System

SANtricity 11.5

NetApp
February 12, 2024

Inhalt

System

Storage Array-Einstellungen

Konzepte

Cache-Einstellungen und Performance

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.

> Möglicher Datenverlust — Wenn Sie die Option* Write Caching ohne Batterien 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 Write Caching ohne Batterien Option 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.

Automatischer Lastausgleich – Übersicht

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.

Damit ein Hostcluster als für den automatischen Lastausgleich geeignet angesehen werden kann, müssen alle Hosts in dieser Gruppe den automatischen Lastausgleich unterstützen können.

Hosttyp unterstützt den automatischen Lastausgleich	Mit diesem Multipath-Treiber
Windows oder Windows Cluster	MPIO mit NetApp E-Series DSM
Linux DM-MP (Kernel 3.10 oder höher)	DM-MP mit `scsi_dh_alua` Gerätehandler
VMware	Natives Multipathing-Plug-in (NMP) mit `VMW_SATP_ALUA Storage Array Type` Plug-in

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 "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.

1. Wechseln Sie zum "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.

2. Aktualisieren und konfigurieren Sie den `/etc/multipath.conf file`.
3. 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.

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 ein HP-UX-Betriebssystem ausgeführt. Und weitere drei führen ein Linux-Betriebssystem aus. Sie müssen als Standard-Host-Betriebssystem Factory Default auswählen.

Anleitungen

Name des Speicher-Arrays bearbeiten

Sie können den Namen des Speicher-Arrays ändern, der in der Titelleiste des SANtricity-Systems Managers angezeigt wird.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Suchen Sie unter **Allgemein** das Feld **Name:**.

   Wenn kein Name des Speicher-Arrays definiert wurde, wird in diesem Feld „Unbekannt“ angezeigt.

3. Klicken Sie auf das Symbol **Bearbeiten** (Bleistift) neben dem Namen des Speicherarrays.

   Das Feld kann bearbeitet werden.

4. 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.

5. Klicken Sie auf das Symbol **Speichern** (Häkchen).

   Wenn Sie das bearbeitbare Feld schließen möchten, ohne Änderungen vorzunehmen, klicken Sie auf das Symbol Abbrechen (X).

Ergebnis

Der neue Name wird in der Titelleiste des SANtricity System Managers angezeigt.

Schalten Sie die Speicher-Array Locator-Leuchten ein

Um den physischen Standort eines Speicherarrays in einem Schrank zu finden, können Sie seine Locator-Leuchten (LED) einschalten.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. 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.

3. 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.

Speicherarray-Uhren synchronisieren

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.

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).

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

1. Wählen Sie Menü:Einstellungen[System].
2. 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.

   Für Simplex-Speicher-Arrays wird nur ein Controller angezeigt.

3. 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.

Speicherarray-Konfiguration speichern

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

> **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

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie **Speicherarray-Konfiguration Speichern**.
3. Wählen Sie die Elemente der Konfiguration aus, die Sie speichern möchten:
   - **Speicher-Array-Einstellungen**
   - **Volume-Konfiguration**
   - **Host-Konfiguration**
   - **Host-to-Volume-Zuweisung**

   > Wenn Sie das Element **Host-to-Volume Zuweisungen** auswählen, werden standardmäßig auch das Element **Volume Configuration** und das Element **Host Configuration** ausgewählt. Sie können **Host-to-Volume-Zuweisungen** nicht speichern, ohne auch **Volume-Konfiguration** und **Host-Konfiguration** zu speichern.
4. 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 eine Storage-Array-Konfiguration auf ein anderes Storage Array zu laden, verwenden Sie den SANtricity Unified Manager.

Löschen Sie die Konfiguration des Speicherarrays

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.

	Datenmenge	Storage Array Durchführt
Löscht Pools und Volume-Gruppen	X	X
Löscht Volumes	X	X
Löscht Hosts und Host-Cluster	X	X
Löscht Host-Zuweisungen	X	X
Löscht den Namen des Speicher-Arrays		X
Setzt die Cache-Einstellungen des Speicherarrays auf die Standardeinstellung zurück		X

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

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie **Speicherarray-Konfiguration Löschen**.
3. Wählen Sie in der Dropdown-Liste entweder **Volume** oder **Storage Array** aus.
4. **Optional**: Wenn Sie die Konfiguration speichern möchten (nicht die Daten), verwenden Sie die Links im Dialogfeld.
5. 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.

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**.

Ergebnis

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** aus.

   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**.

Ändern Sie die Cache-Einstellungen für das Speicher-Array

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:

Cache-Einstellung	Beschreibung
Starten Sie die Spülung des Cache-Bedarfs	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.
Cache-Blockgröße	Die Cache-Blockgröße bestimmt die maximale Größe jedes Cache-Blocks. Diese Einheit ist eine Organisationseinheit für das Cache Management. Standardmäßig ist die Blockgröße 8 KiB. Mit System Manager können die Cache-Blockgröße von 4, 8, 16 oder 32 KiBs beträgt. 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

1. Wählen Sie Menü:Einstellungen[System].
2. Scrollen Sie nach unten zu **zusätzliche Einstellungen** und klicken Sie dann auf **Cache-Einstellungen**

ändern.

Das Dialogfeld Cache-Einstellungen ändern wird geöffnet.

3. Passen Sie die folgenden Werte an:
   - Beginnen 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.
4. Klicken Sie Auf **Speichern**.

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.

Automatische Lastverteilung festlegen

Die Funktion **Automatic Load Balancing** sorgt dafür, dass eingehender I/O-Datenverkehr von den Hosts auf beiden Controllern dynamisch verwaltet und ausgeglichen wird. Diese Funktion ist standardmäßig aktiviert, Sie können sie jedoch im 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

1. Wählen Sie Menü:Einstellungen[System].
2. 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.
3. Bestätigen Sie, indem Sie auf **Ja** klicken, um fortzufahren.

   Wenn Sie diese Option auswählen, schalten Sie die Funktion zwischen aktiviert/deaktiviert ein.

   Wenn diese Funktion von deaktiviert auf aktiviert verschoben wird, wird auch die Funktion Host Connectivity Reporting automatisch aktiviert.

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 ein HP-UX-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**.

Aktivieren oder deaktivieren Sie die veraltete Managementoberfläche

Sie können die Legacy-Managementoberfläche (Symbol) aktivieren oder deaktivieren, eine Kommunikationsmethode zwischen dem Storage-Array und dem Management-Client. 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.

Über diese Aufgabe

Die Einstellung wirkt sich auf die Vorgänge wie folgt aus:

- **Ein** (Standard) — erforderliche Einstellung für Spiegelung, für CLI-Befehle, die nur auf E5700 und E5600 Storage-Arrays betrieben werden, sowie einige andere Tools wie das QuickConnect Utility und der 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

1. Wählen Sie Menü:Einstellungen[System].
2. Blättern Sie nach unten zu **zusätzliche Einstellungen**, und klicken Sie dann auf **Verwaltungsschnittstelle ändern**.
3. Klicken Sie im Dialogfeld auf **Ja**, um fortzufahren.

FAQs

Was ist der Controller Cache?

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.

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.

Was wird Cachespülung?

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. Die Spülzeit in System Manager kann nicht geändert werden. Stattdessen müssen Sie den Befehl Set Storage Array in der Befehlszeilenschnittstelle (CLI) verwenden.

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.

Was ist die Cache-Blockgröße?

Der Controller des Storage Arrays ordnet den Cache in „Blöcke“ zu. Dabei handelt es sich um Speicherblöcke mit einer Größe von 4, 8, 16 oder 32 KiBs. Alle Volumes im Storage-System nutzen denselben Cache-Speicherplatz. Daher können die Volumes nur eine Cache-Blockgröße aufweisen.

Cache-Blöcke sind nicht mit 512-Byte-Blöcken identisch, die vom logischen Block-System der Festplatten verwendet werden.

Applikationen verwenden unterschiedliche Blockgrößen, die wiederum einen Einfluss auf die Storage-Performance haben können. Standardmäßig ist die Blockgröße in System Manager 8 KiB, Sie können den Wert jedoch auf 4, 8, 16 oder 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.

Wann sollte ich Speicherarray-Uhren synchronisieren?

Sie sollten die Controller-Uhren im Speicher-Array manuell synchronisieren, wenn Sie bemerken, dass die in System Manager angezeigten Zeitstempel nicht mit den im Management-Client angezeigten Zeitstempeln (dem Computer, der über den Browser auf System Manager zugreift) ausgerichtet sind. Diese Aufgabe ist nur erforderlich, wenn das NTP (Network Time Protocol) in System Manager nicht aktiviert ist.

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 Synchronisationsstatus über das Dialogfeld **Speicherarray-Uhren**, das auf der Seite System verfügbar ist, überprüfen. 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.

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.

ISCSI-Einstellungen

Konzepte

ISCSI-Terminologie

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

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.

Laufzeit	Beschreibung
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.
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.

Anleitungen

Konfigurieren Sie die iSCSI-Ports

Wenn Ihr Controller eine iSCSI-Hostverbindung enthält, können Sie die iSCSI-Porteinstellungen auf der Seite Hardware oder auf der Seite System 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.

Über diese Aufgabe

Dieser Task beschreibt den Zugriff auf die Konfiguration des iSCSI-Ports über die Seite Hardware. Sie können die Konfiguration auch über die Systemseite aufrufen (Menü:Einstellungen[System]).

Die iSCSI-Einstellungen und -Funktionen werden nur angezeigt, wenn Ihr Speicherarray iSCSI unterstützt.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf **Zurück zum Regal anzeigen**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

3. Klicken Sie auf den Controller mit den iSCSI-Ports, die Sie konfigurieren möchten.

   Das Kontextmenü des Controllers wird angezeigt.

4. Wählen Sie **iSCSI-Ports konfigurieren**.

   > Die Option **iSCSI-Ports konfigurieren** wird nur angezeigt, wenn System Manager iSCSI-Ports am Controller erkennt.

   Das Dialogfeld iSCSI-Ports konfigurieren wird geöffnet.

5. Wählen Sie in der Dropdown-Liste den Port aus, den Sie konfigurieren möchten, und klicken Sie dann auf **Weiter**.
6. 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

Port-Einstellung	Beschreibung
IPv4 aktivieren/IPv6 aktivieren	Wählen Sie eine oder beide Optionen aus, um die Unterstützung für IPv4- und IPv6-Netzwerke zu aktivieren. HINWEIS: Wenn Sie den Portzugriff deaktivieren möchten, deaktivieren Sie beide Kontrollkästchen.
TCP-Listening-Port (verfügbar durch Klicken auf Weitere Porteinstellungen anzeigen)	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.
MTU-Größe (verfügbar durch Klicken auf Weitere Porteinstellungen anzeigen)	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.
ICMP PING-Antworten aktivieren	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 zum Auswählen von IPv4-Einstellungen geöffnet, nachdem Sie auf Weiter geklickt haben. Wenn Sie IPv6 aktivieren ausgewählt haben, wird ein Dialogfeld zum Auswählen von IPv6-Einstellungen geöffnet, nachdem Sie auf Weiter klicken. 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.

7. 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

Port-Einstellung	Beschreibung
Automatische Ermittlung der Konfiguration	Wählen Sie diese Option aus, um die Konfiguration automatisch abzurufen.
Statische Konfiguration manuell festlegen	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.
Aktivieren Sie die VLAN-Unterstützung (verfügbar durch Klicken auf Weitere Einstellungen anzeigen).	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.
aktivieren sie die ethernet-Priorität (verfügbar durch Klicken auf Weitere Einstellungen anzeigen).	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.

8. Klicken Sie Auf **Fertig Stellen**.

Konfigurieren Sie die iSCSI-Authentifizierung

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.

Die iSCSI-Einstellungen und -Funktionen werden nur auf der Seite Einstellungen angezeigt, wenn Ihr Speicher-Array iSCSI unterstützt.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. 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.

3. 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.
4. 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.

   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).

5. 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.
6. 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.

   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).

7. Klicken Sie Auf **Fertig Stellen**.

Ergebnis

Die Authentifizierung erfolgt während der iSCSI-Anmeldesequenz zwischen den Controllern und iSCSI-Hosts, es sei denn, Sie haben keine Authentifizierung angegeben.

Aktivieren Sie die iSCSI-Erkennungseinstellungen

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.

Die iSCSI-Einstellungen und -Funktionen werden nur auf der Seite Einstellungen angezeigt, wenn Ihr Speicher-Array iSCSI unterstützt.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Klicken Sie unter **iSCSI-Einstellungen** auf **Zielermittlungs-Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld **Zielermittlungs-Einstellungen** wird angezeigt. Unter dem Feld iSNS-Server aktivieren… wird im Dialogfeld angezeigt, ob der Controller bereits registriert ist.

3. 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.

     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).
4. 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.
5. Klicken Sie Auf **Speichern**.

Ergebnis

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.

Anzeigen von iSCSI-Statistikpaketen

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.

- **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.
- **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

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Anzeigen von iSCSI-Statistikpaketen** aus.
3. Klicken Sie auf eine Registerkarte, um die verschiedenen Statistikgruppen anzuzeigen.
4. 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.

ISCSI-Sitzung beenden

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

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Anzeigen/Beenden von iSCSI-Sitzungen**.

Eine Liste der aktuellen iSCSI-Sitzungen wird angezeigt.

3. Wählen Sie die Sitzung aus, die Sie beenden möchten
4. Klicken Sie auf **Sitzung beenden**, und bestätigen Sie, dass Sie den Vorgang ausführen möchten.

Anzeigen von iSCSI-Sitzungen

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

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Anzeigen/Beenden von iSCSI-Sitzungen**.

   Eine Liste der aktuellen iSCSI-Sitzungen wird angezeigt.

3. Um zusätzliche Informationen zu einer bestimmten iSCSI-Sitzung anzuzeigen, wählen Sie eine Sitzung aus und klicken dann auf **Details anzeigen**.

Felddetails

Element	Beschreibung
Session Identifier (SSID)	Eine hexadezimale Zeichenfolge, die eine Sitzung zwischen einem iSCSI-Initiator und einem iSCSI-Ziel identifiziert. Die SSID besteht aus ISID und TPGT.
Initiator-Sitzungs-ID (ISID)	Der Initiator-Teil der Session-ID. Der Initiator gibt während der Anmeldung die ISID an.
Zielportalgruppe	Das iSCSI-Ziel.
Ziel-Portal-Gruppen-Tag (TPGT)	Der Zielteil der Sitzungs-ID. Eine 16-Bit numerische Kennung für eine iSCSI-Zielportalgruppe.
ISCSI-Name des Initiators	Der eindeutige weltweite Name des Initiators.
ISCSI-Etikett des Initiators	Die in System Manager festgelegte Benutzerbezeichnung.
ISCSI-Alias des Initiators	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
Host	Ein Server, der ein- und Ausgang an das Speicherarray sendet.
Verbindungs-ID (CID)	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.
Ethernet-Port-ID	Der der Verbindung zugeordnete Controller-Port.
Initiator-IP-Adresse	Die IP-Adresse des Initiators.
Ausgehandelte Anmeldeparameter	Die Parameter, die während der Anmeldung der iSCSI-Sitzung bearbeitet werden.
Authentifizierungsmethode	Die Technik, um Benutzer zu authentifizieren, die Zugriff auf das iSCSI-Netzwerk wollen. Gültige Werte sind **CHAP** und **Keine**.
Header-Digest-Methode	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**.

Element	Beschreibung
Data Digest-Methode	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**.
Maximale Anzahl der Verbindungen	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**.
Ziel-Alias	Die dem Ziel zugeordnete Bezeichnung.
Alias des Initiators	Die dem Initiator zugeordnete Bezeichnung.
Ziel-IP-Adresse	Die IP-Adresse des Ziels für die iSCSI-Sitzung. DNS-Namen werden nicht unterstützt.
Anfängliche R2T	Der anfängliche Status für die Übertragung bereit. Der Status kann entweder **Ja** oder **Nein** sein.
Maximale Burst-Länge	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)**.
Erste Burst-Länge	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)**.
Standardzeit zu warten	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**.
Standardzeit für die Aufbewahrung	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**.
Max. Ausstehender R2T	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**.
Fehler bei Recovery-Stufe	Die Ebene der Fehlerwiederherstellung für diese iSCSI-Sitzung. Der Wert für die Fehlerwiederherstellung ist immer auf **0** gesetzt.
Maximale Länge des Segments für Empfangsdaten	Die maximale Datenmenge, die entweder der Initiator oder das Ziel in einer beliebigen iSCSI-Nutzlastdateneinheit (PDU) empfangen kann.

Element	Beschreibung
Zielname	Der offizielle Name des Ziels (nicht der Alias). Der Zielname mit dem Format *iqn*.
Name des Initiators	Der offizielle Name des Initiators (nicht der Alias). Der Initiatorname, der entweder das Format *iqn* oder *eui* verwendet.

4. 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`.

Konfigurieren Sie iSER-over-InfiniBand-Ports

Wenn der Controller einen iSER-over-InfiniBand-Port enthält, können Sie die Netzwerkverbindung zu dem Host konfigurieren. Die Konfigurationseinstellungen sind auf der Seite Hardware oder auf der Seite System verfügbar.

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.

Über diese Aufgabe

Sie können über die Seite **Hardware** oder über Menü:Einstellungen[System] auf die Konfiguration iSER-over-InfiniBand zugreifen. Diese Aufgabe beschreibt die Konfiguration der Ports auf der Seite **Hardware**.

Die iSER-over-InfiniBand-Einstellungen und -Funktionen werden nur angezeigt, wenn der Controller Ihres Storage-Arrays einen iSER-over-InfiniBand-Port umfasst.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf **Zurück zum Regal anzeigen**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

3. Klicken Sie auf den Controller mit dem iSER-over-InfiniBand-Port, den Sie konfigurieren möchten.

   Das Kontextmenü des Controllers wird angezeigt.

4. Wählen Sie **iSER-over-InfiniBand-Ports konfigurieren**.

   Das Dialogfeld iSER-over-InfiniBand-Ports konfigurieren wird geöffnet.

5. Wählen Sie in der Dropdown-Liste den HIC-Port aus, den Sie konfigurieren möchten, und geben Sie dann die IP-Adresse des Hosts ein.
6. Klicken Sie Auf **Konfigurieren**.

7. Vervollständigen Sie die Konfiguration, und setzen Sie dann den iSER-over-InfiniBand-Port zurück, indem Sie auf **Ja** klicken.

Zeigen Sie iSER-over-InfiniBand-Statistiken an

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.

Sie können über die Systemseite (Menü:Einstellungen[System]) oder über die Support-Seite auf die iSER-over-InfiniBand-Statistiken zugreifen. In diesen Anweisungen wird der Zugriff auf die Statistiken auf der Support-Seite beschrieben.

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **Anzeigen iSER über InfiniBand Statistik**.
3. Klicken Sie auf eine Registerkarte, um die verschiedenen Statistikgruppen anzuzeigen.
4. 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 sämtliche iSER-over-InfiniBand-Statistiken verwendet.

FAQs

Was passiert, wenn ich einen iSNS Server für die Registrierung verwende?

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).

Welche Registrierungsmethoden werden für iSCSI automatisch unterstützt?

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.

Wie interpretiere ich iSER-over-InfiniBand-Statistiken?

Das Dialogfeld **iSER über InfiniBand Statistics** anzeigen 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.

Was muss ich noch tun, um iSER over InfiniBand zu konfigurieren oder zu diagnostizieren?

In der folgenden Tabelle werden die System Manager Funktionen aufgeführt, mit denen Sie iSER-over-InfiniBand-Sitzungen konfigurieren und managen können.

> Die iSER-over-InfiniBand-Einstellungen sind nur verfügbar, wenn der Controller Ihres Storage-Arrays einen iSER-over-InfiniBand-Host-Management-Port umfasst.

Konfiguration und Diagnose von iSER über InfiniBand

Aktion	Standort
Konfigurieren Sie iSER-over-InfiniBand-Ports	1. Wählen Sie **Hardware**. 2. Wählen Sie **Rückseite des Regals anzeigen**. 3. Wählen Sie einen Controller aus. 4. Wählen Sie **iSER-over-InfiniBand-Ports konfigurieren**. Oder 1. Wählen Sie Menü:Einstellungen[System]. 2. Scrollen Sie nach unten nach **iSER über InfiniBand-Einstellungen**, und wählen Sie dann **iSER über InfiniBand-Ports konfigurieren** aus.

Aktion	Standort
Zeigen Sie iSER-over-InfiniBand-Statistiken an	1. Wählen Sie Menü:Einstellungen[System]. 2. Scrollen Sie nach unten nach **iSER über InfiniBand-Einstellungen** und wählen Sie dann **Anzeigen iSER über InfiniBand-Statistik** aus.

System: NVMe Einstellungen

Konzepte

NVMe Übersicht

Einige Controller umfassen einen Port zur Implementierung von NVMe (Non-Volatile Memory Express) über eine InfiniBand Fabric oder über ein RoCE (RDMA over Converged Ethernet) Fabric. 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. Bei SANtricity OS 11.40 und neuer kann ein NVMe Storage-Array (so genannte *Subsystem*) über eine InfiniBand oder RDMA-Fabric aufgerufen werden. 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.

NVMe – Terminologie

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

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.

Laufzeit	Beschreibung
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.
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.

Anleitungen

Konfigurieren Sie NVMe-over-InfiniBand-Ports

Wenn Ihr Controller eine NVMe-over-InfiniBand-Verbindung enthält, können Sie die NVMe-Port-Einstellungen auf der Seite Hardware oder auf der System-Seite 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.

Über diese Aufgabe

Sie können die NVMe over InfiniBand-Konfiguration über die Seite **Hardware** oder über das Menü:Einstellungen[System] aufrufen. Diese Aufgabe beschreibt die Konfiguration der Ports auf der Seite **Hardware**.

Die NVMe-over-InfiniBand-Einstellungen und -Funktionen werden nur angezeigt, wenn der Controller des Storage-Arrays einen NVMe-over-InfiniBand-Port enthält.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf **Zurück zum Regal anzeigen**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

3. Klicken Sie auf den Controller mit dem NVMe over InfiniBand-Port, den Sie konfigurieren möchten.

   Das Kontextmenü des Controllers wird angezeigt.

4. Wählen Sie **NVMe über InfiniBand-Ports konfigurieren** aus.

Das Dialogfeld **NVMe über InfiniBand Ports konfigurieren** wird geöffnet.

5. Wählen Sie in der Dropdown-Liste den HIC-Port aus, den Sie konfigurieren möchten, und geben Sie dann die IP-Adresse des Hosts ein.
6. Klicken Sie Auf **Konfigurieren**.
7. Führen Sie die Konfiguration aus, und setzen Sie den NVMe over InfiniBand-Port zurück, indem Sie auf **Ja** klicken.

Konfigurieren Sie NVMe over RoCE-Ports

Wenn der Controller eine Verbindung für NVMe over RoCE (RDMA over Converged Ethernet) umfasst, können Sie die NVMe-Port-Einstellungen auf der Hardware-Seite oder auf der System-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.

Über diese Aufgabe

Sie können über die Seite **Hardware** oder über Menü:Einstellungen[System] auf die NVMe over RoCE-Konfiguration zugreifen. In dieser Aufgabe wird beschrieben, wie die Ports auf der Seite Hardware konfiguriert werden.

> Die NVMe-over-RoCE-Einstellungen und -Funktionen werden nur angezeigt, wenn der Controller des Storage-Arrays einen NVMe-over-RoCE-Port umfasst.

Schritte

1. Wählen Sie **Hardware**.
2. Wenn die Grafik die Laufwerke anzeigt, klicken Sie auf **Zurück zum Regal anzeigen**.

   Die Grafik ändert sich, um die Controller anstelle der Laufwerke anzuzeigen.

3. Klicken Sie auf den Controller mit dem NVMe-over-RoCE-Port, den Sie konfigurieren möchten.

   Das Kontextmenü des Controllers wird angezeigt.

4. Wählen Sie **NVMe over RoCE Ports konfigurieren** aus.

   Das Dialogfeld NVMe-over-RoCE-Ports konfigurieren wird geöffnet.

5. Wählen Sie in der Dropdown-Liste den HIC-Port aus, den Sie konfigurieren möchten.
6. Klicken Sie Auf **Weiter**.

   Um alle Porteinstellungen anzuzeigen, klicken Sie rechts im Dialogfeld auf den Link **Weitere Porteinstellungen anzeigen**.

Felddetails

Port-Einstellung	Beschreibung
Konfigurierte Geschwindigkeit des ethernet-Ports	Wählen Sie die Geschwindigkeit aus, die der Geschwindigkeitsfähigkeit des SFP am Port entspricht.
IPv4 aktivieren/IPv6 aktivieren	Wählen Sie eine oder beide Optionen aus, um die Unterstützung für IPv4- und IPv6-Netzwerke zu aktivieren. Wenn Sie den Portzugriff deaktivieren möchten, deaktivieren Sie beide Kontrollkästchen.
MTU-Größe (verfügbar durch Klicken auf Weitere Porteinstellungen anzeigen)	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 zum Auswählen von IPv4-Einstellungen geöffnet, nachdem Sie auf Weiter geklickt haben. Wenn Sie IPv6 aktivieren ausgewählt haben, wird ein Dialogfeld zum Auswählen von IPv6-Einstellungen geöffnet, nachdem Sie auf Weiter klicken. 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.

7. Konfigurieren Sie die IPv4- und/oder IPv6-Einstellungen automatisch oder manuell.

Felddetails

Port-Einstellung	Beschreibung
Automatische Ermittlung der Konfiguration	Wählen Sie diese Option aus, um die Konfiguration automatisch abzurufen.
Statische Konfiguration manuell festlegen	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.

8. Klicken Sie Auf **Fertig Stellen**.

Anzeigen der NVMe over Fabrics Statistiken

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** — liefert Statistiken für den NVMe-Controller, einschließlich Timeouts und Verbindungsfehlern.
- **RDMA Interface Statistics** — stellt Statistiken für die RDMA-Schnittstelle bereit, einschließlich empfangener und übertragener Paketinformationen.

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.

Die NVMe over Fabrics Statistiken können Sie über die Systemseite (Menü:Einstellungen[System]) oder über die Support-Seite aufrufen. In diesen Anweisungen wird der Zugriff auf die Statistiken auf der Support-Seite beschrieben.

Schritte

1. Wählen Sie MENU:Support[Support Center > Diagnose].
2. Wählen Sie **View NVMe over Fabrics Statistics** aus.
3. 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 NVMe-Statistiken verwendet.

FAQs

Wie interpretiere ich NVMe-Statistiken über InfiniBand?

Das Dialogfeld **View NVMe over Fabrics Statistics** zeigt Statistiken für das NVMe-Subsystem und die NVMe over InfiniBand-Schnittstelle an. 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. 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.

Wie interpretiere ich NVMe over Fabrics Statistiken?

Im Dialogfeld **View NVMe over Fabrics Statistics** werden Statistiken für das NVMe-Subsystem und die NVMe over RoCE-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. 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.

Was muss ich sonst noch tun, um NVMe over InfiniBand zu konfigurieren oder zu diagnostizieren?

In der folgenden Tabelle werden die Funktionen von System Manager aufgeführt, mit denen Sie NVMe over InfiniBand-Sitzungen konfigurieren und managen können.

> Die NVMe-over-InfiniBand-Einstellungen sind nur verfügbar, wenn der Controller des Storage-Arrays einen NVMe-over-InfiniBand-Port besitzt.

Konfiguration und Diagnose von NVMe over InfiniBand

Aktion	Standort
Konfigurieren Sie NVMe-over-InfiniBand-Ports	1. Wählen Sie **Hardware**. 2. Wählen Sie **Rückseite des Regals anzeigen**. 3. Wählen Sie einen Controller aus. 4. Wählen Sie **NVMe über InfiniBand-Ports konfigurieren** aus. Oder 1. Wählen Sie Menü:Einstellungen[System]. 2. Scrollen Sie nach unten zu **NVMe over InfiniBand settings** und wählen Sie dann **Configure NVMe over InfiniBand Ports** aus.
Anzeigen der NVMe-over-InfiniBand-Statistiken	1. Wählen Sie Menü:Einstellungen[System]. 2. Scrollen Sie nach unten zu **NVMe over InfiniBand settings** und wählen Sie dann **View NVMe over Fabrics Statistics** aus.

Was muss ich sonst noch tun, um NVMe over RoCE zu konfigurieren oder zu diagnostizieren?

NVMe over RoCE kann über die Seiten für Hardware und Einstellungen konfiguriert und gemanagt werden.

> Die NVMe-over-RoCE-Einstellungen sind nur verfügbar, wenn der Controller des Storage-Arrays einen NVMe-over-RoCE-Port umfasst.

Konfiguration und Diagnose von NVMe over RoCE

Aktion	Standort
Konfigurieren Sie NVMe over RoCE-Ports	1. Wählen Sie **Hardware**. 2. Wählen Sie **Rückseite des Regals anzeigen**. 3. Wählen Sie einen Controller aus. 4. Wählen Sie **NVMe over RoCE Ports konfigurieren** aus. Oder 1. Wählen Sie Menü:Einstellungen[System]. 2. Scrollen Sie nach unten zu **NVMe over RoCE settings** und wählen Sie dann **Configure NVMe over RoCE Ports** aus.
Anzeigen der NVMe over Fabrics Statistiken	1. Wählen Sie Menü:Einstellungen[System]. 2. Scrollen Sie nach unten zu **NVMe over RoCE settings** und wählen Sie dann **View NVMe over Fabrics Statistics** aus.

Add-on-Funktionen

Konzepte

Funktionsweise der Add-on-Funktionen

Add-ons sind Funktionen, die nicht in der Standardkonfiguration von System Manager enthalten sind und die Aktivierung eines Schlüssels 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:

1. 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.
2. 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, die

Kennnummer für die Aktivierung von Funktionen und den Aktivierungscode an.

3. Aktivieren Sie mit System Manager die Premium-Funktion oder das Feature Pack mithilfe der Feature-Key-Datei.

Terminologie der Add-on-Funktionen

Erfahren Sie, welche Zusatzfunktionenbedingungen auf Ihr Storage Array Anwendung finden.

Laufzeit	Beschreibung
Kennzeichner Für Feature-Aktivierung	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.
Feature-Schlüsseldatei	Eine Feature-Schlüsseldatei ist eine Datei, die Sie zum Entsperren und Aktivieren einer Premium-Funktion oder eines Feature-Packs erhalten.
Funktionspaket	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.
Premiumfunktion	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.

Anleitungen

Abrufen einer Feature-Schlüsseldatei

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

1. 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.
2. 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.
3. Suchen und notieren Sie den Aktivierungscode der Funktion. Für Features Packs wird dieser Aktivierungscode in den entsprechenden Anweisungen zur Durchführung der Konvertierung angegeben.

   Anweisungen von NetApp finden Sie unter "NetApp E-Series Systems Documentation Center".

   Bei Premium-Funktionen können Sie über die Support-Website auf den Aktivierungscode zugreifen:

   a. Melden Sie sich bei an "NetApp Support".
   b. Wechseln Sie zum Menü:Produkte[Produkte verwalten > Softwarelizenzen].
   c. Geben Sie die Seriennummer für das Speicher-Array-Chassis ein, und klicken Sie dann auf **Los**.
   d. Suchen Sie in der Spalte **Lizenzschlüssel** nach den Aktivierungscodes für die Funktion.
   e. Notieren Sie den Aktivierungscode der Funktion für die gewünschte Funktion.
4. Fordern Sie eine Funktionsschlüsseldatei an, indem Sie eine E-Mail oder ein Textdokument an Ihren Speicheranbieter senden, die folgende Informationen enthält: Chassis-Seriennummer, Feature-Aktivierungscode und die Funktion Identifier aktivieren.

   Sie können auch zu gehen "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.

Aktivieren Sie eine Premiumfunktion

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.

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

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter **Add-ons** die Option **Premium Feature aktivieren**.

   Das Dialogfeld Premium-Funktion aktivieren wird geöffnet.

3. Klicken Sie auf **Durchsuchen** und wählen Sie dann die Schlüsseldatei aus.

   Der Dateiname wird im Dialogfeld angezeigt.

4. Klicken Sie Auf **Aktivieren**.

Funktionspaket aktivieren

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 Durchführung der Konvertierung und zur Vorbereitung des Systems auf die Attribute des neuen Speicherarrays befolgt.

  Konvertierungsanweisungen sind verfügbar unter "NetApp E-Series Systems Documentation Center".

- 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).

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

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter **Add-ons** die Option **Feature Pack ändern**.
3. Klicken Sie auf **Durchsuchen** und wählen Sie dann die Schlüsseldatei aus.

Der Dateiname wird im Dialogfeld angezeigt.

4. Geben Sie in das Feld **CHANGE** ein.
5. 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.

Sicherheitsschlüsselmanagement

Konzepte

Funktionsweise der Laufwerkssicherheitsfunktion

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.

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).

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.

> 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.

Funktionsweise von Sicherheitsschlüsselmanagement

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 befinden sich im persistenten Speicher des Controllers. Führen Sie folgende Schritte durch, um das interne Verschlüsselungsmanagement zu implementieren:

1. Installieren Sie sichere Laufwerke im Speicher-Array. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
2. Stellen Sie sicher, dass die Laufwerksicherheit aktiviert ist. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.
3. 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 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:

1. Installieren Sie sichere Laufwerke im Speicher-Array. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
2. Stellen Sie sicher, dass die Laufwerksicherheit aktiviert ist. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.
3. Füllen Sie eine Client Certificate Signing Request (CSR) für die Authentifizierung zwischen dem Speicher-Array und dem Schlüsselverwaltungsserver aus, und laden Sie sie herunter. Wechseln Sie zum Menü:Einstellungen[Zertifikate > Schlüsselverwaltung > CSR abschließen].
4. Erstellen und laden Sie mithilfe der heruntergeladenen CSR-Datei ein Client-Zertifikat vom Schlüsselverwaltungsserver herunter.
5. Stellen Sie sicher, dass das Clientzertifikat und eine Kopie des Zertifikats für den Schlüsselverwaltungsserver auf Ihrem lokalen Host verfügbar sind.
6. 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.

Terminologie der Laufwerksicherheit

Erfahren Sie, wie die Bedingungen für die Laufwerksicherheit auf Ihr Speicherarray angewendet werden.

Laufzeit	Beschreibung
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.
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.
Management- Client	Ein lokales System (Computer, Tablet usw.), das einen Browser für den Zugriff auf System Manager enthält.

Laufzeit	Beschreibung
Ausdruck übergeben	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. Der Passphrase für die Laufwerksicherheit ist unabhängig vom Administratorkennwort des Speicherarrays.
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.

Laufzeit	Beschreibung
Sicherheitsschlüssel	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.
Kennung des Sicherheitsschlüssels	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.

Anleitungen

Interner Sicherheitsschlüssel erstellen

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.

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.

Der Passphrase für die Laufwerksicherheit ist unabhängig vom Administratorkennwort des Speicherarrays.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter **Security Key Management** die Option **Interner Schlüssel erstellen**.

   Wenn Sie noch keinen Sicherheitsschlüssel generiert haben, wird das Dialogfeld **Sicherheitsschlüssel erstellen** geöffnet.

3. Geben Sie Informationen in die folgenden Felder ein:

   - Definieren Sie eine Sicherheitsschlüssel-ID: Sie können entweder den Standardwert akzeptieren (Storage Array 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.

     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).

   Achten Sie darauf, 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.

4. 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.

   Der Pfad für die heruntergeladene Datei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.

5. Notieren Sie sich die Schlüsselkennung, den Passphrase und den Speicherort der heruntergeladenen Schlüsseldatei, und klicken Sie dann auf **Schließen**.

Ergebnis

Sie können jetzt sichere Volume-Gruppen oder -Pools erstellen oder die Sicherheit bei vorhandenen Volume-Gruppen und -Pools aktivieren.

> 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.

Externen Sicherheitsschlüssel erstellen

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.

  > 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.
- Die Client- und Server-Zertifikate sind auf Ihrem lokalen Host verfügbar, sodass sich das Storage-Array und der Schlüsselverwaltungsserver gegenseitig authentifizieren können. Das Clientzertifikat validiert die Controller, während das Serverzertifikat den Schlüsselverwaltungsserver validiert.

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

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter * Security Key Management* die Option **External Key erstellen** aus.

   > 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.

3. Geben Sie unter **Verbinden mit Key Server** Informationen in die folgenden Felder ein:
   - Adresse des Schlüsselverwaltungsservers — Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein, der für die Schlüsselverwaltung verwendet wird.
   - Port-Nummer des Verschlüsselungsmanagement — Geben Sie die Portnummer ein, die für die Kommunikation mit dem Key Management Interoperability Protocol (KMIP) verwendet wird. Die am häufigsten für die Kommunikation mit dem Verschlüsselungsmanagement-Server verwendete Portnummer ist 5696.
   - Client-Zertifikat auswählen — Klicken Sie auf die erste Schaltfläche Durchsuchen, um die Zertifikatdatei für die Speicher-Array-Controller auszuwählen.
   - Server-Zertifikat des Schlüsselverwaltungsservers auswählen - Klicken Sie auf die zweite Schaltfläche Durchsuchen, um die Zertifikatdatei für den Schlüsselverwaltungsserver auszuwählen.
4. Klicken Sie Auf **Weiter**.
5. Geben Sie unter **Create/Backup Key** Informationen in das folgende Feld ein:
   - 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).

   

   Achten Sie darauf, 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.
6. 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.

   

   Der Pfad für die heruntergeladene Datei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.
7. 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
   ```
8. 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.

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.

Sicherheitsschlüssel ändern

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 der Laufwerke zugreifen können.

Bevor Sie beginnen

Ein Sicherheitsschlüssel ist bereits vorhanden.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie ein Sicherheitsschlüssel geändert und durch einen neuen ersetzt wird. Nach diesem Vorgang wird der alte Schlüssel nicht validiert.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter * Security Key Management* die Option **Change Key**.

   Das Dialogfeld **Sicherheitsschlüssel ändern** wird geöffnet.

3. Geben Sie die folgenden Felder ein.

   - Definieren Sie eine Security Key ID — (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.

     Zusätzliche Zeichen werden automatisch generiert und an beide Enden der eingegebenen Zeichenfolge angehängt. Die generierten Zeichen tragen dazu bei, dass die Kennung eindeutig ist.

   - Definieren Sie eine Passphrase/geben Sie die Passphrase ein — 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).

Achten Sie darauf, Ihre Einträge für eine spätere Verwendung aufzuzeichnen — Wenn Sie ein sicheres Laufwerk aus dem Speicher-Array verschieben müssen, müssen Sie die Kennung und den Ausdruck kennen, um die Laufwerkdaten zu entsperren.

4. Klicken Sie Auf **Ändern**.

   Der neue Sicherheitsschlüssel überschreibt den vorherigen Schlüssel, der nicht mehr gültig ist.

   Der Pfad für die heruntergeladene Datei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.

5. 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.

Wechsel von externem zu internem Verschlüsselungsmanagement

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.

Bevor Sie beginnen

Ein externer Schlüssel wurde erstellt.

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

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter * Security Key Management* die Option **External Key Management deaktivieren** aus.

   Das Dialogfeld * External Key Management* deaktivieren wird geöffnet.

3. 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).

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.

4. Klicken Sie Auf **Deaktivieren**.

   Der Backup-Schlüssel wird auf Ihren lokalen Host heruntergeladen.

5. 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.

Bearbeiten der Einstellungen des Verschlüsselungsmanagementservers

Wenn Sie die externe Schlüsselverwaltung konfiguriert haben, können Sie die Einstellungen des Verschlüsselungsmanagementservers jederzeit anzeigen und bearbeiten.

Bevor Sie beginnen

Externes Verschlüsselungsmanagement muss konfiguriert werden.

Schritte

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter **Security Key Management** die Option **Key Management Server-Einstellungen anzeigen/bearbeiten** aus.
3. Bearbeiten Sie die Informationen in den folgenden Feldern:
   - Adresse des Schlüsselverwaltungsservers — Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein, der für die Schlüsselverwaltung verwendet wird.
   - KMIP-Port-Nummer – Geben Sie die Portnummer ein, die für die Kommunikation mit dem Key Management Interoperability Protocol (KMIP) verwendet wird.
4. Klicken Sie Auf **Speichern**.

Sicherheitsschlüssel sichern

Nach dem Erstellen oder Ändern eines Sicherheitsschlüssels können Sie eine Sicherungskopie der Schlüsseldatei erstellen, falls das Original beschädigt wird.

Bevor Sie beginnen

- Ein Sicherheitsschlüssel ist bereits vorhanden.

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

1. Wählen Sie Menü:Einstellungen[System].
2. Wählen Sie unter * Security Key Management* die Option **Back Up Key**.

   Das Dialogfeld **Sicherheitsschlüssel sichern** wird geöffnet.

3. 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)

   Notieren Sie Ihren Eintrag für die spätere Verwendung. Sie benötigen den Passphrase, um auf die Sicherung dieses Sicherheitsschlüssels zuzugreifen.

4. Klicken Sie Auf **Sichern**.

   Ein Backup des Sicherheitsschlüssels wird auf Ihren lokalen Host heruntergeladen, und dann wird das Dialogfeld **Sicherheitsschlüssel sichern/aufzeichnen** geöffnet.

   Der Pfad für die heruntergeladene Sicherheitsschlüsseldatei hängt möglicherweise vom Standard-Download-Speicherort Ihres Browsers ab.

5. Zeichnen Sie Ihren Passphrase an einem sicheren Ort auf, und klicken Sie dann auf **Schließen**.

Nachdem Sie fertig sind

Sie sollten den Sicherungsschlüssel überprüfen.

Validierung des Sicherheitsschlüssels

Sie können den Sicherheitsschlüssel überprüfen, um sicherzustellen, dass er nicht beschädigt wurde, und um sicherzustellen, dass Sie über einen korrekten Passphrase verfügen.

Bevor Sie beginnen

Ein Sicherheitsschlüssel wurde erstellt.

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

1. Wählen Sie Menü:Einstellungen[System].

2. Wählen Sie unter * Security Key Management* die Option **Validate Key** aus.

   Das Dialogfeld **Sicherheitsschlüssel validieren** wird geöffnet.

3. Klicken Sie auf **Durchsuchen** und wählen Sie dann die Schlüsseldatei aus (z. B. `drivesecurity.slk`).
4. 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.

5. Klicken Sie Auf **Validieren**.

   Die Ergebnisse der Validierung werden im Dialogfeld angezeigt.

6. 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.

Entsperren Sie Laufwerke mit einem Sicherheitsschlüssel

Wenn Sie sichere Laufwerke von einem Speicher-Array in ein anderes verschieben, müssen Sie den entsprechenden Sicherheitsschlüssel in das neue Speicher-Array importieren. Durch das Importieren des Schlüssels werden die Daten auf den Laufwerken freigeschaltet.

Bevor Sie beginnen

- Das Ziel-Storage-Array (in dem Sie die Laufwerke verschieben) muss bereits einen Sicherheitsschlüssel konfiguriert haben. Die migrierten Laufwerke werden erneut auf das Ziel-Storage-Array übertragen.
- 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

In dieser Aufgabe wird beschrieben, wie Daten in sicheren Laufwerken entsperrt werden, die von einem Speicher-Array entfernt und in einem anderen neu installiert wurden. Sobald das Array die Laufwerke erkannt hat, wird ein Zustand „Achtung erforderlich“ sowie der Status „Sicherheitsschlüssel erforderlich“ für diese neu gelegenen Laufwerke angezeigt. Sie können Laufwerkdaten entsperren, indem Sie ihren Sicherheitsschlüssel in das Storage-Array importieren. Während dieses Vorgangs wählen Sie die Sicherheitsschlüsseldatei aus und geben den Passphrase für den Schlüssel ein.

Der 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

1. Wählen Sie Menü:Einstellungen[System].
2. 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.

3. Halten Sie optional die Maus über eine Laufwerksnummer, um die Position des Laufwerks (Shelf-Nummer und Einschubnummer) zu sehen.
4. 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.

5. Geben Sie den Passphrase ein, der dieser Schlüsseldatei zugeordnet ist.

   Die eingegebenen Zeichen sind maskiert.

6. 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.

FAQs

Was muss ich vor der Erstellung eines Sicherheitsschlüssels wissen?

Ein Sicherheitsschlüssel wird von Controllern und sicheren Laufwerken innerhalb eines Storage-Arrays gemeinsam verwendet. Wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt wird, schützt der Sicherheitsschlüssel die Daten vor unberechtigtem Zugriff.

Sie können Sicherheitsschlüssel mit einer der folgenden Methoden erstellen und verwalten:

- Internes Verschlüsselungsmanagement auf dem persistenten Speicher des Controllers.
- Externes Verschlüsselungskeymanagement auf einem externen Verschlüsselungsmanagement-Server.

Bevor Sie einen internen Sicherheitsschlüssel erstellen, müssen Sie Folgendes tun:

1. Installieren Sie sichere Laufwerke im Speicher-Array. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
2. Stellen Sie sicher, dass die Laufwerksicherheit aktiviert ist. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.

Sie können dann einen internen Sicherheitsschlüssel erstellen, der die Definition einer Kennung und einer Passphrase beinhaltet. Die Kennung ist eine Zeichenfolge, die dem Sicherheitsschlüssel zugeordnet ist und

auf dem Controller und allen Laufwerken gespeichert ist, die mit dem Schlüssel verknüpft sind. Der Passphrase wird verwendet, um den Sicherheitsschlüssel für Sicherungszwecke zu verschlüsseln. Wenn Sie fertig sind, wird der Sicherheitsschlüssel auf dem Controller an einem nicht zugänglichen Ort gespeichert. Anschließend können sichere Volume-Gruppen und -Pools erstellt oder die Sicherheit für vorhandene Volume-Gruppen und -Pools aktiviert werden.

Bevor Sie einen externen Sicherheitsschlüssel erstellen, müssen Sie Folgendes tun:

1. Installieren Sie sichere Laufwerke im Speicher-Array. Es können sich bei diesen Laufwerken um vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) oder FIPS-Laufwerke (Federal Information Processing Standard) handelt.
2. Stellen Sie sicher, dass die Laufwerksicherheit aktiviert ist. Wenden Sie sich bei Bedarf an Ihren Storage-Anbieter, um Anweisungen zur Aktivierung der Laufwerkssicherheitsfunktion zu erhalten.
3. Füllen Sie eine Client Certificate Signing Request (CSR) für die Authentifizierung zwischen dem Speicher-Array und dem Schlüsselverwaltungsserver aus, und laden Sie sie herunter. Wechseln Sie zum Menü:Einstellungen[Zertifikate > Schlüsselverwaltung > CSR abschließen].
4. Erstellen und laden Sie mithilfe der heruntergeladenen CSR-Datei ein Client-Zertifikat vom Schlüsselverwaltungsserver herunter.
5. Stellen Sie sicher, dass das Clientzertifikat und eine Kopie des Zertifikats für den Schlüsselverwaltungsserver auf Ihrem lokalen Host verfügbar sind.

Anschließend können Sie einen externen Schlüssel erstellen, der die IP-Adresse des Verschlüsselungsmanagement-Servers und die für die KMIP Kommunikation verwendete Port-Nummer umfasst. Während dieses Prozesses laden Sie auch Zertifikatdateien. Nach Abschluss des Vorgangs stellt das System eine Verbindung zum Schlüsselverwaltungsserver mit den von Ihnen eingegebenen Anmeldedaten her. Anschließend können sichere Volume-Gruppen und -Pools erstellt oder die Sicherheit für vorhandene Volume-Gruppen und -Pools aktiviert werden.

Warum muss ich eine Passphrase definieren?

Der Passphrase wird verwendet, um die auf dem lokalen Management-Client gespeicherte Sicherheitsschlüsseldatei zu verschlüsseln und zu entschlüsseln. Ohne den Passphrase kann der Sicherheitsschlüssel nicht entschlüsselt und verwendet werden, um Daten von einem sicheren Laufwerk zu entsperren, wenn er in einem anderen Speicher-Array neu installiert wird.

Warum sind Sicherheitsinformationen wichtig?

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.

Was muss ich vor dem Sichern eines Sicherheitsschlüssels beachten?

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.

> 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.

> 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.

Was muss ich wissen, bevor sichere Laufwerke entsperrt werden?

Um die Daten von einem sicheren Laufwerk zu entsperren, das in ein neues Speicher-Array migriert wird, müssen Sie dessen Sicherheitsschlüssel importieren.

Beachten Sie vor dem Entsperren von sicheren Laufwerken die folgenden Richtlinien:

- Das Ziel-Storage-Array (in dem Sie die Laufwerke verschieben) muss bereits über einen Sicherheitsschlüssel verfügen. Die migrierten Laufwerke werden erneut auf das Ziel-Storage-Array übertragen.
- Bei den zu migrierenden Laufwerken kennen Sie die Security Key Identifier und den Passphrase, der der Sicherheitsschlüsseldatei entspricht.
- Die Sicherheitsschlüsseldatei steht auf dem Management-Client zur Verfügung (das System mit einem Browser, der zum Zugriff auf System Manager verwendet wird).

Zugriff auf Lese-/Schreibzugriffe

Das Fenster **Drive Settings** enthält Informationen über die Attribute **Drive Security**. „Read/Write Accessible“ ist eines der Attribute, das anzeigt, ob Daten eines Laufwerks gesperrt wurden.

Um **Drive Security** -Attribute 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]).

Was muss ich über die Validierung des Sicherheitsschlüssels wissen?

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.

Worin besteht der Unterschied zwischen internem Sicherheitsschlüssel und externem Sicherheitsschlüsselmanagement?

Wenn Sie die * Drive Security*-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.