Einstellungen

SANtricity 11.6

NetApp
February 12, 2024

Inhalt

Einstellungen

Meldungen

Konzepte

Funktionsweise von Warnmeldungen

Warnungen benachrichtigen Administratoren über wichtige Ereignisse im Speicher-Array. Warnmeldungen können per E-Mail, SNMP-Traps und Syslog gesendet werden.

Die Warnmeldungen werden wie folgt bearbeitet:

1. Ein Administrator konfiguriert mindestens eine der folgenden Warnmeldungsmethoden in System Manager:
   - **E-Mail** — Nachrichten werden an E-Mail-Adressen gesendet.
   - **SNMP** — SNMP-Traps werden an einen SNMP-Server gesendet.
   - **Syslog** — Nachrichten werden an einen Syslog-Server gesendet.
2. Wenn der Ereignismonitor des Speicherarrays ein Problem erkennt, schreibt er Informationen über dieses Problem in das Ereignisprotokoll (verfügbar über **Menü:Support[Ereignisprotokoll]**). Beispielsweise können Probleme auftreten, beispielsweise ein Batterieausfall, eine Komponente, die von optimal nach Offline verschoben wird oder Redundanzfehler im Controller sind.
3. Wenn der Ereignismonitor feststellt, dass das Ereignis „ertabbar“ ist, sendet er eine Benachrichtigung mit den konfigurierten Alarmmethoden (E-Mail, SNMP und/oder Syslog). Alle kritischen Ereignisse werden als „alertable“, zusammen mit einigen Warn- und Informationsereignissen betrachtet.

Konfiguration von Warnungen

Sie können Benachrichtigungen über den Einrichtungsassistenten (nur für E-Mail-Benachrichtigungen) oder über die Seite „Meldungen“ konfigurieren. Um die aktuelle Konfiguration zu überprüfen, gehen Sie zu **Einstellungen › Alarme**.

Im Feld „Meldungen“ wird die Konfiguration der Warnmeldungen angezeigt. Dabei kann es sich um eine der folgenden Optionen handelt:

- Nicht konfiguriert.
- Konfiguriert; mindestens eine Alarmmethode ist eingerichtet. Um zu bestimmen, welche Alarmmethoden konfiguriert sind, zeigen Sie den Cursor auf die Kachel.

Warnmeldungsinformationen

Warnmeldungen können die folgenden Informationstypen enthalten:

- Name des Speicher-Arrays.
- Ereignistyp, der mit einem Eintrag im Ereignisprotokoll zusammenhängt.
- Datum und Uhrzeit des Ereignisses.
- Kurze Beschreibung der Veranstaltung.

Syslog-Warnungen folgen dem RFC 3164-Messaging-Standard.

Warnmeldungen zur Terminologie

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

Komponente	Beschreibung
Ereignisüberwachung	Die Ereignisüberwachung befindet sich im Storage-Array und wird als Hintergrundaufgabe ausgeführt. Wenn die Ereignisüberwachung Anomalien im Storage Array erkennt, schreibt sie Informationen zu den Problemen in das Ereignisprotokoll. Zu den Problemen zählen beispielsweise Ereignisse wie Batteriefehler, der Wechsel von optimal zu Offline oder Redundanzfehler im Controller. Wenn der Ereignismonitor feststellt, dass das Ereignis „ertabbar“ ist, sendet er eine Benachrichtigung mit den konfigurierten Alarmmethoden (E-Mail, SNMP und/oder Syslog). Alle kritischen Ereignisse werden als „alertable“, zusammen mit einigen Warn- und Informationsereignissen betrachtet.
Mailserver	Der Mail-Server wird zum Senden und Empfangen von E-Mail-Warnungen verwendet. Der Server verwendet das Simple Mail Transfer Protocol (SMTP).
SNMP	Das Simple Network Management Protocol (SNMP) ist ein internetbasiertes Protokoll, das zur Verwaltung und gemeinsamen Nutzung von Informationen zwischen Geräten in IP-Netzwerken verwendet wird.
SNMP-Trap	Ein SNMP-Trap ist eine Benachrichtigung, die an einen SNMP-Server gesendet wird. Der Trap enthält Informationen zu wichtigen Problemen mit dem Speicher-Array.
SNMP-Trap-Ziel	Ein SNMP-Trap-Ziel ist eine IPv4- oder IPv6-Adresse des Servers, auf dem ein SNMP-Dienst ausgeführt wird.
Community-Name	Ein Community-Name ist eine Zeichenfolge, die wie ein Kennwort für die Netzwerkserver in einer SNMP-Umgebung fungiert.
MIB-Datei	Die Management Information Base (MIB)-Datei definiert die Daten, die im Speicher-Array überwacht und verwaltet werden. Sie muss mit der SNMP-Dienst-Anwendung auf dem Server kopiert und kompiliert werden. Diese MIB-Datei ist mit der System Manager-Software auf der Support-Website verfügbar.
MIB-Variablen	MIB-Variablen (Management Information Base) können Werte wie den Namen des Speicherarrays, den Array-Speicherort und einen Ansprechpartner als Antwort auf SNMP GetRequests zurückgeben.
Syslog	Syslog ist ein Protokoll, das von Netzwerkgeräten zum Senden von Ereignismeldungen an einen Protokollierungsserver verwendet wird.
UDP	Das User Datagram Protocol (UDP) ist ein Protokoll der Transportschicht, das eine Quell- und Zielportnummer in ihren Paketheader angibt.

Anleitungen

Verwalten von E-Mail-Warnmeldungen

Konfigurieren Sie E-Mail-Server und Empfänger für Warnmeldungen

Um E-Mail-Benachrichtigungen zu konfigurieren, müssen Sie eine E-Mail-Serveradresse und die E-Mail-Adressen der Warnungsempfänger angeben. Es sind bis zu 20 E-Mail-Adressen zulässig.

Bevor Sie beginnen

- Die Adresse des Mail-Servers muss vorhanden sein. Bei der Adresse kann es sich um eine IPv4- oder IPv6-Adresse oder einen vollqualifizierten Domänennamen handeln.

  > Um einen vollständig qualifizierten Domänennamen zu verwenden, müssen Sie auf beiden Controllern einen DNS-Server konfigurieren. Sie können einen DNS-Server auf der Seite Hardware konfigurieren.

- Die als Alarmsender zu verwendenden E-Mail-Adresse muss verfügbar sein. Dies ist die Adresse, die im Feld „von“ der Warnmeldung angezeigt wird. Im SMTP-Protokoll wird eine Absenderadresse benötigt; ohne diese ergibt sich ein Fehler.
- Die E-Mail-Adresse(n) der Warnungsempfänger muss verfügbar sein. Der Empfänger ist in der Regel eine Adresse für einen Netzwerkadministrator oder Speicheradministrator. Sie können bis zu 20 E-Mail-Adressen eingeben.

Über diese Aufgabe

Diese Aufgabe beschreibt die Konfiguration des E-Mail-Servers, die Eingabe von E-Mail-Adressen für den Absender und die Empfänger und das Testen aller von der Seite Warnungen eingegebenen E-Mail-Adressen.

> E-Mail-Benachrichtigungen können auch über den Einrichtungsassistenten konfiguriert werden.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **E-Mail** aus.

   Wenn noch kein E-Mail-Server konfiguriert ist, wird auf der Registerkarte E-Mail „Mailserver konfigurieren“ angezeigt.

3. Wählen Sie **E-Mail-Server Konfigurieren**.

   Das Dialogfeld **Mailserver konfigurieren** wird geöffnet.

4. Geben Sie die Informationen zum Mail-Server ein, und klicken Sie dann auf **Speichern**.
   - **Mail-Server-Adresse** — Geben Sie einen vollständig qualifizierten Domainnamen, eine IPv4-Adresse oder eine IPv6-Adresse des Mail-Servers ein.

     > Um einen vollständig qualifizierten Domänennamen zu verwenden, müssen Sie auf beiden Controllern einen DNS-Server konfigurieren. Sie können einen DNS-Server auf der Seite **Hardware** konfigurieren.

- **E-Mail-Absender-Adresse** — Geben Sie eine gültige E-Mail-Adresse ein, die als Absender der E-Mail verwendet werden soll. Diese Adresse wird im Feld „von“ der E-Mail-Nachricht angezeigt.
- **Kontaktinformationen in E-Mail einfügen** — um die Kontaktdaten des Absenders in die Warnmeldung aufzunehmen, wählen Sie diese Option aus, und geben Sie dann einen Namen und eine Telefonnummer ein. Nach dem Klick auf **Speichern** werden die E-Mail-Adressen auf der Seite **Alarme** auf der Registerkarte **E-Mail** angezeigt.

5. Wählen Sie **E-Mails Hinzufügen**.

   Das Dialogfeld E-Mails hinzufügen wird geöffnet.

6. Geben Sie eine oder mehrere E-Mail-Adressen für die Empfänger der Warnmeldung ein, und klicken Sie dann auf **Hinzufügen**.

   Die E-Mail-Adressen werden auf der Seite „Meldungen“ angezeigt.

7. Wenn Sie sicherstellen möchten, dass die E-Mail-Adressen gültig sind, klicken Sie auf **Alle E-Mails testen**, um Testmeldungen an die Empfänger zu senden.

Ergebnisse

Nachdem Sie E-Mail-Alarme konfiguriert haben, sendet der Ereignismonitor immer dann E-Mail-Nachrichten an die angegebenen Empfänger.

E-Mail-Adressen für Warnmeldungen bearbeiten

Sie können die E-Mail-Adressen der Empfänger, die E-Mail-Benachrichtigungen erhalten, ändern.

Bevor Sie beginnen

Die E-Mail-Adresse, die Sie bearbeiten möchten, muss auf der Registerkarte „E-Mail“ der Seite „Benachrichtigungen“ definiert sein.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **E-Mail** aus.
3. Wählen Sie in der Tabelle **E-Mail-Adresse** die Adresse aus, die Sie ändern möchten, und klicken Sie dann rechts auf das Symbol **Bearbeiten** (Bleistift).

   Die Zeile wird zu einem bearbeitbaren Feld.

4. Geben Sie eine neue Adresse ein, und klicken Sie auf das Symbol **Speichern** (Häkchen).

   Wenn Sie die Änderungen abbrechen möchten, wählen Sie das Symbol **Abbrechen** (X).

Ergebnisse

Auf der Registerkarte „E-Mail“ der Seite „Meldungen“ werden die aktualisierten E-Mail-Adressen angezeigt.

Fügen Sie E-Mail-Adressen für Warnungen hinzu

Sie können bis zu 20 Empfänger für E-Mail-Benachrichtigungen hinzufügen.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **E-Mail** aus.
3. Wählen Sie **E-Mails Hinzufügen**.

   Das Dialogfeld **E-Mails hinzufügen** wird geöffnet.

4. Geben Sie in das leere Feld eine neue E-Mail-Adresse ein. Wenn Sie mehr als eine Adresse hinzufügen möchten, wählen Sie **Weitere E-Mail hinzufügen**, um ein anderes Feld zu öffnen.
5. Klicken Sie Auf **Hinzufügen**.

Ergebnisse

Auf der Registerkarte **E-Mail** der Seite **Alerts** werden die neuen E-Mail-Adressen angezeigt.

Löschen Sie E-Mail-Server oder E-Mail-Adressen für Warnmeldungen

Sie können den zuvor definierten Mail-Server so entfernen, dass Warnmeldungen nicht mehr an die E-Mail-Adressen gesendet werden, oder Sie können einzelne E-Mail-Adressen entfernen.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **E-Mail** aus.
3. Führen Sie in der Tabelle einen der folgenden Schritte aus:
   - Um einen E-Mail-Server zu entfernen, damit Warnmeldungen nicht mehr an die E-Mail-Adressen gesendet werden, wählen Sie die Zeile für den Mail-Server aus.
   - Um eine E-Mail-Adresse zu entfernen, damit Benachrichtigungen nicht mehr an diese Adresse gesendet werden, wählen Sie die Zeile für die zu löschende E-Mail-Adresse aus. Die Schaltfläche **Löschen** oben rechts in der Tabelle steht zur Auswahl.
4. Klicken Sie auf **Löschen** und bestätigen Sie den Vorgang.

E-Mail-Server für Warnmeldungen bearbeiten

Sie können die E-Mail-Server-Adresse und die E-Mail-Absenderadresse ändern, die für E-Mail-Benachrichtigungen verwendet werden.

Bevor Sie beginnen

Die Adresse des Mail-Servers, den Sie ändern, muss verfügbar sein. Bei der Adresse kann es sich um eine IPv4- oder IPv6-Adresse oder einen vollqualifizierten Domänennamen handeln.

> Um einen vollständig qualifizierten Domänennamen zu verwenden, müssen Sie auf beiden Controllern einen DNS-Server konfigurieren. Sie können einen DNS-Server auf der Seite Hardware konfigurieren.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **E-Mail** aus.
3. Wählen Sie **E-Mail-Server Konfigurieren**.

Das Dialogfeld Mailserver konfigurieren wird geöffnet.

4. Bearbeiten Sie die Adresse des E-Mail-Servers, die Absenderinformationen und die Kontaktinformationen.
   - **Mail-Server-Adresse** — Bearbeiten Sie den vollqualifizierten Domainnamen, die IPv4-Adresse oder die IPv6-Adresse des Mailservers.

     Um einen vollständig qualifizierten Domänennamen zu verwenden, müssen Sie auf beiden Controllern einen DNS-Server konfigurieren. Sie können einen DNS-Server auf der Seite Hardware konfigurieren.

   - **E-Mail-Absender-Adresse** — Bearbeiten Sie die E-Mail-Adresse, die als Absender der E-Mail verwendet werden soll. Diese Adresse wird im Feld „von“ der E-Mail-Nachricht angezeigt.
   - **Kontaktinformationen in E-Mail einfügen** — um die Kontaktdaten des Absenders zu bearbeiten, wählen Sie diese Option aus, und bearbeiten Sie dann den Namen und die Telefonnummer.
5. Klicken Sie Auf **Speichern**.

Managen von SNMP-Warnmeldungen

Konfigurieren Sie Communities und Ziele für SNMP-Benachrichtigungen

Um SNMP-Warnungen (Simple Network Management Protocol) zu konfigurieren, müssen Sie mindestens einen Server identifizieren, auf dem der Ereignismonitor des Speicherarrays SNMP-Traps senden kann. Die Konfiguration erfordert einen Community-Namen und eine IP-Adresse für den Server.

Bevor Sie beginnen

- Ein Netzwerkserver muss mit einer SNMP-Dienstanwendung konfiguriert sein. Sie benötigen die Netzwerkadresse dieses Servers (entweder eine IPv4- oder eine IPv6-Adresse), damit der Ereignismonitor Trap-Meldungen an diese Adresse senden kann. Sie können mehrere Server verwenden (bis zu 10 Server sind zulässig).
- Es muss ein Community-Name erstellt werden, der nur aus druckbaren ASCII-Zeichen besteht. Der Community-Name, ein String, der wie ein Kennwort für die Netzwerkserver fungiert, wird in der Regel von einem Netzwerkadministrator erstellt. Es können bis zu 256 Communities erstellt werden.
- Die Management Information Base (MIB)-Datei wurde kopiert und mit der SNMP-Dienst-Anwendung auf dem Server kompiliert. Diese MIB-Datei definiert die Daten, die überwacht und verwaltet werden.

  Wenn Sie nicht über die MIB-Datei, können Sie sie von der NetApp Support-Website erhalten:

  - Gehen Sie zu "NetApp Support".
  - Klicken Sie Auf **Downloads**.
  - Klicken Sie Auf **Software**.
  - Suchen Sie Ihre Verwaltungssoftware (z. B. SANtricity-System-Manager), und klicken Sie dann rechts auf **Los!**.
  - Klicken Sie auf der neuesten Version auf**Anzeigen & Download**.
  - Klicken Sie unten auf der Seite auf **Weiter**.
  - Akzeptieren Sie die EULA.
  - Scrollen Sie nach unten, bis Sie **MIB-Datei für SNMP-Traps** sehen, und klicken Sie dann auf den Link,

um die Datei herunterzuladen.

Über diese Aufgabe

Diese Aufgabe beschreibt, wie Sie den SNMP-Server für Trap-Ziele identifizieren und anschließend Ihre Konfiguration testen.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **SNMP** aus.

   Wenn noch keine Community konfiguriert ist, wird auf der Registerkarte SNMP „Configure Communities“ angezeigt.

3. Wählen Sie * Communities Konfigurieren*.

   Das Dialogfeld **Configure Communities** wird geöffnet.

4. Geben Sie im Feld **Community Name** eine oder mehrere Community-Strings für die Netzwerkserver ein, und klicken Sie dann auf **Speichern**.

   Auf der Seite Warnungen wird „Fallziele hinzufügen“ angezeigt.

5. Wählen Sie **Trap-Ziele Hinzufügen**.

   Das Dialogfeld **Trap-Ziele hinzufügen** wird geöffnet.

6. Geben Sie ein oder mehrere Trap-Ziele ein, wählen Sie die zugehörigen Community-Namen aus, und klicken Sie dann auf **Hinzufügen**.
   - **Trap-Ziel** — Geben Sie eine IPv4- oder IPv6-Adresse des Servers ein, auf dem ein SNMP-Dienst ausgeführt wird.
   - **Community-Name** — Wählen Sie im Dropdown-Menü den Community-Namen für dieses Trap-Ziel aus. (Wenn Sie nur einen Community-Namen definiert haben, wird der Name bereits in diesem Feld angezeigt.)
   - **Authentifizierungsfehler senden Trap** — Wählen Sie diese Option (das Kontrollkästchen) aus, wenn Sie das Trap-Ziel benachrichtigen möchten, wenn eine SNMP-Anfrage aufgrund eines nicht erkannten Community-Namens abgelehnt wird. Nach dem Klicken auf **Hinzufügen** werden die Trap-Ziele und die zugehörigen Community-Namen auf der Seite **SNMP** auf der Registerkarte **Alarme** angezeigt.
7. Um sicherzustellen, dass ein Trap gültig ist, wählen Sie ein Trap-Ziel aus der Tabelle aus, und klicken Sie dann auf **Trap-Ziel testen**, um einen Test-Trap an die konfigurierte Adresse zu senden.

Ergebnisse

Der Ereignismonitor sendet SNMP-Traps an den/die Server(s), wenn ein alertable Ereignis auftritt.

Community-Namen für SNMP-Traps bearbeiten

Sie können Community-Namen für SNMP-Traps bearbeiten und einen anderen Community-Namen einem SNMP-Trap-Ziel zuordnen.

Bevor Sie beginnen

Es muss ein Community-Name erstellt werden, der nur aus druckbaren ASCII-Zeichen besteht. Der Community-Name, ein String, der wie ein Kennwort für die Netzwerkserver fungiert, wird von einem Netzwerkadministrator erstellt.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Ziele und Community-Namen werden in der Tabelle angezeigt.

3. Bearbeiten Sie Community-Namen wie folgt:
   - Um einen Community-Namen zu bearbeiten, wählen Sie **Communities konfigurieren**. Geben Sie den neuen Community-Namen ein und klicken Sie dann auf **Speichern**. Community-Namen können nur aus druckbaren ASCII-Zeichen bestehen.
   - Um einen Community-Namen einem neuen Trap-Ziel zuzuordnen, wählen Sie den Community-Namen aus der Tabelle aus, und klicken Sie dann rechts auf das Symbol **Bearbeiten** (Bleistift). Wählen Sie im Dropdown-Menü Community Name einen neuen Community-Namen für ein SNMP-Trap-Ziel aus und klicken Sie dann auf das Symbol **Speichern** (Häkchen).

     Wenn Sie die Änderungen abbrechen möchten, wählen Sie das Symbol **Abbrechen** (X).

Ergebnisse

Die Registerkarte **SNMP** der Seite **Alerts** zeigt die aktualisierten Communities an.

Fügen Sie Community-Namen für SNMP-Traps hinzu

Sie können bis zu 256 Community-Namen für SNMP-Traps hinzufügen.

Bevor Sie beginnen

Der/die Community-Name(n) muss erstellt werden. Der Community-Name, ein String, der wie ein Kennwort für die Netzwerkserver fungiert, wird in der Regel von einem Netzwerkadministrator erstellt. Es besteht nur aus druckbaren ASCII-Zeichen.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Ziele und Community-Namen werden in der Tabelle angezeigt.

3. Wählen Sie * Communities Konfigurieren*.

   Das Dialogfeld „Communities konfigurieren“ wird geöffnet.

4. Wählen Sie **Weitere Community hinzufügen**.
5. Geben Sie den neuen Community-Namen ein und klicken Sie dann auf **Speichern**.

Ergebnisse

Der neue Community-Name wird auf der Seite **Alerts** auf der Registerkarte **SNMP** angezeigt.

Entfernen Sie den Community-Namen für SNMP-Traps

Sie können einen Community-Namen für SNMP-Traps entfernen.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Ziele und die Community-Namen werden auf der Seite Meldungen angezeigt.

3. Wählen Sie * Communities Konfigurieren*.

   Das Dialogfeld **Configure Communities** wird geöffnet.

4. Wählen Sie den Community-Namen aus, den Sie löschen möchten, und klicken Sie auf das Symbol **Entfernen** (X) ganz rechts.

   Wenn Trap-Ziele mit diesem Community-Namen verknüpft sind, werden im Dialogfeld **Community entfernen bestätigen** die betroffenen Trap-Zieladressen angezeigt.

5. Bestätigen Sie den Vorgang, und klicken Sie dann auf **Entfernen**.

Ergebnisse

Der Community-Name und das zugehörige Trap-Ziel werden von der Seite **Alerts** entfernt.

Konfigurieren Sie SNMP-MIB-Variablen

Für SNMP-Warnungen können Sie optional Management Information Base (MIB)-Variablen konfigurieren, die in SNMP-Traps angezeigt werden. Diese Variablen können den Namen des Speicher-Arrays, den Speicherort des Arrays und einen Ansprechpartner zurückgeben.

Bevor Sie beginnen

Die MIB-Datei muss kopiert und mit der SNMP-Dienst-Anwendung auf dem Server kompiliert werden.

Wenn Sie keine MIB-Datei haben, können Sie es wie folgt erhalten:

- Gehen Sie zu "NetApp Support".
- Klicken Sie Auf **Downloads**.
- Klicken Sie Auf **Software**.
- Suchen Sie Ihre Verwaltungssoftware (z. B. SANtricity-System-Manager), und klicken Sie dann rechts auf **Los!**.
- Klicken Sie auf **Ansicht & Download** auf der neuesten Version.
- Klicken Sie unten auf der Seite auf **Weiter**.
- Akzeptieren Sie die EULA.
- Scrollen Sie nach unten, bis Sie **MIB-Datei für SNMP-Traps** sehen, und klicken Sie dann auf den Link, um die Datei herunterzuladen.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie MIB-Variablen für SNMP-Traps definiert werden. Diese Variablen können als Antwort auf SNMP GetRequests folgende Werte zurückgeben:

- `sysName` (Name für das Speicher-Array)
- `sysLocation` (Speicherort des Speicher-Arrays)

- *sysContact* (Name eines Administrators)

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **SNMP** aus.
3. Wählen Sie **Konfigurieren von SNMP-MIB-Variablen**.

   Das Dialogfeld SNMP-MIB-Variablen konfigurieren wird geöffnet.

4. Geben Sie einen oder mehrere der folgenden Werte ein, und klicken Sie dann auf **Speichern**.
   - **Name** — der Wert für die MIB-Variable *sysName*. Geben Sie beispielsweise einen Namen für das Speicher-Array ein.
   - **Lage** — der Wert für die MIB Variable *sysLocation*. Geben Sie beispielsweise einen Speicherort des Speicher-Arrays ein.
   - **Kontakt** — der Wert für die MIB-Variable *sysContact*. Geben Sie beispielsweise einen Administrator ein, der für das Speicher-Array verantwortlich ist.

Ergebnisse

Diese Werte werden in SNMP-Trap-Meldungen für Storage Array-Warnungen angezeigt.

Fügen Sie Trap-Ziele für SNMP-Warnungen hinzu

Sie können bis zu 10 Server zum Senden von SNMP-Traps hinzufügen.

Bevor Sie beginnen

- Der Netzwerkserver, den Sie hinzufügen möchten, muss mit einer SNMP-Serviceanwendung konfiguriert sein. Sie benötigen die Netzwerkadresse dieses Servers (entweder eine IPv4- oder eine IPv6-Adresse), damit der Ereignismonitor Trap-Meldungen an diese Adresse senden kann. Sie können mehrere Server verwenden (bis zu 10 Server sind zulässig).
- Es muss ein Community-Name erstellt werden, der nur aus druckbaren ASCII-Zeichen besteht. Der Community-Name, ein String, der wie ein Kennwort für die Netzwerkserver fungiert, wird in der Regel von einem Netzwerkadministrator erstellt. Es können bis zu 256 Communities erstellt werden.
- Die Management Information Base (MIB)-Datei wurde kopiert und mit der SNMP-Dienst-Anwendung auf dem Server kompiliert. Diese MIB-Datei definiert die Daten, die überwacht und verwaltet werden.

  Wenn Sie nicht über die MIB-Datei, können Sie sie von der NetApp Support-Website erhalten:

  - Gehen Sie zu "NetApp Support".
  - Klicken Sie Auf **Downloads**.
  - Klicken Sie Auf **Software**.
  - Suchen Sie Ihre Verwaltungssoftware (z. B. SANtricity-System-Manager), und klicken Sie dann rechts auf **Los!**.
  - Klicken Sie auf **Ansicht & Download** auf der neuesten Version.
  - Klicken Sie unten auf der Seite auf **Weiter**.
  - Akzeptieren Sie die EULA.
  - Scrollen Sie nach unten, bis Sie **MIB-Datei für SNMP-Traps** sehen, und klicken Sie dann auf den Link, um die Datei herunterzuladen.

Schritte

1. Wählen Sie **Einstellungen** > **Alarme**.
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die aktuell definierten Trap-Ziele werden in der Tabelle angezeigt.

3. Wählen Sie **Trap Desinations Hinzufügen**.

   Das Dialogfeld Trap-Ziele hinzufügen wird geöffnet.

4. Geben Sie ein oder mehrere Trap-Ziele ein, wählen Sie die zugehörigen Community-Namen aus, und klicken Sie dann auf **Hinzufügen**.
   - **Trap-Ziel** — Geben Sie eine IPv4- oder IPv6-Adresse des Servers ein, auf dem ein SNMP-Dienst ausgeführt wird.
   - **Community-Name** — Wählen Sie im Dropdown-Menü den Community-Namen für dieses Trap-Ziel aus. (Wenn Sie nur einen Community-Namen definiert haben, wird der Name bereits in diesem Feld angezeigt.)
   - **Authentifizierungsfehler senden Trap** — Wählen Sie diese Option (das Kontrollkästchen) aus, wenn Sie das Trap-Ziel benachrichtigen möchten, wenn eine SNMP-Anfrage aufgrund eines nicht erkannten Community-Namens abgelehnt wird. Nach dem Klicken auf **Hinzufügen** werden die Trap-Ziele und die zugehörigen Community-Namen in der Tabelle angezeigt.
5. Um sicherzustellen, dass ein Trap gültig ist, wählen Sie ein Trap-Ziel aus der Tabelle aus, und klicken Sie dann auf **Trap-Ziel testen**, um einen Test-Trap an die konfigurierte Adresse zu senden.

Ergebnisse

Der Ereignismonitor sendet SNMP-Traps an den/die Server(s), wenn ein alertable Ereignis auftritt.

Löschen von Trap-Zielen

Sie können eine Trap-Zieladresse löschen, sodass der Event-Monitor des Speicherarrays keine SNMP-Traps mehr an diese Adresse sendet.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **SNMP** aus.

   Die Trap-Zieladressen werden in der Tabelle angezeigt.

3. Wählen Sie ein Trap-Ziel aus, und klicken Sie dann rechts oben auf der Seite auf **Löschen**.
4. Bestätigen Sie den Vorgang, und klicken Sie dann auf **Löschen**.

   Die Zieladresse wird nicht mehr auf der Seite **Alerts** angezeigt.

Ergebnisse

Das gelöschte Trap-Ziel empfängt keine SNMP-Traps mehr vom Event-Monitor des Speicherarrays.

Managen von Syslog-Warnmeldungen

Konfigurieren Sie den Syslog-Server für Warnmeldungen

Um Syslog-Warnmeldungen zu konfigurieren, müssen Sie eine Syslog-Serveradresse und einen UDP-Port eingeben. Es sind bis zu fünf Syslog-Server zulässig.

Bevor Sie beginnen

- Die Syslog-Serveradresse muss verfügbar sein. Bei dieser Adresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
- UDP-Portnummer des Syslog-Servers muss verfügbar sein. Dieser Port ist normalerweise 514.

Über diese Aufgabe

Diese Aufgabe beschreibt, wie Sie die Adresse und den Port für den Syslog-Server eingeben und anschließend die eingegebene Adresse testen.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **Syslog** aus.

   Wenn noch kein Syslog-Server definiert ist, wird auf der Seite **Alerts** „Add Syslog Servers“ angezeigt.

3. Klicken Sie Auf **Syslog-Server Hinzufügen**.

   Das Dialogfeld **Syslog Server** hinzufügen wird geöffnet.

4. Geben Sie Informationen für einen oder mehrere Syslog-Server ein (maximal fünf), und klicken Sie dann auf **Hinzufügen**.
   - **Server-Adresse** — Geben Sie einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
   - **UDP Port** — normalerweise ist der UDP Port für syslog 514. In der Tabelle werden die konfigurierten Syslog-Server angezeigt.
5. Um eine Testwarnung an die Serveradressen zu senden, wählen Sie **Alle Syslog-Server testen**.

Ergebnisse

Der Ereignismonitor sendet bei jedem Ereignis, das in einem Alarmtabellen stattfindet, Warnmeldungen an den Syslog-Server.

Bearbeiten Sie Syslog-Server für Warnmeldungen

Sie können die Serveradresse bearbeiten, die für den Empfang von Syslog-Warnungen verwendet wird.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **Syslog** aus.
3. Wählen Sie in der Tabelle eine Syslog-Serveradresse aus, und klicken Sie dann auf das Symbol **Bearbeiten** (Bleistift) von rechts.

   Die Zeile wird zu einem bearbeitbaren Feld.

4. Bearbeiten Sie die Serveradresse und die UDP-Portnummer und klicken Sie dann auf das Symbol

Speichern (Häkchen).

Ergebnisse

Die aktualisierte Serveradresse wird in der Tabelle angezeigt.

Fügen Sie Syslog-Server für Warnungen hinzu

Sie können maximal fünf Server für Syslog-Warnmeldungen hinzufügen.

Bevor Sie beginnen

- Die Syslog-Serveradresse muss verfügbar sein. Bei dieser Adresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
- Die UDP-Portnummer des Syslog-Servers muss verfügbar sein. Dieser Port ist normalerweise 514.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **Syslog** aus.
3. Wählen Sie **Syslog-Server Hinzufügen**.

   Das Dialogfeld Syslog Server hinzufügen wird geöffnet.

4. Wählen Sie **Weitere Syslog-Server hinzufügen**.
5. Geben Sie Informationen für den Syslog-Server ein, und klicken Sie dann auf **Hinzufügen**.

   - **Syslog Server Address** — Geben Sie einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
   - **UDP Port** — normalerweise ist der UDP Port für syslog 514.

   Sie können bis zu fünf Syslog-Server konfigurieren.

Ergebnisse

Die Syslog-Server-Adressen werden in der Tabelle angezeigt.

Löschen von Syslog-Servern für Warnmeldungen

Sie können einen Syslog-Server löschen, damit er keine Warnungen mehr erhält.

Schritte

1. Wählen Sie **Einstellungen › Alarme**.
2. Wählen Sie die Registerkarte **Syslog** aus.
3. Wählen Sie eine Syslog-Serveradresse aus, und klicken Sie dann rechts oben auf **Entfernen**.

   Das Dialogfeld Löschen des Syslog-Servers bestätigen wird geöffnet.

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

Ergebnisse

Der entfernte Server empfängt keine Warnmeldungen mehr von der Ereignisüberwachung.

FAQs

Was ist, wenn Alarme deaktiviert sind?

Wenn Administratoren Benachrichtigungen über wichtige Ereignisse im Speicher-Array erhalten sollen, müssen Sie eine Methode zur Alarmierung konfigurieren.

Bei Storage Arrays, die mit SANtricity System Manager verwaltet werden, konfigurieren Sie Warnmeldungen über die Seite „Meldungen“. Alert-Benachrichtigungen können über E-Mail, SNMP-Traps oder Syslog-Nachrichten gesendet werden. Zudem können E-Mail-Benachrichtigungen über den ersten Setup-Assistenten konfiguriert werden.

Wie konfiguriere ich SNMP- oder syslog-Alarme?

Neben E-Mail-Warnungen können Benachrichtigungen auch über SNMP-Traps (Simple Network Management Protocol) oder Syslog-Nachrichten gesendet werden.

Um SNMP- oder Syslog-Warnmeldungen zu konfigurieren, gehen Sie zu MENU:Einstellungen[Warnungen].

Warum sind Zeitstempel zwischen dem Array und Warnungen uneinheitlich?

Wenn das Speicher-Array Warnungen sendet, ist es für die Zeitzone des Zielservers oder Hosts, der die Warnungen empfängt, nicht korrekt. Stattdessen verwendet das Speicher-Array die lokale Zeit (GMT), um den Zeitstempel zu erstellen, der für den Warnungsdatensatz verwendet wird. Aufgrund dessen sind möglicherweise Inkonsistenzen zwischen den Zeitstempel für das Storage-Array und dem Server oder Host, der eine Meldung empfängt, zu erkennen.

Da das Speicherarray beim Senden von Warnungen nicht richtig für die Zeitzone ist, ist der Zeitstempel für die Warnungen GMT-relative, der einen Zeitzonenversatz von Null hat. Um einen Zeitstempel zu berechnen, der Ihrer lokalen Zeitzone angemessen ist, sollten Sie Ihren Stundenversatz von GMT bestimmen und diesen Wert dann von den Zeitstempel hinzufügen oder abziehen.

> Um dieses Problem zu vermeiden, konfigurieren Sie NTP (Network Time Protocol) auf Ihren Speicher-Array-Controllern. NTP stellt sicher, dass die Controller immer mit der richtigen Zeit synchronisiert werden.

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 Write Caching Option 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 unter einem VMware 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 **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).

Ergebnisse

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 **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 **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 **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 die gespeicherte Speicher-Array-Konfiguration auf ein anderes Speicher-Array zu laden, verwenden Sie die SANtricity-Befehlszeilenschnittstelle (SMcli) mit dem `-f` Option zum Anwenden des `.cfg` Datei:

> Sie können eine Speicherarray-Konfiguration auch über die Unified Manager-Oberfläche auf andere Speicher-Arrays laden (wählen Sie **Manage › Import Settings**).

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 **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 **Einstellungen › System**.
2. Wählen Sie im Abschnitt **Allgemein** die Option **Anmelde-Banner konfigurieren** aus.

Das Dialogfeld Anmelde-Banner konfigurieren wird geöffnet.

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

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

4. Klicken Sie Auf **Speichern**.

Ergebnisse

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

Verwalten von Sitzungszeitungen

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

Über diese Aufgabe

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

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

Schritte

1. Wählen Sie **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 32 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 **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:
   - **Starten Sie die Cachespülung der Nachfrage** — Wählen Sie einen Prozentsatz, der für die in Ihrer Umgebung verwendeten I/O-Vorgänge geeignet ist. Wenn Sie sich für einen Wert unter 80 % entscheiden, können Sie eine verminderte Leistung feststellen.
   - **Cache Blockgröße** — Wählen Sie eine Größe, die für Ihre Anwendungen geeignet ist.
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 **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 stellt sicher, dass eingehender I/O-Datenverkehr von den Hosts dynamisch verwaltet und auf beiden Controllern ausgeglichen wird. Diese Funktion ist standardmäßig aktiviert, Sie können sie jedoch 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 **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 unter einem VMware Betriebssystem ausgeführt. Und weitere drei führen ein Linux-Betriebssystem aus. Sie müssen als Standard-Host-Betriebssystem Factory Default auswählen.

Schritte

1. Wählen Sie **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.

Über diese Aufgabe

Standardmäßig ist die ältere Managementoberfläche auf aktiviert. Wenn die Funktion deaktiviert wird,

verwendet das Storage-Array und der Management-Client eine sicherere Kommunikationsmethode (REST-API über HTTPS). Bestimmte Tools und Aufgaben können jedoch beeinträchtigt werden, wenn die Übertragung deaktiviert ist.

> Für das EF600 Storage-System ist diese Funktion standardmäßig deaktiviert.

Die Einstellung wirkt sich auf die Vorgänge wie folgt aus:

- **Ein** (Standard) — erforderliche Einstellung zum Konfigurieren der Spiegelung mit der CLI und einigen anderen Tools, wie dem OCI-Adapter.
- **Aus** — erforderliche Einstellung zur Durchsetzung von Vertraulichkeit bei der Kommunikation zwischen dem Speicher-Array und dem Management-Client und zum Zugriff auf externe Tools. Empfohlene Einstellung bei der Konfiguration eines Verzeichnisservers (LDAP).

Schritte

1. Wählen Sie **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. Sie können den Spülzeitpunkt in System Manager nicht ändern. 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“ ein. Dabei handelt es sich um Speicherblöcke, die 8, 16 und 32 KiB groß sein können. Alle Volumes im Storage-System nutzen denselben Cache-Speicherplatz. Daher können die Volumes nur eine Cache-Blockgröße aufweisen.

Applikationen verwenden unterschiedliche Blockgrößen, die wiederum einen Einfluss auf die Storage-Performance haben können. Standardmäßig ist die Blockgröße in System Manager 32 KiB, Sie können den Wert jedoch auf 8, 16, 32 KiBs festlegen. Kleinere Größen sind eine gute Wahl für Dateisysteme oder Datenbankanwendungen. Eine größere Größe ist eine gute Wahl für Applikationen, die eine umfangreiche Datenübertragung, sequenziellen I/O oder eine hohe Bandbreite, wie z. B. Multimedia, erfordern.

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 Synchronisierungsstatus über das Dialogfeld Speicherarray-Uhren synchronisieren überprüfen, das auf der Seite System verfügbar ist. Wenn die im Dialogfeld angezeigten Zeiten nicht übereinstimmen, führen Sie eine Synchronisierung aus. Sie können dieses Dialogfeld in regelmäßigen Abständen anzeigen, in dem angezeigt wird, ob die Zeitanzeigen der Controller-Uhren auseinander getrieben wurden und nicht mehr synchronisiert sind.

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.

System: 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.
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.

Laufzeit	Beschreibung
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 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.

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

Schritte

1. Wählen Sie **Einstellungen › System**.
2. Wählen Sie unter **iSCSI-Einstellungen** die Option **iSCSI-Ports konfigurieren** aus.

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

3. Wählen Sie den Controller mit den iSCSI-Ports aus, die Sie konfigurieren möchten.
4. Wählen Sie in der Dropdown-Liste den Port aus, den Sie konfigurieren möchten, und klicken Sie dann auf **Weiter**.
5. 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. Wenn Sie den Portzugriff deaktivieren möchten, deaktivieren Sie beide Kontrollkästchen.
TCP-Listening-Port (verfügbar durch Klicken auf **Weitere Port-Einstellungen 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 zur Auswahl von IPv4-Einstellungen geöffnet, nachdem Sie auf **Weiter** geklickt haben. Wenn Sie **IPv6** aktivieren ausgewählt haben, wird ein Dialogfeld zur Auswahl von IPv6-Einstellungen geöffnet, nachdem Sie auf **Weiter** geklickt haben. Wenn Sie beide Optionen ausgewählt haben, wird zuerst das Dialogfeld für IPv4-Einstellungen geöffnet, und nach dem Klicken auf **Weiter** wird das Dialogfeld für IPv6-Einstellungen geöffnet.

6. 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.
ethernet-Priorität aktivieren (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.

7. 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 **Einstellungen › System**.
2. Klicken Sie unter **iSCSI-Einstellungen** auf **Authentifizierung konfigurieren**.

   Das Dialogfeld **Authentifizierung konfigurieren** wird angezeigt, in dem die aktuell eingestellte 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**.

Ergebnisse

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 **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**.

Ergebnisse

Es wird eine Statusleiste angezeigt, da der System Manager versucht, den Controller beim iSNS-Server zu registrieren. Dieser Vorgang kann bis zu fünf Minuten dauern.

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 **Einstellungen › System**.
2. Wählen Sie **Anzeigen von iSCSI-Statistikpaketen** aus.
3. Klicken Sie auf eine Registerkarte, um die verschiedenen Statistikgruppen anzuzeigen.
4. **Optional:** um den Basisplan festzulegen, klicken Sie auf **Neue Basislinie festlegen**.

   Durch das Festlegen der Baseline wird ein neuer Ausgangspunkt für die Erfassung der Statistiken festgelegt. Dieselbe Baseline wird für alle iSCSI-Statistiken verwendet.

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 **Einstellungen › System**.
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. **Optional:** um den Bericht in einer Datei zu speichern, klicken Sie auf **Speichern**.

   Die Datei wird im Ordner Downloads für Ihren Browser mit dem Dateinamen gespeichert `iscsi-session-connections.txt`.

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 **Einstellungen › System**.
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.

Konfigurieren Sie iSER-over-InfiniBand-Ports

Wenn der Controller einen iSER-over-InfiniBand-Port enthält, können Sie die Netzwerkverbindung zu dem Host konfigurieren.

Bevor Sie beginnen

- Der Controller muss einen iSER-over-InfiniBand-Port umfassen, andernfalls sind die iSER-over-InfiniBand-Einstellungen in System Manager nicht verfügbar.
- Sie müssen die IP-Adresse der Hostverbindung kennen.

Schritte

1. Wählen Sie **Einstellungen › System**
2. Wählen Sie unter **iSER over InfiniBand settings Configure iSER over InfiniBand Ports** aus.
3. Klicken Sie auf den Controller mit dem iSER-over-InfiniBand-Port, den Sie konfigurieren möchten. Klicken Sie Auf **Weiter**.
4. Wählen Sie in der Dropdown-Liste den HIC-Port aus, den Sie konfigurieren möchten, und geben Sie dann die IP-Adresse des Hosts ein.
5. Klicken Sie Auf **Fertig Stellen**.
6. Setzen Sie 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.

Schritte

1. Wählen Sie **Einstellungen › System**.
2. Wählen Sie **Anzeigen iSER über InfiniBand Statistik**.
3. Klicken Sie auf eine Registerkarte, um die verschiedenen Statistikgruppen anzuzeigen.
4. **Optional:** um den Basisplan festzulegen, klicken Sie auf **Neue Basislinie festlegen**.

   Durch das Festlegen der Baseline wird ein neuer Ausgangspunkt für die Erfassung der Statistiken festgelegt. Dieselbe Baseline wird für sämtliche iSER-over-InfiniBand-Statistiken verwendet.

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-over-InfiniBand-Statistiken“ zeigt Statistiken zu lokalen Zielen (Protokollen) und iSER-over-InfiniBand-Schnittstellen (IB) an. Alle Statistiken sind schreibgeschützt und können nicht festgelegt werden.

- **Statistiken zu lokalen Zielen (Protokoll)** — stellt Statistiken für das iSER-over-InfiniBand-Ziel bereit, das den Zugriff auf die Speichermedien auf Blockebene anzeigt.
- **ISER-over-InfiniBand-Interface-Statistik** — stellt Statistiken für alle iSER-over-InfiniBand-Ports auf der InfiniBand-Schnittstelle bereit, die Performance-Statistiken und Link-Fehlerinformationen zu den einzelnen Switch-Ports enthalten.

Sie können jede dieser Statistiken als RAW-Statistiken oder als Baseline-Statistiken anzeigen. RAW-Statistiken sind alle Statistiken, die seit dem Start der Controller gesammelt wurden. Baseline-Statistiken sind zeitpunktgenaue Statistiken, die seit dem Festlegen der Baseline-Zeit erfasst wurden.

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 **Einstellungen › System**. 2. Scrollen Sie nach unten nach **iSER über InfiniBand-Einstellungen**, und wählen Sie dann **iSER über InfiniBand-Ports konfigurieren** aus.
Zeigen Sie iSER-over-InfiniBand-Statistiken an	1. Wählen Sie **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 enthalten einen Port für die Implementierung von NVMe (Non-Volatile Memory Express) über Fabrics. NVMe ermöglicht eine High-Performance-Kommunikation zwischen Hosts und dem Storage-Array.

Was ist NVMe?

NVM steht für „nichtflüchtiger Speicher“ und ist persistenter Speicher, der in vielen Arten von Speichergeräten verwendet wird. *NVMe* (NVM Express) ist eine standardisierte Schnittstelle oder ein standardisiertes Protokoll, das speziell für eine hochperformante Multi-Queue-Kommunikation mit NVM-Geräten entwickelt wurde.

Was ist NVMe over Fabrics?

NVMe over Fabrics (NVMe-of) ist eine Technologiespezifikation, die den Datentransfer zwischen einem Host-Computer und Storage über ein Netzwerk zwischen messenbasierten NVMe-Befehlen und -Daten ermöglicht. Auf ein NVMe-Storage-Array (sog. *Subsystem*) kann ein Host über eine Fabric zugreifen. NVMe Befehle sind sowohl auf der Host- als auch auf der Subsystemseite in transportabstrahierten Schichten aktiviert und eingekapselt. Damit erweitert sich die End-to-End-NVMe-High-Performance-Schnittstelle vom Host bis zum Storage und standardisiert und vereinfacht die Befehlszeilen.

NVMe-of-Storage wird einem Host als lokales Block-Storage-Gerät präsentiert. Das Volume (auch „*Namespace*“ genannt) kann wie jedes andere Block-Storage-Gerät in ein Dateisystem eingebunden werden. Mit DER REST-API, dem SMcli oder SANtricity System Manager wird der Storage nach Bedarf bereitgestellt.

Was ist ein qualifizierter NVMe-Name (NVMe Qualified Name, NQN)?

Der NVMe Qualified Name (NQN) wird zur Identifizierung des Remote-Storage-Ziels verwendet. Der für das

Storage-Array qualifizierte NVMe-Name wird immer vom Subsystem zugewiesen und darf nicht geändert werden. Es gibt nur einen für NVMe qualifizierten Namen für das gesamte Array. Der qualifizierte NVMe-Name ist auf 223 Zeichen begrenzt. Sie können ihn mit einem qualifizierten iSCSI-Namen vergleichen.

Was ist ein Namespace und eine Namespace-ID?

Ein Namespace entspricht einer logischen Einheit in SCSI, die ein Volume im Array betrifft. Die Namespace-ID (NSID) entspricht einer Logical Unit Number (LUN) in SCSI. Sie erstellen die NSID zum Erstellungszeitpunkt des Namespace und können sie auf einen Wert zwischen 1 und 255 setzen.

Was ist ein NVMe Controller?

Ähnlich wie bei einem SCSI I_T nexus, der den Pfad vom Host-Initiator zum Ziel des Storage-Systems darstellt, stellt ein während des Host-Verbindungsvorgangs erstellter NVMe-Controller einen Zugriffspfad zwischen einem Host und den Namespaces im Storage-Array bereit. Ein NQN für den Host und eine Host-Port-Kennung identifizieren einen NVMe-Controller eindeutig. Ein NVMe-Controller kann zwar nur einem einzelnen Host zugewiesen werden, kann aber auf diverse Namespaces zugreifen.

Sie konfigurieren, welche Hosts auf welche Namespaces zugreifen können und legen die Namespace-ID für den Host mit dem SANtricity System Manager fest. Anschließend wird bei der Erstellung des NVMe Controllers die Liste der Namespace-IDs, auf die der NVMe Controller zugreifen kann, erstellt und zum Konfigurieren der zulässigen Verbindungen verwendet.

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.

Laufzeit	Beschreibung
NVMe-of	Non-Volatile Memory Express over Fabrics (NVMe-of) ist eine Spezifikation, die die Übertragung von NVMe-Befehlen und -Daten über ein Netzwerk zwischen Host und Storage ermöglicht.
NVMe-Controller	Während der Host-Verbindung wird ein NVMe-Controller erstellt. Es stellt einen Zugriffspfad zwischen einem Host und den Namespaces im Storage-Array bereit.
NVMe-Warteschlange	Zum Übergeben von Befehlen und Nachrichten über die NVMe Schnittstelle wird eine Warteschlange verwendet.
NVMe-Subsystem	Das Storage-Array mit einer NVMe-Host-Verbindung.
RDMA	RDMA (Remote Direct Memory Access) ermöglicht eine direktere Datenverschiebung auf einem Server und wieder zurück, indem es ein Transportprotokoll in der NIC-Hardware (Network Interface Card) implementiert.
ROCE	RDMA over Converged Ethernet (RoCE) ist ein Netzwerkprotokoll, das über ein Ethernet-Netzwerk einen Remote Direct Memory Access (RDMA) ermöglicht.
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 der Controller eine NVMe-over-InfiniBand-Verbindung enthält, können Sie die NVMe-Port-Einstellungen auf der Systemseite 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.

> 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 **Einstellungen › System**.
2. Wählen Sie unter **NVMe over InfiniBand Einstellungen Konfigurieren von NVMe over InfiniBand Ports** aus.
3. Wählen Sie den Controller mit dem NVMe-over-InfiniBand-Port aus, den Sie konfigurieren möchten. Klicken Sie Auf **Weiter**.

4. Wählen Sie den HIC-Port aus der Dropdown-Liste aus, und geben Sie dann die IP-Adresse ein.

   Wenn Sie ein EF600 Speicher-Array mit einer 200-GB-fähigen HIC konfigurieren, werden in diesem Dialogfeld zwei IP-Adressfelder angezeigt, eines für einen physischen Port (extern) und eines für einen virtuellen Port (intern). Sie sollten für beide Ports eine eindeutige IP-Adresse zuweisen. Mit diesen Einstellungen kann der Host einen Pfad zwischen jedem Port und für die HIC einrichten, um eine maximale Performance zu erzielen. Wenn Sie dem virtuellen Port keine IP-Adresse zuweisen, läuft die HIC mit etwa der Hälfte ihrer fähigen Geschwindigkeit.

5. Klicken Sie Auf **Fertig Stellen**.
6. 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) enthält, können Sie die NVMe-Port-Einstellungen 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.

Schritte

1. Wählen Sie **Einstellungen › System**.
2. Wählen Sie unter **NVMe über ROCE-Einstellungen** die Option **Konfigurieren von NVMe über ROCE-Ports** aus.
3. Wählen Sie den Controller mit dem NVMe-over-RoCE-Port aus, den Sie konfigurieren möchten. Klicken Sie Auf **Weiter**.
4. Wählen Sie den HIC-Port aus der Dropdown-Liste aus, den Sie konfigurieren möchten. Klicken Sie Auf **Weiter**.
5. Konfigurieren Sie die Porteinstellungen.

   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 zur Auswahl von IPv4-Einstellungen geöffnet, nachdem Sie auf **Weiter** geklickt haben. Wenn Sie **IPv6** aktivieren ausgewählt haben, wird ein Dialogfeld zur Auswahl von IPv6-Einstellungen geöffnet, nachdem Sie auf **Weiter** geklickt haben. Wenn Sie beide Optionen ausgewählt haben, wird zuerst das Dialogfeld für IPv4-Einstellungen geöffnet, und nach dem Klicken auf **Weiter** wird das Dialogfeld für IPv6-Einstellungen geöffnet.

1. 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. Wenn Sie ein EF600 Speicher-Array mit einer 200-GB-fähigen HIC konfigurieren, werden in diesem Dialogfeld zwei Feldsätze für Netzwerkparameter angezeigt: Eines für einen physischen Port (extern) und eines für einen virtuellen Port (intern). Sie sollten für beide Ports eindeutige Parameter zuweisen. Mit diesen Einstellungen kann der Host einen Pfad zwischen jedem Port und für die HIC einrichten, um eine maximale Performance zu erzielen. Wenn Sie dem virtuellen Port keine IP-Adresse zuweisen, läuft die HIC mit etwa der Hälfte ihrer fähigen Geschwindigkeit.

2. 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** — zeigt Statistiken für den NVMe-Controller und seine Queue an. Der NVMe Controller stellt einen Zugriffspfad zwischen einem Host und den Namespaces im Storage-Array bereit. Sie können die NVMe-Subsystem-Statistiken für Elemente wie Verbindungsfehler, Zurücksetzen und Herunterfahren überprüfen.
- **RDMA Interface Statistics** — stellt Statistiken für alle NVMe over Fabrics Ports auf der RDMA-Schnittstelle bereit, die Performance-Statistiken und Link-Fehlerinformationen enthält, die mit jedem Switch-Port verbunden sind. Diese Registerkarte wird nur angezeigt, wenn NVMe over Fabrics-Ports verfügbar sind.

Sie können jede dieser Statistiken als RAW-Statistiken oder als Baseline-Statistiken anzeigen. RAW-Statistiken sind alle Statistiken, die seit dem Start der Controller gesammelt wurden. Baseline-Statistiken sind zeitpunktgenaue Statistiken, die seit dem Festlegen der Baseline-Zeit erfasst wurden.

Schritte

1. Wählen Sie **Einstellungen › System**.
2. Wählen Sie **View NVMe over Fabrics Statistics** aus.

3. **Optional:** um den Basisplan festzulegen, klicken Sie auf **Neue Basislinie festlegen**.

   Durch das Festlegen der Baseline wird ein neuer Ausgangspunkt für die Erfassung der Statistiken festgelegt. Dieselbe Baseline wird für alle NVMe-Statistiken verwendet.

FAQs

Wie interpretiere ich NVMe over Fabrics Statistiken?

Im Dialogfeld „Statistik von NVMe over Fabrics anzeigen“ werden Statistiken für das NVMe-Subsystem und die RDMA-Schnittstelle angezeigt. Alle Statistiken sind schreibgeschützt und können nicht festgelegt werden.

- **NVMe Subsystem-Statistik** — zeigt Statistiken für den NVMe-Controller und seine Queue an. Der NVMe Controller stellt einen Zugriffspfad zwischen einem Host und den Namespaces im Storage-Array bereit. Sie können die NVMe-Subsystem-Statistiken für Elemente wie Verbindungsfehler, Zurücksetzen und Herunterfahren überprüfen. Für weitere Informationen über diese Statistiken klicken Sie auf **Legende anzeigen für Tabellenüberschriften**.
- **RDMA Interface Statistics** — stellt Statistiken für alle NVMe over Fabrics Ports auf der RDMA-Schnittstelle bereit, die Performance-Statistiken und Link-Fehlerinformationen enthält, die mit jedem Switch-Port verbunden sind. Diese Registerkarte wird nur angezeigt, wenn NVMe over Fabrics-Ports verfügbar sind. Für weitere Informationen zu den Statistiken klicken Sie auf **Legende anzeigen für Tabellenüberschriften**.

Sie können jede dieser Statistiken als RAW-Statistiken oder als Baseline-Statistiken anzeigen. RAW-Statistiken sind alle Statistiken, die seit dem Start der Controller gesammelt wurden. Baseline-Statistiken sind zeitpunktgenaue Statistiken, die seit dem Festlegen der Baseline-Zeit erfasst wurden.

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 **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 **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 **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 **Einstellungen › System**. 2. Scrollen Sie nach unten zu **NVMe over RoCE settings** und wählen Sie dann **View NVMe over Fabrics Statistics** aus.

Warum gibt es zwei IP-Adressen für einen physischen Port?

Das EF600 Storage-Array kann zwei HICs umfassen – einen externen und einen internen.

In dieser Konfiguration ist die externe HIC mit einer internen HIC-Zusatzkarte verbunden. Jeder physische Port, auf den Sie über die externe HIC zugreifen können, hat einen zugeordneten virtuellen Port von der internen HIC.

Um eine maximale 200-GB-Performance zu erreichen, müssen Sie sowohl den physischen als auch den virtuellen Ports eine eindeutige IP-Adresse zuweisen, damit der Host Verbindungen zu jedem Server herstellen kann. Wenn Sie dem virtuellen Port keine IP-Adresse zuweisen, läuft die HIC mit etwa der Hälfte ihrer fähigen Geschwindigkeit.

Warum gibt es zwei Parametersätze für einen physischen Port?

Das EF600 Storage-Array kann zwei HICs umfassen – einen externen und einen internen.

In dieser Konfiguration ist die externe HIC mit einer internen HIC-Zusatzkarte verbunden. Jeder physische Port, auf den Sie über die externe HIC zugreifen können, hat einen zugeordneten virtuellen Port von der internen HIC.

Um eine maximale 200-GB-Performance zu erreichen, müssen Sie Parameter für die physischen und virtuellen Ports zuweisen, damit der Host Verbindungen zu jedem herstellen kann. Wenn Sie dem virtuellen Port keine Parameter zuweisen, läuft die HIC mit ungefähr halber Geschwindigkeit.

System: Add-on-Funktionen

Konzepte

Funktionsweise der Add-on-Funktionen

Add-ons sind Funktionen, die nicht in der Standardkonfiguration von System Manager enthalten sind und möglicherweise einen Schlüssel zur Aktivierung 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, aktivieren Sie den Bezeichner und den Funktionscode für die Aktivierung 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 zu **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 Code für die Aktivierung der Funktion. Für Features Packs wird dieser Code 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. Gehen Sie zu **Software-Lizenzen** für Ihr Produkt.
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, und zwar mit folgenden Informationen: Chassis-Seriennummer, Enable-ID und Code zur Aktivierung der Funktion.

   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 **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 **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.

Befehlszeilenschnittstelle (CLI) herunterladen

Von System Manager können Sie das CLI-Paket (Befehlszeilenschnittstelle)

herunterladen. Die CLI bietet eine textbasierte Methode zur Konfiguration und Überwachung von Speicher-Arrays. Es kommuniziert über HTTPS und verwendet dieselbe Syntax wie die CLI, die im extern installierten Managementsoftwarepaket verfügbar ist. Zum Herunterladen der CLI ist kein Schlüssel erforderlich.

Bevor Sie beginnen

- Eine Java Runtime Environment (JRE), Version 8 und höher, muss auf dem Managementsystem verfügbar sein, auf dem Sie die CLI-Befehle ausführen möchten.

Schritte

1. Wählen Sie **Einstellungen › System**.
2. Wählen Sie unter **Add-ons** die Option **Command Line Interface**.

   Das ZIP-Paket wird in den Browser heruntergeladen.

3. Speichern Sie die ZIP-Datei im Verwaltungssystem, in dem Sie CLI-Befehle für das Speicher-Array ausführen möchten, und extrahieren Sie dann die Datei.

   Sie können jetzt CLI-Befehle von einer Betriebssystemaufforderung ausführen, z. B. von der DOS C:-Eingabeaufforderung. Eine CLI-Befehlsreferenz steht im Menü Hilfe oben rechts in der System Manager-Benutzeroberfläche zur Verfügung.

System: 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 **Einstellungen › System › Verwaltung der Sicherheitsschlüssel › Interner 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. Gehen Sie zu **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 **Einstellungen › System › Verwaltung der Sicherheitsschlüssel › Externer Schlüssel 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.
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 **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:

   - **Einen Sicherheitsschlüssel-Identifier definieren** — Sie können entweder den Standardwert akzeptieren (Speicherarray-Name und Zeitstempel, der von der Controller-Firmware generiert wird) oder Ihren eigenen Wert eingeben. Sie können bis zu 189 alphanumerische Zeichen ohne Leerzeichen, Satzzeichen oder Symbole eingeben.

     > 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**.

Ergebnisse

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 **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:
   - **Key Management Server-Adresse** — Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein, der für die Schlüsselverwaltung verwendet wird.
   - **Nummer des Key Management-Ports** — Geben Sie die Portnummer ein, die für die Kommunikation mit dem Key Management Interoperability Protocol (KMIP) verwendet wird. Die am häufigsten für die Kommunikation mit dem Verschlüsselungsmanagement-Server verwendete Portnummer ist 5696.
   - **Client-Zertifikat auswählen** — Klicken Sie auf die erste **Durchsuchen**-Schaltfläche, um die Zertifikatdatei für die Speicher-Array-Controller auszuwählen.
   - **Wählen Sie das Serverzertifikat des Schlüsselverwaltungsservers** — 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 **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 einen Sicherheitsschlüssel-Identifier --** (nur für interne Sicherheitsschlüssel.) Akzeptieren Sie den Standardwert (Storage Array-Name und Zeitstempel, der von der Controller-Firmware generiert wird) oder geben Sie Ihren eigenen Wert ein. Sie können bis zu 189 alphanumerische Zeichen ohne Leerzeichen, Satzzeichen oder Symbole eingeben.

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

   - **Passphrase definieren/Passphrase erneut eingeben** — Geben Sie in jedes dieser Felder Ihren Passphrase ein. Der Wert kann 8 bis 32 Zeichen lang sein und muss Folgendes enthalten:
     - Ein Großbuchstabe (einer oder mehrere). Beachten Sie, dass die Passphrase Groß- und Kleinschreibung beachtet.
     - Eine Nummer (eine oder mehrere).
     - Ein nicht-alphanumerisches Zeichen wie !, *, @ (eines oder mehrere).

     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 **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 **Einstellungen › Systeme**.
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:

   - **Key Management Server-Adresse** — Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein, der für die Schlüsselverwaltung verwendet wird.

- **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 **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 **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. **Optional:** mit der Maus über eine Laufwerksnummer können Sie die Position des Laufwerks (Regalnummer und Einschubnummer) 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. Gehen Sie zu **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).
- Wenn Sie ein gesperrtes NVMe-Laufwerk zurücksetzen, müssen Sie die Sicherheits-ID des Laufwerks eingeben. Um die Sicherheits-ID zu finden, müssen Sie das Laufwerk physisch entfernen und die PSID-Zeichenfolge (maximal 32 Zeichen) auf dem Laufwerketikett suchen. Stellen Sie sicher, dass das Laufwerk neu installiert ist, bevor Sie den Vorgang starten.

Zugriff auf Lese-/Schreibzugriffe

Das Fenster Laufwerkseinstellungen enthält Informationen zu den Laufwerksicherheitsattributen. „Read/Write Accessible“ ist eines der Attribute, das anzeigt, ob Daten eines Laufwerks gesperrt wurden.

Um die Attribute der Laufwerksicherheit anzuzeigen, gehen Sie zur Seite Hardware. Wählen Sie ein Laufwerk aus, klicken Sie auf **Einstellungen anzeigen** und dann auf **Weitere Einstellungen anzeigen**. Unten auf der Seite ist der Wert für das Attribut Lesen/Schreiben, auf das zugegriffen werden kann, **Ja**, wenn das Laufwerk entsperrt ist. Der Wert für das Attribut Read/Write, das auf die Zugriffsberechtigung zugegriffen werden kann, lautet **Nein, ungültiger Sicherheitsschlüssel**, wenn das Laufwerk gesperrt ist. Sie können ein sicheres Laufwerk entsperren, indem Sie einen Sicherheitsschlüssel importieren (gehen Sie zu Menü:Einstellungen[System > Sichere Laufwerke entsperren]).

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 Laufwerksicherheit-Funktion implementieren, können Sie einen internen Sicherheitsschlüssel oder einen externen Sicherheitsschlüssel verwenden, um Daten zu sperren, wenn ein sicheres Laufwerk aus dem Speicher-Array entfernt wird.

Ein Sicherheitsschlüssel ist eine Zeichenkette, die von den sicheren Laufwerken und Controllern in einem Speicher-Array gemeinsam genutzt wird. Interne Schlüssel befinden sich im persistenten Speicher des Controllers. Externe Schlüssel werden mithilfe eines Key Management Interoperability Protocol (KMIP) auf

einem separaten Verschlüsselungsmanagement-Server aufbewahrt.

Zugriffsmanagement

Konzepte

Funktionsweise von Access Management

Die Zugriffsverwaltung ist eine Methode zur Einrichtung der Benutzerauthentifizierung in SANtricity System Manager.

Die Konfiguration der Zugriffsverwaltung und die Benutzerauthentifizierung funktionieren wie folgt:

1. Ein Administrator meldet sich bei System Manager mit einem Benutzerprofil an, das die Berechtigungen für Sicherheitsadministrator enthält.

   > Bei der ersten Anmeldung wird der Benutzername verwendet `admin` Wird automatisch angezeigt und kann nicht geändert werden. Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

2. Der Administrator navigiert in der Benutzeroberfläche zur Zugriffsverwaltung. Das Storage Array ist vorkonfiguriert zur Verwendung von lokalen Benutzerrollen, bei denen es sich um die Implementierung von RBAC-Funktionen (rollenbasierte Zugriffssteuerung) handelt.
3. Der Administrator konfiguriert eine oder mehrere der folgenden Authentifizierungsmethoden:
   - **Lokale Benutzerrollen** — Authentifizierung wird über im Storage Array erzwungene RBAC-Funktionen gemanagt. Lokale Benutzerrollen umfassen vordefinierte Benutzerprofile und Rollen mit spezifischen Zugriffsberechtigungen. Administratoren können diese lokalen Benutzerrollen als einzige Authentifizierungsmethode verwenden oder in Kombination mit einem Verzeichnisdienst verwenden. Es ist keine Konfiguration erforderlich – abgesehen von der Festlegung von Passwörtern für die Benutzer.
   - **Directory Services** — die Authentifizierung wird über einen LDAP-Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst verwaltet, z. B. über Microsoft Active Directory. Ein Administrator stellt eine Verbindung zum LDAP-Server her und ordnet die LDAP-Benutzer den im Speicher-Array eingebetteten lokalen Benutzerrollen zu.
   - **SAML** — Authentifizierung wird über einen Identitäts-Provider (IdP) mit der Security Assertion Markup Language (SAML) 2.0 verwaltet. Ein Administrator stellt die Verbindung zwischen dem IdP-System und dem Storage-Array her und ordnet anschließend die IdP-Benutzer den im Storage-Array eingebetteten lokalen Benutzerrollen zu.
4. Der Administrator stellt Benutzern die Anmeldeinformationen für System Manager zur Verfügung.
5. Benutzer melden sich beim System an, indem sie ihre Anmeldedaten eingeben.

   > Wenn die Authentifizierung mit SAML und einem SSO (Single Sign On) verwaltet wird, umgehen das System möglicherweise das Anmeldedialogfeld von System Manager.

   Während der Anmeldung führt das System die folgenden Hintergrundaufgaben aus:

   - Authentifiziert Benutzernamen und Kennwort anhand des Benutzerkontos.
   - Legt die Berechtigungen des Benutzers basierend auf den zugewiesenen Rollen fest.

- Ermöglicht dem Benutzer den Zugriff auf Aufgaben in der Benutzeroberfläche.
- Zeigt den Benutzernamen oben rechts in der Schnittstelle an.

In System Manager verfügbare Aufgaben

Der Zugriff auf Aufgaben hängt von den zugewiesenen Rollen eines Benutzers ab. Dazu gehören:

- **Storage Admin** — Vollzugriff auf die Speicherobjekte (z. B. Volumes und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
- **Security Admin** — Zugriff auf die Sicherheitskonfiguration in Access Management, Zertifikatverwaltung, Audit Log Management und die Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder auszuschalten.
- **Support Admin** — Zugriff auf alle Hardware-Ressourcen auf dem Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-Upgrades. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
- **Monitor** — schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

Eine nicht verfügbare Aufgabe ist entweder ausgegraut oder wird in der Benutzeroberfläche nicht angezeigt. Beispielsweise kann ein Benutzer mit der Rolle „Monitor“ alle Informationen zu Volumes anzeigen, jedoch keinen Zugriff auf Funktionen zum Ändern des Volumes haben. Die Registerkarten für Funktionen wie **Kopierdienste** und **zum Workload hinzufügen** werden ausgegraut; es sind nur **Einstellungen anzeigen/bearbeiten** verfügbar.

Einschränkungen bei SANtricity Unified Manager und SANtricity Storage Manager

Wenn SAML für ein Storage-Array konfiguriert ist, können Benutzer Storage für dieses Array nicht über die SANtricity Unified Manager oder die SANtricity Storage Manager-Schnittstellen ermitteln oder managen.

Wenn lokale Benutzerrollen und Verzeichnisdienste konfiguriert sind, müssen Benutzer Anmeldeinformationen eingeben, bevor eine der folgenden Funktionen ausgeführt wird:

- Umbenennen des Speicher-Arrays
- Aktualisieren der Controller-Firmware
- Laden einer Speicherarray-Konfiguration
- Ausführen eines Skripts
- Es wird versucht, einen aktiven Vorgang auszuführen, wenn eine nicht verwendete Sitzung abgelaufen ist

Terminologie für das Zugriffsmanagement

Erfahren Sie, wie die Bedingungen für das Zugriffsmanagement auf Ihr Storage Array Anwendung finden.

Laufzeit	Beschreibung
Active Directory	Active Directory (AD) ist ein Microsoft-Verzeichnisdienst, der LDAP für Windows-Domänennetzwerke verwendet.

Laufzeit	Beschreibung
Verbindlich	Bindevorgänge werden zur Authentifizierung von Clients auf dem Verzeichnisserver verwendet. Binding erfordert in der Regel Konto- und Kennwortanmeldeinformationen, aber einige Server erlauben anonyme Bindevorgänge.
CA	Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer, die sichere Verbindungen zwischen Clients und Servern ermöglichen.
Zertifikat	Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).
IDP	Ein Identitäts-Provider (IdP) ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert und festgestellt werden können, ob dieser Benutzer erfolgreich authentifiziert wurde. Der IdP kann so konfiguriert werden, dass er Multi-Faktor-Authentifizierung bietet und eine beliebige Benutzerdatenbank, wie z. B. Active Directory, verwendet. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich.
LDAP	Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll für den Zugriff auf verteilte Verzeichnisinformationsdienste und die Wartung. Mit diesem Protokoll können viele verschiedene Anwendungen und Dienste eine Verbindung zum LDAP-Server zur Überprüfung von Benutzern herstellen.
RBAC	Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) ist eine Methode zur Regulierung des Zugriffs auf Computer- oder Netzwerkressourcen, basierend auf den Rollen einzelner Benutzer. RBAC-Kontrollen werden auf dem Storage Array durchgesetzt und umfassen vordefinierte Rollen.
SAML	Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für die Authentifizierung und Autorisierung zwischen zwei Einheiten. SAML ermöglicht Multi-Faktor-Authentifizierung, bei der Benutzer zwei oder mehr Elemente zur Identitätsnachweise bereitstellen müssen (z. B. ein Passwort und ein Fingerabdruck). Die integrierte SAML-Funktion des Speicherarrays ist SAML2.0-konform für Identitätsbehauptung, Authentifizierung und Autorisierung.
SP	Ein Service-Provider (SP) ist ein System, das die Benutzerauthentifizierung und den Zugriff steuert. Wenn Access Management mit SAML konfiguriert ist, fungiert das Storage-Array als Dienstanbieter für die Anforderung der Authentifizierung vom Identity Provider.
SSO	Bei Single Sign On (SSO) handelt es sich um einen Authentifizierungsservice, mit dem ein Satz an Anmeldeinformationen auf mehrere Anwendungen zugreifen kann.

Berechtigungen für zugeordnete Rollen

Die auf dem Storage-Array erzwungenen RBAC-Funktionen (rollenbasierte Zugriffssteuerung) umfassen vordefinierte Benutzerprofile, die mit einer oder mehreren zugewiesenen Rollen ausgestattet sind. Jede Rolle umfasst Berechtigungen für den Zugriff auf Aufgaben in SANtricity System Manager.

Auf Benutzerprofile und zugeordnete Rollen kann über **Menü:Einstellungen[Zugriffsmanagement > Lokale Benutzerrollen]** auf der Benutzeroberfläche eines entweder System Managers zugegriffen werden.

Die Rollen ermöglichen Benutzern den Zugriff auf Aufgaben wie folgt:

- **Storage Admin** — Vollzugriff auf die Speicherobjekte (z. B. Volumes und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
- **Security Admin** — Zugriff auf die Sicherheitskonfiguration in Access Management, Zertifikatverwaltung, Audit Log Management und die Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder auszuschalten.
- **Support Admin** — Zugriff auf alle Hardware-Ressourcen auf dem Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-Upgrades. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
- **Monitor** — schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

Wenn ein Benutzer über keine Berechtigungen für eine bestimmte Aufgabe verfügt, ist diese Aufgabe entweder ausgegraut oder wird nicht in der Benutzeroberfläche angezeigt.

Zugriffsverwaltung mit lokalen Benutzerrollen

Administratoren können für das Zugriffsmanagement die im Storage Array erzwungenen RBAC-Funktionen (rollenbasierte Zugriffssteuerung) nutzen. Diese Funktionen werden als „lokale Benutzerrollen“ bezeichnet.

Konfigurationsworkflow

Lokale Benutzerrollen sind für das Speicher-Array vorkonfiguriert. Um lokale Benutzerrollen für die Authentifizierung zu verwenden, können Administratoren Folgendes tun:

1. Ein Administrator meldet sich bei SANtricity System Manager mit einem Benutzerprofil an, das Berechtigungen für Sicherheitsadministratoren enthält.

   Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

2. Ein Administrator überprüft die Benutzerprofile, die vordefiniert sind und nicht geändert werden können.
3. **Optional:** der Administrator weist für jedes Benutzerprofil neue Passwörter zu.
4. Benutzer melden sich mit ihren zugewiesenen Anmeldedaten am System an.

Vereinfachtes

Bei der Verwendung von nur lokalen Benutzerrollen für die Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben ausführen:

- Passwörter ändern.
- Legen Sie eine Mindestlänge für Passwörter fest.
- Benutzern erlauben, sich ohne Passwörter anzumelden.

Zugriffsmanagement mit Verzeichnisdiensten

Für die Zugriffsverwaltung können Administratoren einen LDAP-Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst wie Microsoft Active Directory verwenden.

Konfigurationsworkflow

Wenn ein LDAP-Server und ein Verzeichnisdienst im Netzwerk verwendet werden, funktioniert die Konfiguration wie folgt:

1. Ein Administrator meldet sich bei SANtricity System Manager mit einem Benutzerprofil an, das Berechtigungen für Sicherheitsadministratoren enthält.

   Der `admin` Der Benutzer hat vollen Zugriff auf alle Funktionen im System.

2. Der Administrator gibt die Konfigurationseinstellungen für den LDAP-Server ein. Zu den Einstellungen gehören der Domain-Name, die URL und die Bind-Kontoinformationen.
3. Wenn der LDAP-Server ein sicheres Protokoll (LDAPS) verwendet, lädt der Administrator eine Zertifikatskette für die Authentifizierung zwischen dem LDAP-Server und dem Speicher-Array hoch.
4. Nachdem die Serververbindung hergestellt wurde, ordnet der Administrator die Benutzergruppen den Rollen des Speicherarrays zu. Diese Rollen sind vordefiniert und können nicht geändert werden.
5. Der Administrator testet die Verbindung zwischen dem LDAP-Server und dem Speicher-Array.
6. Benutzer melden sich mit ihren zugewiesenen LDAP/Directory Services-Anmeldedaten am System an.

Vereinfachtes

Bei der Verwendung von Verzeichnisdiensten zur Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben ausführen:

- Fügen Sie einen Verzeichnisserver hinzu.
- Bearbeiten der Einstellungen des Verzeichnisservers.
- Zuordnen von LDAP-Benutzern zu lokalen Benutzerrollen.
- Entfernen Sie einen Verzeichnisserver.

Zugriffsmanagement mit SAML

Für die Zugriffsverwaltung können Administratoren die in das Array integrierten Funktionen der Security Assertion Markup Language (SAML) 2.0 verwenden.

Konfigurationsworkflow

Die SAML-Konfiguration funktioniert wie folgt:

1. Ein Administrator meldet sich bei System Manager mit einem Benutzerprofil an, das die Berechtigungen für

Sicherheitsadministrator enthält.

> Der `admin` Der Benutzer hat vollständigen Zugriff auf alle Funktionen in System Manager.

2. Der Administrator wechselt zur Registerkarte **SAML** unter Zugriffsverwaltung.
3. Ein Administrator konfiguriert die Kommunikation mit dem Identity Provider (IdP). Ein IdP ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert werden und festgestellt wird, ob der Benutzer erfolgreich authentifiziert wurde. Zum Konfigurieren der Kommunikation mit dem Storage-Array lädt der Administrator die IdP-Metadatendatei aus dem IdP-System herunter und lädt die Datei anschließend mit System Manager zum Hochladen auf das Storage-Array ein.
4. Ein Administrator stellt eine Vertrauensbeziehung zwischen dem Dienstanbieter und dem IdP her. Ein Dienstanbieter steuert die Benutzerautorisierung. In diesem Fall fungiert der Controller im Speicher-Array als Service Provider. Zum Konfigurieren der Kommunikation verwendet der Administrator System Manager zum Exportieren einer Service-Provider-Metadatendatei für jeden Controller. Aus dem IdP-System importiert der Administrator diese Metadatendateien in das IdP.

> Administratoren sollten außerdem sicherstellen, dass das IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.

5. Der Administrator ordnet die Rollen des Storage-Arrays den in IdP definierten Benutzerattributen zu. Dazu verwendet der Administrator System Manager zum Erstellen der Zuordnungen.
6. Der Administrator testet die SSO-Anmeldung an der IdP-URL. Dieser Test stellt sicher, dass das Storage-Array und das IdP kommunizieren können.

> Sobald SAML aktiviert ist, können Sie sie über die Benutzeroberfläche nicht deaktivieren oder die IdP-Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an den technischen Support, um Hilfe zu erhalten.

7. In System Manager aktiviert der Administrator SAML für das Storage-Array.
8. Benutzer melden sich mit ihren SSO-Anmeldedaten am System an.

Vereinfachtes

Bei der Verwendung von SAML zur Authentifizierung können Administratoren die folgenden Managementaufgaben ausführen:

- Neue Rollenzuordnungen ändern oder erstellen
- Exportieren Sie die Dateien von Dienstanbietern

Zugriffsbeschränkungen

Wenn SAML aktiviert ist, können Benutzer Speicher für dieses Array nicht über den SANtricity Unified Manager oder die SANtricity Storage Manager-Schnittstellen ermitteln oder managen.

Außerdem können die folgenden Clients nicht auf Services und Ressourcen des Speicherarrays zugreifen:

- Enterprise Management-Fenster (EMW)
- Befehlszeilenschnittstelle (CLI)
- Software Developer Kits (SDK)-Clients

- In-Band-Clients
- REST-API-Clients für die HTTP-Standardauthentifizierung
- Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an

Anleitungen

Zeigen Sie lokale Benutzerrollen an

Auf der Registerkarte Lokale Benutzerrollen können Sie die Zuordnungen der Benutzerprofile zu den Standardrollen anzeigen. Diese Zuordnungen sind Teil der RBAC (rollenbasierte Zugriffssteuerung), die im Storage Array durchgesetzt wird.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

Über diese Aufgabe

Die Benutzerprofile und Zuordnungen können nicht geändert werden. Es können nur Passwörter geändert werden.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.

   Die Benutzerprofile sind in der Tabelle aufgeführt:

   - **Root Admin** (admin) — Super-Administrator, der Zugriff auf alle Funktionen im System hat. Dieses Benutzerprofil enthält alle Rollen.
   - **Storage Admin** (Storage) — der Administrator für die gesamte Storage-Bereitstellung verantwortlich. Dieses Benutzerprofil umfasst die folgenden Rollen: Storage-Administrator, Support-Administrator und Monitor.
   - **Security Admin** (Security) — der für die Sicherheitskonfiguration verantwortliche Benutzer, einschließlich Zugriffsverwaltung, Zertifikatverwaltung und Secure-Enabled Drive-Funktionen. Dieses Benutzerprofil umfasst die folgenden Rollen: Security Admin und Monitor.
   - **Support Admin** (Support) — der Benutzer ist verantwortlich für Hardware-Ressourcen, Ausfalldaten und Firmware-Upgrades. Dieses Benutzerprofil umfasst die folgenden Rollen: Unterstützen Sie Admin und Monitor.
   - **Monitor** (Monitor) — Ein Benutzer mit schreibgeschütztem Zugriff auf das System. Dieses Benutzerprofil enthält nur die Rolle Monitor.

Passwörter ändern

Sie können die Benutzerpasswörter für jedes Benutzerprofil in Access Management ändern.

Bevor Sie beginnen

- Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-Berechtigungen enthält.
- Sie müssen das lokale Administratorkennwort kennen.

Über diese Aufgabe

Beachten Sie bei der Auswahl eines Passworts die folgenden Richtlinien:

- Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Einstellung für ein Mindestpasswort erfüllen oder überschreiten (unter „Einstellungen anzeigen/bearbeiten“).
- Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt.
- Nachgestellte Leerzeichen werden nicht von Kennwörtern entfernt, wenn sie eingestellt sind. Achten Sie darauf, Leerzeichen einzugeben, wenn diese im Passwort enthalten waren.
- Um die Sicherheit zu erhöhen, verwenden Sie mindestens 15 alphanumerische Zeichen, und ändern Sie das Passwort häufig.

> Durch Ändern des Passworts in System Manager wird es auch in der Befehlszeilenschnittstelle (CLI) geändert. Außerdem führen Kennwortänderungen dazu, dass die aktive Sitzung des Benutzers beendet wird.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
3. Wählen Sie einen Benutzer aus der Tabelle aus.

   Die Schaltfläche Kennwort ändern steht zur Verfügung.

4. Wählen Sie **Passwort Ändern**.

   Das Dialogfeld Kennwort ändern wird geöffnet.

5. Wenn für lokale Benutzerpasswörter keine Mindestkennwortlänge festgelegt ist, können Sie das Kontrollkästchen aktivieren, damit der ausgewählte Benutzer ein Kennwort für den Zugriff auf das Speicher-Array eingeben muss. Anschließend können Sie das neue Passwort für den ausgewählten Benutzer eingeben.
6. Geben Sie Ihr lokales Administratorpasswort ein und klicken Sie dann auf **Ändern**.

Ergebnisse

Wenn der Benutzer derzeit angemeldet ist, wird die aktive Sitzung des Benutzers durch die Kennwortänderung beendet.

Ändern Sie die Einstellungen für das lokale Benutzerpasswort

Sie können die erforderliche Mindestlänge für alle neuen oder aktualisierten lokalen Benutzerpasswörter im Speicher-Array festlegen. Sie können lokalen Benutzern auch ohne Eingabe eines Kennworts den Zugriff auf das Speicher-Array erlauben.

Bevor Sie beginnen

- Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-Berechtigungen enthält.

Über diese Aufgabe

Beachten Sie die folgenden Richtlinien, wenn Sie die Mindestlänge für lokale Benutzerpasswörter festlegen:

- Die Einstellung von Änderungen wirkt sich nicht auf vorhandene lokale Benutzerpasswörter aus.

- Die Mindestlänge für lokale Benutzerpasswörter muss zwischen 0 und 30 Zeichen liegen.
- Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Mindestlängeneinstellung erfüllen oder überschreiten.
- Legen Sie keine Mindestlänge für das Passwort fest, wenn lokale Benutzer ohne Eingabe eines Kennworts auf das Speicher-Array zugreifen möchten.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte * Lokale Benutzerrollen* aus.
3. Wählen Sie die Schaltfläche **Einstellungen anzeigen/bearbeiten**.

   Das Dialogfeld **Lokale Benutzerpassworteinstellungen** wird geöffnet.

4. Führen Sie einen der folgenden Schritte aus:
   - Um lokalen Benutzern den Zugriff auf das Speicher-Array zu ermöglichen, ohne ein Passwort einzugeben, deaktivieren Sie das Kontrollkästchen „Alle lokalen Benutzerpasswörter müssen mindestens sein“.
   - Um eine Mindestkennwortlänge für alle lokalen Benutzerpasswörter festzulegen, aktivieren Sie das Kontrollkästchen „Alle lokalen Benutzerpasswörter müssen mindestens sein“ und verwenden Sie dann das Spinner-Feld, um die erforderliche Mindestlänge für alle lokalen Benutzerpasswörter festzulegen.

     Neue lokale Benutzerpasswörter müssen die aktuelle Einstellung erfüllen oder überschreiten.

5. Klicken Sie Auf **Speichern**.

Verzeichnisserver hinzufügen

Um die Authentifizierung für die Zugriffsverwaltung zu konfigurieren, können Sie die Kommunikation zwischen dem Speicher-Array und einem LDAP-Server herstellen und die LDAP-Benutzergruppen den vordefinierten Rollen des Arrays zuordnen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
- LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich Domänenname, Server-URL und optional Benutzername und Kennwort für das Bindekonto.
- Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette des LDAP-Servers auf Ihrem lokalen Computer installiert sein.

Über diese Aufgabe

Das Hinzufügen eines Verzeichnisservers ist ein zweistufiger Prozess. Geben Sie zuerst den Domain-Namen und die URL ein. Wenn Ihr Server ein sicheres Protokoll verwendet, müssen Sie auch ein CA-Zertifikat zur Authentifizierung hochladen, wenn es von einer nicht standardmäßigen Signierungsbehörde signiert ist. Wenn Sie über Anmeldedaten für ein Bindekonto verfügen, können Sie auch Ihren Benutzernamen und Ihr Kennwort eingeben. Als Nächstes werden die Benutzergruppen des LDAP-Servers den vordefinierten Rollen des Speicher-Arrays zugeordnet.

Während des Verfahrens zum Hinzufügen eines LDAP-Servers wird die alte Verwaltungsschnittstelle deaktiviert. Die alte Managementoberfläche (Symbol) ist eine Methode der Kommunikation zwischen dem Storage-Array und dem Management-Client. Wenn die Option deaktiviert ist, nutzen das Storage-Array und der Management-Client eine sicherere Kommunikationsmethode (REST-API über HTTPS).

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie auf der Registerkarte **Directory Services** die Option **Add Directory Server** aus.

   Das Dialogfeld Add Directory Server wird geöffnet.

3. Geben Sie auf der Registerkarte **Server-Einstellungen** die Anmeldeinformationen für den LDAP-Server ein.

Felddetails

Einstellung	Beschreibung
Konfigurationseinstellungen	Domäne(en)
Geben Sie den Domänennamen des LDAP-Servers ein. Geben Sie für mehrere Domänen die Domänen in eine kommagetrennte Liste ein. Der Domänenname wird in der Anmeldung (*username@Domain*) verwendet, um anzugeben, gegen welchen Verzeichnisserver sich authentifizieren soll.	Server-URL
Geben Sie die URL für den Zugriff auf den LDAP-Server in Form von ein `ldap[s]://host:*port*`.	Zertifikat hochladen (optional)

Einstellung	Beschreibung
Dieses Feld wird nur angezeigt, wenn ein LDAPS-Protokoll im obigen Feld Server-URL angegeben wird. Klicken Sie auf **Durchsuchen** und wählen Sie ein CA-Zertifikat zum Hochladen aus. Dies ist das vertrauenswürdige Zertifikat oder die Zertifikatskette, die für die Authentifizierung des LDAP-Servers verwendet wird.	Konto binden (optional)
Geben Sie ein schreibgeschütztes Benutzerkonto ein, um Suchanfragen auf dem LDAP-Server und für die Suche in den Gruppen durchzuführen. Geben Sie den Kontonamen im LDAP-Format ein. Wenn der Bindebenutzer beispielsweise „bind-Benutzer“ heißt, können Sie einen Wert wie „CN=bindact,CN=users, DC=cpoc,DC=local“ eingeben.	Bindepasswort (optional)

Einstellung	Beschreibung
Dieses Feld wird angezeigt, wenn Sie oben ein Bindungskonto eingeben. Geben Sie das Passwort für das Bindekonto ein.	Testen Sie die Serververbindung, bevor Sie sie hinzufügen
Aktivieren Sie dieses Kontrollkästchen, wenn Sie sicherstellen möchten, dass das Speicher-Array mit der eingegebenen LDAP-Serverkonfiguration kommunizieren kann. Der Test erfolgt, nachdem Sie unten im Dialogfeld auf **Hinzufügen** geklickt haben. Wenn dieses Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die Konfiguration nicht hinzugefügt. Sie müssen den Fehler beheben oder das Kontrollkästchen deaktivieren, um den Test zu überspringen und die Konfiguration hinzuzufügen.	**Berechtigungs-Einstellungen**
Basis-DN suchen	Geben Sie den LDAP-Kontext ein, um nach Benutzern zu suchen, normalerweise in Form von `CN=Users, DC=copc, DC=local`.
Attribut Benutzername	Geben Sie das Attribut ein, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: `sAMAccountName`.

Einstellung	Beschreibung
Gruppenattribut(e)	Geben Sie eine Liste der Gruppenattribute für den Benutzer ein, die für die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: `memberOf, managedObjects`.

4. Klicken Sie auf die Registerkarte **Rollenzuordnung**.
5. Weisen Sie den vordefinierten Rollen LDAP-Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.

   Felddetails

Einstellung	Beschreibung
Zuordnungen	Gruppen-DN
Geben Sie den Group Distinguished Name (DN) für die zu zugeordnete LDAP-Benutzergruppe an.	Rollen

> Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

1. Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.
2. Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf **Hinzufügen**.

   Das System führt eine Validierung durch und stellt sicher, dass das Speicher-Array und der LDAP-Server kommunizieren können. Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die im Dialogfeld eingegebenen Anmeldeinformationen, und geben Sie die Informationen ggf. erneut ein.

Bearbeiten Sie die Einstellungen des Verzeichnisservers und die Rollenzuordnungen

Wenn Sie zuvor einen Verzeichnisserver in der Zugriffsverwaltung konfiguriert haben, können Sie dessen Einstellungen jederzeit ändern. Zu den Einstellungen gehören die Informationen zur Serververbindung und die Zuordnungen von Gruppen zu Rollen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Ein Verzeichnisserver muss definiert werden.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **Directory Services** aus.
3. Wenn mehr als ein Server definiert ist, wählen Sie den Server aus der Tabelle aus, den Sie bearbeiten möchten.
4. Wählen Sie **Einstellungen Anzeigen/Bearbeiten**.

   Das Dialogfeld **Directory Server Settings** wird geöffnet.

5. Ändern Sie auf der Registerkarte **Server-Einstellungen** die gewünschten Einstellungen.

Einstellung	Beschreibung
Konfigurationseinstellungen	Domäne(en)
Der/die Domänenname(n) des/der LDAP-Server(e). Geben Sie für mehrere Domänen die Domänen in eine kommagetrennte Liste ein. Der Domänenname wird in der Anmeldung (*username@Domain*) verwendet, um anzugeben, gegen welchen Verzeichnisserver sich authentifizieren soll.	Server-URL
Die URL für den Zugriff auf den LDAP-Server in Form von `ldap[s]://host:*port*`.	Konto binden (optional)
Das schreibgeschützte Benutzerkonto für Suchabfragen am LDAP-Server und für die Suche in den Gruppen.	Bindepasswort (optional)
Das Kennwort für das Bindekonto. (Dieses Feld wird angezeigt, wenn ein Bindekonto eingegeben wird.)	Testen Sie vor dem Speichern die Serververbindung

Einstellung	Beschreibung
Überprüft, ob das Speicher-Array mit der LDAP-Serverkonfiguration kommunizieren kann. Der Test erfolgt, nachdem Sie unten im Dialogfeld auf **Speichern** geklickt haben. Wenn dieses Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die Konfiguration nicht geändert. Sie müssen den Fehler beheben oder das Kontrollkästchen deaktivieren, um den Test zu überspringen und die Konfiguration erneut zu bearbeiten.	**Berechtigungseinstellungen**
Basis-DN suchen	Der LDAP-Kontext für die Suche nach Benutzern, in der Regel in Form von `CN=Users, DC=copc, DC=local`.
Attribut Benutzername	Das Attribut, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: `sAMAccountName`.
Gruppenattribut(e)	Eine Liste der Gruppenattribute für den Benutzer, die für die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: `memberOf, managedObjects`.

6. Ändern Sie auf der Registerkarte **Rollenzuordnung** die gewünschte Zuordnung.

Einstellung	Beschreibung
Zuordnungen	Gruppen-DN
Der Domain-Name für die LDAP-Benutzergruppe, die zugeordnet werden soll.	Rollen

> Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

7. Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.

8. Klicken Sie Auf **Speichern**.

Ergebnisse

Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.

Verzeichnisserver entfernen

Um die Verbindung zwischen einem Verzeichnisserver und dem Speicher-Array zu unterbrechen, können Sie die Serverinformationen von der Seite Zugriffsverwaltung entfernen. Sie möchten diese Aufgabe möglicherweise ausführen, wenn Sie einen neuen Server konfiguriert haben und den alten dann entfernen möchten.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

Über diese Aufgabe

Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **Directory Services** aus.
3. Wählen Sie in der Liste den Verzeichnisserver aus, den Sie löschen möchten.
4. Klicken Sie Auf **Entfernen**.

   Das Dialogfeld **Directory Server entfernen** wird geöffnet.

5. Typ `remove` Klicken Sie im Feld auf **Entfernen**.

   Die Konfigurationseinstellungen des Verzeichnisservers, die Berechtigungseinstellungen und Rollenzuordnungen werden entfernt. Benutzer können sich nicht mehr mit Anmeldeinformationen von diesem Server anmelden.

Konfigurieren Sie SAML

Zum Konfigurieren der Authentifizierung für das Zugriffsmanagement können Sie die im Speicher-Array integrierten SAML-Funktionen (Security Assertion Markup Language) verwenden. Mit dieser Konfiguration wird eine Verbindung zwischen einem Identitätsanbieter und dem Speicheranbieter hergestellt.

Über diese Aufgabe

Ein Identitäts-Provider (IdP) ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert und festgestellt werden können, ob dieser Benutzer erfolgreich authentifiziert wurde. Der IdP kann so konfiguriert werden, dass er Multi-Faktor-Authentifizierung bietet und eine beliebige Benutzerdatenbank, wie z. B. Active Directory, verwendet. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich. Ein Service-Provider (SP) ist ein System, das die Benutzerauthentifizierung und den Zugriff steuert. Wenn Access Management mit SAML konfiguriert ist, fungiert das Storage-Array als Dienstanbieter für die Anforderung der Authentifizierung vom Identity Provider. Um eine Verbindung zwischen dem IdP und dem Storage-Array

herzustellen, teilen Sie Metadatendateien zwischen diesen beiden Einheiten gemeinsam. Als Nächstes ordnen Sie die IdP-Benutzereinheiten den Storage-Array-Rollen zu. Und schließlich testen Sie die Verbindung und SSO-Anmeldedaten, bevor Sie SAML aktivieren.

> **SAML und Directory Services**. Wenn Sie SAML aktivieren, wenn Directory Services als Authentifizierungsmethode konfiguriert sind, ersetzt SAML die Directory Services in System Manager. Wenn Sie SAML später deaktivieren, wird die Konfiguration der Verzeichnisdienste wieder in die vorherige Konfiguration zurückgeführt.

> **Bearbeiten und Deaktivieren.** Sobald SAML aktiviert ist, können Sie es nicht über die Benutzeroberfläche deaktivieren, noch können Sie die IdP-Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an den technischen Support, um Hilfe zu erhalten.

Die Konfiguration der SAML-Authentifizierung erfolgt in mehreren Schritten.

Schritt 1: Laden Sie die IdP-Metadatendatei hoch

Um das Storage-Array mit IdP-Verbindungsinformationen bereitzustellen, importieren Sie IdP-Metadaten in System Manager.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Ein IdP-Administrator hat ein IdP-System konfiguriert.
- Ein IdP-Administrator hat sichergestellt, dass der IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.
- Ein Administrator hat sichergestellt, dass die IdP-Server- und -Controller-Uhren synchronisiert werden (entweder über einen NTP-Server oder durch Anpassen der Controller-Uhreinstellungen).
- Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, das für den Zugriff auf System Manager verwendet wird.

Über diese Aufgabe

In dieser Aufgabe laden Sie eine Metadatendatei aus dem IdP in den System Manager hoch. Das IdP-System benötigt diese Metadaten, um Authentifizierungsanforderungen an die richtige URL weiterzuleiten und die erhaltenen Antworten zu validieren. Sie müssen nur eine Metadatendatei für das Storage-Array hochladen, selbst wenn es zwei Controller gibt.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **SAML** aus.

   Auf der Seite wird eine Übersicht der Konfigurationsschritte angezeigt.

3. Klicken Sie auf den Link * Import Identity Provider (IdP) file*.

   Das Dialogfeld **Import Identity Provider File** wird geöffnet.

4. Klicken Sie auf **Durchsuchen**, um die IdP-Metadatendatei auszuwählen und auf Ihr lokales System hochzuladen.

Nach der Auswahl der Datei wird die IdP-Entity-ID angezeigt.

5. Klicken Sie Auf **Import**.

Schritt 2: Exportieren Sie die Dateien des Dienstanbieters

Um eine Vertrauensbeziehung zwischen dem IdP und dem Storage-Array herzustellen, importieren Sie die Metadaten des Service-Providers in das IdP.

Bevor Sie beginnen

- Sie kennen die IP-Adresse oder den Domain-Namen der einzelnen Controller im Storage-Array.

Über diese Aufgabe

In dieser Aufgabe exportieren Sie Metadaten aus den Controllern (eine Datei für jeden Controller). Die IdP benötigt diese Metadaten, um eine Vertrauensbeziehung zu den Controllern aufzubauen und Autorisierungsanforderungen zu bearbeiten. Die Datei enthält Informationen wie den Domänennamen oder die IP-Adresse des Controllers, sodass das IdP mit den Service-Providern kommunizieren kann.

Schritte

1. Klicken Sie auf den Link **Export Service Provider Files**.

   Das Dialogfeld **Export Service Provider Files** wird geöffnet.

2. Geben Sie die Controller-IP-Adresse oder den DNS-Namen in das Feld **Controller A** ein, und klicken Sie dann auf **Exportieren**, um die Metadatendatei auf Ihrem lokalen System zu speichern. Wenn das Speicher-Array zwei Controller enthält, wiederholen Sie diesen Schritt für den zweiten Controller im Feld **Controller B**.

   Nachdem Sie auf **Export** geklickt haben, werden die Metadaten des Dienstanbieters auf Ihr lokales System heruntergeladen. Notieren Sie sich, wo die Datei gespeichert ist.

3. Suchen Sie im lokalen System die Metadatendatei(en) des Serviceanbieters, die Sie exportiert haben.

   Es gibt eine XML-formatierte Datei für jeden Controller.

4. Importieren Sie vom IdP-Server die Metadatendatei(en) des Dienstanbieters, um die Vertrauensbeziehung herzustellen. Sie können die Dateien entweder direkt importieren oder manuell die Controller-Informationen aus den Dateien eingeben.

Schritt 3: Rollen zuordnen

Um Benutzern Autorisierung und Zugriff auf System Manager zu ermöglichen, müssen Sie die IdP-Benutzerattribute und Gruppenmitgliedschaften den vordefinierten Rollen des Speicherarrays zuordnen.

Bevor Sie beginnen

- Ein IdP-Administrator hat Benutzerattribute und Gruppenmitgliedschaften im IdP-System konfiguriert.
- Die IdP-Metadatendatei wird in System Manager importiert.
- Für die Vertrauensbeziehung wird für jeden Controller eine Metadatendatei des Dienstanbieters in das IdP-System importiert.

Über diese Aufgabe

In dieser Aufgabe verwenden Sie System Manager, um IdP-Gruppen den lokalen Benutzerrollen zuzuordnen.

Schritte

1. Klicken Sie auf den Link, um System Manager-Rollen zuzuordnen.

   Das Dialogfeld Rollenzuordnung wird geöffnet.

2. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.

   Felddetails

Einstellung	Beschreibung
Zuordnungen	Benutzerattribut
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-Gruppe an.	Attributwert
Geben Sie den Attributwert für die zu zugeordnete Gruppe an.	Rollen

   Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

3. Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.

   Rollenzuordnungen können geändert werden, nachdem SAML aktiviert ist.

4. Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf **Speichern**.

Schritt 4: SSO-Anmeldung testen

Um sicherzustellen, dass das IdP-System und das Speicherarray kommunizieren können, können Sie optional eine SSO-Anmeldung testen. Dieser Test wird auch während des letzten Schritts zur Aktivierung von SAML durchgeführt.

Bevor Sie beginnen

- Die IdP-Metadatendatei wird in System Manager importiert.
- Für die Vertrauensbeziehung wird für jeden Controller eine Metadatendatei des Dienstanbieters in das IdP-System importiert.

Schritte

1. Klicken Sie auf den Link **SSO-Login testen**.

   Zum Eingeben von SSO-Anmeldedaten wird ein Dialogfeld geöffnet.

2. Geben Sie die Anmeldeinformationen für einen Benutzer mit Sicherheitsadministratorrechten und Überwachungsberechtigungen ein.

   Ein Dialogfeld wird geöffnet, während das System die Anmeldung testet.

3. Suchen Sie nach einer Meldung für den erfolgreichen Test. Wenn der Test erfolgreich abgeschlossen wurde, fahren Sie mit dem nächsten Schritt zur Aktivierung von SAML fort.

   Wenn der Test nicht erfolgreich abgeschlossen wird, wird eine Fehlermeldung mit weiteren Informationen angezeigt. Stellen Sie sicher, dass:

   - Der Benutzer gehört zu einer Gruppe mit Berechtigungen für Security Admin und Monitor.
   - Die Metadaten, die Sie für den IdP-Server hochgeladen haben, sind korrekt.
   - Die Controller-Adressen in den SP-Metadatendateien sind korrekt.

Schritt 5: SAML aktivieren

Ihr letzter Schritt ist die Aktivierung der SAML-Benutzerauthentifizierung.

Bevor Sie beginnen

- Die IdP-Metadatendatei wird in System Manager importiert.
- Für die Vertrauensbeziehung wird für jeden Controller eine Metadatendatei des Dienstanbieters in das IdP-System importiert.
- Mindestens ein Monitor und eine Sicherheitsadministratorzuordnung sind konfiguriert.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie die SAML-Konfiguration für die Benutzerauthentifizierung abgeschlossen wird. Während dieses Prozesses werden Sie vom System auch aufgefordert, eine SSO-Anmeldung zu testen. Der SSO-Anmelde-Test wird im vorherigen Schritt beschrieben.

> **Bearbeiten und Deaktivieren.** Sobald SAML aktiviert ist, können Sie es nicht über die Benutzeroberfläche deaktivieren, noch können Sie die IdP-Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an den technischen Support, um Hilfe zu erhalten.

Schritte

1. Wählen Sie auf der Registerkarte **SAML** den Link **SAML** aktivieren.

   Das Dialogfeld **SAML aktivieren** aktivieren wird geöffnet.

2. Typ `enable`, Und klicken Sie dann auf **Aktivieren**.
3. Geben Sie die Benutzeranmeldeinformationen für einen SSO-Anmeldetest ein.

Ergebnisse

Nachdem das System SAML aktiviert hat, werden alle aktiven Sitzungen beendet und die Authentifizierung von Benutzern über SAML beginnt.

SAML-Rollenzuordnungen ändern

Wenn Sie zuvor SAML für Access Management konfiguriert haben, können Sie die Rollenzuordnungen zwischen den IdP-Gruppen und den vordefinierten Rollen des

Speicherarrays ändern.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Ein IdP-Administrator hat Benutzerattribute und Gruppenmitgliedschaften im IdP-System konfiguriert.
- SAML wurde konfiguriert und aktiviert.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **SAML** aus.
3. Wählen Sie **Rollenzuordnung**.

   Das Dialogfeld **Rollenzuordnung** wird geöffnet.

4. Weisen Sie den vordefinierten Rollen IdP-Benutzerattribute und -Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.

   Achten Sie darauf, dass Sie Ihre Berechtigungen nicht entfernen, während SAML aktiviert ist, oder Sie verlieren den Zugriff auf System Manager.

   Felddetails

Einstellung	Beschreibung
Zuordnungen	Benutzerattribut
Geben Sie das Attribut (z. B. „Mitglied von“) für die zuzuordnenden SAML-Gruppe an.	Attributwert
Geben Sie den Attributwert für die zu zugeordnete Gruppe an.	Rollen

   Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

1. **Optional:** Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.
2. Klicken Sie Auf **Speichern**.

Ergebnisse

Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen beendet. Nur Ihre aktuelle

Benutzersitzung bleibt erhalten.

Exportieren Sie SAML-Dienstanbieter-Dateien

Bei Bedarf können die Metadaten von Service-Providern für das Storage-Array exportiert und die Datei(en) in das IdP-System (Identity Provider) importiert werden.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- SAML wurde konfiguriert und aktiviert.

Über diese Aufgabe

In dieser Aufgabe exportieren Sie Metadaten aus den Controllern (eine Datei für jeden Controller). Die IdP benötigt diese Metadaten, um eine Vertrauensbeziehung zu den Controllern aufzubauen und Authentifizierungsanforderungen zu verarbeiten. Die Datei enthält Informationen wie den Domänennamen des Controllers oder die IP-Adresse, die das IdP zum Senden von Anforderungen verwenden kann.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **SAML** aus.
3. Wählen Sie **Export**.

   Das Dialogfeld **Export Service Provider Files** wird geöffnet.

4. Klicken Sie für jeden Controller auf **Exportieren**, um die Metadatendatei auf Ihrem lokalen System zu speichern.

   > Die Domain-Name-Felder für jeden Controller sind schreibgeschützt.

   Notieren Sie sich, wo die Datei gespeichert ist.

5. Suchen Sie im lokalen System die Metadatendatei(en) des Serviceanbieters, die Sie exportiert haben.

   Es gibt eine XML-formatierte Datei für jeden Controller.

6. Importieren Sie vom IdP-Server die Metadatendatei(en) des Dienstanbieters. Sie können die Dateien entweder direkt importieren oder manuell die Controller-Informationen von ihnen eingeben.
7. Klicken Sie Auf **Schließen**.

Zeigen Sie die Aktivität des Prüfprotokolls an

Durch die Anzeige von Prüfprotokollen können Benutzer mit Sicherheitsadministratorberechtigungen Benutzeraktionen, Authentifizierungsfehler, ungültige Anmeldeversuche und die Lebensdauer der Benutzersitzung überwachen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **Prüfprotokoll** aus.

   Die Aktivität des Überwachungsprotokolls wird im Tabellenformat angezeigt, das die folgenden Informationspalten enthält:

   - **Datum/Uhrzeit** — Zeitstempel, wann das Speicherarray das Ereignis erkannt hat (in GMT).
   - **Benutzername** — der Benutzername, der dem Ereignis zugeordnet ist. Bei nicht authentifizierten Aktionen im Speicher-Array wird „N/A“ als Benutzername angezeigt. Nicht authentifizierte Aktionen können vom internen Proxy oder einem anderen Mechanismus ausgelöst werden.
   - **Statuscode** — HTTP-Statuscode der Operation (200, 400 usw.) und beschreibenden Text, der dem Ereignis zugeordnet ist.
   - **URL abgerufen** — vollständige URL (einschließlich Host) und Abfragezeichenfolge.
   - **Client-IP-Adresse** — IP-Adresse des Clients, der dem Ereignis zugeordnet ist.
   - **Quelle** — Logging-Quelle, die mit dem Ereignis verknüpft ist, kann System Manager, CLI, Web Services oder Support Shell sein.
3. Verwenden Sie die Auswahl auf der Seite „Überwachungsprotokoll“, um Ereignisse anzuzeigen und zu verwalten.

Auswahldetails

Auswahl	Beschreibung
Zeigt Ereignisse aus dem…	Grenzwerte für Ereignisse, die nach Datumsbereich angezeigt werden (letzte 24 Stunden, letzte 7 Tage, letzte 30 Tage oder ein benutzerdefinierter Datumsbereich).
Filtern	Begrenzungsereignisse, die durch die in das Feld eingegebenen Zeichen angezeigt werden. Verwenden Sie Anführungszeichen (") für eine genaue Wortabgleiche, geben Sie ein `OR` Um ein oder mehrere Wörter zurückzugeben, oder geben Sie einen Bindestrich (--) ein, um Wörter auszulassen.
Aktualisierung	Wählen Sie **Aktualisieren**, um die Seite auf die aktuellen Ereignisse zu aktualisieren.
Einstellungen Anzeigen/Bearbeiten	Wählen Sie **Einstellungen anzeigen/bearbeiten** aus, um ein Dialogfeld zu öffnen, in dem Sie eine vollständige Protokollrichtlinie und eine Ebene der zu protokollierenden Aktionen festlegen können.
Löschen von Ereignissen	Wählen Sie **Löschen** aus, um ein Dialogfeld zu öffnen, in dem Sie alte Ereignisse von der Seite entfernen können.
Spalten ein-/ausblenden	Klicken Sie auf das Spaltensymbol **ein-/ausblenden** So wählen Sie zusätzliche Spalten aus, die in der Tabelle angezeigt werden sollen. Weitere Spalten sind: • **Methode** — die HTTP-Methode (z. B. POST, GET, DELETE usw.). • **CLI Befehl ausgeführt** — der CLI-Befehl (Grammatik) ausgeführt für Secure CLI Anfragen. • **CLI Rückgabestatus** — Ein CLI-Statuscode oder eine Anforderung für Eingabedateien vom Client. • **Symbol-Verfahren** — das Symbol-Verfahren ausgeführt. • **SSH Event Type** — Secure Shell (SSH) Ereignistyp, wie Login, Logout und Login_fail. • **SSH Session PID** — Prozess-ID-Nummer der SSH-Sitzung. • **SSH Sitzungsdauer(en)** — die Anzahl der Sekunden, die der Benutzer angemeldet war.
Spaltenfilter ein- oder ausschalten	Klicken Sie auf das Symbol **Umschalten** Zum Öffnen von Filterfeldern für jede Spalte. Geben Sie in ein Spaltenfeld Zeichen ein, um die durch diese Zeichen angezeigten Ereignisse einzuschränken. Klicken Sie erneut auf das Symbol, um die Filterfelder zu schließen.
Änderungen rückgängig machen	Klicken Sie auf das Symbol **Rückgängig** Um die Tabelle auf die Standardkonfiguration zurückzugeben.

Auswahl	Beschreibung
Exportieren	Klicken Sie auf **Exportieren**, um die Tabellendaten in einer kommagetrennten Datei (CSV) zu speichern.

Richtlinien für Prüfprotokolle definieren

Sie können die Überschreibungsrichtlinie und die im Audit-Protokoll aufgezeichneten Ereignistypen ändern.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

Über diese Aufgabe

Dieser Task beschreibt, wie die Einstellungen für das Überwachungsprotokoll geändert werden, einschließlich der Richtlinie zum Überschreiben alter Ereignisse und der Richtlinie für die Aufzeichnung von Ereignistypen.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **Audit Log**aus.
3. Wählen Sie **Einstellungen Anzeigen/Bearbeiten**.

   Das Dialogfeld **Audit Log Settings** wird geöffnet.

4. Ändern Sie die Überschreibungsrichtlinie oder die Arten der aufgezeichneten Ereignisse.

Felddetails

Einstellung	Beschreibung
Überschreibungsrichtlinie	Legt die Richtlinie zum Überschreiben alter Ereignisse fest, wenn die maximale Kapazität erreicht ist: • **Die ältesten Ereignisse im Audit-Protokoll können überschrieben werden, wenn das Audit-Protokoll voll ist** — überschreibt die alten Ereignisse, wenn das Audit-Protokoll 50,000 Datensätze erreicht. • **Das manuelle Löschen von Audit-Protokollereignissen ist erforderlich** — gibt an, dass Ereignisse nicht automatisch gelöscht werden; stattdessen erscheint eine Schwellenwertwarnung im festgelegten Prozentsatz. Ereignisse müssen manuell gelöscht werden. ⓘ Wenn die Überschreibungsrichtlinie deaktiviert ist und die Einträge des Prüfprotokolls die maximale Grenze erreichen, wird Benutzern der Zugriff auf System Manager ohne die Berechtigung des Sicherheitsadministrators verweigert. Um den Systemzugriff für Benutzer ohne Sicherheitsadministrator-Berechtigungen wiederherzustellen, muss ein Benutzer, der der Rolle Sicherheitsadministrator zugewiesen ist, die alten Ereignisdatensätze löschen. ⓘ Überschreibungsrichtlinien gelten nicht, wenn ein Syslog-Server für die Archivierung von Audit-Protokollen konfiguriert ist.
Level der zu protokollierenden Aktionen	Legt die Arten von zu protokollierenden Ereignissen fest: • **Änderungsereignisse aufzeichnen** — zeigt nur Ereignisse an, bei denen eine Benutzeraktion eine Systemänderung beinhaltet. • **Alle Änderungen und schreibgeschützten Ereignisse** — zeigt alle Ereignisse an, einschließlich einer Benutzeraktion, die das Lesen oder Herunterladen von Informationen beinhaltet.

5. Klicken Sie Auf **Speichern**.

Löschen von Ereignissen aus dem Auditprotokoll

Sie können das Audit-Protokoll von alten Ereignissen löschen, wodurch das Suchen durch Ereignisse leichter zu verwalten ist. Sie haben die Möglichkeit, alte Ereignisse beim Löschen in einer CSV-Datei (kommagetrennte Werte) zu speichern.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

Über diese Aufgabe

Diese Aufgabe beschreibt, wie alte Ereignisse aus dem Prüfprotokoll entfernt werden.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **Prüfprotokoll** aus.
3. Wählen Sie **Löschen**.

   Das Dialogfeld Prüfprotokoll löschen wird geöffnet.

4. Wählen Sie oder geben Sie die Anzahl der ältesten Ereignisse ein, die Sie löschen möchten.
5. Wenn Sie die gelöschten Ereignisse in eine CSV-Datei exportieren möchten (empfohlen), lassen Sie das Kontrollkästchen aktiviert. Sie werden aufgefordert, einen Dateinamen und Speicherort einzugeben, wenn Sie im nächsten Schritt auf **Löschen** klicken. Wenn Sie keine Ereignisse in einer CSV-Datei speichern möchten, aktivieren Sie das Kontrollkästchen, um die Auswahl aufzuheben.
6. Klicken Sie Auf **Löschen**.

   Ein Bestätigungsdialogfeld wird geöffnet.

7. Typ `delete` Klicken Sie im Feld auf **Löschen**.

   Die ältesten Ereignisse werden von der Seite „Überwachungsprotokoll“ entfernt.

Syslog-Server für Audit-Protokolle konfigurieren

Wenn Sie Auditprotokolle auf einem externen Syslog-Server archivieren möchten, können Sie die Kommunikation zwischen diesem Server und dem Speicher-Array konfigurieren. Nach der Verbindungsherstellung werden Audit-Protokolle automatisch auf dem Syslog-Server gespeichert.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Die Syslog-Serveradresse, das Protokoll und die Portnummer müssen verfügbar sein. Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
- Wenn Ihr Server ein sicheres Protokoll verwendet (z. B. TLS), muss auf Ihrem lokalen System ein Zertifikat für Zertifizierungsstellen (CA) verfügbar sein. CA-Zertifikate identifizieren Website-Eigentümer für sichere Verbindungen zwischen Servern und Clients.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie auf der Registerkarte **Audit Log** die Option **Configure Syslog Servers** aus.

   Das Dialogfeld **Syslog Server konfigurieren** wird geöffnet.

3. Klicken Sie Auf **Hinzufügen**.

   Das Dialogfeld **Syslog Server** hinzufügen wird geöffnet.

4. Geben Sie Informationen für den Server ein, und klicken Sie dann auf **Hinzufügen**.
   - **Server-Adresse** — Geben Sie einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
   - **Protokoll** — Wählen Sie aus der Dropdown-Liste ein Protokoll aus (z. B. TLS, UDP oder TCP).
   - **Zertifikat hochladen (optional)** — Wenn Sie das TLS-Protokoll ausgewählt haben und noch kein signiertes CA-Zertifikat hochgeladen haben, klicken Sie auf **Durchsuchen**, um eine Zertifikatdatei hochzuladen. Audit-Protokolle werden nicht ohne vertrauenswürdiges Zertifikat auf einem Syslog-Server archiviert.

     > Wenn das Zertifikat später ungültig wird, schlägt der TLS-Handshake fehl. Als Ergebnis wird eine Fehlermeldung in das Auditprotokoll geschrieben und Meldungen werden nicht mehr an den Syslog-Server gesendet. Um dieses Problem zu lösen, müssen Sie das Zertifikat auf dem Syslog-Server reparieren und dann zu **Einstellungen › Audit Log › Configure Syslog Servers › Test All** wechseln.

   - **Port** — Geben Sie die Portnummer für den Syslog-Empfänger ein.

     Nach dem Klicken auf **Hinzufügen** wird das Dialogfeld **Syslog Server konfigurieren** geöffnet und der konfigurierte Syslog-Server auf der Seite angezeigt.

5. Um die Serververbindung mit dem Speicher-Array zu testen, wählen Sie **Alle testen**.

Ergebnisse

Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-Server gesendet. Frühere Protokolle werden nicht übertragen.

Bearbeiten Sie die Syslog-Servereinstellungen für Audit-Protokolldatensätze

Sie können die Einstellungen für den Syslog-Server ändern, der für die Archivierung von Audit-Protokollen verwendet wird, und auch ein neues Zertifikat für die Zertifizierungsstelle (Certificate Authority, CA) für den Server hochladen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Die Syslog-Serveradresse, das Protokoll und die Portnummer müssen verfügbar sein. Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
- Wenn Sie ein neues CA-Zertifikat hochladen, muss das Zertifikat auf Ihrem lokalen System verfügbar sein.

Schritte

1. Wählen Sie **Einstellungen › Zugriffsmanagement**.
2. Wählen Sie auf der Registerkarte **Audit Log** die Option **Configure Syslog Servers** aus.

   Konfigurierte Syslog-Server werden auf der Seite angezeigt.

3. Um die Serverinformationen zu bearbeiten, wählen Sie rechts neben dem Servernamen das Symbol **Bearbeiten** (Bleistift) aus und nehmen Sie die gewünschten Änderungen in den folgenden Feldern vor:
    - **Server-Adresse** — Geben Sie einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
    - **Protokoll** — Wählen Sie aus der Dropdown-Liste ein Protokoll aus (z. B. TLS, UDP oder TCP).
    - **Port** — Geben Sie die Portnummer für den Syslog-Empfänger ein.
4. Wenn Sie das Protokoll in das sichere TLS-Protokoll (entweder von UDP oder TCP) geändert haben, klicken Sie auf **Vertrautes Zertifikat importieren**, um ein CA-Zertifikat hochzuladen.
5. Um die neue Verbindung mit dem Speicher-Array zu testen, wählen Sie **Alle testen**.

Ergebnisse

Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-Server gesendet. Frühere Protokolle werden nicht übertragen.

FAQs

Warum kann ich mich nicht anmelden?

Wenn Sie beim Versuch, sich bei System Manager anzumelden, einen Fehler erhalten, überprüfen Sie die möglichen Ursachen.

Fehler beim Anmelden bei System Manager können aus einem der folgenden Gründe auftreten:

- Sie haben einen falschen Benutzernamen oder ein falsches Passwort eingegeben.
- Sie verfügen über unzureichende Berechtigungen.
- Der Verzeichnisserver (falls konfiguriert) ist möglicherweise nicht verfügbar. Wenn dies der Fall ist, melden Sie sich mit einer lokalen Benutzerrolle an.
- Sie haben mehrmals versucht, sich erfolglos anzumelden, was den Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, bis Sie sich erneut anmelden können.
- Eine Sperrbedingung wurde ausgelöst und Ihr Prüfprotokoll ist möglicherweise voll. Wechseln Sie zu Zugriffsmanagement und löschen Sie alte Ereignisse aus dem Revisionsprotokoll.
- SAML-Authentifizierung ist aktiviert. Aktualisieren Sie Ihren Browser, um sich anzumelden.

Aus einem der folgenden Gründe können Anmeldefehler bei einem Remote-Speicher-Array auftreten:

- Sie haben ein falsches Kennwort eingegeben.
- Sie haben mehrmals versucht, sich erfolglos anzumelden, was den Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, um sich erneut anzumelden.
- Die maximale Anzahl an Client-Verbindungen, die auf dem Controller verwendet werden, wurde erreicht. Suchen Sie nach mehreren Benutzern oder Clients.

Was muss ich vor dem Hinzufügen eines Verzeichnisservers wissen?

Stellen Sie vor dem Hinzufügen eines Verzeichnisservers in der Zugriffsverwaltung sicher, dass Sie die folgenden Anforderungen erfüllen.

- Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.

- LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich Domänenname, Server-URL und optional Benutzername und Kennwort für das Bindekonto.
- Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette des LDAP-Servers auf Ihrem lokalen Computer installiert sein.

Was muss ich über die Zuordnung von Speicher-Array-Rollen wissen?

Bevor Sie Gruppen zu Rollen zuordnen, lesen Sie die folgenden Richtlinien durch.

Die integrierten RBAC-Funktionen (rollenbasierte Zugriffssteuerung) des Storage-Arrays umfassen folgende Rollen:

- **Storage Admin** — Vollzugriff auf die Speicherobjekte (z. B. Volumes und Disk Pools), aber kein Zugriff auf die Sicherheitskonfiguration.
- **Security Admin** — Zugriff auf die Sicherheitskonfiguration in Access Management, Zertifikatverwaltung, Audit Log Management und die Möglichkeit, die alte Management-Schnittstelle (Symbol) ein- oder auszuschalten.
- **Support Admin** — Zugriff auf alle Hardware-Ressourcen auf dem Speicher-Array, Ausfalldaten, MEL-Ereignisse und Controller-Firmware-Upgrades. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
- **Monitor** — schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

Verzeichnisdienste

Wenn Sie einen LDAP-Server (Lightweight Directory Access Protocol) und Verzeichnisdienste verwenden, stellen Sie sicher, dass:

- Ein Administrator hat im Verzeichnisdienst Benutzergruppen definiert.
- Sie kennen die Gruppen-Domain-Namen für die LDAP-Benutzergruppen.
- Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

SAML

Wenn Sie die im Speicher-Array integrierten SAML-Funktionen (Security Assertion Markup Language) verwenden, stellen Sie sicher, dass:

- Ein IdP-Administrator (Identity Provider) hat im IdP-System Benutzerattribute und Gruppenmitgliedschaften konfiguriert.
- Sie kennen die Namen der Gruppenmitgliedschaft.
- Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich. Der System Manager funktioniert ohne die vorhandene Monitorrolle nicht ordnungsgemäß für alle Benutzer.

Welche externen Verwaltungstools können von dieser Änderung betroffen sein?

Wenn Sie bestimmte Änderungen in System Manager vornehmen, z. B. das Wechseln der Managementoberfläche oder die Verwendung von SAML für eine Authentifizierungsmethode, sind einige externe Tools und Funktionen möglicherweise von der Verwendung eingeschränkt.

Managementoberfläche

Tools, die direkt mit der älteren Managementoberfläche (Symbol), z. B. SANtricity SMI-S Provider oder OnCommand Insight (OCI), kommunizieren, funktionieren nur, wenn die Einstellung für die ältere Managementoberfläche aktiviert ist. Darüber hinaus können Sie keine alten CLI-Befehle verwenden oder Spiegelungsvorgänge durchführen, wenn diese Einstellung deaktiviert ist.

Weitere Informationen erhalten Sie vom technischen Support.

SAML-Authentifizierung

Wenn SAML aktiviert ist, können die folgenden Clients nicht auf Storage-Array-Services und -Ressourcen zugreifen:

- Enterprise Management-Fenster (EMW)
- Befehlszeilenschnittstelle (CLI)
- Software Developer Kits (SDK)-Clients
- In-Band-Clients
- REST-API-Clients für die HTTP-Standardauthentifizierung
- Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an

Weitere Informationen erhalten Sie vom technischen Support.

Was muss ich vor der Konfiguration und Aktivierung von SAML wissen?

Bevor Sie die SAML-Funktionen (Security Assertion Markup Language) für die Authentifizierung konfigurieren und aktivieren, müssen Sie sicherstellen, dass Sie die folgenden Anforderungen erfüllen und SAML-Einschränkungen verstehen.

Anforderungen

Bevor Sie beginnen, stellen Sie sicher, dass:

- Ein Identitäts-Provider (IdP) ist in Ihrem Netzwerk konfiguriert. Ein IdP ist ein externes System, mit dem Anmeldeinformationen von einem Benutzer angefordert werden und festgestellt wird, ob der Benutzer erfolgreich authentifiziert wurde. Ihr Sicherheitsteam ist für die Instandhaltung des IdP verantwortlich.
- Ein IdP-Administrator hat Benutzerattribute und Gruppen im IdP-System konfiguriert.
- Ein IdP-Administrator hat sichergestellt, dass der IdP die Möglichkeit unterstützt, eine Name-ID bei der Authentifizierung zurückzugeben.
- Ein Administrator hat sichergestellt, dass die IdP-Server- und -Controller-Uhren synchronisiert werden (entweder über einen NTP-Server oder durch Anpassen der Controller-Uhreinstellungen).
- Eine IdP-Metadatendatei wird vom IdP-System heruntergeladen und ist auf dem lokalen System verfügbar, das für den Zugriff auf System Manager verwendet wird.
- Sie kennen die IP-Adresse oder den Domain-Namen der einzelnen Controller im Storage-Array.

Einschränkungen

Zusätzlich zu den oben genannten Anforderungen sollten Sie sich mit den folgenden Einschränkungen vertraut machen:

- Sobald SAML aktiviert ist, können Sie sie über die Benutzeroberfläche nicht deaktivieren oder die IdP-Einstellungen bearbeiten. Wenn Sie die SAML-Konfiguration deaktivieren oder bearbeiten müssen, wenden Sie sich an den technischen Support, um Hilfe zu erhalten. Es wird empfohlen, die SSO-Anmeldungen zu testen, bevor Sie SAML im letzten Konfigurationsschritt aktivieren. (Das System führt auch einen SSO-Anmeldetest vor Aktivierung von SAML durch.)
- Wenn Sie SAML zukünftig deaktivieren, stellt das System automatisch die vorherige Konfiguration wieder her (lokale Benutzerrollen und/oder Verzeichnisdienste).
- Wenn Verzeichnisdienste derzeit für die Benutzerauthentifizierung konfiguriert sind, überschreibt SAML diese Konfiguration.
- Wenn SAML konfiguriert ist, können die folgenden Clients nicht auf Speicher-Array-Ressourcen zugreifen:
  - Enterprise Management-Fenster (EMW)
  - Befehlszeilenschnittstelle (CLI)
  - Software Developer Kits (SDK)-Clients
  - In-Band-Clients
  - REST-API-Clients für die HTTP-Standardauthentifizierung
  - Melden Sie sich mithilfe des standardmäßigen REST-API-Endpunkts an

Welche Arten von Ereignissen werden im Auditprotokoll aufgezeichnet?

Das Revisionsprotokoll kann Änderungsereignisse oder sowohl Änderungs- als auch schreibgeschützte Ereignisse aufzeichnen.

Abhängig von den Richtlinieneinstellungen werden die folgenden Ereignistypen angezeigt:

- **Änderungsereignisse** — Benutzeraktionen aus System Manager heraus, die Änderungen am System, z. B. die Bereitstellung von Speicher, mit sich bringen.
- **Modifizierung und schreibgeschützte Ereignisse** — Benutzeraktionen, die Änderungen am System beinhalten, sowie Ereignisse, die Informationen anzeigen oder herunterladen, wie zum Beispiel die Anzeige von Volume-Zuweisungen.

Was muss ich vor der Konfiguration eines Syslog-Servers wissen?

Sie können Audit-Protokolle auf einem externen Syslog-Server archivieren.

Beachten Sie vor der Konfiguration eines Syslog-Servers die folgenden Richtlinien.

- Stellen Sie sicher, dass Sie die Serveradresse, das Protokoll und die Portnummer kennen. Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
- Wenn Ihr Server ein sicheres Protokoll verwendet (z. B. TLS), muss auf Ihrem lokalen System ein Zertifikat für Zertifizierungsstellen (CA) verfügbar sein. CA-Zertifikate identifizieren Website-Eigentümer für sichere Verbindungen zwischen Servern und Clients.
- Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-Server gesendet. Frühere Protokolle werden nicht übertragen.
- Die Einstellungen der Überschreibrichtlinie (verfügbar unter **Ansicht/Einstellungen bearbeiten**) haben keinen Einfluss auf das Management von Protokollen mit einer Syslog-Serverkonfiguration.
- Auditprotokolle folgen dem Nachrichtenformat RFC 5424.

Der Syslog-Server empfängt keine Audit-Protokolle mehr. Was mache ich?

Wenn Sie einen Syslog-Server mit einem TLS-Protokoll konfiguriert haben, kann der Server keine Meldungen empfangen, wenn das Zertifikat aus irgendeinem Grund ungültig wird. Eine Fehlermeldung über das ungültige Zertifikat wird im Auditprotokoll veröffentlicht.

Um dieses Problem zu lösen, müssen Sie zuerst das Zertifikat für den Syslog-Server reparieren. Wenn eine gültige Zertifikatskette vorhanden ist, gehen Sie zu **Einstellungen › Audit Log › Configure Syslog Servers › Test All**.

Zertifikate

Konzepte

Funktionsweise von Zertifikaten

Zertifikate sind digitale Dateien, die Online-Einheiten wie Websites und Server für eine sichere Kommunikation im Internet identifizieren.

Zertifikate stellen sicher, dass die Webkommunikation in verschlüsselter Form, privat und unverändert, nur zwischen dem angegebenen Server und dem angegebenen Client übertragen wird. Mit System Manager können Sie Zertifikate zwischen dem Browser auf einem Host-Managementsystem (als Client fungieren) und den Controllern in einem Storage-System (als Server fungieren) verwalten.

Ein Zertifikat kann von einer vertrauenswürdigen Behörde signiert werden, oder es kann selbst signiert werden. „Unterzeichnen“ bedeutet einfach, dass jemand die Identität des Eigentümers validiert und festgestellt hat, dass seine Geräte vertrauenswürdig sind. Die Storage Arrays werden mit einem automatisch generierten, selbstsignierten Zertifikat auf jedem Controller ausgeliefert. Sie können weiterhin die selbst signierten Zertifikate verwenden oder CA-signierte Zertifikate für eine sicherere Verbindung zwischen den Controllern und den Host-Systemen erhalten.

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

Signierte Zertifikate

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

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

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

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

Selbstsignierte Zertifikate

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

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

Zertifikate, die für den Schlüsselverwaltungsserver verwendet werden

Wenn Sie einen externen Schlüsselverwaltungsserver mit der Laufwerkssicherheitsfunktion verwenden, können Sie auch Zertifikate zur Authentifizierung zwischen diesem Server und den Controllern verwalten.

Terminologie des Zertifikats

Die folgenden Begriffe gelten für das Zertifikatmanagement.

Laufzeit	Beschreibung
CA	Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer, die sichere Verbindungen zwischen Clients und Servern ermöglichen.
CSR	Eine Zertifikatsignierungsanforderung (CSR) ist eine Nachricht, die von einem Antragsteller an eine Zertifizierungsstelle (CA) gesendet wird. Der CSR überprüft die Informationen, die die Zertifizierungsstelle zum ausstellen eines Zertifikats benötigt.

Laufzeit	Beschreibung
Zertifikat	Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).
Zertifikatskette	Eine Dateihierarchie, die den Zertifikaten eine Sicherheitsschicht hinzufügt. In der Regel umfasst die Kette ein Stammzertifikat oben in der Hierarchie, ein oder mehrere Zwischenzertifikate und die Serverzertifikate, die die Entitäten identifizieren.
Client-Zertifikat	Für das Management von Sicherheitsschlüssel validiert ein Client-Zertifikat die Controller des Speicherarrays, damit der Schlüsselverwaltungsserver ihre IP-Adressen anvertrauen kann.
Zwischenzertifikat	Ein oder mehrere Zwischenzertifikate verzweigen von der Root in der Zertifikatkette. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten fungieren sollen.
Zertifikat für Schlüsselmanagement-Server	Für das Sicherheitsschlüsselmanagement validiert ein Zertifikat für den Schlüsselmanagement-Server den Server, damit das Storage-Array seiner IP-Adresse vertrauen kann.
Schlüsselspeicher	Ein Schlüsselspeicher ist ein Repository auf Ihrem Host-Managementsystem, das private Schlüssel enthält, zusammen mit ihren entsprechenden öffentlichen Schlüsseln und Zertifikaten. Diese Schlüssel und Zertifikate identifizieren Ihre eigenen Einheiten, z. B. die Controller.
OCSP-Server	Der OCSP-Server (Online Certificate Status Protocol) ermittelt, ob die Zertifizierungsstelle vor ihrem geplanten Ablaufdatum Zertifikate widerrufen hat und blockiert dann den Zugriff des Benutzers auf einen Server, wenn das Zertifikat widerrufen wird.
Stammzertifikat	Das Stammzertifikat befindet sich oben in der Hierarchie in der Zertifikatskette und enthält einen privaten Schlüssel, der zum Signieren anderer Zertifikate verwendet wird. Das Root identifiziert eine bestimmte CA-Organisation. Wenn Sie dieselbe Zertifizierungsstelle für alle Netzwerkgeräte verwenden, benötigen Sie nur ein Stammzertifikat.
Signiertes Zertifikat	Ein Zertifikat, das von einer Zertifizierungsstelle (CA) validiert wird. Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt zwischen einem Server und einem Client über eine HTTPS-Verbindung gesendet werden. Darüber hinaus enthält ein signiertes Zertifikat Details über den Eigentümer des Unternehmens (in der Regel ein Server oder eine Website) und eine digitale Signatur bestehend aus Buchstaben und Zahlen. Ein signiertes Zertifikat nutzt eine Vertrauenskette und wird daher am häufigsten in Produktionsumgebungen verwendet. Auch als „CA-signiertes Zertifikat“ oder als „Managementzertifikat“ bezeichnet.

Laufzeit	Beschreibung
Selbstsigniertes Zertifikat	Ein selbstsigniertes Zertifikat wird vom Eigentümer des Unternehmens validiert. Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt zwischen einem Server und einem Client über eine HTTPS-Verbindung gesendet werden. Es enthält auch eine digitale Signatur, die aus Buchstaben und Zahlen besteht. Ein selbstsigniertes Zertifikat verwendet nicht dieselbe Vertrauenskette wie ein CA-signiertes Zertifikat und wird daher am häufigsten in Testumgebungen eingesetzt. Auch als vorinstalliertes Zertifikat bezeichnet.
Serverzertifikat	Das Server-Zertifikat befindet sich unten in der Zertifikatskette. Es identifiziert Ihre spezifische Einheit, z. B. eine Website oder ein anderes Gerät. Jeder Controller in einem Storage-System benötigt ein separates Serverzertifikat.

Anleitungen

Verwenden Sie CA-signierte Zertifikate für Controller

Sie können Zertifikate von CA-signierte für die sichere Kommunikation zwischen den Controllern und dem Browser erhalten, der für den Zugriff auf System Manager verwendet wird.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

Über diese Aufgabe

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

Schritt 1: Eine CSR für die Controller abschließen und einreichen

Sie müssen zuerst für jeden Controller im Speicher-Array eine CSR-Datei (Certificate Signing Request) generieren und dann die Datei(en) an eine Zertifizierungsstelle (CA) senden.

Bevor Sie beginnen

- Sie müssen die IP-Adresse oder den DNS-Namen jedes Controllers kennen.

Über diese Aufgabe

Der CSR stellt Informationen über Ihre Organisation, die IP-Adresse oder den DNS-Namen des Controllers und ein Schlüsselpaar zur Verfügung, das den Webserver im Controller identifiziert. Während dieser Aufgabe wird eine CSR-Datei erzeugt, wenn es nur einen Controller im Speicher-Array und zwei CSR-Dateien gibt, wenn es zwei Controller gibt.

> Generieren Sie nach der Übermittlung an die CA keine neue CSR. Wenn Sie eine CSR erstellen, erstellt das System ein privates und öffentliches Schlüsselpaar. Der öffentliche Schlüssel ist Teil des CSR, während der private Schlüssel im Schlüsselspeicher aufbewahrt wird. Wenn Sie die signierten Zertifikate erhalten und in den Schlüsselspeicher importieren, stellt das System sicher, dass sowohl der private als auch der öffentliche Schlüssel das ursprüngliche Paar sind. Daher dürfen Sie nach dem Einreichen einer CSR an die CA keine neue CSR generieren. Wenn Sie dies tun, generieren die Controller neue Schlüssel, und die Zertifikate, die Sie von der CA erhalten, funktionieren nicht.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte **Array Management** die Option **Complete CSR** aus.

> Wenn ein Dialogfeld angezeigt wird, in dem Sie aufgefordert werden, ein selbstsigniertes Zertifikat für den zweiten Controller anzunehmen, klicken Sie zum Fortfahren auf **Selbstsigniertes Zertifikat akzeptieren**.

3. Geben Sie die folgenden Informationen ein, und klicken Sie dann auf **Weiter**:
   - **Organisation** — der vollständige, rechtliche Name Ihres Unternehmens oder Ihrer Organisation. Fügen Sie Suffixe wie Inc. Oder Corp. Mit ein
   - **Organisationseinheit (optional)** — die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet.
   - **Stadt/Ort** — die Stadt, in der sich Ihr Speicher-Array oder Geschäft befindet.
   - **Bundesland/Region (optional)** — der Staat oder die Region, in der sich Ihr Speicher-Array oder Ihr Geschäft befindet.
   - **Land ISO Code** — der zweistellige ISO-Code Ihres Landes (International Organization for Standardization), wie z. B. die USA.

> Einige Felder sind möglicherweise bereits mit den entsprechenden Informationen ausgefüllt, z. B. mit der IP-Adresse des Controllers. Ändern Sie die vorausgefüllten Werte nur, wenn Sie sich sicher sind, dass sie nicht korrekt sind. Wenn Sie zum Beispiel noch keinen CSR-Vorgang abgeschlossen haben, wird die Controller-IP-Adresse auf „`localhost.`“ gesetzt. In diesem Fall müssen Sie „`localhost`“ in den DNS-Namen oder die IP-Adresse des Controllers ändern.

4. Überprüfen oder geben Sie die folgenden Informationen über Controller A in Ihrem Speicher-Array ein:
   - **Controller Ein gemeinsamer Name** — die IP-Adresse oder der DNS-Name von Controller A wird standardmäßig angezeigt. Stellen Sie sicher, dass diese Adresse korrekt ist. Sie muss mit den Angaben übereinstimmen, die Sie für den Zugriff auf System Manager im Browser eingeben.
   - **Controller Eine alternative IP-Adresse** — Wenn der gemeinsame Name eine IP-Adresse ist, können Sie optional weitere IP-Adressen oder Aliase für Controller A eingeben Verwenden Sie für mehrere Einträge ein kommagetrenntes Format.
   - **Controller Ein alternativer DNS-Name** — Wenn der gemeinsame Name ein DNS-Name ist, geben Sie weitere DNS-Namen für Controller A. ein Verwenden Sie für mehrere Einträge ein kommagetrenntes Format. Falls es keine alternativen DNS-Namen gibt, aber Sie im ersten Feld einen DNS-Namen eingegeben haben, kopieren Sie diesen Namen hier. Wenn das Speicher-Array nur über einen Controller verfügt, steht die **Finish**-Taste zur Verfügung. Wenn das Speicher-Array über zwei Controller verfügt, steht die Schaltfläche **Weiter** zur Verfügung.

> Klicken Sie nicht auf den Link **Skip this Step**, wenn Sie eine CSR-Anfrage erstellen. Dieser Link wird in Fehlerwiederherstellungssituationen bereitgestellt. In seltenen Fällen kann eine CSR-Anfrage auf einem Controller fehlschlagen, aber nicht auf dem anderen. Über diesen Link können Sie den Schritt zum Erstellen einer CSR-Anfrage für Controller A überspringen, wenn er bereits definiert ist, und mit dem nächsten Schritt zum erneuten Erstellen einer CSR-Anfrage auf Controller B fortfahren

5. Wenn nur ein Controller vorhanden ist, klicken Sie auf **Fertig stellen**. Wenn zwei Controller vorhanden sind, klicken Sie auf **Weiter**, um die Daten für Controller B einzugeben (wie oben), und klicken Sie dann

auf **Fertig stellen**.

Für einen einzelnen Controller wird eine CSR-Datei auf Ihr lokales System heruntergeladen. Für Dual Controller werden zwei CSR-Dateien heruntergeladen. Der Speicherort des Downloads hängt von Ihrem Browser ab.

6. Suchen Sie die heruntergeladenen CSR-Dateien. Der Speicherort des Ordners hängt vom Browser ab.
7. Senden Sie die CSR-Datei(en) an eine CA und fordern Sie signierte Zertifikate im PEM-Format an.
8. Warten Sie, bis die Zertifizierungsstelle die Zertifikate zurückgibt, und gehen Sie dann zu Schritt 2: Importieren Sie signierte Zertifikate für Controller.

Schritt 2: Importieren Sie signierte Zertifikate für Controller

Nachdem Sie signierte Zertifikate erhalten haben, importieren Sie die Dateien für die Controller.

Bevor Sie beginnen

- Die CA hat signierte Zertifikatdateien zurückgegeben.
- Die Dateien sind auf Ihrem lokalen System verfügbar.
- Wenn die CA ein verkettetes Zertifikat (z. B. eine .p7b-Datei) lieferte, müssen Sie die verkettete Datei in einzelne Dateien entpacken: Das Stammzertifikat, ein oder mehrere Zwischenzertifikate und die Serverzertifikate, die die Controller identifizieren. Sie können die Windows verwenden `certmgr` Dienstprogramm zum Auspacken der Dateien (Rechtsklick und wählen Sie **Alle Aufgaben › Export**). Wenn die Exporte abgeschlossen sind, wird für jede Zertifikatdatei in der Kette eine CER-Datei angezeigt.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Sie die Zertifikatdateien hochladen.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte **Array Management** die Option **Import**.

   Es wird ein Dialogfeld zum Importieren der Zertifikatdatei(en) geöffnet.

3. Klicken Sie auf die Schaltflächen **Durchsuchen**, um zuerst die Root- und Zwischendateien auszuwählen und dann jedes Serverzertifikat für die Controller auszuwählen. Die Root- und Zwischendateien sind für beide Controller gleich. Nur die Serverzertifikate sind für jeden Controller eindeutig.

   Die Dateinamen werden im Dialogfeld angezeigt.

4. Klicken Sie Auf **Import**.

   Die Datei(en) werden hochgeladen und validiert.

Ergebnisse

Die Sitzung wird automatisch beendet. Sie müssen sich erneut anmelden, damit die Zertifikate wirksam werden. Wenn Sie sich erneut anmelden, wird das neue CA-signierte Zertifikat für Ihre Sitzung verwendet.

Managementzertifikate zurücksetzen

Sie können die Zertifikate auf den Controllern von der Verwendung von CA-signierten Zertifikaten zurück auf die werkseitig eingestellten, selbstsignierten Zertifikate

zurücksetzen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- CA-signierte Zertifikate müssen bereits importiert werden.

Über diese Aufgabe

Mit der Funktion Reset werden die aktuellen CA-signierten Zertifikatdateien von jedem Controller gelöscht. Die Controller werden dann mithilfe selbstsignierter Zertifikate wiederhergestellt.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte **Array Management** die Option **Zurücksetzen**.

   Es wird ein Dialogfeld „Bestätigen **Management Certificates** zurücksetzen“ geöffnet.

3. Typ `reset` Klicken Sie im Feld auf **Zurücksetzen**.

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

Ergebnisse

Die Controller werden mithilfe von selbstsignierten Zertifikaten wiederhergestellt. Das System fordert Benutzer daher auf, das selbstsignierte Zertifikat für ihre Sitzungen manuell anzunehmen.

Anzeigen importierter Zertifikatinformationen

Auf der Seite Zertifikate können Sie den Zertifikatstyp, die ausstellende Behörde und den gültigen Datumsbereich der Zertifikate für das Speicher-Array anzeigen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

Schritte

1. Wählen Sie Menü:Einstellungen[Zertifikate].
2. Wählen Sie eine der Registerkarten aus, um Informationen zu den Zertifikaten anzuzeigen.

Registerkarte	Beschreibung
Array-Management	Zeigen Sie Informationen zu den für jeden Controller importierten CA-signierten Zertifikaten an, einschließlich der Root-Datei, der Zwischendatei(en) und der Serverdatei(en).

Registerkarte	Beschreibung
Bewährt	Informationen über alle anderen Arten von Zertifikaten anzeigen, die für die Controller importiert wurden. Verwenden Sie das Filterfeld unter **Zertifikate anzeigen, die…** sind, um entweder vom Benutzer installierte oder vorinstallierte Zertifikate anzuzeigen. • **Vom Benutzer installiert**. Zertifikate, die ein Benutzer auf das Speicher-Array hochgeladen hat. Dies kann vertrauenswürdige Zertifikate enthalten, wenn der Controller als Client (anstelle eines Servers), LDAPS-Zertifikate und Identity Federation-Zertifikate fungiert. • **Vorinstalliert**. Im Speicher-Array enthaltene selbstsignierte Zertifikate.
Verschlüsselungs-Management	Zeigen Sie Informationen zu den für einen externen Schlüsselverwaltungsserver importierten CA-signierten Zertifikaten an.

Importieren Sie Zertifikate für Controller, wenn Sie als Clients fungieren

Wenn der Controller eine Verbindung zurückweist, weil er die Vertrauenskette für einen Netzwerkserver nicht validieren kann, können Sie ein Zertifikat über die Registerkarte „Trusted“ importieren, auf der der Controller (als Client agiert) die Kommunikation von diesem Server akzeptieren kann.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Die Zertifikatdateien werden auf Ihrem lokalen System installiert.

Über diese Aufgabe

Das Importieren von Zertifikaten aus der Registerkarte „Trusted“ ist möglicherweise erforderlich, wenn Sie zulassen möchten, dass andere Server die Controller kontaktieren (z. B. ein LDAP-Server oder ein Syslog-Server, der TLS verwendet).

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte * Trusted* die Option **Import** aus.

   Es wird ein Dialogfeld zum Importieren der vertrauenswürdigen Zertifikatdateien geöffnet.

3. Klicken Sie auf **Durchsuchen**, um die Zertifikatdateien für die Controller auszuwählen.

   Die Dateinamen werden im Dialogfeld angezeigt.

4. Klicken Sie Auf **Import**.

Ergebnisse

Die Dateien werden hochgeladen und validiert.

Überprüfung des Zertifikatsannuls aktivieren

Sie können automatische Überprüfungen auf widerrief Zertifikate aktivieren, sodass ein OCSP-Server (Online Certificate Status Protocol) Benutzer daran blockiert, nicht sichere Verbindungen zu machen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Auf beiden Controllern wird ein DNS-Server konfiguriert, wodurch ein vollständig qualifizierter Domain-Name für den OCSP-Server verwendet werden kann. Diese Aufgabe ist auf der Seite Hardware verfügbar.
- Wenn Sie Ihren eigenen OCSP-Server angeben möchten, müssen Sie die URL dieses Servers kennen.

Über diese Aufgabe

Die automatische Überprüfung des Widerrufs ist hilfreich, wenn die CA ein Zertifikat falsch ausgestellt hat oder ein privater Schlüssel gefährdet ist.

Während dieser Aufgabe können Sie einen OCSP-Server konfigurieren oder den in der Zertifikatdatei angegebenen Server verwenden. Der OCSP-Server prüft, ob die CA Zertifikate vor ihrem geplanten Ablaufdatum widerrufen hat, und blockiert dann den Zugriff des Benutzers auf einen Standort, wenn das Zertifikat widerrufen wird.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie die Registerkarte * Trusted* aus.

   Sie können auch die Überprüfung des Widerrufs über die Registerkarte * Key Management* aktivieren.

3. Klicken Sie auf **Sonstige Aufgaben**, und wählen Sie im Dropdown-Menü die Option **Überprüfung der Widerruherstellung aktivieren** aus.
4. Wählen Sie **Ich möchte die Sperrprüfung aktivieren** aus, damit im Kontrollkästchen ein Häkchen angezeigt wird und im Dialogfeld zusätzliche Felder angezeigt werden.
5. Im Feld **OCSP Responder Address** können Sie optional eine URL für einen OCSP Responder-Server eingeben. Wenn Sie keine Adresse eingeben, verwendet das System die URL des OCSP-Servers aus der Zertifikatsdatei.
6. Klicken Sie auf **Testadresse**, um sicherzustellen, dass das System eine Verbindung zur angegebenen URL öffnen kann.
7. Klicken Sie Auf **Speichern**.

Ergebnisse

Wenn das Speicher-Array versucht, eine Verbindung mit einem Server mit einem widerrufenen Zertifikat herzustellen, wird die Verbindung verweigert und ein Ereignis protokolliert.

Vertrauenswürdige Zertifikate löschen

Sie können die vom Benutzer installierten Zertifikate löschen, die zuvor über die Registerkarte „Vertrauenswürdig“ importiert wurden.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Wenn Sie ein vertrauenswürdiges Zertifikat mit einer neuen Version aktualisieren, muss das aktualisierte Zertifikat importiert werden, bevor Sie das alte Zertifikat löschen.

> Möglicherweise verlieren Sie den Zugriff auf ein System, wenn Sie ein Zertifikat löschen, das zur Authentifizierung der Controller und eines anderen Servers, z. B. eines LDAP-Servers verwendet wird, bevor Sie ein Ersatzzertifikat importieren.

Über diese Aufgabe

Diese Aufgabe beschreibt das Löschen von vom Benutzer installierten Zertifikaten. Die vorinstallierten, selbstsignierten Zertifikate können nicht gelöscht werden.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie die Registerkarte * Trusted* aus.

   In der Tabelle sind die vertrauenswürdigen Zertifikate des Speicher-Arrays aufgeführt.

3. Wählen Sie in der Tabelle das Zertifikat aus, das Sie entfernen möchten.
4. Klicken Sie auf **Sonstige Aufgaben › Löschen**

   Das Dialogfeld Vertrauenswürdiges Zertifikat bestätigen wird geöffnet.

5. Typ `delete` Klicken Sie im Feld auf **Löschen**.

Verwenden Sie CA-signierte Zertifikate zur Authentifizierung mit einem Schlüsselverwaltungsserver

Für die sichere Kommunikation zwischen einem Schlüsselverwaltungsserver und den Speicher-Array-Controllern müssen Sie die entsprechenden Zertifikatssätze konfigurieren.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

Über diese Aufgabe

Die Authentifizierung zwischen den Controllern und einem Schlüsselverwaltungsserver ist ein zweistufiges Verfahren.

Schritt 1: CSR für die Authentifizierung mit einem Schlüsselverwaltungsserver abschließen und einreichen

Sie müssen zuerst eine CSR-Datei (Certificate Signing Request) generieren und dann mithilfe des CSR ein signiertes Clientzertifikat von einer Zertifizierungsstelle (CA) anfordern, die vom Schlüsselverwaltungsserver vertrauenswürdig ist. Sie können auch mithilfe der heruntergeladenen CSR-Datei ein Client-Zertifikat vom Schlüsselverwaltungsserver erstellen und herunterladen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

Über diese Aufgabe

Diese Aufgabe beschreibt, wie Sie die CSR-Datei generieren, die Sie dann verwenden, um ein signiertes Client-Zertifikat von einer CA anzufordern, die vom Schlüsselverwaltungsserver vertrauenswürdig ist. Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit der wichtige Management-Server seine KMIP-Anforderungen (Key Management Interoperability Protocol) anvertrauen kann. Während dieser Aufgabe müssen Sie Informationen über Ihr Unternehmen angeben.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte * Key Management* die Option **Complete CSR** aus.
3. Geben Sie die folgenden Informationen ein:
   - **Allgemeiner Name** — Ein Name, der diese CSR identifiziert, wie z.B. den Namen des Speicherarrays, der in den Zertifikatdateien angezeigt wird.
   - **Organisation** — der vollständige, rechtliche Name Ihres Unternehmens oder Ihrer Organisation. Fügen Sie Suffixe wie Inc. Oder Corp. Mit ein
   - **Organisationseinheit (optional)** — die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet.
   - **Stadt/Ort** — die Stadt oder der Ort, in dem sich Ihre Organisation befindet.
   - **Bundesland/Region (optional)** — der Staat oder die Region, in der sich Ihre Organisation befindet.
   - **Land ISO Code** — der zweistellige ISO-Code (International Organization for Standardization), wie die USA, wo sich Ihre Organisation befindet.
4. Klicken Sie Auf **Download**.

   Eine CSR-Datei wird auf Ihrem lokalen System gespeichert.

5. Fordern Sie ein signiertes Clientzertifikat von einer Zertifizierungsstelle an, die vom Schlüsselverwaltungsserver vertrauenswürdig ist.
6. Wenn Sie ein Clientzertifikat besitzen, gehen Sie zu Schritt 2: Importieren Sie Zertifikate für den Schlüsselverwaltungsserver.

Schritt 2: Importieren Sie Zertifikate für den Schlüsselverwaltungsserver

Im nächsten Schritt importieren Sie Zertifikate zur Authentifizierung zwischen dem Storage-Array und dem Schlüsselverwaltungsserver. Es gibt zwei Arten von Zertifikaten: Das Clientzertifikat überprüft die Controller des Speicherarrays, während das Zertifikat für den Schlüsselverwaltungsserver den Server validiert.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Sie haben eine signierte Client-Zertifikatdatei (siehe Schritt 1: CSR für die Authentifizierung mit einem Schlüsselverwaltungsserver abschließen und einreichen), und Sie haben diese Datei auf den Host kopiert, auf den Sie auf System Manager zugreifen. Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit der wichtige Management-Server seine KMIP-Anforderungen (Key Management Interoperability Protocol) anvertrauen kann.
- Sie müssen die Serverzertifikatdatei vom Schlüsselverwaltungsserver abrufen und diese Datei anschließend auf den Host kopieren, auf dem Sie auf System Manager zugreifen. Ein Zertifikat für den Schlüsselmanagementserver validiert den Schlüsselmanagementserver, damit das Storage-Array seiner IP-Adresse vertrauen kann.

Weitere Informationen zum Serverzertifikat finden Sie in der Dokumentation für Ihren Schlüsselverwaltungsserver.

Über diese Aufgabe

In dieser Aufgabe wird beschrieben, wie Zertifikatdateien für die Authentifizierung zwischen den Speicher-Array-Controllern und dem Schlüsselverwaltungsserver hochgeladen werden. Sie müssen sowohl die Client-Zertifikatdatei für die Controller als auch die Serverzertifikatdatei für den Schlüsselverwaltungsserver laden.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie auf der Registerkarte * Key Management* die Option **Import** aus.

   Es wird ein Dialogfeld zum Importieren der Zertifikatdateien geöffnet.

3. Klicken Sie neben **Select Client Certificate** auf die Schaltfläche **Browse**, um die Clientzertifikatdatei für die Controller des Speicherarrays auszuwählen.

   Der Dateiname wird im Dialogfeld angezeigt.

4. Neben **Wählen Sie das Serverzertifikat des Schlüsselverwaltungsservers**, klicken Sie auf die Schaltfläche **Durchsuchen**, um die Serverzertifikatdatei für Ihren Schlüsselverwaltungsserver auszuwählen.

   Der Dateiname wird im Dialogfeld angezeigt.

5. Klicken Sie Auf **Import**.

   Die Dateien werden hochgeladen und validiert.

Export von Zertifikaten für den Schlüsselverwaltungsserver

Sie können ein Zertifikat für einen Schlüsselverwaltungsserver auf Ihrem lokalen Computer speichern.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Zertifikate müssen bereits importiert werden.

Schritte

1. Wählen Sie **Einstellungen › Zertifikate**.
2. Wählen Sie die Registerkarte * Key Management* aus.
3. Wählen Sie in der Tabelle das Zertifikat aus, das Sie exportieren möchten, und klicken Sie dann auf **Exportieren**.

   Ein Dialogfeld „Speichern“ wird geöffnet.

4. Geben Sie einen Dateinamen ein und klicken Sie auf **Speichern**.

FAQs

Warum wird das Dialogfeld „Zugriff auf anderen Controller nicht möglich“ angezeigt?

Wenn Sie bestimmte Vorgänge im Zusammenhang mit CA-Zertifikaten ausführen (z. B. ein Zertifikat importieren), wird möglicherweise ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, ein selbstsigniertes Zertifikat für den zweiten Controller anzunehmen.

In Speicher-Arrays mit zwei Controllern (Duplexkonfigurationen) wird dieses Dialogfeld manchmal angezeigt, wenn SANtricity System Manager nicht mit dem zweiten Controller kommunizieren kann oder wenn Ihr Browser das Zertifikat während eines bestimmten Punktes nicht akzeptieren kann.

Wenn dieses Dialogfeld geöffnet wird, klicken Sie auf **Selbstsigniertes Zertifikat akzeptieren**, um fortzufahren. Wenn Sie in einem anderen Dialogfeld zur Eingabe eines Passworts aufgefordert werden, geben Sie Ihr Administratorpasswort ein, das zum Zugriff auf System Manager verwendet wird.

Wenn dieses Dialogfeld erneut angezeigt wird und Sie keine Zertifikataufgabe abschließen können, führen Sie einen der folgenden Schritte aus:

- Verwenden Sie einen anderen Browsertyp, um auf diesen Controller zuzugreifen, das Zertifikat zu akzeptieren und fortzufahren.
- Greifen Sie mit System Manager auf den zweiten Controller zu, akzeptieren Sie das selbstsignierte Zertifikat, kehren Sie dann zum ersten Controller zurück und fahren Sie fort.

Wie weiß ich, welche Zertifikate zum externen Verschlüsselungsmanagement in System Manager hochgeladen werden müssen?

Für das externe Verschlüsselungsmanagement importieren Sie zwei Arten von Zertifikaten zur Authentifizierung zwischen dem Storage-Array und dem Schlüsselverwaltungsserver, damit sich die beiden Entitäten gegenseitig vertrauen können.

Ein Client-Zertifikat validiert die Controller des Storage-Arrays, damit der wichtige Management-Server seine KMIP-Anforderungen (Key Management Interoperability Protocol) anvertrauen kann. Um ein Client-Zertifikat zu erhalten, verwenden Sie System Manager, um eine CSR für das Speicher-Array abzuschließen. Anschließend können Sie die CSR auf einen Schlüsselverwaltungsserver hochladen und von dort aus ein Clientzertifikat generieren. Wenn Sie über ein Clientzertifikat verfügen, kopieren Sie diese Datei auf den Host, auf den Sie auf System Manager zugreifen.

Ein Zertifikat für den Schlüsselmanagementserver validiert den Schlüsselmanagementserver, damit das Storage-Array seiner IP-Adresse vertrauen kann. Rufen Sie die Serverzertifikatdatei vom Schlüsselverwaltungsserver ab, und kopieren Sie diese Datei dann auf den Host, auf dem Sie auf System Manager zugreifen.

Was muss ich über die Überprüfung des Annullierung von Zertifikaten wissen?

Mit System Manager können Sie mithilfe eines OCSP-Servers (Online Certificate Status Protocol) nach widerrufenen Zertifikaten suchen, anstatt Zertifikatsperrlisten (Certificate Revocation Lists, CRLs) hochzuladen.

Zurückwiderrufen Zertifikate sollten nicht mehr vertrauenswürdig sein. Ein Zertifikat kann aus mehreren

Gründen widerrufen werden; beispielsweise wenn die Zertifizierungsstelle (CA) das Zertifikat nicht ordnungsgemäß ausgestellt hat, ein privater Schlüssel kompromittiert wurde oder die identifizierte Entität nicht den Richtlinienanforderungen entspricht.

Nachdem Sie in System Manager eine Verbindung zu einem OCSP-Server hergestellt haben, führt das Speicherarray eine Widerrufs-Prüfung durch, wenn es eine Verbindung zu einem AutoSupport-Server, einem externen Schlüsselverwaltungsserver (EKMS), einem Lightweight Directory Access Protocol over SSL (LDAPS)-Server oder einem Syslog-Server herstellt. Das Speicher-Array versucht, die Zertifikate dieser Server zu validieren, um sicherzustellen, dass sie nicht widerrufen wurden. Der Server gibt dann für dieses Zertifikat einen Wert von „gut“, „gesperrt“ oder „unbekannt“ zurück. Wenn das Zertifikat widerrufen wird oder das Array nicht den OCSP-Server kontaktieren kann, wird die Verbindung abgelehnt.

> Wenn Sie eine OCSP-Antwortadresse in System Manager oder in der Befehlszeilenschnittstelle (CLI) angeben, wird die OCSP-Adresse, die in der Zertifikatsdatei gefunden wurde, überschrieben.

Für welche Servertypen wird die Überprüfung des Widerrufs aktiviert?

Das Speicher-Array führt Sperrprüfungen durch, wenn es eine Verbindung zu einem AutoSupport-Server, einem externen Schlüsselverwaltungsserver (EKMS), einem Lightweight Directory Access Protocol over SSL (LDAPS)-Server oder einem Syslog-Server herstellt.