung gesendet wird, wenn das AutoSupport-System den Testversand erhält.
     - Wenn Sie Nachrichten verschlüsseln möchten, wählen Sie **SMTPS** oder **STARTTLS** für den Verschlüsselungstyp aus, und wählen Sie dann die Portnummer für verschlüsselte Nachrichten aus. Wählen Sie andernfalls * Keine*.
     - Geben Sie bei Bedarf einen Benutzernamen und ein Kennwort für die Authentifizierung mit dem ausgehenden Absender und dem E-Mail-Server ein.
4. Klicken Sie auf **Testkonfiguration**, um die Verbindung zum Server des technischen Supports mit den angegebenen Lieferparametern zu testen. Wenn Sie die AutoSupport On-Demand-Funktion aktiviert haben, testet das System auch die Verbindung für die AutoSupport OnDemand-Entsendungsbereitstellung.

   Wenn der Konfigurationstest fehlschlägt, überprüfen Sie Ihre Konfigurationseinstellungen, und führen Sie den Test erneut aus. Wenden Sie sich an den technischen Support, wenn der Test weiterhin fehlschlägt.

5. Klicken Sie Auf **Speichern**.

Was sind Konfigurationsdaten?

Wenn Sie Konfigurationsdaten erfassen auswählen, speichert das System den aktuellen Status der RAID-Konfigurationsdatenbank.

Die RAID-Konfigurationsdatenbank umfasst alle Daten für Volume-Gruppen und Festplatten-Pools auf dem Controller. Die Funktion Konfigurationsdaten erfassen speichert die gleichen Informationen wie der CLI-Befehl für `save storageArray dbmDatabase`.

Was muss ich vor einem Upgrade der SANtricity OS Software beachten?

Bevor Sie die Software und Firmware des Controllers aktualisieren, sollten Sie diese Elemente beachten.

- Sie haben das Dokument und das gelesen `readme.txt` Datei und haben festgestellt, dass Sie das Upgrade durchführen möchten.
- Sie wissen, ob Sie Ihre IOM-Firmware aktualisieren möchten.

  In der Regel sollten Sie alle Komponenten gleichzeitig aktualisieren. Sie können jedoch entscheiden, die IOM-Firmware nicht zu aktualisieren, wenn Sie sie nicht als Teil des Upgrades der SANtricity OS Controller Software aktualisieren möchten oder wenn Sie vom technischen Support aufgefordert wurden, Ihre IOM-Firmware herunterzustufen (Sie können nur die Firmware über die Befehlszeilenschnittstelle herunterstufen).

- Sie wissen, ob Sie die NVSRAM-Controller-Datei aktualisieren möchten.

  In der Regel sollten Sie alle Komponenten gleichzeitig aktualisieren. Sie entscheiden sich jedoch möglicherweise nicht, die NVSRAM-Controller-Datei zu aktualisieren, wenn Ihre Datei entweder gepatcht wurde oder eine benutzerdefinierte Version ist und Sie sie nicht überschreiben möchten.

- Sie wissen, ob Sie jetzt oder später aktivieren möchten.

  Gründe für eine spätere Aktivierung sind u. a.:

  - **Tageszeit** — die Aktivierung der Software und Firmware kann eine lange Zeit dauern, so dass Sie möglicherweise warten möchten, bis I/O-Lasten leichter sind. Der Controller-Failover während der Aktivierung, sodass die Performance möglicherweise niedriger ist als üblich, bis das Upgrade abgeschlossen ist.
  - **Paketyp** — möglicherweise möchten Sie die neue Software und Firmware auf einem Speicher-Array testen, bevor Sie die Dateien auf anderen Speicher-Arrays aktualisieren.

Diese Komponenten sind Bestandteil des Upgrades der SANtricity OS Controller Software:

- **Management Software** — System Manager ist die Software, die das Speicher-Array verwaltet.
- **Controller-Firmware** — Controller-Firmware verwaltet den I/O zwischen Hosts und Volumes.
- **Controller NVSRAM** — Controller NVSRAM ist eine Controller-Datei, die die Standardeinstellungen für die Controller angibt.
- **IOM-Firmware** — die I/O-Modul-Firmware (IOM) verwaltet die Verbindung zwischen einem Controller und einem Festplatten-Shelf. Es überwacht auch den Status der Komponenten.
- **Supervisor Software** — Supervisor Software ist die virtuelle Maschine auf einem Controller, in dem die Software ausgeführt wird.

Im Rahmen des Upgrades muss möglicherweise auch der Multipath-/Failover-Treiber und/oder der HBA-Treiber des Hosts aktualisiert werden, damit der Host mit den Controllern korrekt interagieren kann.

Informationen zum ermitteln, ob dies der Fall ist, finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Wenn Ihr Storage-Array nur einen Controller enthält oder kein Multipath-Treiber installiert ist, beenden Sie die I/O-Aktivität 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.

Nehmen Sie während des Upgrades keine Änderungen am Storage Array vor.

Was muss ich wissen, bevor ich die automatische EAM-Synchronisierung unterhalte?

Das Aussetzung der automatischen Synchronisierung von IOM verhindert, dass die IOM-Firmware beim nächsten Upgrade einer SANtricity OS-Controller-Software aktualisiert wird.

Normalerweise werden Controller-Software und IOM-Firmware als Bundle aktualisiert. Sie können die automatische EAM-Synchronisierung unterbrechen, wenn Sie über einen speziellen Build der IOM-Firmware verfügen, den Sie in Ihrem Gehäuse erhalten möchten. Andernfalls werden Sie beim nächsten Controller-Software-Upgrade auf die IOM-Firmware, die mit der Controller-Software gebündelt ist, zurückgesetzt.

Warum läuft mein Firmware-Upgrade so langsam voran?

Der Fortschritt des Firmware-Upgrades hängt von der Gesamtlast des Systems ab.

Sollte während eines Online-Upgrades der Laufwerk-Firmware ein Volume-Transfer während des schnellen Rekonstruktionsvorgangs durchgeführt werden, initiiert das System eine vollständige Rekonstruktion für das übertragene Volume. Dieser Vorgang kann sehr viel Zeit in Anspruch nehmen. Die tatsächliche komplette Rekonstruktionszeit hängt von mehreren Faktoren ab, einschließlich der Menge der I/O-Aktivitäten während des Rekonstruktionsvorgangs, der Anzahl der Laufwerke in der Volume-Gruppe, der Einstellung für die Priorität bei der Wiederherstellung und der Laufwerk-Performance.

Was muss ich vor dem Aktualisieren der Laufwerk-Firmware beachten?

Achten Sie vor dem Aktualisieren der Laufwerk-Firmware auf diese Elemente.

- Als Vorsichtsmaßnahme erstellen Sie Ihre Daten mittels Disk-to-Disk Backup, Volume-Kopie (in einer Volume-Gruppe, die nicht von der geplanten Firmware-Aktualisierung betroffen ist) oder einer Remote-Spiegelung.
- Möglicherweise möchten Sie nur einige wenige Laufwerke aktualisieren, um das Verhalten der neuen Firmware zu testen, um sicherzustellen, dass sie ordnungsgemäß funktioniert. Wenn die neue Firmware ordnungsgemäß funktioniert, aktualisieren Sie die verbleibenden Laufwerke.
- Wenn Laufwerke ausgefallen sind, beheben Sie sie, bevor Sie das Firmware-Upgrade starten.
- Wenn die Laufwerke offline aktualisiert werden können, stoppen Sie die I/O-Aktivität aller Volumes, die mit den Laufwerken verbunden sind. Wenn die I/O-Aktivität angehalten ist, können keine Konfigurationsvorgänge für diese Volumes durchgeführt werden.
- Entfernen Sie während des Upgrades der Laufwerk-Firmware keine Laufwerke.
- Nehmen Sie während des Upgrades der Laufwerk-Firmware keine Konfigurationsänderungen am

Speicher-Array vor.

Wie wähle ich die Art des Upgrades aus?

Je nach Status des Pools oder der Volume-Gruppe wählen Sie die Art des Upgrades, die auf dem Laufwerk ausgeführt werden soll.

- **Online**

  Wenn der Pool oder die Volume-Gruppe Redundanz unterstützt und optimal ist, können Sie die Online-Methode verwenden, um die Festplatten-Firmware zu aktualisieren. Die Online-Methode lädt Firmware *herunter, während das Speicherarray I/O* zu den zugehörigen Volumes verarbeitet, die diese Laufwerke verwenden. Sie müssen die I/O-Vorgänge für die zugehörigen Volumes, die diese Laufwerke verwenden, nicht anhalten. Diese Laufwerke werden nacheinander auf die Volumes aktualisiert, die mit den Laufwerken verbunden sind. Wenn das Laufwerk einem Pool oder einer Volume-Gruppe nicht zugewiesen ist, kann seine Firmware über die Online- oder Offline-Methode aktualisiert werden. Die Systemleistung kann beeinträchtigt werden, wenn Sie die Online-Methode zur Aktualisierung der Laufwerk-Firmware verwenden.

- **Offline**

  Wenn der Pool oder die Volume-Gruppe keine Redundanz unterstützt (RAID 0) oder sich beeinträchtigt, müssen Sie die Offline-Methode verwenden, um die Laufwerk-Firmware zu aktualisieren. Die Offline-Methode führt ein Upgrade der Firmware _nur durch, während alle I/O-Aktivitäten zu den zugehörigen Volumes, die diese Laufwerke verwenden, angehalten werden. Sie müssen alle I/O-Vorgänge für alle zugehörigen Volumes beenden, die diese Laufwerke verwenden. Wenn das Laufwerk einem Pool oder einer Volume-Gruppe nicht zugewiesen ist, kann seine Firmware durch die Online- oder Offline-Methode aktualisiert werden.

Management mehrerer Arrays mit SANtricity Unified Manager 7

Hauptschnittstelle

Übersicht über die SANtricity Unified Manager Schnittstelle

SANtricity Unified Manager ist eine webbasierte Schnittstelle, mit der Sie mehrere Storage Arrays in einer Ansicht managen können.

Hauptseite

Wenn Sie sich bei Unified Manager anmelden, öffnet sich die Hauptseite zu **Verwalten - Alle**. Auf dieser Seite können Sie eine Liste der erkannten Speicher-Arrays in Ihrem Netzwerk durchblättern, ihren Status anzeigen und Vorgänge auf einem einzelnen Array oder einer Gruppe von Arrays durchführen.

Navigationsleiste rechts in der Seitenleiste

Die Funktionen von Unified Manager können über die Navigationsleiste in der Seitenleiste aufgerufen werden.

Werden	Beschreibung
Managen	Erkennung von Speicher-Arrays im Netzwerk, Starten von SANtricity System Manager für ein Array, Importieren von Einstellungen von einem Array in mehrere Arrays und Verwalten von Array-Gruppen Aktivieren Sie die Kontrollkästchen neben den Array-Namen, um Vorgänge für sie auszuführen, z. B. das Importieren von Einstellungen und das Erstellen von Array-Gruppen. Die Ellipsen am Ende jeder Zeile bieten ein Inline-Menü für Operationen auf einem einzelnen Array, wie z. B. Umbenennen.
Betrieb	Zeigen Sie den Fortschritt von Batch-Operationen an, z. B. den Import von Einstellungen von einem Array in ein anderes. Einige Vorgänge sind nicht verfügbar, wenn ein Speicherarray einen nicht optimalen Status hat.
Zertifikatmanagement	Verwalten von Zertifikaten zur Authentifizierung zwischen Browsern und Clients.
Zugriffsmanagement	Einrichtung der Benutzerauthentifizierung für die Unified Manager Schnittstelle
Unterstützung	Optionen für technischen Support, Ressourcen und Ansprechpartner

Schnittstelleneinstellungen und Hilfe

Oben rechts in der Benutzeroberfläche können Sie auf die Hilfe und andere Dokumentation zugreifen. Sie können auch auf Verwaltungsoptionen zugreifen, die über das Dropdown-Menü neben Ihrem Anmeldenamen verfügbar sind.

Benutzeranmeldungen und Passwörter

Der aktuelle Benutzer, der am System angemeldet ist, wird oben rechts auf der Schnittstelle angezeigt.

Weitere Informationen zu Benutzern und Kennwörtern finden Sie unter:

- "Legen Sie den Schutz des Admin-Passworts fest"
- "Ändern Sie das Admin-Passwort"
- "Passwörter für lokale Benutzerprofile ändern"

Unterstützte Browser

Auf SANtricity Unified Manager kann über verschiedene Browsertypen zugegriffen werden.

Die folgenden Browser und Versionen werden unterstützt.

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

Der Web Services Proxy muss installiert und für den Browser verfügbar sein.

Legen Sie den Schutz des Admin-Passworts fest

Sie müssen SANtricity Unified Manager mit einem Administratorkennwort konfigurieren, um ihn vor unbefugtem Zugriff zu schützen.

Admin-Passwort und Benutzerprofile

Wenn Sie Unified Manager zum ersten Mal starten, werden Sie aufgefordert, ein Administratorpasswort festzulegen. Jeder Benutzer mit dem Admin-Passwort kann Konfigurationsänderungen an den Speicher-Arrays vornehmen.

Zusätzlich zum Admin-Passwort enthält die Unified Manager-Schnittstelle vorkonfigurierte Benutzerprofile mit einer oder mehreren Rollen, die ihnen zugeordnet sind. Weitere Informationen finden Sie unter "Funktionsweise von Access Management".

Die Benutzer und Zuordnungen können nicht geändert werden. Es können nur Passwörter geändert werden. Informationen zum Ändern von Passwörtern finden Sie unter:

- "Ändern Sie das Admin-Passwort"
- "Passwörter für lokale Benutzerprofile ändern"

Session-Timeouts

Die Software fordert Sie zur Eingabe des Passworts nur einmal während einer einzigen Verwaltungssitzung auf. Eine Sitzung läuft nach 30 Minuten Inaktivität standardmäßig aus. Zu diesem Zeitpunkt müssen Sie das Passwort erneut eingeben. Wenn ein anderer Benutzer von einem anderen Management-Client auf die Software zugreift und das Passwort während der Sitzung ändert, werden Sie beim nächsten Versuch eines Konfigurationsvorgangs oder einer Ansicht aufgefordert, ein Passwort einzugeben.

Aus Sicherheitsgründen können Sie versuchen, ein Passwort nur fünf Mal einzugeben, bevor die Software den Status „Sperre“ eingibt. In diesem Zustand lehnt die Software nachfolgende Passwortversuche ab. Sie müssen 10 Minuten warten, um den Status „Normal“ zurückzusetzen, bevor Sie erneut versuchen, ein Passwort einzugeben.

Sie können Sitzungszeitausfälle anpassen oder Sitzungszeitausfälle komplett deaktivieren. Weitere Informationen finden Sie unter "Verwalten von Sitzungszeitungen".

Ändern Sie das Admin-Passwort

Sie können das Admin-Passwort ändern, das für den Zugriff auf SANtricity Unified Manager verwendet wird.

Bevor Sie beginnen

- Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-Berechtigungen enthält.
- Sie müssen das aktuelle Admin-Passwort kennen.

Über diese Aufgabe

Beachten Sie bei der Auswahl eines Passworts die folgenden Richtlinien:

- Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt.
- Nachgestellte Leerzeichen werden nicht aus Kennwörtern entfernt, wenn sie gesetzt sind. Achten Sie darauf, Leerzeichen einzugeben, wenn diese im Passwort enthalten waren.
- Um die Sicherheit zu erhöhen, verwenden Sie mindestens 15 alphanumerische Zeichen, und ändern Sie das Passwort häufig.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
3. Wählen Sie den **admin**-Benutzer aus der Tabelle aus.

   Die Schaltfläche Kennwort ändern steht zur Verfügung.

4. Wählen Sie **Passwort Ändern**.

   Das Dialogfeld Kennwort ändern wird geöffnet.

5. Wenn für lokale Benutzerpasswörter keine Mindestkennwortlänge festgelegt ist, aktivieren Sie das Kontrollkästchen, damit der Benutzer ein Kennwort für den Zugriff auf das System eingeben muss.
6. Geben Sie das neue Passwort in die beiden Felder ein.
7. Geben Sie Ihr lokales Administratorpasswort ein, um diesen Vorgang zu bestätigen, und klicken Sie dann auf **Ändern**.

Verwalten von Sitzungszeitungen

Sie können Timeouts für SANtricity Unified Manager konfigurieren, sodass Benutzer inaktive Sitzungen nach einer bestimmten Zeit getrennt werden.

Über diese Aufgabe

Standardmäßig beträgt das Sitzungszeitlimit für Unified Manager 30 Minuten. Sie können diese Zeit anpassen oder Sitzungszeitausfälle ganz deaktivieren.

> Wenn Access Management unter Verwendung der in das Array integrierten SAML-Funktionen (Security Assertion Markup Language) konfiguriert wird, kann es zu einer Sitzungszeitüberschreitung kommen, wenn die SSO-Sitzung des Benutzers die maximale Grenze erreicht. Dies kann vor dem Timeout der System Manager-Sitzung auftreten.

Schritte

1. Wählen Sie in der Menüleiste den Dropdown-Pfeil neben Ihrem Benutzernamen aus.
2. Wählen Sie **Zeitüberschreitung der Sitzung aktivieren/deaktivieren**.

   Das Dialogfeld „Session-Timeout aktivieren/deaktivieren“ wird geöffnet.

3. Verwenden Sie die Spinner-Regler, um die Zeit in Minuten zu erhöhen oder zu verringern.

   Die minimale Zeitüberschreitung, die Sie einstellen können, beträgt 15 Minuten.

   > Deaktivieren Sie zum Deaktivieren der Sitzungszeitzeiten das Kontrollkästchen **Zeitdauer festlegen…**.

4. Klicken Sie Auf **Speichern**.

Storage-Arrays durchführt

Übersicht über die Bestandsaufnahme

Zum Managen von Storage-Ressourcen müssen Sie zuerst die Storage-Arrays im Netzwerk erkennen.

Wie entdecke ich Arrays?

Verwenden Sie die Seite Hinzufügen/Entdecken, um die zu verwaltenden Speicher-Arrays im Netzwerk Ihres Unternehmens zu suchen und hinzuzufügen. Sie können mehrere Arrays ermitteln oder ein einziges Array erkennen. Dazu geben Sie Netzwerk-IP-Adressen ein, und Unified Manager versucht dann individuelle Verbindungen zu jeder IP-Adresse in diesem Bereich.

Weitere Informationen:

- "Überlegungen bei der Array-Ermittlung"
- "Erkennung mehrerer Storage-Arrays"
- "Erkennen Sie ein einzelnes Array"

Wie managt ich Arrays?

Nachdem Sie Arrays entdeckt haben, gehen Sie zur Seite **Verwalten - Alle**. Auf dieser Seite können Sie eine Liste der erkannten Speicher-Arrays in Ihrem Netzwerk durchblättern, ihren Status anzeigen und Vorgänge auf einem einzelnen Array oder einer Gruppe von Arrays durchführen.

Wenn Sie ein einzelnes Array verwalten möchten, können Sie es auswählen und System Manager öffnen.

Weitere Informationen:

- "Überlegungen für den Zugriff auf System Manager"
- "Management eines individuellen Storage Arrays"
- "Anzeigen des Status des Speicherarrays"

Konzepte

Überlegungen bei der Array-Ermittlung

Bevor SANtricity Unified Manager Storage-Ressourcen anzeigen und verwalten kann, muss er die Storage-Arrays ermitteln, die Sie im Netzwerk Ihres Unternehmens managen möchten. Sie können mehrere Arrays ermitteln oder ein einziges Array erkennen.

Erkennung mehrerer Storage-Arrays

Wenn Sie mehrere Arrays ermitteln möchten, geben Sie einen Netzwerk-IP-Adressbereich ein, und Unified Manager versucht dann individuelle Verbindungen zu jeder IP-Adresse in diesem Bereich. Jedes erfolgreich erreichte Speicher-Array wird auf der Seite „Entdecken“ angezeigt und kann Ihrer Management-Domäne hinzugefügt werden.

Erkennen eines einzelnen Speicher-Arrays

Wenn Sie ein einzelnes Array ermitteln möchten, geben Sie für einen der Controller im Speicher-Array die einzelne IP-Adresse ein, und das individuelle Speicher-Array wird hinzugefügt.

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

Benutzeranmeldeinformationen

Im Rahmen des Erkennungsvorgangs müssen Sie für jedes Speicherarray, das Sie hinzufügen möchten, das Administratorpasswort angeben.

Zertifikate für Webservices

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

- * Vertrauenswürdige Zertifikate*

Bei Arrays, die von Unified Manager entdeckt wurden, müssen Sie möglicherweise zusätzliche vertrauenswürdige Zertifikate installieren, die von der Zertifizierungsstelle bereitgestellt werden.

Verwenden Sie die Schaltfläche **Import**, um diese Zertifikate zu importieren. Wenn Sie zuvor mit diesem Array verbunden haben, sind ein oder beide Controller-Zertifikate entweder abgelaufen, annulliert oder fehlen ein Stammzertifikat oder ein Zwischenzertifikat in der Zertifikatkette. Sie müssen das abgelaufene oder widersetzte Zertifikat ersetzen oder das fehlende Stammzertifikat oder Zwischenzertifikat hinzufügen, bevor Sie das Speicher-Array verwalten.

- **Selbstsignierte Zertifikate**

  Es können auch selbstsignierte Zertifikate verwendet werden. Wenn der Administrator versucht, Arrays zu ermitteln, ohne signierte Zertifikate zu importieren, zeigt Unified Manager ein Fehlerdialogfeld an, in dem der Administrator das selbstsignierte Zertifikat akzeptieren kann. Das selbstsignierte Zertifikat des Speicher-Arrays wird als vertrauenswürdig gekennzeichnet und das Speicher-Array wird Unified Manager hinzugefügt.

  Wenn Sie den Verbindungen zum Speicher-Array nicht vertrauen, wählen Sie **Abbrechen** und validieren Sie die Sicherheitszertifikatstrategie des Speicher-Arrays, bevor Sie das Speicher-Array zu Unified Manager hinzufügen.

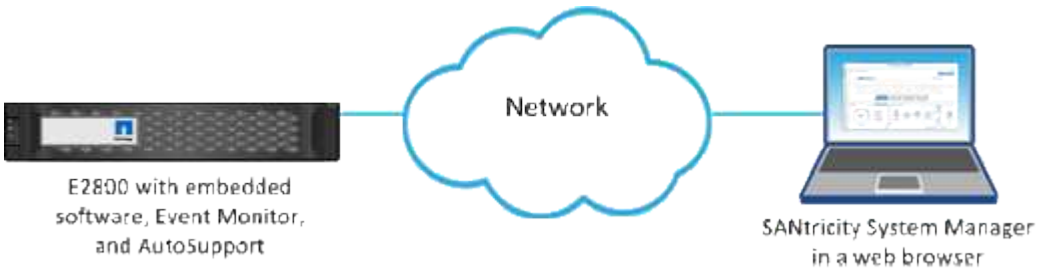
Überlegungen für den Zugriff auf SANtricity System Manager

Sie wählen ein oder mehrere Speicher-Arrays aus und öffnen SANtricity System Manager mit der Option Start, wenn Sie Speicher-Arrays konfigurieren und verwalten möchten.

System Manager ist eine eingebettete Applikation auf den Controllern, die über einen Ethernet-Management-Port mit dem Netzwerk verbunden ist. Es umfasst alle Array-basierten Funktionen.

Um auf System Manager zugreifen zu können, müssen Sie Folgendes haben:

- Eines der hier aufgeführten Array-Modelle: "E-Series Hardware im Überblick"
- Eine Out-of-Band-Verbindung zu einem Netzwerk-Management-Client mit einem Webbrowser.



Arrays erkennen

Erkennung mehrerer Storage-Arrays

Sie erkennen mehrere Arrays, um alle Speicher-Arrays im Subnetz zu erkennen, in dem sich der Verwaltungsserver befindet, und um automatisch die ermittelten Arrays zu Ihrer Verwaltungsdomäne hinzuzufügen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das die Berechtigungen für den Sicherheitsadministrator enthält.
- Das Speicher-Array muss ordnungsgemäß eingerichtet und konfiguriert sein.
- Passwörter für das Storage-Array müssen mithilfe der Kachel „System Manager Access Management“ eingerichtet werden.
- Um nicht vertrauenswürdige Zertifikate zu lösen, müssen Sie vertrauenswürdige Zertifikatdateien von einer Zertifizierungsstelle (CA) haben, und die Zertifikatdateien sind auf Ihrem lokalen System verfügbar.

Das Erkennen von Arrays ist ein mehrstufiges Verfahren.

Schritt 1: Geben Sie die Netzwerkadresse ein

Sie geben einen Netzwerkaddress Range ein, um im lokalen Subnetzwerk zu suchen. Jedes erfolgreich erreichte Speicher-Array wird auf der Seite Erkennung angezeigt und kann Ihrer Management-Domäne hinzugefügt werden.

Wenn Sie den Ermittlungsvorgang aus irgendeinem Grund beenden möchten, klicken Sie auf **Erkennung stoppen**.

Schritte

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

   Das Dialogfeld Hinzufügen/Entdecken wird angezeigt.

2. Wählen Sie das Optionsfeld **Alle Speicher-Arrays in einem Netzwerkbereich** aus.
3. Geben Sie die Startnetzwerkadresse und die Endung der Netzwerkadresse ein, um im lokalen Teilnetzwerk zu suchen, und klicken Sie dann auf **Erkennung starten**.

   Der Erkennungsvorgang wird gestartet. Dieser Erkennungsvorgang kann mehrere Minuten dauern. Die Tabelle auf der Seite „Entdecken“ wird bei der Erkennung der Speicher-Arrays ausgefüllt.

   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. Überprüfen Sie die Liste der erkannten Speicher-Arrays.
5. Aktivieren Sie das Kontrollkästchen neben einem beliebigen Speicher-Array, das Sie Ihrer Management-Domäne hinzufügen möchten, und klicken Sie dann auf **Weiter**.

   Unified Manager führt eine Überprüfung der Anmeldeinformationen für jedes Array durch, das Sie der Management-Domäne hinzufügen. Möglicherweise müssen Sie alle selbstsignierten Zertifikate und nicht vertrauenswürdigen Zertifikate, die mit diesem Array verknüpft sind, auflösen.

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

Schritt 2: Lösen Sie selbst signierte Zertifikate während der Ermittlung

Während der Bestandsaufnahme überprüft das System, ob die Speicher-Arrays Zertifikate von einer vertrauenswürdigen Quelle verwenden.

Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie den Verbindungen zu den erkannten Speicherarrays vertrauen, fahren Sie mit der nächsten Karte im Assistenten fort. Die selbstsignierten Zertifikate werden als vertrauenswürdig markiert und die Speicher-Arrays werden zu Unified Manager 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 zu Unified Manager hinzufügen.
2. Klicken Sie auf **Weiter**, um mit dem nächsten Schritt im Assistenten fortzufahren.

Schritt 3: Lösen Sie nicht vertrauenswürdige Zertifikate während der Ermittlung

Nicht vertrauenswürdige Zertifikate treten auf, wenn ein Speicher-Array versucht, eine sichere Verbindung zu Unified Manager herzustellen, die Verbindung jedoch nicht als sicher bestätigt werden kann. Während der Array-Ermittlung können Sie nicht vertrauenswürdige Zertifikate auflösen, indem Sie ein Zertifikat (CA-Zertifikat) importieren, das von einem vertrauenswürdigen Dritten ausgestellt wurde.

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.
- Ein oder beide Zertifikate werden widerrufen.
- Ein oder beide Zertifikate fehlen ein Stammzertifikat oder ein Zwischenzertifikat.

Schritte

1. Aktivieren Sie das Kontrollkästchen neben einem beliebigen Speicherarray, für das Sie nicht vertrauenswürdige Zertifikate auflösen möchten, und wählen Sie dann die Schaltfläche **Importieren**.

   Es wird ein Dialogfeld zum Importieren der vertrauenswürdigen Zertifikatdateien geöffnet.

2. Klicken Sie auf **Durchsuchen**, um die Zertifikatdateien für die Speicher-Arrays auszuwählen.

   Die Dateinamen werden im Dialogfeld angezeigt.

3. Klicken Sie Auf **Import**.

   Die Dateien werden hochgeladen und validiert.

   > Jedes Speicherarray mit nicht vertrauenswürdigen Zertifikatproblemen, die nicht gelöst wurden, wird Unified Manager nicht hinzugefügt.

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

Schritt 4: Geben Sie Passwörter ein

Sie müssen die Passwörter für die Speicher-Arrays eingeben, die Sie Ihrer Management-Domäne hinzufügen möchten.

Schritte

1. Geben Sie das Passwort für jedes Speicher-Array ein, das Sie zu Unified Manager hinzufügen möchten.
2. **Optional:** Speicher-Arrays einer Gruppe zuordnen: Wählen Sie aus der Dropdown-Liste die gewünschte

Gruppe aus, die mit den ausgewählten Speicher-Arrays verknüpft werden soll.

3. Klicken Sie Auf **Fertig Stellen**.

Nachdem Sie fertig sind

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

Es kann mehrere Minuten dauern, bis Unified Manager eine Verbindung zu den angegebenen Storage-Arrays hergestellt hat.

Erkennen Sie ein einzelnes Array

Verwenden Sie die Option Single Storage Array hinzufügen/erkennen, um ein einzelnes Speicher-Array manuell zu ermitteln und dem Netzwerk Ihres Unternehmens hinzuzufügen.

Bevor Sie beginnen

- Das Speicher-Array muss ordnungsgemäß eingerichtet und konfiguriert sein.
- Passwörter für das Storage-Array müssen mithilfe der Kachel „System Manager Access Management“ eingerichtet werden.

Schritte

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

   Das Dialogfeld Hinzufügen/Entdecken wird angezeigt.

2. Wählen Sie das Optionsfeld **Entdecken Sie ein einzelnes Speicherarray**.
3. Geben Sie die IP-Adresse für einen der Controller im Speicher-Array ein, und klicken Sie dann auf **Erkennung starten**.

   Es kann mehrere Minuten dauern, bis sich Unified Manager mit dem angegebenen Storage-Array verbindet.

   Die Meldung Speicher-Array nicht zugänglich wird angezeigt, wenn die Verbindung zur IP-Adresse des angegebenen Controllers nicht erfolgreich ist.

4. Lösen Sie gegebenenfalls selbstsignierte Zertifikate, wenn Sie dazu aufgefordert werden.

   Im Rahmen der Bestandsaufnahme überprüft das System, ob die erkannten Speicher-Arrays Zertifikate von einer vertrauenswürdigen Quelle verwenden. Wenn ein digitales Zertifikat für ein Speicherarray nicht gefunden werden kann, werden Sie aufgefordert, das nicht von einer anerkannten Zertifizierungsstelle (CA) signierte Zertifikat zu lösen, indem eine Sicherheitsausnahme hinzugefügt wird.

5. Lösen Sie ggf. nicht vertrauenswürdige Zertifikate, wenn Sie dazu aufgefordert werden.

   Nicht vertrauenswürdige Zertifikate treten auf, wenn ein Speicher-Array versucht, eine sichere Verbindung zu Unified Manager herzustellen, die Verbindung jedoch nicht als sicher bestätigt werden kann. Lösen Sie nicht vertrauenswürdige Zertifikate, indem Sie ein Zertifikat der Zertifizierungsstelle (CA) importieren, das von einem vertrauenswürdigen Dritten ausgestellt wurde.

6. Klicken Sie Auf **Weiter**.

7. **Optional:** das erkannte Speicher-Array einer Gruppe zuordnen: Wählen Sie aus der Dropdown-Liste die gewünschte Gruppe aus, die mit dem Speicher-Array verknüpft werden soll.

   Die Gruppe „Alle“ ist standardmäßig ausgewählt.

8. Geben Sie das Administratorkennwort für das Speicherarray ein, das Sie Ihrer Management-Domäne hinzufügen möchten, und klicken Sie dann auf **OK**.

Nachdem Sie fertig sind

Das Speicher-Array wird Unified Manager hinzugefügt und, falls angegeben, wird es auch der ausgewählten Gruppe hinzugefügt.

Wenn die automatische Erfassung von Support-Daten aktiviert ist, werden Support-Daten automatisch für ein von Ihnen hinzufügsames Speicher-Array erfasst.

Management von Arrays

Anzeigen des Status des Speicherarrays

SANtricity Unified Manager zeigt den Status jedes erkannten Speicher-Arrays an.

Gehen Sie zur Seite **Verwalten - Alle**. Auf dieser Seite können Sie den Status der Verbindung zwischen dem Web Services Proxy und diesem Speicher-Array anzeigen.

Die Statusanzeigen sind in der folgenden Tabelle beschrieben.

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.
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 vorkommen, wenn der Web Services Proxy gestartet wird und noch keine Kontakte zum Speicher-Array hergestellt wurden oder das Speicher-Array offline ist und seit dem Start des Web Services Proxy noch nie kontaktiert wurde.
Offline	Der Web Services Proxy hatte sich bereits zuvor an das Speicher-Array gewandt, doch inzwischen sind sämtliche Verbindungen verloren gegangen.

Management eines individuellen Storage Arrays

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

Schritte

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

   Das System öffnet ein neues Fenster und zeigt die Anmeldeseite von System Manager an.

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

Ändern Sie die Passwörter für das Speicherarray

Sie können die Passwörter aktualisieren, die für die Anzeige und den Zugriff auf Speicher-Arrays in SANtricity Unified Manager verwendet werden.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Storage Admin-Berechtigungen enthält.
- 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 in Unified Manager darauf zugreifen können. Dies kann notwendig sein, wenn das Array-Passwort in System Manager geändert wurde und jetzt auch in Unified Manager geändert werden muss.

Schritte

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

Entfernen Sie die Storage-Arrays von SANtricity Unified Manager

Sie können ein oder mehrere Storage Arrays entfernen, wenn Sie es nicht mehr über SANtricity Unified Manager 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 die Seite **Verwalten** aus.

2. Wählen Sie ein oder mehrere Speicherarrays aus, die Sie entfernen möchten.
3. Menü wählen:Sonstige Aufgaben[Speicher-Array entfernen].

   Das Storage Array wird aus allen Ansichten in SANtricity Unified Manager entfernt.

Einstellungen werden importiert

Einstellungen Importübersicht

Mit der Funktion „Einstellungen importieren“ können Sie einen Batch-Vorgang zum Importieren der Einstellungen von einem Array in mehrere Arrays durchführen. Diese Funktion spart Zeit, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Welche Einstellungen können importiert werden?

Sie können Alarmmethoden, AutoSupport-Konfigurationen, Verzeichnisdienste-Konfigurationen, Storage-Konfigurationen (z. B. Volume-Gruppen und Pools) und Systemeinstellungen (wie den automatischen Lastausgleich) importieren.

Weitere Informationen:

- "Funktionsweise der Importeinstellungen"
- "Anforderungen für die Replizierung von Storage-Konfigurationen"

Wie führe ich einen Batch-Import durch?

Öffnen Sie System Manager auf einem Storage Array, das als Quelle verwendet werden soll, und konfigurieren Sie die gewünschten Einstellungen. Gehen Sie dann von Unified Manager zur Seite Verwalten und importieren Sie die Einstellungen in ein oder mehrere Arrays.

Weitere Informationen:

- "Warnungseinstellungen importieren"
- "AutoSupport-Einstellungen importieren"
- "Einstellungen für Verzeichnisdienste importieren"
- "Importieren der Speicherkonfigurationseinstellungen"
- "Systemeinstellungen importieren"

Konzepte

Funktionsweise der Importeinstellungen

Mit SANtricity Unified Manager können Sie Einstellungen von einem Storage-Array in mehrere Storage-Arrays importieren. Die Funktion „Importeinstellungen“ ist ein Batch-Vorgang, der Zeit spart, wenn Sie mehrere Arrays im Netzwerk konfigurieren müssen.

Für den Import verfügbare Einstellungen

Die folgenden Konfigurationen können in mehrere Arrays 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.
- **Speicherkonfiguration** — Konfigurationen im Zusammenhang mit folgenden:
  - Volumes (nur Thick Volumes und nicht Repository Volumes)
  - Volume-Gruppen und -Pools
  - Zuweisung von Hot-Spare-Laufwerken
- **Systemeinstellungen** — Konfigurationen in Bezug auf folgende Komponenten:
  - Medien-Scan-Einstellungen für ein Volume
  - SSD-Einstellungen
  - Automatischer Lastausgleich (ohne Berichterstellung für Hostkonnektivität)

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 Unified Manager auf die Seite **Verwalten** und importieren Sie die Einstellungen.
4. Überprüfen Sie auf der Seite **Operationen** die Ergebnisse der 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 Controller-Typ kann sich zwischen Quell- und Ziel-Arrays unterscheiden (beispielsweise beim Import von einer E2800 in eine E5700), 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.
- Thin Volumes sind beim Importvorgang nicht enthalten.

Verwenden Sie Batch-Importe

Warnungseinstellungen importieren

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

- Warnmeldungen werden in System Manager für das Speicherarray konfiguriert, das als Quelle verwendet werden soll (Menü:Einstellungen[Warnungen]).
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).

Über diese Aufgabe

Sie können E-Mail-, SNMP- oder Syslog-Warnungen für den Importvorgang auswählen. Die importierten Einstellungen umfassen:

- **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 **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 Einstellungen aus, die Sie importieren möchten, 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 ein Array nicht in diesem Dialogfeld angezeigt, wenn Unified Manager nicht mit dem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es über Zertifikat-, Kennwort- oder Netzwerkprobleme verfügt).

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.

Ergebnisse

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

AutoSupport-Einstellungen importieren

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

- AutoSupport ist in System Manager für das Storage-Array konfiguriert, das als Quelle verwendet werden soll (Menü:Support[Support Center]).
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).

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 **Einstellungen importieren**.

   Der Assistent für Importeinstellungen wird geöffnet.

2. Wählen Sie im Dialogfeld Einstellungen auswählen die Option **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 Einstellungen aus, die Sie importieren möchten, 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 ein Array nicht in diesem Dialogfeld angezeigt, wenn Unified Manager nicht mit dem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es über Zertifikat-, Kennwort- oder Netzwerkprobleme verfügt).

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.

Ergebnisse

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

Einstellungen für Verzeichnisdienste importieren

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

- Verzeichnisdienste werden in System Manager für das Speicherarray konfiguriert, das als Quelle verwendet werden soll (Menü:Einstellungen[Zugriffsmanagement]).
- Die vorhandene Konfiguration für die Ziel-Speicher-Arrays wird in System Manager gesichert (Menü:Einstellungen[System > Speicherarray-Konfiguration speichern]).

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 **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 Einstellungen aus, die Sie importieren möchten, 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 ein Array nicht in diesem Dialogfeld angezeigt, wenn Unified Manager nicht mit dem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es über Zertifikat-, Kennwort- oder Netzwerkprobleme verfügt).

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.

Ergebnisse

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

Systemeinstellungen importieren

Sie können die Systemkonfiguration 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

- 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]).

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 **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 Einstellungen aus, die Sie importieren möchten, 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 ein Array nicht in diesem Dialogfeld angezeigt, wenn Unified Manager nicht mit dem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es über Zertifikat-, Kennwort- oder Netzwerkprobleme verfügt).

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.

Ergebnisse

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

Importieren der Speicherkonfigurationseinstellungen

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

- Storage ist in SANtricity 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]).
- 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.
  - Thin Volumes sind beim Importvorgang nicht enthalten.

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 **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 Einstellungen aus, die Sie importieren möchten, 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 ein Array nicht in diesem Dialogfeld angezeigt, wenn Unified Manager nicht mit dem Array kommunizieren kann (z. B. wenn es offline ist oder wenn es über Zertifikat-, Kennwort- oder Netzwerkprobleme verfügt).

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.

Ergebnisse

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

FAQs

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 SANtricity 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 all 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).

Array-Gruppen

Gruppenübersicht

Auf der Seite „Gruppen managen“ können Sie eine Reihe von Speicher-Array-Gruppen erstellen, um die Verwaltung zu erleichtern.

Was sind Array-Gruppen?

Sie können Ihre physische und virtualisierte Infrastruktur 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.

Es gibt zwei Arten von 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.

Wie konfiguriere ich Gruppen?

Auf der Seite „Gruppen verwalten“ können Sie eine Gruppe erstellen und dieser Gruppe Arrays hinzufügen.

Weitere Informationen:

- "Speicherarray-Gruppe konfigurieren"

Speicherarray-Gruppe konfigurieren

Sie erstellen Speichergruppen und fügen dann Speicher-Arrays zu den Gruppen hinzu.

Das Konfigurieren von Gruppen ist ein zweistufiges Verfahren.

Schritt 1: Gruppe erstellen

Sie erstellen zuerst eine Gruppe. 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**.

Schritt 2: Speicher-Array zu Gruppe hinzufügen

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.**

Entfernen Sie Speicher-Arrays aus der Gruppe

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**.

Speicherarray-Gruppe löschen

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**.

Benennen Sie die Speicherarray-Gruppe 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.**

Upgrades

Übersicht zum Upgrade Center

Im Upgrade Center können Sie SANtricity OS Software und NVSRAM Upgrades für mehrere Storage Arrays managen.

Wie funktionieren Upgrades?

Sie laden die neueste Betriebssystemsoftware herunter und aktualisieren dann ein oder mehrere Arrays.

Workflow-Upgrade

Die folgenden Schritte ermöglichen einen grundlegenden Workflow bei der Durchführung von Software-Upgrades.

1. Sie laden die aktuelle SANtricity OS Softwaredatei von der Support-Website herunter. (Auf der Support-Seite ist ein Link von Unified Manager verfügbar) Speichern Sie die Datei auf dem Management-Host-System (dem Host, auf dem Sie in einem Browser auf Unified Manager zugreifen), und entpacken Sie die Datei anschließend.
2. In Unified Manager laden Sie die Softwaredatei des SANtricity-Betriebssystems und die NVSRAM-Datei in das Repository (ein Bereich des Web-Services-Proxyservers, auf dem Dateien gespeichert sind). Sie können Dateien entweder über das Menü:Upgrade Center[Upgrade SANtricity OS Software oder über Upgrade Center > Software-Repository verwalten] hinzufügen.
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 Software Upgrade SANtricity OS

(Menü:Upgrade Center [Upgrade SANtricity OS Software]) die Software-Datei SANtricity OS 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 Upgrades führt Unified Manager die folgenden Aufgaben aus:
   a. 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.
   b. Überträgt die Upgrade-Dateien an jeden Controller.
   c. Bootet die Controller neu und aktiviert die neue SANtricity OS Software, die jeweils einen Controller umfasst. Während der Aktivierung wird die vorhandene SANtricity OS-Datei durch die neue Datei ersetzt.

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

Sofortiges oder stufenweise Upgrade

Sie können das Upgrade sofort aktivieren oder es für einen späteren Zeitpunkt 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. Je nach I/O-Last und Cache-Größe kann ein Controller-Upgrade in der Regel zwischen 15 und 25 Minuten dauern. 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.

Um die stufenweise Software zu aktivieren, gehen Sie zum Menü:Support[Upgrade Center] und klicken Sie im Bereich SANtricity OS-Controller-Software-Upgrade auf **Aktivieren**.

Zustandsprüfung

Eine Integritätsprüfung wird im Rahmen des Upgrade-Prozesses ausgeführt, Sie können aber auch vor dem Start eine Integritätsprüfung separat durchführen (siehe Menü:Upgrade Center [Health Check vor dem Upgrade]).

Bei der Integritätsprüfung werden alle Storage-Systemkomponenten bewertet, um sicherzustellen, dass das Upgrade fortgesetzt werden kann. Die folgenden Bedingungen können das Upgrade verhindern:

- Ausgefallene zugewiesene Laufwerke
- Hot Spares werden verwendet
- Unvollständige Volume-Gruppen
- Exklusive Vorgänge ausgeführt
- Fehlende Volumes

- Controller befindet sich im Status „nicht optimal“
- Übermäßige Anzahl von Ereignisprotokollereignissen
- Fehler bei der Validierung der Konfigurationsdatenbank
- Laufwerke mit alten Versionen von DACstore

Was muss ich vor einem Upgrade beachten?

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

Aktuelle Versionen

Sie können die aktuellen Softwareversionen des SANtricity Betriebssystems von der Seite Verwalten von Unified Manager 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 den einzelnen Zeilen auf die SANtricity OS-Version 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 "NetApp Interoperabilitätsmatrix". Lesen Sie auch die Verfahren in den Express-Leitfäden für Ihr Betriebssystem. Express-Leitfäden finden Sie im "E-Series und SANtricity Dokumentation".

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.

Aktualisieren von Software und Firmware

Führen Sie eine Integritätsprüfung vor dem Upgrade 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.

Upgrade von SANtricity OS

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

- Die neuesten Dateien des SANtricity Betriebssystems sind auf dem Host-System verfügbar, auf dem der SANtricity Web Services Proxy und Unified Manager ausgeführt werden.
- 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.

> Auf Systemen muss SANtricity OS 11.70.5 ausgeführt werden, um ein Upgrade auf 11.80.x oder höher durchzuführen.

Über diese Aufgabe

```
[NOTE]
====
Risiko eines Datenverlusts oder einer Beschädigung des Storage Arrays:
Nehmen Sie während des Upgrades keine Änderungen am Storage Array vor.
Halten Sie den Strom für das Speicher-Array aufrecht.
```

```
====
.Schritte
. 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.
. Wählen Sie in der Hauptansicht *Verwalten* aus, und wählen Sie dann ein
oder mehrere Speicher-Arrays aus, die Sie aktualisieren möchten.
. Wählen Sie MENU:Upgrade Center[Upgrade SANtricity OS Software].
+
Die Seite SANtricity OS-Software aktualisieren wird angezeigt.

. Laden Sie das neueste Software-Paket für SANtricity OS von der NetApp
Support-Website auf Ihren lokalen Computer herunter.
+
.. Klicken Sie auf *Neue Datei zum Software-Repository hinzufügen*.
.. Klicken Sie auf den Link, um die neuesten *SANtricity OS Downloads* zu
finden.
.. Klicken Sie auf den Link *Letzte Version herunterladen*.
.. Folgen Sie den restlichen Anweisungen, um die SANtricity OS-Datei und
die NVSRAM-Datei auf Ihren lokalen Computer herunterzuladen.


+
[NOTE]
====
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.

====
. Wählen Sie die Betriebssystemsoftware und die NVSRAM-Datei aus, die Sie
zum Aktualisieren der Controller verwenden möchten:
+
.. Wählen Sie aus der Dropdown-Liste *Select a SANtricity OS Software
file* die Betriebssystemdatei aus, die Sie auf Ihren lokalen Rechner
heruntergeladen haben.
+
Wenn mehrere Dateien verfügbar sind, werden die Dateien vom neuesten Datum
bis zum ältesten Datum sortiert.

+
[NOTE]
====
```

Das Software-Repository enthält alle Softwaredateien, die dem Web Services Proxy zugeordnet sind. 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.

====
.. 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.

. 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.

. *Optional:* um die Software-Datei auf die Speicher-Arrays zu übertragen, ohne sie zu aktivieren, wählen Sie das Kontrollkästchen *Betriebssystemsoftware auf die Speicher-Arrays übertragen, als bereitgestellt markieren und zu einem späteren Zeitpunkt aktivieren*.
. Klicken Sie Auf *Start*.
. Je nachdem, ob Sie jetzt oder später aktiviert haben, führen Sie einen der folgenden Schritte aus:
+
** Geben Sie *TRANSFER* ein, um zu bestätigen, dass Sie die vorgeschlagenen Betriebssystemversionen auf den Arrays übertragen möchten, die Sie für die Aktualisierung ausgewählt haben, und klicken Sie dann auf *Transfer*.
+
Um die übertragene Software zu aktivieren, wählen Sie MENU:Upgrade Center[Staged OS Software aktivieren].

** Geben Sie *UPGRADE* ein, um zu bestätigen, dass Sie die vorgeschlagenen Betriebssystemversionen auf den Arrays übertragen und aktivieren möchten, die Sie aktualisieren möchten, 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. Sie können auf die Ellipsen (...) klicken und
*Protokoll speichern* wählen, 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.


. *Optional:* nach Abschluss des Upgrades sehen Sie eine Liste der für ein
bestimmtes Speicherarray aktualisierten Versionen, indem Sie auf die
Ellipsen (...) klicken und dann *Protokoll speichern* wählen.
+
Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen
gespeichert `upgrade_log-<date>.json`.




[[ID4eeb7cbb130d38b2f776f38da3f63f65]]
= Aktivieren Sie die stufenweise Betriebssystemsoftware
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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.

[NOTE]
====
Sie können den Aktivierungsvorgang nach dem Start nicht beenden.

====
.Schritte
. Wählen Sie in der Hauptansicht *Verwalten*. Klicken Sie bei Bedarf auf die Spalte Status, um oben auf der Seite alle Storage Arrays mit dem Status „OS Upgrade (Aktivierung ausstehend)“ zu sortieren.
. Wählen Sie einen oder mehrere Speicher-Arrays aus, für die Sie Software aktivieren möchten, und wählen Sie dann Menü:Upgrade Center[Activate Staged OS 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. Sie können auf die Ellipsen (...) klicken und *Protokoll speichern* wählen, 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.

. *Optional:* nach Abschluss der Aktivierung sehen Sie eine Liste dessen, was für ein bestimmtes Speicherarray aktiviert wurde, indem Sie auf die Ellipsen (...) klicken und dann *Protokoll speichern* wählen.
+
Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert `activate_log-<date>.json`.

[[ID6a081bce9870ac80d5468fb22718c34c]]
= Software-Repository managen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Das Software-Repository enthält alle Softwaredateien, die dem Web Services Proxy zugeordnet sind.

Wenn Sie die Datei nicht sehen, die Sie verwenden möchten, können Sie mithilfe der Option Software-Repository verwalten eine oder mehrere SANtricity-Betriebssystemdateien auf das Hostsystem importieren, auf dem der Webservices-Proxy und Unified Manager ausgeführt werden. Sie können auch festlegen, dass eine oder mehrere SANtricity OS-Dateien gelöscht werden sollen, die im Software-Repository verfügbar sind.

.Bevor Sie beginnen
Wenn Sie SANtricity OS-Dateien hinzufügen, stellen Sie sicher, dass die Betriebssystemdateien auf Ihrem lokalen System verfügbar sind.

.Schritte
. Wählen Sie in der Hauptansicht *Verwalten* und dann Menü:Upgrade Center[Software-Repository verwalten].
+
Das Dialogfeld Software-Repository verwalten wird angezeigt.

. Führen Sie eine der folgenden Aktionen aus:
+
[cols="25h,~"]

```
|===
| Option | Tun Sie das


 a|
Importieren
 a|
.. Klicken Sie Auf *Import.*
.. 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`.

.. Wählen Sie eine oder mehrere Betriebssystemdateien aus, die Sie
hinzufügen möchten, und klicken Sie dann auf *Import*.




 a|
Löschen
 a|
.. Wählen Sie eine oder mehrere Betriebssystemdateien aus, die Sie aus dem
Software-Repository entfernen möchten.
.. Klicken Sie Auf *Löschen*.


|===


.Ergebnisse
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.



[[ID58726813e0de6987d6100afa636dcefe]]
= Software für das überstaltete Betriebssystem löschen
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
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
. Wählen Sie in der Hauptansicht *Verwalten* und dann Menü:Upgrade
Center[Staged OS Software löschen].
+
Das Dialogfeld „Staged OS Software löschen“ wird geöffnet und listet alle
erkannten Speichersysteme mit ausstehender Software oder NVSRAM auf.

. Filtern oder sortieren Sie die Speichersysteme in der Liste, falls
erforderlich, so dass Sie alle Systeme mit stufenweise Software anzeigen
können.
. Aktivieren Sie die Kontrollkästchen für die Speichersysteme mit
ausstehender Software, die Sie löschen möchten.
. Klicken Sie Auf *Löschen*.
+
Der Status des Vorgangs wird im Dialogfeld angezeigt.




:leveloffset: -1


:leveloffset: -1


= Spiegelung

:leveloffset: +1


[[ID232b8bae378cc90b99e465d34874dda5]]
= Spiegelung – Übersicht
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```

```
Mithilfe der Spiegelungsfunktionen können Daten entweder asynchron oder
synchron zwischen einem lokalen Storage-Array und einem Remote-Storage-
Array repliziert werden.

[NOTE]
====
Synchrones Spiegeln ist auf dem Storage-System EF600/EF600C oder
EF300/EF300C nicht verfügbar.

====


== Was ist Spiegelung?

SANtricity-Applikationen beinhalten zwei Arten von Spiegelung: Asynchron
und synchron. Die asynchrone Spiegelung kopiert Daten-Volumes nach Bedarf
oder nach einem Zeitplan. So werden Ausfallzeiten, die auf
Datenbeschädigung oder -Verlust zurückzuführen sind, minimiert oder
vermieden. Bei der synchronen Spiegelung werden Daten-Volumes in Echtzeit
repliziert, um eine kontinuierliche Verfügbarkeit zu gewährleisten.

Weitere Informationen:

* xref:{relative_path}mirroring-overview.html["Funktionsweise von
Spiegelung"]
* xref:{relative_path}mirroring-terminology.html["Terminologie wird
gespiegelt"]




== Wie konfiguriere ich Spiegelung?

Sie konfigurieren asynchrone oder synchrone Spiegelung in Unified Manager
und managen dann die Synchronisierung mit System Manager.

Weitere Informationen:

* xref:{relative_path}mirroring-configuration-workflow.html["Spiegelung
des Konfigurations-Workflows"]
* xref:{relative_path}requirements-for-using-mirroring.html["Anforderungen
für die Verwendung von Spiegelung"]
* xref:{relative_path}create-asynchronous-mirrored-pair-um.html["Erstellen
eines asynchronen gespiegelten Paares"]
* xref:{relative_path}create-synchronous-mirrored-pair-um.html["Erstellen
eines synchronen gespiegelten Paares"]
```

= Konzepte

:leveloffset: +1

[[ID681cbb4e679a9bed4ce65eaf8bf1cb68]]
= Funktionsweise von Spiegelung
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity Unified Manager enthält Konfigurationsoptionen für die SANtricity-Spiegelungsfunktionen, mit denen Administratoren Daten zur Datensicherung zwischen zwei Storage Arrays replizieren können.

[NOTE]
====
Synchrones Spiegeln ist auf dem Storage-System EF600/EF600C oder EF300/EF300C nicht verfügbar.

====

== Arten der Spiegelung

SANtricity-Applikationen beinhalten zwei Arten von Spiegelung: Asynchron und synchron.

Die asynchrone Spiegelung kopiert Daten-Volumes nach Bedarf oder nach einem Zeitplan. So werden Ausfallzeiten, die auf Datenbeschädigung oder -Verlust zurückzuführen sind, minimiert oder vermieden. Das asynchrone Spiegeln erfasst den Status des primären Volumes zu einem bestimmten Zeitpunkt und kopiert nur die Daten, die sich seit der letzten Bildaufzeichnung geändert haben. Der primäre Standort kann sofort aktualisiert werden, während der sekundäre Standort mit der Bandbreite aktualisiert werden kann. Die Informationen werden im Cache gespeichert und später gesendet, sobald Netzwerkressourcen verfügbar sind. Diese Art der Spiegelung ist ideal für periodische Prozesse wie Backups und Archivierungen.

Bei der synchronen Spiegelung werden Daten-Volumes in Echtzeit repliziert,

um eine kontinuierliche Verfügbarkeit zu gewährleisten. Der Zweck besteht darin, ein Recovery Point Objective (RPO) von null Datenverlust zu erreichen, indem eine Kopie wichtiger Daten verfügbar ist, falls auf einem der beiden Storage Arrays ein Ausfall auftritt. Die Kopie ist zu jedem Zeitpunkt identisch mit den Produktionsdaten. Jedes Mal, wenn ein Schreibvorgang auf dem primären Volume ausgeführt wird, wird auf dem sekundären Volume ein Schreibvorgang vorgenommen. Der Host erhält keine Bestätigung, dass der Schreibvorgang erfolgreich war, bis das sekundäre Volume mit den Änderungen auf dem primären Volume aktualisiert wurde. Diese Art von Spiegelung ist ideal für Business Continuity-Zwecke wie Disaster Recovery.

== Unterschiede zwischen Spiegelungstypen

In der folgenden Tabelle werden die Hauptunterschiede zwischen den beiden Spiegelungstypen beschrieben.

[cols="1a,1a,1a"]
|===
| Attribut | Asynchron | Synchron

 a|
Replikationsmethode
 a|
Zeitpunktgenau: Die Spiegelung wird nach Bedarf oder automatisch gemäß einem benutzerdefinierten Zeitplan durchgeführt.
 a|
Continuous -- die Spiegelung wird automatisch kontinuierlich ausgeführt und kopiert die Daten von jedem Host-Schreibvorgang.

 a|
Entfernung
 a|
Unterstützt große Entfernungen zwischen den Arrays. In der Regel ist die Entfernung nur durch die Fähigkeiten des Netzwerks und der Channel-Erweiterungstechnologie begrenzt.
 a|
Beschränkt auf kürzere Entfernungen zwischen den Arrays. In der Regel muss die Entfernung ca. 10 km (6.2 Meilen) vom lokalen Storage-Array entfernt sein, um die Anforderungen bezüglich Latenz und Applikations-Performance zu erfüllen.

```
 a|
Kommunikationsmethode
 a|
Einem standardmäßigen IP- oder Fibre Channel-Netzwerk an.
 a|
Nur Fibre Channel-Netzwerk.



 a|
Volume-Typen
 a|
Standard oder Thin
 a|
Nur Standard.

|===



[[IDcc6cf96a067b9fbc9408402acb1ca928]]
= Spiegelung des Konfigurations-Workflows
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
In SANtricity Unified Manager wird die asynchrone oder synchrone
Spiegelung konfiguriert und anschließend mit SANtricity System Manager die
Synchronisierung verwaltet.



== Workflow für asynchrone Spiegelung

Die asynchrone Spiegelung umfasst den folgenden Workflow:

. Die Erstkonfiguration in Unified Manager durchführen:
+
.. Wählen Sie das lokale Speicher-Array als Quelle für den Datentransfer
aus.
.. Erstellen oder Auswählen einer vorhandenen SpiegelungsConsistency
Group: Dies ist ein Container für das primäre Volume auf dem lokalen Array
```

und dem sekundären Volume auf dem Remote-Array. Das primäre und sekundäre Volume werden als „gespiegeltes Paar“ bezeichnet. Wenn Sie zum ersten Mal die Spiegelkonsistent-Gruppe erstellen, legen Sie fest, ob Sie manuelle oder geplante Synchronisierungen durchführen möchten.
.. Wählen Sie ein primäres Volume aus dem lokalen Speicher-Array aus, und bestimmen Sie dann die reservierte Kapazität. Die reservierte Kapazität ist die physisch zugewiesene Kapazität, die für den Kopiervorgang verwendet werden soll.
.. Wählen Sie ein Remote-Speicher-Array als Ziel des Transfers, ein sekundäres Volume, und legen Sie dann seine reservierte Kapazität fest.
.. Beginnen Sie den ersten Datentransfer vom primären Volume zum sekundären Volume. Je nach Volume-Größe kann dieser erste Transfer mehrere Stunden dauern.

. Den Fortschritt der ersten Synchronisierung überprüfen:
+
.. Starten Sie in Unified Manager den System Manager für das lokale Array.
.. Zeigen Sie in System Manager den Status des Spiegelungsvorgangs an. Nach Abschluss der Spiegelung ist der Status des gespiegelten Paares „optimal“.

. Optional können Sie nachfolgende Datentransfers in System Manager neu terminieren oder manuell durchführen. Es werden nur neue und geänderte Blöcke vom primären Volume auf das sekundäre Volume übertragen.
+
[NOTE]
====
Da die asynchrone Replizierung periodisch erfolgt, kann das System die geänderten Blöcke konsolidieren und Netzwerkbandbreite sparen. Der Schreibdurchsatz und die Schreiblatenz sind nur minimal beeinträchtigt.

====

== Workflow für synchrones Spiegeln

Die synchrone Spiegelung umfasst den folgenden Workflow:

. Die Erstkonfiguration in Unified Manager durchführen:
+
.. Wählen Sie ein lokales Speicher-Array als Quelle für den Datentransfer aus.
.. Wählen Sie ein primäres Volume aus dem lokalen Speicher-Array aus.

```
.. Wählen Sie ein Remote-Speicher-Array als Ziel für den Datentransfer
aus, und wählen Sie dann ein sekundäres Volume aus.
.. Wählen Sie Synchronisierungsprioritäten und Neusynchronisierung aus.
.. Beginnen Sie den ersten Datentransfer vom primären Volume zum
sekundären Volume. Je nach Volume-Größe kann dieser erste Transfer mehrere
Stunden dauern.


. Den Fortschritt der ersten Synchronisierung überprüfen:
+
.. Starten Sie in Unified Manager den System Manager für das lokale Array.
.. Zeigen Sie in System Manager den Status des Spiegelungsvorgangs an.
Nach Abschluss der Spiegelung ist der Status des gespiegelten Paares
„optimal“. Die beiden Arrays versuchen, während des normalen Betriebs
synchronisiert zu bleiben. Es werden nur neue und geänderte Blöcke vom
primären Volume auf das sekundäre Volume übertragen.


. Optional können Sie die Synchronisierungseinstellungen in System Manager
ändern.
+
[NOTE]
====
Da die synchrone Replizierung kontinuierlich erfolgt, muss die
Replizierungsverbindung zwischen den beiden Standorten ausreichend
Bandbreitenkapazität bereitstellen.

====




[[ID3e7bc43970ec4dce286093a13e1f2461]]
= Terminologie wird gespiegelt
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Erfahren Sie, wie die Spiegelungsbedingungen auf Ihr Storage-Array
angewendet werden.

[cols="25h,~"]
|===
| Laufzeit | Beschreibung
```

a|
Lokales Storage-Array
a|
Das lokale Storage-Array ist das Storage-Array, auf dem Sie arbeiten.

a|
Spiegelung der Konsistenzgruppe
a|
Eine gespiegelte Konsistenzgruppe ist ein Container für ein oder mehrere gespiegelte Paare. Für asynchrone Spiegelungsvorgänge müssen Sie eine Konsistenzgruppe erstellen. Alle gespiegelten Paare in einer Gruppe werden gleichzeitig resynchronisiert, sodass ein konsistenter Wiederherstellungspunkt beibehalten wird.

Bei der synchronen Spiegelung werden keine Konsistenzgruppen verwendet.

a|
Gespiegeltes Paar
a|
Ein gespiegeltes Paar besteht aus zwei Volumes, einem primären Volume und einem sekundären Volume.

Bei der asynchronen Spiegelung gehört ein gespiegeltes Paar immer einer gespiegelten Konsistenzgruppe an. Schreibvorgänge werden zunächst auf dem primären Volume durchgeführt und dann auf das sekundäre Volume repliziert. Jedes gespiegelte Paar in einer Spiegelkonsistent-Gruppe verwendet dieselben Synchronisierungseinstellungen.

a|
Primäres Volume
a|
Das primäre Volume eines gespiegelten Paars ist das zu spiegelnden Quell-Volume.

a|
Remote Storage Array
a|

```
Das Remote Storage Array wird in der Regel als sekundärer Standort
bezeichnet, der in der Regel ein Replikat der Daten in einer
Spiegelungskonfiguration enthält.



 a|
Reservierte Kapazität
 a|
Reservierte Kapazität ist die zugewiesene physische Kapazität, die für
jeden Kopierdienst- und Storage-Objekt verwendet wird. Er ist nicht direkt
vom Host lesbar.

Diese Volumes sind erforderlich, damit der Controller permanent
Informationen speichern kann, die erforderlich sind, um die Spiegelung in
einem Betriebszustand zu halten. Sie enthalten Informationen wie Delta-
Protokolle und Copy-on-Write-Daten.



 a|
Sekundäres Volume
 a|
Das sekundäre Volume eines gespiegelten Paars befindet sich normalerweise
an einem sekundären Standort und enthält ein Replikat der Daten.



 a|
Synchronisierung
 a|
Die Synchronisierung erfolgt bei der ersten Synchronisierung zwischen dem
lokalen Speicher-Array und dem Remote-Speicher-Array. Die Synchronisierung
findet auch statt, wenn primäre und sekundäre Volumes nach einer
Kommunikationsunterbrechung nicht mehr synchronisiert werden. Wenn die
Kommunikationsverbindung wieder funktioniert, werden alle nicht
replizierten Daten mit dem Storage-Array des sekundären Volumes
synchronisiert.

|===



[[IDc86c42c5a2131ce1835a83db5c5b8ee8]]
= Anforderungen für die Verwendung von Spiegelung
:allow-uri-read:
:experimental:
```

```
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie die Spiegelung konfigurieren möchten, beachten Sie die folgenden
Anforderungen.



== Unified Manager

* Der Web Services Proxy-Dienst muss ausgeführt werden.
* Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung
ausgeführt werden.
* Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array
anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr
eigenes Sicherheitszertifikat mit Unified Manager installieren und zum
Menü:Zertifikat[Zertifikatverwaltung] navigieren.




== Storage-Arrays durchführt

[NOTE]
====
Synchrones Spiegeln ist für das EF600/EF600C oder EF300/EF300C Storage-
Array nicht verfügbar.

====
* Sie müssen über zwei Storage-Arrays verfügen.
* Jedes Speicher-Array muss zwei Controller haben.
* Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
* Jeder Controller im primären Array und im sekundären Array muss über
einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk
verbunden sein.
* Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens
7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
* Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays
kennen.
* Sie benötigen genügend freie Kapazität auf dem Remote-Speicher-Array, um
ein sekundäres Volume zu erstellen, das dem primären Volume entspricht
oder dessen Größe Sie spiegeln möchten.
* Asynchrones Spiegeln wird auf Controllern mit Fibre Channel (FC)- oder
iSCSI-Host-Ports unterstützt, während synchrones Spiegeln nur auf
```

Controllern mit FC Host-Ports unterstützt wird.

== Konnektivitätsanforderungen erfüllen

Für die Spiegelung über eine FC-Schnittstelle (asynchron oder synchron) ist Folgendes erforderlich:

* Jeder Controller des Storage-Arrays ordnet den am höchsten nummerierten FC-Host-Port der Spiegelung zu.
* Wenn der Controller sowohl Basis-FC-Ports als auch Host-Schnittstellenkarten (HIC) FC-Ports hat, ist der Port mit der höchsten Nummer auf einer HIC. Alle Hosts, die am dedizierten Port angemeldet sind, werden abgemeldet, und es werden keine Anmeldeanforderungen für den Host akzeptiert. I/O-Anfragen auf diesem Port werden nur von Controllern akzeptiert, die an Spiegelungsvorgängen beteiligt sind.
* Die dedizierten Spiegelungs-Ports müssen an eine FC-Fabric-Umgebung angeschlossen werden, die den Verzeichnisdienst und die Nameservice-Schnittstellen unterstützt. Insbesondere werden FC-AL und Point-to-Point nicht als Konnektivitätsoptionen zwischen den Controllern unterstützt, die an gespiegelten Beziehungen beteiligt sind.

Die Spiegelung über eine iSCSI-Schnittstelle (nur asynchron) erfordert Folgendes:

* Im Gegensatz zu FC erfordert iSCSI keinen dedizierten Port. Wenn Sie asynchrone Spiegelung in iSCSI-Umgebungen einsetzen, müssen Sie keine der Front-End iSCSI-Ports des Storage-Arrays für die asynchrone Spiegelung verwenden. Diese Ports werden sowohl für asynchronen Spiegeldatenverkehr als auch für Array-I/O-Verbindungen gemeinsam genutzt.
* Der Controller verfügt über eine Liste der Remote-Speichersysteme, mit denen der iSCSI-Initiator versucht, eine Sitzung einzurichten. Der erste Port, der eine iSCSI-Verbindung erfolgreich herstellt, wird für die anschließende Kommunikation mit dem Remote-Speicher-Array verwendet. Wenn die Kommunikation fehlschlägt, wird eine neue Sitzung unter Verwendung aller verfügbaren Ports versucht.
* ISCSI-Ports werden auf Array-Ebene für Port konfiguriert. Intercontroller Kommunikation für Konfigurationsnachrichten und Datentransfer verwendet die globalen Einstellungen, einschließlich Einstellungen für:
+
** VLAN: Sowohl lokale als auch Remote-Systeme müssen die gleiche VLAN-Einstellung für die Kommunikation haben

** ISCSI-Listening-Port
** Jumbo-Frames
** Ethernet-Priorität

[NOTE]
====
Die iSCSI-Intercontroller-Kommunikation muss einen Host-Connect-Port und nicht den Management-Ethernet-Port verwenden.

====

== Kandidaten für gespiegelte Volumes

* RAID-Level, Caching-Parameter und Segmentgröße können auf den primären und sekundären Volumes eines gespiegelten Paars unterschiedlich sein.
+

NOTE: Bei EF600- und EF300-Controllern müssen die primären und sekundären Volumes eines asynchronen gespiegelten Paares dasselbe Protokoll, Tray-Level, Segmentgröße, Sicherheitstyp und RAID-Level erfüllen. Nicht geeignete asynchrone gespiegelte Paare werden nicht in der Liste der verfügbaren Volumes angezeigt.

* Das sekundäre Volume muss mindestens so groß sein wie das primäre Volume.
* Ein Volume kann nur an einer Spiegelbeziehung beteiligt sein.
* Für ein synchrones gespiegeltes Paar müssen die primären und sekundären Volumes Standard-Volumes sein. Es können keine dünnen Volumes oder Snapshot Volumes sein.
* Für die synchrone Spiegelung gibt es eine Begrenzung für die Anzahl der Volumes, die auf einem bestimmten Storage Array unterstützt werden. Stellen Sie sicher, dass die Anzahl der konfigurierten Volumes in Ihrem Speicher-Array kleiner als das unterstützte Limit ist. Wenn das synchrone Spiegeln aktiv ist, werden die zwei reservierten Kapazitäts-Volumes, die erstellt werden, mit der Volume-Obergrenze verglichen.
* Beim asynchronen Spiegeln müssen das primäre Volume und das sekundäre Volume dieselben Laufwerksicherheitsfunktionen aufweisen.
+
** Wenn das primäre Volume FIPS-fähig ist, muss das sekundäre Volume FIPS-fähig sein.
** Wenn das primäre Volume FDE-fähig ist, muss das sekundäre Volume FDE-fähig sein.
** Wenn das primäre Volume keine Laufwerkssicherheit verwendet, darf das

sekundäre Volume keine Laufwerkssicherheit verwenden.

== Reservierte Kapazität

Asynchrones Spiegeln:

* Ein reserviertes Kapazitäts-Volume ist für ein primäres Volume und ein sekundäres Volume in einem gespiegelten Paar für das Protokollieren von Schreibinformationen erforderlich, um nach einem Controller-Reset und anderen temporären Unterbrechungen wiederherzustellen.
* Da sowohl das primäre Volume als auch das sekundäre Volume in einem gespiegelten Paar zusätzliche reservierte Kapazität benötigen, müssen Sie sicherstellen, dass auf beiden Storage-Arrays in der Spiegelbeziehung freie Kapazität verfügbar ist.

Synchrones Spiegeln:

* Für ein primäres Volume und ein sekundäres Volume zur Protokollierung von Schreibinformationen zum Wiederherstellen nach Controller-Resets und anderen vorübergehenden Unterbrechungen ist die reservierte Kapazität erforderlich.
* Die reservierten Kapazitäts-Volumes werden automatisch bei aktivierter synchronen Spiegelung erstellt. Da sowohl das primäre Volume als auch das sekundäre Volume in einem gespiegelten Paar reservierte Kapazität benötigen, müssen Sie sicherstellen, dass auf beiden Storage-Arrays, die an der Beziehung zur synchronen Spiegelung beteiligt sind, ausreichend freie Kapazität zur Verfügung steht.

== Laufwerkssicherheit

* Wenn Sie sichere Laufwerke verwenden, müssen das primäre und das sekundäre Volume über kompatible Sicherheitseinstellungen verfügen. Diese Beschränkung wird nicht durchgesetzt, deshalb müssen Sie sie selbst überprüfen.
* Bei Verwendung von sicheren Laufwerken sollten das primäre Volume und das sekundäre Volume denselben Laufwerkstyp verwenden. Diese Beschränkung wird nicht durchgesetzt, deshalb müssen Sie sie selbst überprüfen.
* Wenn Sie Data Assurance (da) verwenden, müssen das primäre Volume und

das sekundäre Volume über dieselben da-Einstellungen verfügen.

:leveloffset: -1

= Konfigurieren Sie die Spiegelung

:leveloffset: +1

[[ID23055acef11dd9698f1f219d1c5c3dbe]]
= Erstellen eines asynchronen gespiegelten Paares
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Zum Konfigurieren der asynchronen Spiegelung erstellen Sie ein gespiegeltes Paar, das ein primäres Volume auf dem lokalen Array und ein sekundäres Volume des Remote-Arrays umfasst.

.Bevor Sie beginnen
Bevor Sie ein gespiegeltes Paar erstellen, erfüllen Sie die folgenden Anforderungen für Unified Manager:

* Der Web Services Proxy-Dienst muss ausgeführt werden.
* Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung ausgeführt werden.
* Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr eigenes Sicherheitszertifikat mit Unified Manager installieren und zum Menü:Zertifikat[Zertifikatverwaltung] navigieren.

Stellen Sie außerdem sicher, dass Sie die folgenden Anforderungen an Storage Arrays und Volumes erfüllen:

* Jedes Speicher-Array muss zwei Controller haben.
* Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
* Jeder Controller im primären Array und im sekundären Array muss über einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk

verbunden sein.
* Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens 7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
* Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays kennen.
* Sie benötigen genügend freie Kapazität auf dem Remote-Speicher-Array, um ein sekundäres Volume zu erstellen, das dem primären Volume entspricht oder dessen Größe Sie spiegeln möchten.
* Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel Fabric- oder iSCSI-Schnittstelle verbunden.
* Sie haben sowohl die primären als auch die sekundären Volumes erstellt, die Sie in der asynchronen Spiegelbeziehung verwenden möchten.
* Das sekundäre Volume muss mindestens so groß sein wie das primäre Volume.

.Über diese Aufgabe
Der Prozess zum Erstellen eines asynchronen gespiegelten Paares ist ein mehrstufiges Verfahren.

== Schritt 1: Erstellen oder wählen Sie eine gespiegelte Konsistenzgruppe aus

In diesem Schritt erstellen Sie eine neue Konsistenzgruppe für die Spiegelung, oder wählen Sie eine vorhandene Konsistenzgruppe aus. Eine gespiegelte Konsistenzgruppe ist ein Container für die primären und sekundären Volumes (das gespiegelte Paar) und gibt die gewünschte Resynchronisierung (manuell oder automatisch) für alle Paare in der Gruppe an.

.Schritte
. Wählen Sie auf der Seite *Verwalten* das lokale Speicher-Array aus, das Sie für die Quelle verwenden möchten.
. Wählen Sie Menü:Aktionen[Asynchronous Mirrored Pair erstellen].
+
Der Assistent Asynchronous Mirrored Pair erstellen wird geöffnet.

. Wählen Sie entweder eine vorhandene SpiegelungsConsistency Group aus oder erstellen Sie eine neue Konsistenzgruppe.
+
Um eine vorhandene Gruppe auszuwählen, stellen Sie sicher, dass *eine vorhandene SpiegelungsConsistency Group* ausgewählt ist, und wählen Sie dann die Gruppe aus der Tabelle aus. Eine Konsistenzgruppe kann mehrere gespiegelte Paare enthalten.

+
Gehen Sie zum Erstellen einer neuen Gruppe wie folgt vor:

+
.. Wählen Sie *Eine neue Spiegelkonsistent-Gruppe* aus und klicken Sie dann auf *Weiter*.
.. Geben Sie einen eindeutigen Namen ein, der am besten die Daten auf den Volumes beschreibt, die zwischen den beiden Speicher-Arrays gespiegelt werden. Ein Name kann nur aus Buchstaben, Zahlen und den Sonderzeichen Unterstrichen (_), Bindestrich (-) und dem Hash-Zeichen (#) bestehen. Ein Name darf 30 Zeichen nicht überschreiten und darf keine Leerzeichen enthalten.
.. Wählen Sie das Remote Storage Array aus, auf dem Sie eine Mirror-Beziehung zum lokalen Speicher-Array herstellen möchten.
+
[NOTE]
====
Wenn Ihr Remote-Speicher-Array passwortgeschützt ist, fordert das System zur Eingabe eines Kennworts auf.

====
.. Wählen Sie aus, ob Sie die gespiegelten Paare manuell oder automatisch synchronisieren möchten:
+
*** *Manuell* -- Wählen Sie diese Option, um die Synchronisierung für alle gespiegelten Paare innerhalb dieser Gruppe manuell zu starten. Beachten Sie, dass Sie, wenn Sie später eine Neusynchronisierung durchführen möchten, System Manager für das primäre Speicher-Array starten und dann zum Menü:Speicher[Asynchronous Mirroring] wechseln müssen, die Gruppe auf der Registerkarte *Mirror Consistency Groups* auswählen und dann Menü:Mehr[manuell neu synchronisieren] auswählen.
*** *Automatisch* -- Wählen Sie das gewünschte Intervall in *Minuten*, *Stunden* oder *Tagen* aus, vom Beginn des vorherigen Updates bis zum Beginn des nächsten Updates. Wenn beispielsweise das Synchronisierungsintervall auf 30 Minuten eingestellt ist und der Synchronisationsprozess um 4:00 Uhr beginnt, beginnt der nächste Vorgang um 4:30 Uhr

.. Wählen Sie die gewünschten Warnmeldungseinstellungen aus:
+
*** Geben Sie bei manuellen Synchronisierungen den Schwellenwert (definiert durch den Prozentsatz der verbleibenden Kapazität) für den Zeitpunkt an, an dem Benachrichtigungen empfangen werden.
*** Für automatische Synchronisierungen können Sie drei Arten der Alarmierung festlegen: Wenn die Synchronisierung in einer bestimmten

Zeitspanne nicht abgeschlossen wurde, wenn die Daten der Wiederherstellungspunkt auf dem Remote-Array älter als ein bestimmtes Zeitlimit sind und sich die reservierte Kapazität einem bestimmten Schwellenwert nähert (definiert durch den Prozentsatz der verbleibenden Kapazität).

. Wählen Sie *Weiter* und gehen Sie zu <<Schritt 2: Wählen Sie das primäre Volumen>>.
+
Wenn Sie eine neue gespiegelte Konsistenzgruppe definiert haben, erstellt Unified Manager zuerst die gespiegelte Konsistenzgruppe im lokalen Storage Array und erstellt dann die gespiegelte Konsistenzgruppe im Remote-Storage-Array. Sie können die gespiegelte Konsistenzgruppe anzeigen und verwalten, indem Sie System Manager für jedes Array starten.

+
[NOTE]
====
Wenn Unified Manager die SpiegelungsConsistency Group erfolgreich auf dem lokalen Speicher-Array erstellt, diese aber nicht auf dem Remote-Speicher-Array erstellt, wird die SpiegelConsistency Group automatisch aus dem lokalen Speicher-Array gelöscht. Wenn ein Fehler auftritt, während Unified Manager versucht, die gespiegelte Konsistenzgruppe zu löschen, müssen Sie sie manuell löschen.

====

== Schritt 2: Wählen Sie das primäre Volumen

In diesem Schritt wählen Sie das primäre Volume aus, das in der Spiegelbeziehung verwendet werden soll, und weisen seine reservierte Kapazität zu. Wenn Sie ein primäres Volume auf dem lokalen Speicher-Array auswählen, zeigt das System eine Liste aller berechtigten Volumes für dieses gespiegelte Paar an. Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser Liste nicht angezeigt.

Alle Volumes, die Sie der Spiegelungs-Consistency Group auf dem lokalen Speicher-Array hinzufügen, besitzen die primäre Rolle in der Spiegelbeziehung.

.Schritte

. Wählen Sie aus der Liste der berechtigten Volumes ein Volume aus, das Sie als primäres Volume verwenden möchten, und klicken Sie dann auf *Weiter*, um die reservierte Kapazität zuzuweisen.
. Wählen Sie aus der Liste der teilnahmeberechtigten Kandidaten die reservierte Kapazität für das primäre Volume aus.
+
Beachten Sie folgende Richtlinien:

+
** Die Standardeinstellung für die reservierte Kapazität ist 20 % der Kapazität des Basis-Volumes, und in der Regel reicht diese Kapazität aus. Wenn Sie den Prozentsatz ändern, klicken Sie auf *Kandidaten aktualisieren*.
** Die erforderliche Kapazität variiert abhängig von der Häufigkeit und Größe der I/O-Schreibvorgänge auf dem primären Volume und wie lange Sie die Kapazität beibehalten müssen.
** Im Allgemeinen wählen Sie eine größere Kapazität für reservierte Kapazität aus, wenn eine oder beide Bedingungen vorhanden sind:
+
*** Sie beabsichtigen, das gespiegelte Paar für einen langen Zeitraum zu halten.
*** Ein großer Prozentsatz an Datenblöcken ändert sich auf dem primären Volume aufgrund von hoher I/O-Aktivität. Mithilfe von historischen Performance-Daten oder anderen Betriebssystem-Utilities können Sie typische I/O-Aktivitäten für das primäre Volume ermitteln.

. Wählen Sie *Weiter* und gehen Sie zu <<Schritt 3: Wählen Sie das sekundäre Volumen>>.

== Schritt 3: Wählen Sie das sekundäre Volumen

In diesem Schritt wählen Sie das sekundäre Volume aus, das in der Spiegelbeziehung verwendet werden soll, und weisen seine reservierte Kapazität zu. Wenn Sie ein sekundäres Volume auf dem Remote-Speicher-Array auswählen, zeigt das System eine Liste aller berechtigten Volumes für dieses gespiegelte Paar an. Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser Liste nicht angezeigt.

Alle Volumes, die Sie der Spiegelungs-Konsistenzgruppe auf dem Remote-Speicher-Array hinzufügen, übernehmen die sekundäre Rolle in der Spiegelbeziehung.

.Schritte
. Wählen Sie aus der Liste der berechtigten Volumes ein Volume aus, das Sie als sekundäres Volume im gespiegelten Paar verwenden möchten, und klicken Sie dann auf *Weiter*, um die reservierte Kapazität zuzuweisen.
. Wählen Sie aus der Liste der teilnahmeberechtigten Kandidaten die reservierte Kapazität für das sekundäre Volume aus.
+
Beachten Sie folgende Richtlinien:

+
** Die Standardeinstellung für die reservierte Kapazität ist 20 % der Kapazität des Basis-Volumes, und in der Regel reicht diese Kapazität aus. Wenn Sie den Prozentsatz ändern, klicken Sie auf *Kandidaten aktualisieren*.
** Die erforderliche Kapazität variiert abhängig von der Häufigkeit und Größe der I/O-Schreibvorgänge auf dem primären Volume und wie lange Sie die Kapazität beibehalten müssen.
** Im Allgemeinen wählen Sie eine größere Kapazität für reservierte Kapazität aus, wenn eine oder beide Bedingungen vorhanden sind:
+
*** Sie beabsichtigen, das gespiegelte Paar für einen langen Zeitraum zu halten.
*** Ein großer Prozentsatz an Datenblöcken ändert sich auf dem primären Volume aufgrund von hoher I/O-Aktivität. Mithilfe von historischen Performance-Daten oder anderen Betriebssystem-Utilities können Sie typische I/O-Aktivitäten für das primäre Volume ermitteln.

. Wählen Sie *Fertig stellen*, um die asynchrone Spiegelsequenz abzuschließen.

.Ergebnisse
Unified Manager führt die folgenden Aktionen durch:

* Startet die erste Synchronisierung zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array.
* Legt die reservierte Kapazität für das gespiegelte Paar auf dem lokalen Speicher-Array und auf dem Remote-Speicher-Array fest.

NOTE: Wenn es sich bei dem zu spiegelnden Volume um ein Thin Volume handelt, werden während der ersten Synchronisierung nur die

```
bereitgestellten Blöcke (zugewiesene Kapazität statt gemeldete Kapazität)
auf das sekundäre Volume übertragen. Dadurch wird die Datenmenge
reduziert, die übertragen werden muss, um die erste Synchronisierung
abzuschließen.



[[IDf8347bf94eed5e3e4444049440d8d2ed]]
= Erstellen eines synchronen gespiegelten Paares
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Zur Konfiguration der synchronen Spiegelung erstellen Sie ein gespiegeltes
Paar, das ein primäres Volume auf dem lokalen Array und ein sekundäres
Volume des Remote-Arrays umfasst.

[NOTE]
====
Diese Funktion ist für das Speichersystem EF600/EF600C oder EF300/EF300C
nicht verfügbar.

====
.Bevor Sie beginnen
Bevor Sie ein gespiegeltes Paar erstellen, erfüllen Sie die folgenden
Anforderungen für Unified Manager:

* Der Web Services Proxy-Dienst muss ausgeführt werden.
* Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung
ausgeführt werden.
* Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array
anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr
eigenes Sicherheitszertifikat mit Unified Manager installieren und zum
Menü:Zertifikat[Zertifikatverwaltung] navigieren.


Stellen Sie außerdem sicher, dass Sie die folgenden Anforderungen an
Storage Arrays und Volumes erfüllen:

* Die beiden Storage Arrays, die Sie für die Spiegelung verwenden möchten,
werden in Unified Manager entdeckt.
* Jedes Speicher-Array muss zwei Controller haben.
* Jeder Controller im primären Array und im sekundären Array muss über
```

einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk verbunden sein.
* Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens 7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
* Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays kennen.
* Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel Fabric verbunden.
* Sie haben sowohl die primären als auch die sekundären Volumes erstellt, die Sie in der Beziehung zur synchronen Spiegelung verwenden möchten.
* Das primäre Volume muss ein Standard-Volume sein. Es kann sich nicht um ein Thin-Volume oder ein Snapshot-Volume handelt.
* Das sekundäre Volume muss ein Standard-Volume sein. Es kann sich nicht um ein Thin-Volume oder ein Snapshot-Volume handelt.
* Das sekundäre Volume sollte mindestens so groß sein wie das primäre Volume.

.Über diese Aufgabe
Das Erstellen von synchronen gespiegelten Paaren ist ein mehrstufiges Verfahren.

== Schritt 1: Wählen Sie das primäre Volumen

In diesem Schritt wählen Sie das primäre Volume aus, das in der Beziehung zur synchronen Spiegelung verwendet werden soll. Wenn Sie ein primäres Volume auf dem lokalen Speicher-Array auswählen, zeigt das System eine Liste aller berechtigten Volumes für dieses gespiegelte Paar an. Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser Liste nicht angezeigt. Das ausgewählte Volume besitzt die primäre Rolle in der Spiegelbeziehung.

.Schritte
. Wählen Sie auf der Seite *Verwalten* das lokale Speicher-Array aus, das Sie für die Quelle verwenden möchten.
. Menü wählen:Aktionen[Synchronous Mirrored Pair erstellen].
+
Der Assistent Synchronous Mirrored Pair erstellen wird geöffnet.

. Wählen Sie aus der Liste der berechtigten Volumes ein Volume aus, das Sie als primäres Volume in der Spiegelung verwenden möchten.
. Wählen Sie *Weiter* und gehen Sie zu <<Schritt 2: Wählen Sie das sekundäre Volumen>>.

```
== Schritt 2: Wählen Sie das sekundäre Volumen

In diesem Schritt wählen Sie das sekundäre Volume aus, das in der
Spiegelbeziehung verwendet werden soll. Wenn Sie ein sekundäres Volume auf
dem Remote-Speicher-Array auswählen, zeigt das System eine Liste aller
berechtigten Volumes für dieses gespiegelte Paar an. Alle Volumes, die
nicht für die Verwendung geeignet sind, werden in dieser Liste nicht
angezeigt. Das ausgewählte Volumen hält die sekundäre Rolle in der
Spiegelbeziehung.

.Schritte
. Wählen Sie das Remote Storage Array aus, auf dem Sie eine Mirror-
Beziehung zum lokalen Speicher-Array herstellen möchten.
+
[NOTE]
====
Wenn Ihr Remote-Speicher-Array passwortgeschützt ist, fordert das System
zur Eingabe eines Kennworts auf.

====
+
** Die Liste der Storage-Arrays wird nach ihrem Storage-Array-Namen
benannt. Wenn Sie kein Speicher-Array genannt haben, wird es als
„unbenannt“ aufgeführt.
** Wenn das zu verwendende Speicher-Array nicht in der Liste aufgeführt
ist, stellen Sie sicher, dass es in Unified Manager erkannt wurde.


. Wählen Sie aus der Liste der berechtigten Volumes ein Volume aus, das
Sie als sekundäres Volume in der Spiegelung verwenden möchten.
+
[NOTE]
====
Wird ein sekundäres Volume mit einer Kapazität ausgewählt, die größer als
das primäre Volume ist, so ist die nutzbare Kapazität auf die Größe des
primären Volumes beschränkt.

====
. Klicken Sie auf *Weiter* und gehen Sie zu <<Schritt 3:
Synchronisierungseinstellungen auswählen>>.




== Schritt 3: Synchronisierungseinstellungen auswählen
```

In diesem Schritt wählen Sie die Einstellungen aus, die bestimmen, wie Daten nach einer Kommunikationsunterbrechung synchronisiert werden. Sie können die Priorität festlegen, mit der der Controller-Eigentümer des primären Volumes nach einer Kommunikationsunterbrechung Daten mit dem sekundären Volume neu synchronisiert. Sie müssen außerdem die Resynchronisierung-Richtlinie entweder manuell oder automatisch auswählen.

.Schritte
. Verwenden Sie den Schieberegler, um die Synchronisationspriorität festzulegen.
+
Die Synchronisierungspriorität legt fest, wie viele der Systemressourcen verwendet werden, um die erste Synchronisierung abzuschließen und die Neusynchronisierung nach einer Kommunikationsunterbrechung im Vergleich zu Service-I/O-Anforderungen zu ermöglichen.

+
Die in diesem Dialogfeld festgelegte Priorität gilt sowohl für das primäre Volume als auch für das sekundäre Volume. Sie können die Rate für das primäre Volume zu einem späteren Zeitpunkt ändern, indem Sie zu System Manager wechseln und Menü:Storage[Synchronous Mirroring > More > Edit Settings] auswählen.

+
Es gibt fünf Prioritätsraten für die Synchronisierung:

+
** Am Niedrigsten
** Niedrig
** Mittel
** Hoch
** Höchste
+
Wenn die Synchronisierungspriorität auf die niedrigste Rate eingestellt ist, wird die I/O-Aktivität priorisiert und die Neusynchronisierung dauert länger. Wenn die Synchronisierungspriorität auf die höchste Rate festgelegt ist, wird der Neusynchronisierung nach Priorität geordnet, aber die I/O-Aktivität für das Speicher-Array ist möglicherweise betroffen.

. Wählen Sie aus, ob Sie die gespiegelten Paare auf dem Remote-Speicher-Array entweder manuell oder automatisch neu synchronisieren möchten.
+
** *Manuell* (die empfohlene Option) -- Wählen Sie diese Option aus, damit

die Synchronisierung manuell fortgesetzt werden muss, nachdem die Kommunikation auf einem gespiegelten Paar wiederhergestellt wurde. Diese Option bietet die beste Möglichkeit für die Wiederherstellung von Daten.
** *Automatisch* -- Wählen Sie diese Option, um die Neusynchronisierung automatisch zu starten, nachdem die Kommunikation auf einem gespiegelten Paar wiederhergestellt wurde.
+
Um die Synchronisierung manuell fortzusetzen, wählen Sie System Manager und Menü:Speicherung[Synchronous Mirroring], markieren Sie das gespiegelte Paar in der Tabelle, und wählen Sie unter *Mehr* *Resume*.

. Klicken Sie auf *Fertig stellen*, um die Synchronspiegelung abzuschließen.

.Ergebnisse
Wenn die Spiegelung aktiviert ist, führt das System folgende Aktionen durch:

* Startet die erste Synchronisierung zwischen dem lokalen Speicher-Array und dem Remote-Speicher-Array.
* Legt die Synchronisierungspriorität und die Resynchronisierungsrichtlinie fest.
* Behält sich den Port mit der höchsten Nummer der HIC des Controllers bei der Datenübertragung mit gespiegelten Daten vor.
+
Auf diesem Port empfangene I/O-Anfragen werden nur von dem bevorzugten Remote-Controller-Eigentümer des sekundären Volumes im gespiegelten Paar akzeptiert. (Reservierungen für das primäre Volume sind zulässig.)

* Erstellt zwei reservierte Kapazitäts-Volumes, eines für jeden Controller, die zum Protokollieren von Schreibinformationen für die Wiederherstellung nach Controller-Resets und anderen temporären Unterbrechungen verwendet werden.
+
Die Kapazität eines jeden Volumes beträgt 128 MiB. Wenn die Volumes jedoch in einen Pool aufgenommen werden, wird 4 gib für jedes Volume reserviert.

.Nachdem Sie fertig sind
Wechseln Sie zu System Manager und wählen Sie MENU:Startseite[Vorgänge in Bearbeitung anzeigen], um den Fortschritt des Synchronspiegelung-Vorgangs anzuzeigen. Dieser Vorgang kann langwierig sein und die System-Performance beeinträchtigen.

```
:leveloffset: -1


= FAQs

:leveloffset: +1


[[IDba09181f8b05941d49380aa18115c395]]
= Was muss ich wissen, bevor ich eine gespiegelte Konsistenzgruppe
erstellt?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Befolgen Sie die folgenden Richtlinien, bevor Sie eine gespiegelte
Konsistenzgruppe erstellen.

Erfüllen Sie die folgenden Anforderungen für Unified Manager:

* Der Web Services Proxy-Dienst muss ausgeführt werden.
* Unified Manager muss auf Ihrem lokalen Host über eine HTTPS-Verbindung
ausgeführt werden.
* Unified Manager muss gültige SSL-Zertifikate für das Speicher-Array
anzeigen. Sie können ein selbstsigniertes Zertifikat akzeptieren oder Ihr
eigenes Sicherheitszertifikat mit Unified Manager installieren und zum
Menü:Zertifikat[Zertifikatverwaltung] navigieren.


Erfüllen Sie außerdem die folgenden Anforderungen an Storage-Arrays:

* Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
* Jedes Speicher-Array muss zwei Controller haben.
* Jeder Controller im primären Array und im sekundären Array muss über
einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk
verbunden sein.
* Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens
7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
* Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays
kennen.
```

```
* Ihre lokalen und Remote-Speicher-Arrays sind über eine Fibre Channel
Fabric- oder iSCSI-Schnittstelle verbunden.


[NOTE]
====
Synchrones Spiegeln ist auf dem Storage-System EF600/EF600C oder
EF300/EF300C nicht verfügbar.

====



[[ID6cd242c5da492e5b4d5c9707d4aac083]]
= Was muss ich vor der Erstellung eines gespiegelten Paares wissen?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Befolgen Sie vor dem Erstellen eines gespiegelten Paares diese
Richtlinien.

* Sie müssen über zwei Storage-Arrays verfügen.
* Jedes Speicher-Array muss zwei Controller haben.
* Die beiden Storage Arrays müssen in Unified Manager erkannt werden.
* Jeder Controller im primären Array und im sekundären Array muss über
einen konfigurierten Ethernet-Managementport verfügen und mit dem Netzwerk
verbunden sein.
* Die Speicher-Arrays verfügen über eine Firmware-Version von mindestens
7.84. (Beide können unterschiedliche OS-Versionen ausführen.)
* Sie müssen das Passwort für die lokalen und Remote-Speicher-Arrays
kennen.
* Sie benötigen genügend freie Kapazität auf dem Remote-Speicher-Array, um
ein sekundäres Volume zu erstellen, das dem primären Volume entspricht
oder dessen Größe Sie spiegeln möchten.
* Asynchrones Spiegeln wird auf Controllern mit Fibre Channel (FC)- oder
iSCSI-Host-Ports unterstützt, während synchrones Spiegeln nur auf
Controllern mit FC Host-Ports unterstützt wird.


[NOTE]
====
Synchrones Spiegeln ist auf dem Storage-System EF600/EF600C oder
EF300/EF300C nicht verfügbar.
```

```
====



[[ID7bba3d1735839c1ae1b4870c8b534d1a]]
= Warum sollte ich diesen Prozentsatz ändern?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die reservierte Kapazität ist normalerweise 20 % des Basis-Volumes für
asynchrone Spiegelungsvorgänge. In der Regel ist diese Kapazität
ausreichend.

Die benötigte Kapazität ist abhängig von Häufigkeit und Größe der I/O-
Schreibvorgänge auf dem Basis-Volume und wie lange Sie den Kopierdienst
des Storage-Objekts verwenden möchten. Im Allgemeinen wählen Sie einen
größeren Prozentsatz für die reservierte Kapazität aus, wenn eine oder
beide Bedingungen vorhanden sind:

* Wenn sich der Kopierdienst eines bestimmten Storage-Objekts sehr lange
Lebensdauer hat.
* Wenn sich ein großer Prozentsatz an Datenblöcken auf dem Basis-Volume
aufgrund von hoher I/O-Aktivität ändert. Mithilfe von historischen
Performance-Daten oder anderen Betriebssystem-Dienstprogrammen können Sie
die typischen I/O-Aktivitäten für das Basis-Volume ermitteln.




[[ID22c095386e21ca36657461967a9dd15a]]
= Warum kann ich mehr als einen Kandidaten für reservierte Kapazität
sehen?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn sich mehrere Volumes in einem Pool oder einer Volume-Gruppe befinden,
die dem für das Storage-Objekt ausgewählten Kapazitätsprozentsatz
entsprechen, werden mehrere Kandidaten angezeigt.
```

```
Sie können die Liste der empfohlenen Kandidaten aktualisieren, indem Sie
den Prozentsatz des physischen Speicherplatzes ändern, den Sie im Basis-
Volume für Kopierdienste reservieren möchten. Die besten Kandidaten werden
basierend auf Ihrer Auswahl angezeigt.



[[ID90cb7f13698f1c6d53ae343f5e1f0c96]]
= Warum sehe ich nicht alle meine Bände?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie ein primäres Volume für ein gespiegeltes Paar auswählen, werden
in einer Liste alle berechtigten Volumes angezeigt.

Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser
Liste nicht angezeigt. Volumes sind aus folgenden Gründen möglicherweise
nicht verfügbar:

* Die Lautstärke ist nicht optimal.
* Das Volume beteiligt sich bereits an einer Spiegelbeziehung.
* Für das synchrone Spiegeln müssen primäre und sekundäre Volumes eines
gespiegelten Paars Standard-Volumes sein. Es können keine dünnen Volumes
oder Snapshot Volumes sein.
* Bei der asynchronen Spiegelung müssen Thin Volumes die automatische
Erweiterung aktiviert haben.



NOTE: Bei EF600- und EF300-Controllern müssen die primären und sekundären
Volumes eines asynchronen gespiegelten Paares dasselbe Protokoll, Tray-
Level, Segmentgröße, Sicherheitstyp und RAID-Level erfüllen. Nicht
geeignete asynchrone gespiegelte Paare werden nicht in der Liste der
verfügbaren Volumes angezeigt.



[[ID4f3b8a2b4e67583d90130bbdec10cadc]]
= Warum sehe ich nicht alle Volumes auf dem Remote-Speicher-Array?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
```

```
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie ein sekundäres Volume auf dem Remote-Speicher-Array auswählen,
werden alle für dieses gespiegelte Paar geeigneten Volumes in einer Liste
angezeigt.

Alle Volumes, die nicht für die Verwendung geeignet sind, werden in dieser
Liste nicht angezeigt. Die Volumes können aus den folgenden Gründen nicht
berechtigt sein:

* Das Volume ist ein nicht standardmäßiges Volume, wie z. B. ein Snapshot-
Volume.
* Die Lautstärke ist nicht optimal.
* Das Volume beteiligt sich bereits an einer Spiegelbeziehung.
* Bei der asynchronen Spiegelung stimmen die Thin Volume-Attribute des
primären Volumes und des sekundären Volumes nicht überein.
* Wenn Sie Data Assurance (da) verwenden, müssen das primäre Volume und
das sekundäre Volume über dieselben da-Einstellungen verfügen.
+
** Wenn das primäre Volume mit da aktiviert ist, muss das sekundäre Volume
mit da aktiviert sein.
** Wenn das primäre Volume nicht da aktiviert ist, darf das sekundäre
Volume nicht als da-aktiviert verwendet werden.


* Beim asynchronen Spiegeln müssen das primäre Volume und das sekundäre
Volume dieselben Laufwerksicherheitsfunktionen aufweisen.
+
** Wenn das primäre Volume FIPS-fähig ist, muss das sekundäre Volume FIPS-
fähig sein.
** Wenn das primäre Volume FDE-fähig ist, muss das sekundäre Volume FDE-
fähig sein.
** Wenn das primäre Volume keine Laufwerkssicherheit verwendet, darf das
sekundäre Volume keine Laufwerkssicherheit verwenden.




[[ID0a7a8e0e72ed67fa2bda5b7fbcbeeae7]]
= Welche Auswirkungen hat die Synchronisierungspriorität auf die
Synchronisierungsraten?
:allow-uri-read:
:icons: font
```

```
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die Synchronisierungspriorität definiert, wie viel Verarbeitungszeit für
Synchronisierungsaktivitäten im Verhältnis zur Systemleistung zugewiesen
wird.

Der Controller-Eigentümer des primären Volume führt diesen Vorgang im
Hintergrund durch. Gleichzeitig verarbeitet der Controller-Inhaber lokale
I/O-Schreibvorgänge auf das primäre Volume und verbundene Remote-
Schreibvorgänge auf das sekundäre Volume. Da durch die Resynchronisierung
der Controller-Verarbeitungsressourcen von der I/O-Aktivität umgeleitet
werden, kann eine Neusynchronisierung die Performance der Host-Applikation
nach sich ziehen.

Beachten Sie diese Richtlinien, um zu ermitteln, wie lange eine
Synchronisierungspriorität dauern könnte und wie sich die
Synchronisierungsprioritäten auf die Systemleistung auswirken können.

Diese Prioritätsraten sind verfügbar:

* Am Niedrigsten
* Niedrig
* Mittel
* Hoch
* Höchste


Die niedrigste Prioritätsrate unterstützt die System-Performance, die
Neusynchronisierung dauert jedoch länger. Die höchste Prioritätsrate
unterstützt eine Neusynchronisierung, aber die System-Performance ist
möglicherweise beeinträchtigt.

Diese Leitlinien entsprechen ungefähr den Unterschieden zwischen den
Prioritäten.

[cols="45h,~"]
|===
| Prioritätsrate für vollständige Synchronisierung | Verstrichene Zeit im
Vergleich zur höchsten Synchronisationsrate


 a|
Am Niedrigsten
 a|
```

```
Etwa achtmal so lange wie bei der höchsten Prioritätsrate.



 a|
Niedrig
 a|
Etwa sechsmal so lange wie bei der höchsten Prioritätsrate.



 a|
Mittel
 a|
Etwa dreieinhalb Mal so lang wie bei der höchsten Prioritätsrate.



 a|
Hoch
 a|
Etwa doppelt so lange wie bei der höchsten Prioritätsrate.

|===
Volume-Größe und Host-I/O-Rate-Lasten wirken sich auf den Vergleich der
Synchronisierungszeit aus.



[[IDb99e941107bfd63b6eae910b7f03faef]]
= Warum wird empfohlen, eine manuelle Synchronisierungsrichtlinie zu
verwenden?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die manuelle Neusynchronisierung wird empfohlen, da Sie damit den
Neusynchronisierung so verwalten können, dass dadurch keine Möglichkeit
zum Wiederherstellen von Daten besteht.

Wenn Sie eine automatische Resynchronisierung verwenden und während der
Neusynchronisierung intermittierende Kommunikationsprobleme auftreten,
können die Daten auf dem sekundären Volume vorübergehend beschädigt
werden. Nach Abschluss der Resynchronisierung werden die Daten korrigiert.
```

```
:leveloffset: -1


:leveloffset: -1


= Zertifikate

:leveloffset: +1


[[IDa49d8be1941b290217459b9b8935c07c]]
= Zertifikatübersicht
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Mit der Zertifikatverwaltung können Sie Zertifikatsignierungsanforderungen
(CSRs) erstellen, Zertifikate importieren und vorhandene Zertifikate
verwalten.



== Was sind Zertifikate?

_Zertifikate_ sind digitale Dateien, die Online-Einheiten wie Websites und
Server für eine sichere Kommunikation im Internet identifizieren. Es gibt
zwei Arten von Zertifikaten: Ein _signiertes Zertifikat_ wird von einer
Zertifizierungsstelle (CA) validiert und ein _selbst-signiertes
Zertifikat_ wird vom Eigentümer des Unternehmens anstelle eines Dritten
validiert.

Weitere Informationen:

* xref:{relative_path}how-certificates-work-unified.html["Funktionsweise
von Zertifikaten"]
* xref:{relative_path}certificate-terminology-unified.html["Terminologie
des Zertifikats"]
```

```
== Wie konfiguriere ich Zertifikate?

In der Zertifikatverwaltung können Sie Zertifikate für die Management
Station konfigurieren, die Unified Manager hostet, und auch Zertifikate
für die Controller in den Arrays importieren.

Weitere Informationen:

* xref:{relative_path}use-ca-signed-certificate-um.html["Verwenden Sie CA-
signierte Zertifikate für das Managementsystem"]
* xref:{relative_path}import-array-certificates-unified.html["Importieren
Sie Zertifikate für Arrays"]




= Konzepte

:leveloffset: +1


[[ID1b6b7255aafa503c89e8ba18885feab2]]
= Funktionsweise von Zertifikaten
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Zertifikate sind digitale Dateien, die Online-Einheiten wie Websites und
Server für eine sichere Kommunikation im Internet identifizieren.



== Signierte Zertifikate

Zertifikate stellen sicher, dass die Webkommunikation in verschlüsselter
Form, privat und unverändert, nur zwischen dem angegebenen Server und dem
angegebenen Client übertragen wird. Mit Unified Manager 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 Eigentümers validiert 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.

[NOTE]
====
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.

====
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 „`Trusted`". 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.

== Zertifikate für Unified Manager

Die Unified Manager-Schnittstelle wird mit dem Web Services Proxy auf einem Host-System installiert. Wenn Sie einen Browser öffnen und eine Verbindung zu Unified Manager herstellen möchten, versucht der Browser, durch die Suche nach einem digitalen Zertifikat zu überprüfen, ob der Host eine vertrauenswürdige Quelle ist. Wenn der Browser kein von einer Zertifizierungsstelle signiertes Zertifikat für den Server findet, wird eine Warnmeldung angezeigt. Von dort aus können Sie auf der Website fortfahren, um das selbstsignierte Zertifikat für diese Sitzung zu akzeptieren. Oder Sie können signierte digitale Zertifikate von einer Zertifizierungsstelle erhalten, damit die Warnmeldung nicht mehr angezeigt wird.

```
== Zertifikate für Controller

Während einer Unified Manager-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 der Web Services Proxy-Server eingehende
Clientanforderungen von diesen Controllern authentifizieren kann.



[[IDd979a220e369cb2d999d12e4cb3eaf8a]]
= Terminologie des Zertifikats
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die folgenden Begriffe gelten für das Zertifikatmanagement.

[cols="25h,~"]
|===
| Laufzeit | Beschreibung


 a|
CA
 a|
Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die
elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-
Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer,
die sichere Verbindungen zwischen Clients und Servern ermöglichen.



 a|
CSR
 a|
Eine Zertifikatsignierungsanforderung (CSR) ist eine Nachricht, die von
einem Antragsteller an eine Zertifizierungsstelle (CA) gesendet wird. Der
CSR überprüft die Informationen, die die Zertifizierungsstelle zum
ausstellen eines Zertifikats benötigt.
```

a|
Zertifikat
a|
Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).

a|
Zertifikatskette
a|
Eine Dateihierarchie, die den Zertifikaten eine Sicherheitsschicht hinzufügt. In der Regel umfasst die Kette ein Stammzertifikat oben in der Hierarchie, ein oder mehrere Zwischenzertifikate und die Serverzertifikate, die die Entitäten identifizieren.

a|
Zwischenzertifikat
a|
Ein oder mehrere Zwischenzertifikate verzweigen von der Root in der Zertifikatkette. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten fungieren sollen.

a|
Schlüsselspeicher
a|
Ein Schlüsselspeicher ist ein Repository auf Ihrem Host-Managementsystem, das private Schlüssel enthält, zusammen mit ihren entsprechenden öffentlichen Schlüsseln und Zertifikaten. Diese Schlüssel und Zertifikate identifizieren Ihre eigenen Einheiten, z. B. die Controller.

a|
Stammzertifikat
a|

Das Stammzertifikat befindet sich oben in der Hierarchie in der Zertifikatskette und enthält einen privaten Schlüssel, 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.

Signiertes Zertifikat
Ein Zertifikat, das von einer Zertifizierungsstelle (CA) validiert wird. Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt zwischen einem Server und einem Client über eine HTTPS-Verbindung gesendet werden. Darüber hinaus enthält ein signiertes Zertifikat Details über den Eigentümer des Unternehmens (in der Regel ein Server oder eine Website) und eine digitale Signatur bestehend aus Buchstaben und Zahlen. Ein signiertes Zertifikat nutzt eine Vertrauenskette und wird daher am häufigsten in Produktionsumgebungen verwendet. Auch als „CA-signiertes Zertifikat“ oder als „Managementzertifikat“ bezeichnet.

Selbstsigniertes Zertifikat
Ein selbstsigniertes Zertifikat wird vom Eigentümer des Unternehmens validiert. Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt zwischen einem Server und einem Client über eine HTTPS-Verbindung gesendet werden. Es enthält auch eine digitale Signatur, die aus Buchstaben und Zahlen besteht. Ein selbstsigniertes Zertifikat verwendet nicht dieselbe Vertrauenskette wie ein CA-signiertes Zertifikat und wird daher am häufigsten in Testumgebungen eingesetzt. Auch als vorinstalliertes Zertifikat bezeichnet.

Serverzertifikat
Das Server-Zertifikat befindet sich unten in der Zertifikatskette. Es identifiziert Ihre spezifische Einheit, z. B. eine Website oder ein anderes Gerät. Jeder Controller in einem Storage-System benötigt ein separates Serverzertifikat.

```
 a|
Treuhandgeschäft
 a|
Ein Truststore ist ein Repository, das Zertifikate von vertrauenswürdigen
Drittanbietern, wie z. B. CAS, enthält.

|===



:leveloffset: -1


[[ID8e93744908eb583933e0a3dc91d80106]]
= Verwenden Sie CA-signierte Zertifikate für das Managementsystem
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können CA-signierte Zertifikate für sicheren Zugriff auf das
Managementsystem, das SANtricity Unified Manager hostet, erhalten und
importieren.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.

.Über diese Aufgabe
Die Verwendung von CA-signierten Zertifikaten ist ein dreistufiges
Verfahren.



== 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 der Web
Services Proxy und Unified Manager installiert sind.

[NOTE]
====
```

```
Alternativ können Sie eine CSR-Datei mit einem Tool wie OpenSSL generieren
und zu überspringen <<Schritt 2: CSR-Datei senden>>.

====
.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie auf der Registerkarte Verwaltung die Option *CSR abschließen*
aus.
. 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.


. Geben Sie die folgenden Informationen über das Hostsystem ein, auf dem
der Web Services Proxy installiert ist:
+
** *Allgemeiner Name* -- die IP-Adresse oder der DNS-Name des Hostsystems,
auf dem der Web Services Proxy installiert ist. Stellen Sie sicher, dass
diese Adresse korrekt ist, sie muss mit den Angaben übereinstimmen, die
Sie für den Zugriff auf Unified Manager im Browser eingeben. 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.


. 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.
. Klicken Sie Auf *Fertig Stellen*.
. Gehen Sie zu <<Schritt 2: CSR-Datei senden>>.

== Schritt 2: CSR-Datei senden

Nachdem Sie eine CSR-Datei (Certificate Signing Request) erstellt haben, senden Sie sie an eine Certificate Authority (CA), um signierte Managementzertifikate für das System zu erhalten, das Unified Manager und den Web Services Proxy hostet.

NOTE: 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
. Suchen Sie die heruntergeladene CSR-Datei.
+
Der Speicherort des Downloads hängt von Ihrem Browser ab.

. Senden Sie die CSR-Datei an eine CA (z. B. Verisign oder DigiCert), und fordern Sie signierte Zertifikate im PEM-Format an.
+
[CAUTION]
====
Nachdem Sie eine CSR-Datei an die CA gesendet haben, generieren SIE keine andere CSR-Datei. Wenn Sie eine CSR generieren, 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.

====
. Wenn die Zertifizierungsstelle die signierten Zertifikate zurückgibt, gehen Sie zu <<Schritt 3: Import Management Zertifikate>>.

== Schritt 3: Import Management Zertifikate

Nachdem Sie von der Zertifizierungsstelle (CA) signierte Zertifikate erhalten haben, importieren Sie die Zertifikate in das Host-System, auf dem die Web Services Proxy- und Unified Manager-Schnittstelle installiert sind.

.Bevor Sie beginnen
* Sie haben von der Zertifizierungsstelle signierte Zertifikate erhalten. 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 die Windows verwenden `certmgr` Dienstprogramm zum Auspacken der Dateien (Rechtsklick und wählen Sie Menü: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 haben die Zertifikatdateien auf das Hostsystem kopiert, auf dem der Web Services Proxy ausgeführt wird.

.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie auf der Registerkarte Verwaltung die Option *Import*.
+
Es wird ein Dialogfeld zum Importieren der Zertifikatdateien geöffnet.

. 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.

. Klicken Sie Auf *Import*.

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

[[IDb77d7c3d7282eac003ec417a6388d397]]
= Managementzertifikate zurücksetzen

```
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können das Managementzertifikat in den ursprünglichen, werkseitig
selbstsignierten Status zurücksetzen.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.

.Über diese Aufgabe
Diese Aufgabe löscht das aktuelle Managementzertifikat vom Host-System,
auf dem Web Services Proxy und Unified Manager installiert sind. Nach dem
Zurücksetzen des Zertifikats wird das Host-System auf das selbstsignierte
Zertifikat zurückgesetzt.

.Schritte
. Wählen Sie *Einstellungen > Zertifikate*.
. Wählen Sie die Registerkarte *Array Management* und dann *Reset*.
+
Das Dialogfeld „Zertifikat zurücksetzen bestätigen“ wird geöffnet.

. Typ `reset` Klicken Sie im Feld 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.



.Ergebnisse
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.



= Verwenden Sie Array-Zertifikate
```

```
:leveloffset: +1


[[ID3104f4c641004be7fa5f8c82b002abef]]
= Importieren Sie Zertifikate für Arrays
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Bei Bedarf können Zertifikate für die Speicher-Arrays importiert werden,
sodass sie sich mit dem System authentifizieren können, das SANtricity
Unified Manager hostet. Zertifikate können von einer Zertifizierungsstelle
(CA) signiert oder selbst signiert werden.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine
Zertifikatfunktionen angezeigt.
* Wenn Sie vertrauenswürdige Zertifikate importieren, müssen die
Zertifikate für die Speicher-Array-Controller mit System Manager
importiert werden.


.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie die Registerkarte * Trusted* aus.
+
Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-
Arrays gemeldet wurden.

. 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.
+
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.

. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf
*Import*.
+
Das Zertifikat wird hochgeladen und validiert.
```

```
[[IDaf15771ae703f02d3866e5ab9f031240]]
= Vertrauenswürdige Zertifikate löschen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
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.

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

====
.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie die Registerkarte * Trusted* aus.
. Wählen Sie ein oder mehrere Zertifikate in der Tabelle aus, und klicken
Sie dann auf *Löschen*.
+
[NOTE]
====
Die Funktion *Löschen* steht für vorinstallierte Zertifikate nicht zur
Verfügung.

====
+
Das Dialogfeld Vertrauenswürdiges Zertifikat bestätigen wird geöffnet.

. Bestätigen Sie den Löschvorgang, und klicken Sie dann auf *Löschen*.
+
Das Zertifikat wird aus der Tabelle entfernt.
```

```
[[IDf1d82d5843a7c0bb5b599c4959ba4f88]]
= Lösen Sie nicht vertrauenswürdige Zertifikate
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Nicht vertrauenswürdige Zertifikate treten auf, wenn ein Speicher-Array
versucht, eine sichere Verbindung zu SANtricity Unified Manager
herzustellen, die Verbindung jedoch nicht als sicher bestätigt.

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
* Sie müssen mit einem Benutzerprofil angemeldet sein, das die
Berechtigungen für den Sicherheitsadministrator enthält.
* Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat
importieren möchten:
+
** 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
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.
* Ein oder beide Zertifikate werden widerrufen.
* Ein oder beide Zertifikate fehlen ein Stammzertifikat oder ein
Zwischenzertifikat.
```

.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie die Registerkarte * Trusted* aus.
+
Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-Arrays gemeldet wurden.

. 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.
+
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.

. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf *Import*.
+
Das Zertifikat wird hochgeladen und validiert.

:leveloffset: -1

= Verwalten von Zertifikaten

:leveloffset: +1

[[ID33d04116a0a1ee6d8cf2150fd024d30e]]
= Anzeigen von Zertifikaten
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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.

.Bevor Sie beginnen

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

.Schritte
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie eine der folgenden Registerkarten aus:
+
** *Management* -- zeigt das Zertifikat für das System, das den Web Services Proxy hostet. Ein Managementzertifikat kann von einer Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Die Lösung ermöglicht den sicheren Zugriff auf Unified Manager.
** *Trusted* -- zeigt Zertifikate an, auf die Unified Manager für Speicher-Arrays und andere Remote-Server, z. B. einen LDAP-Server, zugreifen kann. Die Zertifikate können von einer Zertifizierungsstelle (CA) ausgestellt oder selbst signiert werden.

. 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*.

[[ID66ae141aebfa8c56e314210b06ad48c8]]
= Exportieren von Zertifikaten
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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
. Wählen Sie *Zertifikatverwaltung*.
. Wählen Sie eine der folgenden Registerkarten aus:
+
** *Management* -- zeigt das Zertifikat für das System, das den Web Services Proxy hostet. Ein Managementzertifikat kann von einer

```
Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Die
Lösung ermöglicht den sicheren Zugriff auf Unified Manager.
** *Trusted* -- zeigt Zertifikate an, auf die Unified Manager für
Speicher-Arrays und andere Remote-Server, z. B. einen LDAP-Server,
zugreifen kann. Die Zertifikate können von einer Zertifizierungsstelle
(CA) ausgestellt oder selbst signiert werden.


. Wählen Sie auf der Seite ein Zertifikat aus, und klicken Sie dann am
Ende der Zeile auf die Ellipsen.
. Klicken Sie auf *Exportieren* und speichern Sie dann die
Zertifikatdatei.
. Öffnen Sie die Datei in Ihrer Zertifikatanzeige-Anwendung.




:leveloffset: -1


:leveloffset: -1


= Zugriffsmanagement

:leveloffset: +1


[[ID1c0ee513eb69ea353ee51758ed3d4157]]
= Zugriffsmanagement – Überblick
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die Zugriffsverwaltung ist eine Methode zur Konfiguration der
Benutzerauthentifizierung in SANtricity Unified Manager.



== Welche Authentifizierungsmethoden sind verfügbar?

Folgende Authentifizierungsmethoden sind verfügbar:

* *Lokale Benutzerrollen* -- Authentifizierung wird über RBAC-Funktionen
```

```
(rollenbasierte Zugriffssteuerung) verwaltet. Lokale Benutzerrollen
umfassen vordefinierte Benutzerprofile und Rollen mit spezifischen
Zugriffsberechtigungen.
* *Directory Services* -- die Authentifizierung wird über einen LDAP-
Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst
verwaltet, z. B. über Microsoft Active Directory.
* *SAML* -- Authentifizierung wird über einen Identitäts-Provider (IdP)
mit SAML 2.0 verwaltet.


Weitere Informationen:

* xref:{relative_path}how-access-management-works-
unified.html["Funktionsweise von Access Management"]
* xref:{relative_path}access-management-terminology-
unified.html["Terminologie für das Zugriffsmanagement"]
* xref:{relative_path}permissions-for-mapped-roles-
unified.html["Berechtigungen für zugeordnete Rollen"]
* xref:{relative_path}access-management-with-saml.html["SAML"]




== Wie konfiguriere ich Access Management?

Die SANtricity-Software ist für die Verwendung lokaler Benutzerrollen
vorkonfiguriert. Wenn Sie LDAP verwenden möchten, können Sie es auf der
Seite Zugriffsverwaltung konfigurieren.

Weitere Informationen:

* xref:{relative_path}access-management-with-local-user-roles-
unified.html["Zugriffsverwaltung mit lokalen Benutzerrollen"]
* xref:{relative_path}access-management-with-directory-services-
unified.html["Zugriffsmanagement mit Verzeichnisdiensten"]
* xref:{relative_path}configure-saml.html["Konfigurieren Sie SAML"]




= Konzepte

:leveloffset: +1


[[IDd1e10eb6355fe85cf38efe50f8468468]]
= Funktionsweise von Access Management
```

```
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Verwenden Sie die Zugriffsverwaltung, um die Benutzerauthentifizierung in
SANtricity Unified Manager einzurichten.



== Konfigurationsworkflow

Die Zugriffsmanagement-Konfiguration funktioniert wie folgt:

. Ein Administrator meldet sich bei Unified Manager mit einem
Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren
enthält.
+
[NOTE]
====
Bei der ersten Anmeldung wird der Benutzername verwendet `admin` Wird
automatisch angezeigt und kann nicht geändert werden. Der `admin` Der
Benutzer hat vollen Zugriff auf alle Funktionen im System. Das Passwort
muss bei der ersten Anmeldung festgelegt werden.

====
. Der Administrator navigiert zur Zugriffsverwaltung in der
Benutzeroberfläche, die vorkonfigurierte lokale Benutzerrollen enthält.
Diese Rollen sind eine Implementierung von RBAC-Funktionen (rollenbasierte
Zugriffssteuerung).
. Der Administrator konfiguriert eine oder mehrere der folgenden
Authentifizierungsmethoden:
+
** *Lokale Benutzerrollen* -- Authentifizierung wird über RBAC-Funktionen
verwaltet. Lokale Benutzerrollen umfassen vordefinierte Benutzer und
Rollen mit bestimmten Zugriffsberechtigungen. Administratoren können diese
lokalen Benutzerrollen als einzige Authentifizierungsmethode verwenden
oder in Kombination mit einem Verzeichnisdienst verwenden. Es ist keine
Konfiguration erforderlich – abgesehen von der Festlegung von Passwörtern
für die Benutzer.
** *Directory Services* -- die Authentifizierung wird über einen LDAP-
Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst
verwaltet, z. B. über Microsoft Active Directory. Ein Administrator stellt
eine Verbindung zum LDAP-Server her und ordnet die LDAP-Benutzer den
```

lokalen Benutzerrollen zu.
** *SAML* -- Authentifizierung wird über einen Identitäts-Provider (IdP) mit der Security Assertion Markup Language (SAML) 2.0 verwaltet. Ein Administrator stellt die Verbindung zwischen dem IdP-System und dem Storage-Array her und ordnet anschließend die IdP-Benutzer den im Storage-Array eingebetteten lokalen Benutzerrollen zu.

. Der Administrator stellt Benutzern die Anmeldeinformationen für Unified Manager zur Verfügung.
. Benutzer melden sich beim System an, indem sie ihre Anmeldedaten eingeben. Während der Anmeldung führt das System die folgenden Hintergrundaufgaben aus:
+
** Authentifiziert Benutzernamen und Kennwort anhand des Benutzerkontos.
** Legt die Berechtigungen des Benutzers basierend auf den zugewiesenen Rollen fest.
** Bietet dem Benutzer Zugriff auf Funktionen in der Benutzeroberfläche.
** Zeigt den Benutzernamen im oberen Banner an.

== Funktionen in Unified Manager verfügbar

Der Zugriff auf Funktionen hängt von den zugewiesenen Rollen eines Benutzers ab. Dazu gehören:

* *Storage Admin* -- Vollständiger Lese-/Schreibzugriff auf Speicherobjekte auf den Arrays, aber kein Zugriff auf die Sicherheitskonfiguration.
* *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access Management und Certificate Management.
* *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf Speicher-Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
* *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

Eine nicht verfügbare Funktion ist entweder ausgegraut oder wird in der Benutzeroberfläche nicht angezeigt.

```
[[IDd4d72a7c006f9444490c1e58a6419c62]]
= Terminologie für das Zugriffsmanagement
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Erfahren Sie, wie die Bedingungen für das Zugriffsmanagement für
SANtricity Unified Manager gelten.

[cols="25h,~"]
|===
| Laufzeit | Beschreibung


 a|
Active Directory
 a|
Active Directory (AD) ist ein Microsoft-Verzeichnisdienst, der LDAP für
Windows-Domänennetzwerke verwendet.



 a|
Verbindlich
 a|
Bindevorgänge werden zur Authentifizierung von Clients auf dem
Verzeichnisserver verwendet. Binding erfordert in der Regel Konto- und
Kennwortanmeldeinformationen, aber einige Server erlauben anonyme
Bindevorgänge.



 a|
CA
 a|
Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die
elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-
Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer,
die sichere Verbindungen zwischen Clients und Servern ermöglichen.



 a|
Zertifikat
```

a|	Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).
a| LDAP	a| Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll für den Zugriff auf verteilte Verzeichnisinformationsdienste und die Wartung. Mit diesem Protokoll können viele verschiedene Anwendungen und Dienste eine Verbindung zum LDAP-Server zur Überprüfung von Benutzern herstellen.
a| RBAC	a| Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) ist eine Methode zur Regulierung des Zugriffs auf Computer- oder Netzwerkressourcen, basierend auf den Rollen einzelner Benutzer. Unified Manager enthält vordefinierte Rollen.
a| SAML	a| Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für die Authentifizierung und Autorisierung zwischen zwei Einheiten. SAML ermöglicht Multi-Faktor-Authentifizierung, bei der Benutzer zwei oder mehr Elemente zur Identitätsnachweise bereitstellen müssen (z. B. ein Passwort und ein Fingerabdruck). Die in das Storage Array integrierte SAML-Funktion ist mit SAML2.0 zur Identitätsprüfung, Authentifizierung und Autorisierung kompatibel.
a| SSO	a| Bei Single Sign On (SSO) handelt es sich um einen

```
Authentifizierungsservice, mit dem ein Satz an Anmeldeinformationen auf
mehrere Anwendungen zugreifen kann.



 a|
Web Services Proxy
 a|
Der Web Services Proxy, der Zugriff über HTTPS-Standardmechanismen
bereitstellt, ermöglicht Administratoren die Konfiguration von
Managementservices für Speicher-Arrays. Der Proxy kann auf Windows- oder
Linux-Hosts installiert werden. Die Unified Manager-Schnittstelle ist mit
dem Web Services Proxy verfügbar.

|===



[[ID57186eaeac00558ce2682cebf7b2464d]]
= Berechtigungen für zugeordnete Rollen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Die RBAC-Funktionen (rollenbasierte Zugriffssteuerung) umfassen
vordefinierte Benutzer, wobei eine oder mehrere Rollen zugewiesen sind.
Jede Rolle umfasst Berechtigungen für den Zugriff auf Aufgaben in
SANtricity Unified Manager.

Die Rollen ermöglichen Benutzern den Zugriff auf Aufgaben wie folgt:

* *Storage Admin* -- Vollständiger Lese-/Schreibzugriff auf
Speicherobjekte auf den Arrays, aber kein Zugriff auf die
Sicherheitskonfiguration.
* *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management und Certificate Management.
* *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf Speicher-
Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte
oder die Sicherheitskonfiguration.
* *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


Wenn ein Benutzer über keine Berechtigungen für eine bestimmte Funktion
```

```
verfügt, ist diese Funktion entweder zur Auswahl nicht verfügbar oder wird
nicht in der Benutzeroberfläche angezeigt.



[[ID39ac0ffbf2bf6eccadf3dcfe2334c124]]
= Zugriffsverwaltung mit lokalen Benutzerrollen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Administratoren können die in SANtricity Unified Manager erzwungenen RBAC-
Funktionen (rollenbasierte Zugriffssteuerung) nutzen. Diese Funktionen
werden als „lokale Benutzerrollen“ bezeichnet.



== Konfigurationsworkflow

Lokale Benutzerrollen sind im System vorkonfiguriert. Um lokale
Benutzerrollen für die Authentifizierung zu verwenden, können
Administratoren Folgendes tun:

. Ein Administrator meldet sich bei Unified Manager mit einem
Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren
enthält.
+
[NOTE]
====
Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

====
. Ein Administrator überprüft die Benutzerprofile, die vordefiniert sind
und nicht geändert werden können.
. Optional weist der Administrator jedem Benutzerprofil neue Passwörter
zu.
. Benutzer melden sich mit ihren zugewiesenen Anmeldedaten am System an.



== Vereinfachtes

Bei der Verwendung von nur lokalen Benutzerrollen für die
```

```
Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben
ausführen:

* Passwörter ändern.
* Legen Sie eine Mindestlänge für Passwörter fest.
* Benutzern erlauben, sich ohne Passwörter anzumelden.




[[ID41530009dccae47b2b9f6ce97d191a1b]]
= Zugriffsmanagement mit Verzeichnisdiensten
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Administratoren können einen LDAP-Server (Lightweight Directory Access
Protocol) und einen Verzeichnisdienst wie Microsoft Active Directory
verwenden.



== Konfigurationsworkflow

Wenn ein LDAP-Server und ein Verzeichnisdienst im Netzwerk verwendet
werden, funktioniert die Konfiguration wie folgt:

. Ein Administrator meldet sich bei Unified Manager mit einem
Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren
enthält.
+
[NOTE]
====
Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

====
. Der Administrator gibt die Konfigurationseinstellungen für den LDAP-
Server ein. Zu den Einstellungen gehören der Domain-Name, die URL und die
Bind-Kontoinformationen.
. Wenn der LDAP-Server ein sicheres Protokoll (LDAPS) verwendet, lädt der
Administrator eine Zertifikatskette für die Authentifizierung zwischen dem
LDAP-Server und dem Hostsystem, auf dem der Web Services Proxy installiert
ist, hoch.
. Nachdem die Serververbindung hergestellt wurde, ordnet der Administrator
```

die Benutzergruppen den lokalen Benutzerrollen zu. Diese Rollen sind vordefiniert und können nicht geändert werden.
. Der Administrator testet die Verbindung zwischen dem LDAP-Server und dem Web Services Proxy.
. Benutzer melden sich mit ihren zugewiesenen LDAP/Directory Services-Anmeldedaten am System an.

== Vereinfachtes

Bei der Verwendung von Verzeichnisdiensten zur Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben ausführen:

* Fügen Sie einen Verzeichnisserver hinzu.
* Bearbeiten der Einstellungen des Verzeichnisservers.
* Zuordnen von LDAP-Benutzern zu lokalen Benutzerrollen.
* Entfernen Sie einen Verzeichnisserver.
* Passwörter ändern.
* Legen Sie eine Mindestlänge für Passwörter fest.
* Benutzern erlauben, sich ohne Passwörter anzumelden.

[[IDf4c4251b853a996d0b67ac82efde92cd]]
= Zugriffsmanagement mit SAML
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Für die Zugriffsverwaltung können Administratoren die in das Array integrierten Funktionen der Security Assertion Markup Language (SAML) 2.0 verwenden.

== Konfigurationsworkflow

Die SAML-Konfiguration funktioniert wie folgt:

. Ein Administrator meldet sich bei Unified Manager mit einem Benutzerprofil an, das Sicherheitsadministratorberechtigungen enthält.

+
[NOTE]
====
Der `admin` Der Benutzer hat vollständigen Zugriff auf alle Funktionen in System Manager.

====
. Der Administrator wechselt zur Registerkarte *SAML* unter Zugriffsverwaltung.
. Ein Administrator konfiguriert die Kommunikation mit dem Identity Provider (IdP). Ein IdP ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert werden und festgestellt wird, ob der Benutzer erfolgreich authentifiziert wurde. Um die Kommunikation mit dem Speicher-Array zu konfigurieren, lädt der Administrator die IdP-Metadatendatei vom IdP-System herunter und lädt die Datei dann mithilfe von Unified Manager auf das Speicher-Array hoch.
. Ein Administrator stellt eine Vertrauensbeziehung zwischen dem Dienstanbieter und dem IdP her. Ein Dienstanbieter steuert die Benutzerautorisierung. In diesem Fall fungiert der Controller im Speicher-Array als Service Provider. Zum Konfigurieren der Kommunikation verwendet der Administrator Unified Manager, um eine Service Provider-Metadatendatei für den Controller zu exportieren. Vom IdP-System importiert der Administrator dann die Metadatendatei in das IdP.
+
[NOTE]
====
Administratoren sollten außerdem sicherstellen, dass das IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.

====
. Der Administrator ordnet die Rollen des Storage-Arrays den in IdP definierten Benutzerattributen zu. Dazu verwendet der Administrator Unified Manager zum Erstellen der Zuordnungen.
. Der Administrator testet die SSO-Anmeldung an der IdP-URL. Dieser Test stellt sicher, dass das Storage-Array und das IdP kommunizieren können.
+
[CAUTION]
====
Sobald SAML aktiviert ist, können Sie sie über die Benutzeroberfläche nicht deaktivieren oder die IdP-Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an den technischen Support, um Hilfe zu erhalten.

====
. Über Unified Manager aktiviert der Administrator SAML für das Storage-

```
Array.
. Benutzer melden sich mit ihren SSO-Anmeldedaten am System an.




== Vereinfachtes

Bei der Verwendung von SAML zur Authentifizierung können Administratoren
die folgenden Managementaufgaben ausführen:

* Neue Rollenzuordnungen ändern oder erstellen
* Exportieren Sie die Dateien von Dienstanbietern




== Zugriffsbeschränkungen

Wenn SAML aktiviert ist, können Benutzer Speicher für dieses Array nicht
über die vorhandene Storage Manager-Schnittstelle ermitteln oder
verwalten.

Außerdem können die folgenden Clients nicht auf Services und Ressourcen
des Speicherarrays zugreifen:

* Enterprise Management-Fenster (EMW)
* Befehlszeilenschnittstelle (CLI)
* Software Developer Kits (SDK)-Clients
* In-Band-Clients
* REST-API-Clients für die HTTP-Standardauthentifizierung
* Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an




:leveloffset: -1


= Lokale Benutzerrollen verwenden

:leveloffset: +1


[[IDea83142c3fb4cc5da66131bdbb16ba91]]
= Zeigen Sie lokale Benutzerrollen an
:allow-uri-read:
```

```
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Auf der Registerkarte Lokale Benutzerrollen können Sie die Zuordnungen der
Benutzer zu den Standardrollen anzeigen. Diese Zuordnungen sind Teil der
RBAC (rollenbasierte Zugriffssteuerung), die im Web Services Proxy für
SANtricity Unified Manager durchgesetzt wird.

.Bevor Sie beginnen
Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.

.Über diese Aufgabe
Die Benutzer und Zuordnungen können nicht geändert werden. Es können nur
Passwörter geändert werden.

.Schritte
. Wählen Sie *Zugriffsmanagement*.
. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
+
Die Benutzer sind in der Tabelle aufgeführt:

+
** *Admin* -- Super-Administrator, der Zugriff auf alle Funktionen im
System hat. Dieser Benutzer enthält alle Rollen.
** *Storage* -- der Administrator, der für die gesamte Storage-
Bereitstellung verantwortlich ist. Dieser Benutzer umfasst die folgenden
Rollen: Storage-Administrator, Support-Administrator und Monitor.
** *Sicherheit* -- der für die Sicherheitskonfiguration verantwortliche
Benutzer, einschließlich Zugriffsverwaltung und Zertifikatverwaltung.
Dieser Benutzer umfasst die folgenden Rollen: Security Admin und Monitor.
** *Support* -- der Benutzer, der für Hardware-Ressourcen, Ausfalldaten
und Firmware-Upgrades verantwortlich ist. Dieser Benutzer enthält die
folgenden Rollen: Unterstützen Sie Admin und Monitor.
** *Monitor* -- ein Benutzer mit schreibgeschütztem Zugriff auf das
System. Dieser Benutzer enthält nur die Rolle „Monitor“.
** *rw* (lesen/schreiben) -- dieser Benutzer enthält die folgenden Rollen:
Speicheradministrator, Supportadministrator und Monitor.
** *Ro* (schreibgeschützt) -- dieser Benutzer enthält nur die Rolle
Monitor.
```

```
[[ID834d73fdf1e0609bdc44a66b6d889ada]]
= Passwörter für lokale Benutzerprofile ändern
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Sie können die Benutzerpasswörter für jeden Benutzer in der
Zugriffsverwaltung ändern.

.Bevor Sie beginnen
* Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-
Berechtigungen enthält.
* Sie müssen das lokale Administratorkennwort kennen.


.Über diese Aufgabe
Beachten Sie bei der Auswahl eines Passworts die folgenden Richtlinien:

* Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Einstellung
für ein Mindestpasswort erfüllen oder überschreiten (unter „Einstellungen
anzeigen/bearbeiten“).
* Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt.
* Nachgestellte Leerzeichen werden nicht aus Kennwörtern entfernt, wenn
sie gesetzt sind. Achten Sie darauf, Leerzeichen einzugeben, wenn diese im
Passwort enthalten waren.
* Um die Sicherheit zu erhöhen, verwenden Sie mindestens 15
alphanumerische Zeichen, und ändern Sie das Passwort häufig.


.Schritte
. Wählen Sie *Zugriffsmanagement*.
. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
. Wählen Sie einen Benutzer aus der Tabelle aus.
+
Die Schaltfläche Kennwort ändern steht zur Verfügung.

. Wählen Sie *Passwort Ändern*.
+
Das Dialogfeld Kennwort ändern wird geöffnet.

. Wenn für lokale Benutzerpasswörter keine Mindestkennwortlänge festgelegt
```

ist, können Sie das Kontrollkästchen aktivieren, damit der Benutzer ein Passwort für den Zugriff auf das System eingeben muss.
. Geben Sie das neue Kennwort für den ausgewählten Benutzer in die beiden Felder ein.
. Geben Sie Ihr lokales Administratorpasswort ein, um diesen Vorgang zu bestätigen, und klicken Sie dann auf *Ändern*.

.Ergebnisse
Wenn der Benutzer derzeit angemeldet ist, wird die aktive Sitzung des Benutzers durch die Kennwortänderung beendet.

[[ID37dca524dbd806ccaf578bce74b1b09b]]
= Ändern Sie die Einstellungen für das lokale Benutzerpasswort
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Sie können die erforderliche Mindestlänge für alle neuen oder aktualisierten lokalen Benutzerpasswörter festlegen. Außerdem können lokale Benutzer ohne Eingabe eines Kennworts auf das System zugreifen.

.Bevor Sie beginnen
Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-Berechtigungen enthält.

.Über diese Aufgabe
Beachten Sie die folgenden Richtlinien, wenn Sie die Mindestlänge für lokale Benutzerpasswörter festlegen:

* Die Einstellung von Änderungen hat keine Auswirkung auf vorhandene lokale Benutzerpasswörter.
* Die Mindestlänge für lokale Benutzerpasswörter muss zwischen 0 und 30 Zeichen liegen.
* Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Mindestlängeneinstellung erfüllen oder überschreiten.
* Legen Sie keine Mindestlänge für das Passwort fest, wenn lokale Benutzer ohne Eingabe eines Kennworts auf das System zugreifen möchten.

.Schritte
. Wählen Sie *Zugriffsmanagement*.

```
. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
. Wählen Sie *Einstellungen Anzeigen/Bearbeiten*.
+
Das Dialogfeld Einstellungen für das lokale Benutzerpasswort wird
geöffnet.

. Führen Sie einen der folgenden Schritte aus:
+
** Um lokalen Benutzern den Zugriff auf das System zu ermöglichen _ohne_
ein Passwort einzugeben, deaktivieren Sie das Kontrollkästchen „Alle
lokalen Benutzerpasswörter müssen mindestens sein“.
** Um eine Mindestkennwortlänge für alle lokalen Benutzerpasswörter
festzulegen, aktivieren Sie das Kontrollkästchen „Alle lokalen
Benutzerpasswörter müssen mindestens sein“. Verwenden Sie dann das
Spinner-Feld, um die erforderliche Mindestlänge für alle lokalen
Benutzerpasswörter festzulegen.
+
Neue lokale Benutzerpasswörter müssen die aktuelle Einstellung erfüllen
oder überschreiten.



. Klicken Sie Auf *Speichern*.




:leveloffset: -1


= Verzeichnisdienste verwenden

:leveloffset: +1


[[ID684a4efd99da341a9d7d888c7d97a884]]
= Verzeichnisserver hinzufügen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um die Authentifizierung für die Zugriffsverwaltung zu konfigurieren,
stellen Sie eine Kommunikation zwischen einem LDAP-Server und dem Host
her, auf dem der Web Services Proxy für SANtricity Unified Manager
```

```
ausgeführt wird. Anschließend ordnen Sie die LDAP-Benutzergruppen den
lokalen Benutzerrollen zu.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
* LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich
Domänenname, Server-URL und optional Benutzername und Kennwort für das
Bindekonto.
* Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette
des LDAP-Servers auf Ihrem lokalen Computer installiert sein.


.Über diese Aufgabe
Das Hinzufügen eines Verzeichnisservers ist ein zweistufiger Prozess.
Geben Sie zuerst den Domain-Namen und die URL ein. Wenn Ihr Server ein
sicheres Protokoll verwendet, müssen Sie auch ein CA-Zertifikat zur
Authentifizierung hochladen, wenn es von einer nicht standardmäßigen
Signierungsbehörde signiert ist. Wenn Sie über Anmeldedaten für ein
Bindekonto verfügen, können Sie auch Ihren Benutzernamen und Ihr Kennwort
eingeben. Als Nächstes werden die Benutzergruppen des LDAP-Servers lokalen
Benutzerrollen zugeordnet.

.Schritte
. Wählen Sie *Zugriffsmanagement*.
. Wählen Sie auf der Registerkarte *Directory Services* die Option *Add
Directory Server* aus.
+
Das Dialogfeld Add Directory Server wird geöffnet.

. Geben Sie auf der Registerkarte *Server-Einstellungen* die
Anmeldeinformationen für den LDAP-Server ein.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Konfigurationseinstellungen*
```

 a|
Domäne(en)
 a|
Geben Sie den Domänennamen des LDAP-Servers ein. Geben Sie für mehrere Domänen die Domänen in eine kommagetrennte Liste ein. Der Domänenname wird in der Anmeldung (_username_@_Domain_) verwendet, um anzugeben, gegen welchen Verzeichnisserver sich authentifizieren soll.

 a|
Server-URL
 a|
Geben Sie die URL für den Zugriff auf den LDAP-Server in Form von ein `ldap[s]://*host*:*port*`.

 a|
Zertifikat hochladen (optional)
 a|

NOTE: Dieses Feld wird nur angezeigt, wenn ein LDAPS-Protokoll im obigen Feld Server-URL angegeben wird.

Klicken Sie auf *Durchsuchen* und wählen Sie ein CA-Zertifikat zum Hochladen aus. Dies ist das vertrauenswürdige Zertifikat oder die Zertifikatskette, die für die Authentifizierung des LDAP-Servers verwendet wird.

 a|
Konto binden (optional)
 a|
Geben Sie ein schreibgeschütztes Benutzerkonto ein, um Suchanfragen auf dem LDAP-Server und für die Suche in den Gruppen durchzuführen. Geben Sie den Kontonamen im LDAP-Format ein. Wenn der Bindebenutzer beispielsweise „bind-Konto“ heißt, können Sie einen Wert wie eingeben `CN=bindacct,CN=Users,DC=cpoc,DC=local`.

 a|
Bindepasswort (optional)
 a|

NOTE: Dieses Feld wird angezeigt, wenn Sie ein Bindungskonto eingeben.

Geben Sie das Passwort für das Bindekonto ein.

a|
Testen Sie die Serververbindung, bevor Sie sie hinzufügen
a|
Aktivieren Sie dieses Kontrollkästchen, wenn Sie sicherstellen möchten, dass das System mit der eingegebenen LDAP-Serverkonfiguration kommunizieren kann. Der Test erfolgt, nachdem Sie unten im Dialogfeld auf *Hinzufügen* geklickt haben.

Wenn dieses Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die Konfiguration nicht hinzugefügt. Sie müssen den Fehler beheben oder das Kontrollkästchen deaktivieren, um den Test zu überspringen und die Konfiguration hinzuzufügen.

a|
Berechtigungseinstellungen

a|
Basis-DN suchen
a|
Geben Sie den LDAP-Kontext ein, um nach Benutzern zu suchen, normalerweise in Form von `CN=Users, DC=cpoc, DC=local`.

a|
Attribut Benutzername
a|
Geben Sie das Attribut ein, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: `sAMAccountName`.

a|
Gruppenattribut(e)
a|
Geben Sie eine Liste der Gruppenattribute für den Benutzer ein, die für

```
die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: `memberOf,
managedObjects`.

|===
====
. Klicken Sie auf die Registerkarte *Rollenzuordnung*.
. Weisen Sie den vordefinierten Rollen LDAP-Gruppen zu. Einer Gruppe
können mehrere Rollen zugewiesen sein.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Gruppen-DN
 a|
Geben Sie den Group Distinguished Name (DN) für die zu zugeordnete LDAP-
Benutzergruppe an. Reguläre Ausdrücke werden unterstützt. Diese speziellen
regulären Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich (\)
entgangen werden, wenn sie nicht Teil eines regulären Ausdrucksmusters
sind: \.[]{}()<>*+-=!?^



 a|
Rollen
 a|
Klicken Sie in das Feld, und wählen Sie eine der lokalen Benutzerrollen
aus, die dem Gruppen-DN zugeordnet werden sollen. Sie müssen jede Rolle,
die Sie für diese Gruppe aufnehmen möchten, einzeln auswählen. Die
Monitorrolle ist erforderlich, um sich in SANtricity Unified Manager mit
den anderen Rollen anzumelden. Die zugeordneten Rollen umfassen die
folgenden Berechtigungen:

** *Storage Admin* -- Vollständiger Lese-/Schreibzugriff auf
Speicherobjekte auf den Arrays, aber kein Zugriff auf die
Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
```

```
Management und Certificate Management.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf Speicher-
Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte
oder die Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


|===
====
+

NOTE: Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich.

. Klicken Sie auf *Weitere Zuordnungen hinzufügen*, um weitere Gruppen-zu-
Rolle-Zuordnungen einzugeben.
. Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf *Hinzufügen*.
+
Das System führt eine Validierung durch und stellt sicher, dass das
Speicher-Array und der LDAP-Server kommunizieren können. Wenn eine
Fehlermeldung angezeigt wird, überprüfen Sie die im Dialogfeld
eingegebenen Anmeldeinformationen, und geben Sie die Informationen ggf.
erneut ein.




[[ID018a56f0dce75ebcc1c19946b860185c]]
= Bearbeiten Sie die Einstellungen des Verzeichnisservers und die
Rollenzuordnungen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie zuvor einen Verzeichnisserver in der Zugriffsverwaltung
konfiguriert haben, können Sie dessen Einstellungen jederzeit ändern. Zu
den Einstellungen gehören die Informationen zur Serververbindung und die
Zuordnungen von Gruppen zu Rollen.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
```

```
Zugriffsverwaltungsfunktionen nicht angezeigt.
* Ein Verzeichnisserver muss definiert werden.


.Schritte
. Wählen Sie *Zugriffsmanagement*.
. Wählen Sie die Registerkarte *Directory Services* aus.
. Wenn mehr als ein Server definiert ist, wählen Sie den Server aus der
Tabelle aus, den Sie bearbeiten möchten.
. Wählen Sie *Einstellungen Anzeigen/Bearbeiten*.
+
Das Dialogfeld Verzeichnisservereinstellungen wird geöffnet.

. Ändern Sie auf der Registerkarte *Server-Einstellungen* die gewünschten
Einstellungen.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Konfigurationseinstellungen*



 a|
Domäne(en)
 a|
Der/die Domänenname(n) des/der LDAP-Server(e). Geben Sie für mehrere
Domänen die Domänen in eine kommagetrennte Liste ein. Der Domänenname wird
in der Anmeldung (_username_@_Domain_) verwendet, um anzugeben, gegen
welchen Verzeichnisserver sich authentifizieren soll.



 a|
Server-URL
 a|
Die URL für den Zugriff auf den LDAP-Server in Form von
`ldap[s]://host:port`.
```

```
 a|
Konto binden (optional)
 a|
Das schreibgeschützte Benutzerkonto für Suchabfragen am LDAP-Server und
für die Suche in den Gruppen.



 a|
Bindepasswort (optional)
 a|
Das Kennwort für das Bindekonto. (Dieses Feld wird angezeigt, wenn ein
Bindekonto eingegeben wird.)



 a|
Testen Sie vor dem Speichern die Serververbindung
 a|
Überprüft, ob das System mit der LDAP-Serverkonfiguration kommunizieren
kann. Der Test erfolgt nach dem Klicken auf *Speichern*. Wenn dieses
Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die
Konfiguration nicht geändert. Sie müssen den Fehler beheben oder das
Kontrollkästchen deaktivieren, um den Test zu überspringen und die
Konfiguration erneut zu bearbeiten.



 a|
*Berechtigungseinstellungen*



 a|
Basis-DN suchen
 a|
Der LDAP-Kontext für die Suche nach Benutzern, in der Regel in Form von
`CN=Users, DC=cpoc, DC=local`.



 a|
Attribut Benutzername
 a|
Das Attribut, das zur Authentifizierung an die Benutzer-ID gebunden ist.
Beispiel:
`sAMAccountName`.
```

```
 a|
Gruppenattribut(e)
 a|
Eine Liste der Gruppenattribute für den Benutzer, die für die Zuordnung
von Gruppen zu Rollen verwendet werden. Beispiel:
`memberOf, managedObjects`.

|===
====
. Ändern Sie auf der Registerkarte *Rollenzuordnung* die gewünschte
Zuordnung.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Gruppen-DN
 a|
Der Domain-Name für die LDAP-Benutzergruppe, die zugeordnet werden soll.
Reguläre Ausdrücke werden unterstützt. Diese speziellen regulären
Ausdruckszeichen müssen mit einem umgekehrten Schrägstrich (\) entgangen
werden, wenn sie nicht Teil eines regulären Ausdrucksmusters sind:

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



 a|
Rollen
 a|
Die Rollen, die dem Gruppen-DN zugeordnet werden sollen. Sie müssen jede
Rolle, die Sie für diese Gruppe aufnehmen möchten, einzeln auswählen. Die
Monitorrolle ist erforderlich, um sich in SANtricity Unified Manager mit
den anderen Rollen anzumelden. Dazu gehören folgende Rollen:
```

```
** *Storage Admin* -- Vollständiger Lese-/Schreibzugriff auf
Speicherobjekte auf den Arrays, aber kein Zugriff auf die
Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management und Certificate Management.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf Speicher-
Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte
oder die Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


|===
====
+

NOTE: Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich.

. Klicken Sie auf *Weitere Zuordnungen hinzufügen*, um weitere Gruppen-zu-
Rolle-Zuordnungen einzugeben.
. Klicken Sie Auf *Speichern*.


.Ergebnisse
Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen
beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.



[[ID6990ddaa89457d86c7ecffee1d33d981]]
= Verzeichnisserver entfernen
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Um die Verbindung zwischen einem Verzeichnisserver und dem Web Services
Proxy zu unterbrechen, können Sie die Serverinformationen von der Seite
Zugriffsverwaltung entfernen. Sie möchten diese Aufgabe möglicherweise
ausführen, wenn Sie einen neuen Server konfiguriert haben und den alten
dann entfernen möchten.

.Bevor Sie beginnen
```

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

.Über diese Aufgabe
Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.

.Schritte
. Wählen Sie *Zugriffsmanagement*.
. Wählen Sie die Registerkarte *Directory Services* aus.
. Wählen Sie in der Liste den Verzeichnisserver aus, den Sie löschen möchten.
. Klicken Sie Auf *Entfernen*.
+
Das Dialogfeld Verzeichnisserver entfernen wird geöffnet.

. Typ `remove` Klicken Sie im Feld auf *Entfernen*.
+
Die Konfigurationseinstellungen des Verzeichnisservers, die Berechtigungseinstellungen und Rollenzuordnungen werden entfernt. Benutzer können sich nicht mehr mit Anmeldeinformationen von diesem Server anmelden.

:leveloffset: -1

= Verwenden Sie SAML

:leveloffset: +1

[[ID06fe6d3b590475efd3d351072062d9b1]]
= Konfigurieren Sie SAML
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Zum Konfigurieren der Authentifizierung für das Zugriffsmanagement können

Sie die im Speicher-Array integrierten SAML-Funktionen (Security Assertion Markup Language) verwenden. Mit dieser Konfiguration wird eine Verbindung zwischen einem Identitätsanbieter und dem Speicheranbieter hergestellt.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
* Sie müssen die IP-Adresse oder den Domänennamen des Controllers im Speicher-Array kennen.
* Ein IdP-Administrator hat ein IdP-System konfiguriert.
* Ein IdP-Administrator hat sichergestellt, dass der IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.
* Ein Administrator hat sichergestellt, dass der IdP-Server und die Controller-Uhr synchronisiert werden (entweder über einen NTP-Server oder durch Anpassung der Controller-Uhreinstellungen).
* Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, das für den Zugriff auf Unified Manager verwendet wird.

.Über diese Aufgabe
Ein Identitäts-Provider (IdP) ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert und festgestellt werden können, ob dieser Benutzer erfolgreich authentifiziert wurde. Der IdP kann so konfiguriert werden, dass er Multi-Faktor-Authentifizierung bietet und eine beliebige Benutzerdatenbank, wie z. B. Active Directory, verwendet. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich. Ein Service-Provider (SP) ist ein System, das die Benutzerauthentifizierung und den Zugriff steuert. Wenn Access Management mit SAML konfiguriert ist, fungiert das Storage-Array als Dienstanbieter für die Anforderung der Authentifizierung vom Identity Provider. Um eine Verbindung zwischen dem IdP und dem Storage-Array herzustellen, teilen Sie Metadatendateien zwischen diesen beiden Einheiten gemeinsam. Als Nächstes ordnen Sie die IdP-Benutzereinheiten den Storage-Array-Rollen zu. Und schließlich testen Sie die Verbindung und SSO-Anmeldedaten, bevor Sie SAML aktivieren.

[NOTE]
====
SAML und Directory Services. Wenn Sie SAML aktivieren, wenn die Verzeichnisdienste als Authentifizierungsmethode konfiguriert sind, ersetzt SAML die Verzeichnisdienste in Unified Manager. Wenn Sie SAML später deaktivieren, wird die Konfiguration der Verzeichnisdienste wieder in die vorherige Konfiguration zurückgeführt.

```
====
[CAUTION]
====
*Bearbeiten und Deaktivieren.* Sobald SAML aktiviert ist, können Sie es
nicht über die Benutzeroberfläche deaktivieren, noch können Sie die IdP-
Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren
oder bearbeiten müssen, wenden Sie sich an den technischen Support, um
Hilfe zu erhalten.

====
Die Konfiguration der SAML-Authentifizierung erfolgt in mehreren
Schritten.



== Schritt 1: Laden Sie die IdP-Metadatendatei hoch

Um IdP-Verbindungsinformationen für das Storage-Array bereitzustellen,
importieren Sie IdP-Metadaten in Unified Manager. Das IdP-System benötigt
diese Metadaten, um Authentifizierungsanforderungen an die richtige URL
weiterzuleiten und die erhaltenen Antworten zu validieren.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *SAML* aus.
+
Auf der Seite wird eine Übersicht der Konfigurationsschritte angezeigt.

. Klicken Sie auf den Link * Import Identity Provider (IdP) file*.
+
Das Dialogfeld „Datei des Identitätsanbieters importieren“ wird geöffnet.

. Klicken Sie auf *Durchsuchen*, um die IdP-Metadatendatei auszuwählen und
auf Ihr lokales System hochzuladen.
+
Nach der Auswahl der Datei wird die IdP-Entity-ID angezeigt.

. Klicken Sie Auf *Import*.



== Schritt 2: Exportieren Sie die Dateien des Dienstanbieters

Um eine Vertrauensbeziehung zwischen dem IdP und dem Storage-Array
herzustellen, importieren Sie die Metadaten des Service-Providers in das
IdP. Das IdP benötigt diese Metadaten, um eine Vertrauensbeziehung zum
```

Controller herzustellen und Autorisierungsanforderungen zu verarbeiten. Die Datei enthält Informationen wie den Domänennamen oder die IP-Adresse des Controllers, sodass das IdP mit den Service-Providern kommunizieren kann.

.Schritte
. Klicken Sie auf den Link *Export Service Provider Files*.
+
Das Dialogfeld Dateien des Dienstanbieters exportieren wird geöffnet.

. Geben Sie die Controller-IP-Adresse oder den DNS-Namen in das Feld *Controller A* ein, und klicken Sie dann auf *Exportieren*, um die Metadatendatei auf Ihrem lokalen System zu speichern.
+
Nachdem Sie auf *Export* geklickt haben, werden die Metadaten des Dienstanbieters auf Ihr lokales System heruntergeladen. Notieren Sie sich, wo die Datei gespeichert ist.

. Suchen Sie vom lokalen System aus die XML-formatierte Service Provider-Metadatendatei, die Sie exportiert haben.
. Importieren Sie vom IdP-Server die Metadatendatei des Dienstanbieters, um die Vertrauensbeziehung herzustellen. Sie können die Datei entweder direkt importieren oder die Controller-Informationen manuell aus der Datei eingeben.

== Schritt 3: Rollen zuordnen

Um Benutzern die Autorisierung und den Zugriff auf Unified Manager zu ermöglichen, müssen Sie die IdP-Benutzerattribute und Gruppenmitgliedschaften den vordefinierten Rollen des Speicherarrays zuordnen.

.Bevor Sie beginnen
* Ein IdP-Administrator hat Benutzerattribute und Gruppenmitgliedschaften im IdP-System konfiguriert.
* Die IdP-Metadatendatei wird in Unified Manager importiert.
* Für die Vertrauensstellung wird eine Service Provider-Metadatendatei für den Controller in das IdP-System importiert.

.Schritte
. Klicken Sie auf den Link für *Mapping Unified Manager*-Rollen.
+
Das Dialogfeld Rollenzuordnung wird geöffnet.

```
. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen
zu. Einer Gruppe können mehrere Rollen zugewiesen sein.
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Benutzerattribut
 a|
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-
Gruppe an.



 a|
Attributwert
 a|
Geben Sie den Attributwert für die zu zugeordnete Gruppe an. Reguläre
Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen
müssen mit einem umgekehrten Schrägstrich entgangen werden (`\`Wenn sie
nicht Teil eines regulären Ausdrucksmusters sind: \.[]{}()<>*+-=!?^



 a|
Rollen
 a|
Klicken Sie in das Feld, und wählen Sie eine der Rollen des Speicherarrays
aus, die dem Attribut zugeordnet werden sollen. Sie müssen jede Rolle
einzeln auswählen, die Sie einschließen möchten. Die Rolle Monitor ist
zusammen mit den anderen Rollen für die Anmeldung bei Unified Manager
erforderlich. Die Sicherheitsadministratorrolle ist auch für mindestens
eine Gruppe erforderlich.

Die zugeordneten Rollen umfassen die folgenden Berechtigungen:
```

```
** *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes
und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management, Zertifikatverwaltung, Audit Log Management und die
Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder
auszuschalten.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem
Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-
Upgrades. Kein Zugriff auf Speicherobjekte oder die
Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


|===
====
+
[NOTE]
====
Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Unified Manager funktioniert für keinen
Benutzer ordnungsgemäß, ohne dass die Überwachungsfunktion vorhanden ist.

====
. Klicken Sie auf *Weitere Zuordnungen hinzufügen*, um weitere Gruppen-zu-
Rolle-Zuordnungen einzugeben.
+
[NOTE]
====
Rollenzuordnungen können geändert werden, nachdem SAML aktiviert ist.

====
. Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf *Speichern*.




== Schritt 4: SSO-Anmeldung testen

Um sicherzustellen, dass das IdP-System und das Speicherarray
kommunizieren können, können Sie optional eine SSO-Anmeldung testen.
Dieser Test wird auch während des letzten Schritts zur Aktivierung von
SAML durchgeführt.

.Bevor Sie beginnen
* Die IdP-Metadatendatei wird in Unified Manager importiert.
* Für die Vertrauensstellung wird eine Service Provider-Metadatendatei für
```

den Controller in das IdP-System importiert.

.Schritte
. Klicken Sie auf den Link *SSO-Login testen*.
+
Zum Eingeben von SSO-Anmeldedaten wird ein Dialogfeld geöffnet.

. Geben Sie die Anmeldeinformationen für einen Benutzer mit Sicherheitsadministratorrechten und Überwachungsberechtigungen ein.
+
Ein Dialogfeld wird geöffnet, während das System die Anmeldung testet.

. Suchen Sie nach einer Meldung für den erfolgreichen Test. Wenn der Test erfolgreich abgeschlossen wurde, fahren Sie mit dem nächsten Schritt zur Aktivierung von SAML fort.
+
Wenn der Test nicht erfolgreich abgeschlossen wird, wird eine Fehlermeldung mit weiteren Informationen angezeigt. Stellen Sie sicher, dass:

+
** Der Benutzer gehört zu einer Gruppe mit Berechtigungen für Security Admin und Monitor.
** Die Metadaten, die Sie für den IdP-Server hochgeladen haben, sind korrekt.
** Die Controller-Adresse in den SP-Metadatendateien ist korrekt.

== Schritt 5: SAML aktivieren

Der letzte Schritt besteht darin, die SAML-Konfiguration für die Benutzerauthentifizierung abzuschließen. Während dieses Prozesses werden Sie vom System auch aufgefordert, eine SSO-Anmeldung zu testen. Der SSO-Anmelde-Test wird im vorherigen Schritt beschrieben.

.Bevor Sie beginnen
* Die IdP-Metadatendatei wird in Unified Manager importiert.
* Für die Vertrauensstellung wird eine Service Provider-Metadatendatei für den Controller in das IdP-System importiert.
* Mindestens ein Monitor und eine Sicherheitsadministratorzuordnung sind konfiguriert.

```
[CAUTION]
====
*Bearbeiten und Deaktivieren.* Sobald SAML aktiviert ist, können Sie es
nicht über die Benutzeroberfläche deaktivieren, noch können Sie die IdP-
Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren
oder bearbeiten müssen, wenden Sie sich an den technischen Support, um
Hilfe zu erhalten.

====
.Schritte
. Wählen Sie auf der Registerkarte *SAML* den Link *SAML* aktivieren.
+
Das Dialogfeld SAML aktivieren bestätigen wird geöffnet.

. Typ `enable`, Und klicken Sie dann auf *Aktivieren*.
. Geben Sie die Benutzeranmeldeinformationen für einen SSO-Anmeldetest
ein.


.Ergebnisse
Nachdem das System SAML aktiviert hat, werden alle aktiven Sitzungen
beendet und die Authentifizierung von Benutzern über SAML beginnt.



[[IDd1d99dd1924dd67b365fc1fa9848a68f]]
= SAML-Rollenzuordnungen ändern
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie zuvor SAML für Access Management konfiguriert haben, können Sie
die Rollenzuordnungen zwischen den IdP-Gruppen und den vordefinierten
Rollen des Speicherarrays ändern.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* Ein IdP-Administrator hat Benutzerattribute und Gruppenmitgliedschaften
im IdP-System konfiguriert.
* SAML wurde konfiguriert und aktiviert.
```

```
.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *SAML* aus.
. Wählen Sie *Rollenzuordnung*.
+
Das Dialogfeld Rollenzuordnung wird geöffnet.

. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen
zu. Einer Gruppe können mehrere Rollen zugewiesen sein.
+
[CAUTION]
====
Achten Sie darauf, dass Sie Ihre Berechtigungen nicht entfernen, während
SAML aktiviert ist, sonst verlieren Sie den Zugriff auf Unified Manager.

====
+
.Felddetails
[%collapsible]
====
[cols="25h,~"]
|===
| Einstellung | Beschreibung


 a|
*Zuordnungen*



 a|
Benutzerattribut
 a|
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-
Gruppe an.



 a|
Attributwert
 a|
Geben Sie den Attributwert für die zu zugeordnete Gruppe an.
```

```
 a|
Rollen
 a|
Klicken Sie in das Feld, und wählen Sie eine der Rollen des Speicherarrays
aus, die dem Attribut zugeordnet werden sollen. Sie müssen jede Rolle, die
Sie für diese Gruppe aufnehmen möchten, einzeln auswählen. Die Rolle
Monitor ist zusammen mit den anderen Rollen für die Anmeldung bei Unified
Manager erforderlich. Eine Sicherheitsadministratorrolle muss mindestens
einer Gruppe zugewiesen werden. Die zugeordneten Rollen umfassen die
folgenden Berechtigungen:

** *Storage Admin* -- Vollzugriff auf die Speicherobjekte (z. B. Volumes
und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
** *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management, Zertifikatverwaltung, Audit Log Management und die
Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder
auszuschalten.
** *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf dem
Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-
Upgrades. Kein Zugriff auf Speicherobjekte oder die
Sicherheitskonfiguration.
** *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


|===
====
+

NOTE: Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Unified Manager funktioniert für keinen
Benutzer ordnungsgemäß, ohne dass die Überwachungsfunktion vorhanden ist.

. Klicken Sie optional auf *Weitere Zuordnungen hinzufügen*, um weitere
Gruppen-zu-Rolle-Zuordnungen einzugeben.
. Klicken Sie Auf *Speichern*.


.Ergebnisse
Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen
beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.



[[IDd2607d4f49f2c736d78579afd739c198]]
= Exportieren Sie SAML-Dienstanbieter-Dateien
:allow-uri-read:
```

```
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Bei Bedarf können Sie Service-Provider-Metadaten für das Speicher-Array
exportieren und die Datei erneut in das Identity Provider (IdP)-System
importieren.

.Bevor Sie beginnen
* Sie müssen mit einem Benutzerprofil angemeldet sein, das
Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die
Zugriffsverwaltungsfunktionen nicht angezeigt.
* SAML wurde konfiguriert und aktiviert.


.Über diese Aufgabe
In dieser Aufgabe exportieren Sie Metadaten vom Controller. Das IdP
benötigt diese Metadaten, um eine Vertrauensbeziehung zum Controller
herzustellen und Authentifizierungsanforderungen zu verarbeiten. Die Datei
enthält Informationen wie den Domänennamen des Controllers oder die IP-
Adresse, die das IdP zum Senden von Anforderungen verwenden kann.

.Schritte
. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
. Wählen Sie die Registerkarte *SAML* aus.
. Wählen Sie *Export*.
+
Das Dialogfeld Dateien des Dienstanbieters exportieren wird geöffnet.

. Klicken Sie auf *Export*, um die Metadatendatei auf Ihrem lokalen System
zu speichern.
+
[NOTE]
====
Das Feld für den Domänennamen ist schreibgeschützt.

====
+
Notieren Sie sich, wo die Datei gespeichert ist.

. Suchen Sie vom lokalen System aus die XML-formatierte Service Provider-
Metadatendatei, die Sie exportiert haben.
. Importieren Sie vom IdP-Server die Metadatendatei des Dienstanbieters.
```

```
Sie können die Datei entweder direkt importieren oder die Controller-
Informationen manuell eingeben.
. Klicken Sie Auf *Schließen*.




:leveloffset: -1


= FAQs

:leveloffset: +1


[[IDb5d5c6edc698ea8c17b12193e1862392]]
= Warum kann ich mich nicht anmelden?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Wenn Sie bei der Anmeldung einen Fehler erhalten, überprüfen Sie diese
möglichen Ursachen.

Aus einem der folgenden Gründe können Anmeldefehler auftreten:

* Sie haben einen falschen Benutzernamen oder ein falsches Passwort
eingegeben.
* Sie verfügen über unzureichende Berechtigungen.
* Sie haben mehrmals versucht, sich erfolglos anzumelden, was den
Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, bis Sie sich erneut
anmelden können.
* SAML-Authentifizierung ist aktiviert. Aktualisieren Sie Ihren Browser,
um sich anzumelden.




[[ID1cce83aaf724d4943286bc19c0d98257]]
= Was muss ich vor dem Hinzufügen eines Verzeichnisservers wissen?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
Bevor Sie einen Verzeichnisserver in Access Management hinzufügen, müssen
Sie bestimmte Anforderungen erfüllen.

* Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
* LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich
Domänenname, Server-URL und optional Benutzername und Kennwort für das
Bindekonto.
* Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette
des LDAP-Servers auf Ihrem lokalen Computer installiert sein.




[[ID7ec18716c33098eedc18367c70581aab]]
= Was muss ich über die Zuordnung von Speicher-Array-Rollen wissen?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Überprüfen Sie die Richtlinien, bevor Sie Gruppen zu Rollen zuordnen.

Die RBAC-Funktionen (rollenbasierte Zugriffssteuerung) umfassen folgende
Rollen:

* *Storage Admin* -- Vollständiger Lese-/Schreibzugriff auf
Speicherobjekte auf den Arrays, aber kein Zugriff auf die
Sicherheitskonfiguration.
* *Security Admin* -- Zugriff auf die Sicherheitskonfiguration in Access
Management und Certificate Management.
* *Support Admin* -- Zugriff auf alle Hardware-Ressourcen auf Speicher-
Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte
oder die Sicherheitskonfiguration.
* *Monitor* -- schreibgeschützter Zugriff auf alle Speicherobjekte, aber
kein Zugriff auf die Sicherheitskonfiguration.


[NOTE]
====
Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich.
```

```
====
Wenn Sie einen LDAP-Server (Lightweight Directory Access Protocol) und
Verzeichnisdienste verwenden, stellen Sie sicher, dass:

* Ein Administrator hat im Verzeichnisdienst Benutzergruppen definiert.
* Sie kennen die Gruppen-Domain-Namen für die LDAP-Benutzergruppen.




== SAML

Wenn Sie die im Speicher-Array integrierten SAML-Funktionen (Security
Assertion Markup Language) verwenden, stellen Sie sicher, dass:

* Ein IdP-Administrator (Identity Provider) hat im IdP-System
Benutzerattribute und Gruppenmitgliedschaften konfiguriert.
* Sie kennen die Namen der Gruppenmitgliedschaft.
* Sie kennen den Attributwert für die zu zugeordnete Gruppe. Reguläre
Ausdrücke werden unterstützt. Diese speziellen regulären Ausdruckszeichen
müssen mit einem umgekehrten Schrägstrich entgangen werden (`\`) Wenn sie
nicht Teil eines regulären Ausdrucksmusters sind:
+
[listing]
----
\.[]{}()<>*+-=!?^$|
----
* Die Überwachungsrolle ist für alle Benutzer, einschließlich des
Administrators, erforderlich. Unified Manager funktioniert für keinen
Benutzer ordnungsgemäß, ohne dass die Überwachungsfunktion vorhanden ist.




[[IDd0dfa78c003a84b0b8173510d5898b98]]
= Was muss ich vor der Konfiguration und Aktivierung von SAML wissen?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Bevor Sie die SAML-Funktionen (Security Assertion Markup Language) für die
Authentifizierung konfigurieren und aktivieren, müssen Sie sicherstellen,
dass Sie die folgenden Anforderungen erfüllen und SAML-Einschränkungen
verstehen.
```

== Anforderungen

Bevor Sie beginnen, stellen Sie sicher, dass:

* Ein Identitäts-Provider (IdP) ist in Ihrem Netzwerk konfiguriert. Ein IdP ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert werden und festgestellt wird, ob der Benutzer erfolgreich authentifiziert wurde. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich.
* Ein IdP-Administrator hat Benutzerattribute und Gruppen im IdP-System konfiguriert.
* Ein IdP-Administrator hat sichergestellt, dass der IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.
* Ein Administrator hat sichergestellt, dass der IdP-Server und die Controller-Uhr synchronisiert werden (entweder über einen NTP-Server oder durch Anpassung der Controller-Uhreinstellungen).
* Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, auf dem der Zugriff auf Unified Manager erfolgt.
* Sie kennen die IP-Adresse oder den Domain-Namen des Controllers im Speicher-Array.

== Einschränkungen

Zusätzlich zu den oben genannten Anforderungen sollten Sie sich mit den folgenden Einschränkungen vertraut machen:

* Sobald SAML aktiviert ist, können Sie sie über die Benutzeroberfläche nicht deaktivieren oder die IdP-Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an den technischen Support, um Hilfe zu erhalten. Es wird empfohlen, die SSO-Anmeldungen zu testen, bevor Sie SAML im letzten Konfigurationsschritt aktivieren. (Das System führt auch einen SSO-Anmeldetest vor Aktivierung von SAML durch.)
* Wenn Sie SAML zukünftig deaktivieren, stellt das System automatisch die vorherige Konfiguration wieder her (lokale Benutzerrollen und/oder Verzeichnisdienste).
* Wenn Verzeichnisdienste derzeit für die Benutzerauthentifizierung konfiguriert sind, überschreibt SAML diese Konfiguration.
* Wenn SAML konfiguriert ist, können die folgenden Clients nicht auf Speicher-Array-Ressourcen zugreifen:

```
+
** Enterprise Management-Fenster (EMW)
** Befehlszeilenschnittstelle (CLI)
** Software Developer Kits (SDK)-Clients
** In-Band-Clients
** REST-API-Clients für die HTTP-Standardauthentifizierung
** Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an




[[IDf4201715020c6e432dae8f918fd339d9]]
= Welche lokalen Benutzer gibt es?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Lokale Benutzer sind im System vordefiniert und enthalten bestimmte
Berechtigungen.

Zu den lokalen Benutzern gehören:

* *Admin* -- Super-Administrator, der Zugriff auf alle Funktionen im
System hat. Dieser Benutzer enthält alle Rollen. Das Passwort muss bei der
ersten Anmeldung festgelegt werden.
* *Storage* -- der Administrator, der für die gesamte Storage-
Bereitstellung verantwortlich ist. Dieser Benutzer umfasst die folgenden
Rollen: Storage-Administrator, Support-Administrator und Monitor. Dieses
Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
* *Sicherheit* -- der für die Sicherheitskonfiguration verantwortliche
Benutzer, einschließlich Zugriffsverwaltung und Zertifikatverwaltung.
Dieser Benutzer umfasst die folgenden Rollen: Security Admin und Monitor.
Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
* *Support* -- der Benutzer, der für Hardware-Ressourcen, Ausfalldaten und
Firmware-Upgrades verantwortlich ist. Dieser Benutzer enthält die
folgenden Rollen: Unterstützen Sie Admin und Monitor. Dieses Konto wird
deaktiviert, bis ein Kennwort festgelegt ist.
* *Monitor* -- ein Benutzer mit schreibgeschütztem Zugriff auf das System.
Dieser Benutzer enthält nur die Rolle „Monitor“. Dieses Konto wird
deaktiviert, bis ein Kennwort festgelegt ist.
* *rw* (lesen/schreiben) -- dieser Benutzer enthält die folgenden Rollen:
Speicheradministrator, Supportadministrator und Monitor. Dieses Konto wird
```

```
deaktiviert, bis ein Kennwort festgelegt ist.
* *Ro* (schreibgeschützt) -- dieser Benutzer enthält nur die Rolle
Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.




:leveloffset: -1


:leveloffset: -1


:leveloffset: -1


[[ID55343647dd844af63dd976f0206c6a99]]
= Frühere Versionen
:allow-uri-read:
:icons: font
:relative_path: ./
:imagesdir: {root_path}{relative_path}./media/


[role="lead"]
Die nachfolgenden Links führen zu Dokumentationen für ältere Versionen der
E-Series Hardware und SANtricity Software. Die Links führen Sie zu einer
anderen Dokumentationswebsite.



== Hardware-Dokumentation für frühere Versionen

*
https://library.netapp.com/ecm/ecm_download_file/ECMLP2484026["Installatio
n von E2712, E2724, E5612, E5624 Controller-Laufwerksfächern und DE1600
und DE5600 ErweiterungsLaufwerksfächern"^]
*
https://library.netapp.com/ecm/ecm_download_file/ECMLP2484072["Installiere
n Sie E2760 und E5660 Controller-Laufwerksfächer und DE6600
ErweiterungsLaufwerksfächern"^]
*
https://library.netapp.com/ecm/ecm_download_file/ECMLP2484108["Installatio
n von EF560 Flash-Arrays und DE5600 Flash-Erweiterungsfächern"^]
* https://mysupport.netapp.com/info/web/ECMP11392380.html["Installieren
älterer Systeme"^]
* https://mysupport.netapp.com/info/web/ECMP11751516.html["Wartung älterer
```

```
Systeme"^]
*
https://mysupport.netapp.com/ecm/ecm_download_file/ECMP1394872["Hinzufügen
eines zweiten Controllers zu E2600 und E2700"^]
* https://library.netapp.com/ecm/ecm_download_file/ECMLP2353447["Ändern
oder Hinzufügen von Host-Protokollen"^]
* https://mysupport.netapp.com/ecm/ecm_download_file/ECMP1656638["Von AC
zu DC-Strom konvertieren"^]
*
https://library.netapp.com/ecm/ecm_download_file/ECMLP2589397["Controller
Upgrade Guide – Ältere Controller-Modelle"^]



== Softwaredokumentation für frühere Versionen



=== SANtricity Version 11.8

* https://docs.netapp.com/us-en/e-series-santricity-118/index.html["Die
Hilfe zu System Manager"^]
* https://docs.netapp.com/us-en/e-series-santricity-
118/index.html["Unified Manager-Hilfe"^]




=== SANtricity Version 11.7

* https://docs.netapp.com/us-en/e-series-santricity-117/index.html["Die
Hilfe zu System Manager"^]
* https://docs.netapp.com/us-en/e-series-santricity-
117/index.html["Unified Manager-Hilfe"^]




=== SANtricity Version 11.6

* https://docs.netapp.com/us-en/e-series-santricity-116/index.html["Die
Hilfe zu System Manager"^]
* https://docs.netapp.com/us-en/e-series-santricity-
116/index.html["Unified Manager-Hilfe"^]
```

```
=== SANtricity Version 11.5

* https://docs.netapp.com/us-en/e-series-santricity-115/index.html["Die
Hilfe zu System Manager"^]




=== SANtricity Version 11.4

* https://mysupport.netapp.com/ecm/ecm_get_file/ECMLP2862590["HILFE BEI
AMW (E2700, E5600/EF560)"^]
* https://mysupport.netapp.com/ecm/ecm_get_file/ECMLP2862588["EMW-HILFE
(E2700, E5600/EF560)"^]




[[ID47f9c212694b5211403bd822b6c41b0a]]
= Rechtliche Hinweise
:hardbreaks:
:allow-uri-read:
:icons: font
:linkattrs:
:relative_path: ./
:imagesdir: {root_path}{relative_path}./media/


[role="lead lead"]
Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen,
Marken, Patente und mehr.



== Urheberrecht

link:https://www.netapp.com/company/legal/copyright/["https://www.netapp.c
om/company/legal/copyright/"^]



== Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten
Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können
```

Marken der jeweiligen Eigentümer sein.

link:https://www.netapp.com/company/legal/trademarks/["https://www.netapp.com/company/legal/trademarks/"^]

== Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

link:https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf["https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf"^]

== Datenschutzrichtlinie

link:https://www.netapp.com/company/legal/privacy-policy/["https://www.netapp.com/company/legal/privacy-policy/"^]

== Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

https://library.netapp.com/ecm/ecm_download_file/ECMLP3334467["Hinweis zum SANtricity OS für die E-Series/EF-Series"]

:leveloffset: -1

<<<
Copyright-Informationen