



Controller

E-Series storage systems

NetApp
January 20, 2026

Inhalt

Controller	1
Erfahren Sie mehr über Upgrades von E-Series Controllern	1
Controller-Komponenten	1
Wann wird dieses Verfahren durchgeführt	1
Überlegungen zu Upgrades der E-Series	1
Hardware- und Firmware-Anforderungen erfüllen	1
Upgrade-Kompatibilität	2
SAS-Gehäuse	7
Investitionsschutz durch SAS-2 zu SAS-3	8
Vorbereitung für das Upgrade der E-Series Controller	8
Entfernen Sie die E-Series Controller	13
Schritt 1: Controller entfernen	13
Schritt 2: Entfernen Sie den Akku	14
Installation neuer E-Series Controller	15
Schritt 1: Batterie einbauen	15
Schritt 2: Installieren Sie den neuen Controller-Behälter	16
E-Series Laufwerke freischalten	16
Internes Verschlüsselungsmanagement	16
Externes Verschlüsselungskeymanagement	17
Abschließen des E-Series Controller-Upgrades	18
Schritt 1: Controller einschalten	18
Schritt 2: Überprüfen Sie den Status der Controller und Fächer	20
Schritt 3: Validieren der Controller-Softwareversion	21

Controller

Erfahren Sie mehr über Upgrades von E-Series Controllern

Sie können ein Upgrade Ihres Storage-Arrays durch den Austausch vorhandener Controller durchführen.

Controller-Komponenten

Ein Controller besteht aus einer Hauptplatine, Firmware und Software. Sie steuert die Laufwerke und implementiert auch die Management Software-Funktionen.

Wann wird dieses Verfahren durchgeführt

In der Regel verwenden Sie diese Vorgehensweise, wenn Sie alle Controller auf ein anderes Modell oder eine andere Plattform aktualisieren möchten. Bei diesem Verfahren werden alle Controller in einem Controller-Laufwerksfach ausgetauscht

Sie können dieses Verfahren auch in folgenden Situationen verwenden:

- Wenn bei allen Controllern in einem Controller-Laufwerksfach ein Hardwarefehler auftreten und nicht mehr funktionsfähig ist.
- Um die zwei Inline-Speichermodule (DIMMs) in der Controller-Laufwerksfach zu aktualisieren, indem beide Controller durch dasselbe Controller-Modell ersetzt werden, jedoch durch unterschiedliche DIMMs.



Die HIC-Upgrade-Szenarien werden in diesem Verfahren nicht behandelt. Weitere Informationen finden Sie im HIC Verfahren zum Hinzufügen, Aktualisieren und Austauschen Ihres E-Series Systems.

Überlegungen zu Upgrades der E-Series

Lesen Sie vor dem Controller-Upgrade die folgenden Überlegungen durch.



In finden Sie "[E-Series Hardware im Überblick](#)" spezifische Informationen zu unterstützten Konfigurationen für jeden E-Series Controller.

Hardware- und Firmware-Anforderungen erfüllen

• Duplex- und Simplex-Controller-Upgrades

Bei Duplex-Controller-Laufwerkseinschüben ersetzen Sie beide Controller. Bei simplex-Controller-Laufwerkseinschüben ersetzen Sie den einen Controller. In beiden Fällen müssen Sie das Controller-Laufwerksfach ausschalten. Daher können Sie erst nach erfolgreichem Abschluss des Austauschs auf Daten auf dem Speicher-Array zugreifen.

• Fächer und Regale

Storage-Arrays mit einem E-Series Controller Shelf werden in der Regel über die Benutzeroberfläche von SANtricity System Manager gemanagt.

- **Controller-Batterien**

Ein neuer Controller wird ohne installierte Batterie geliefert. Wenn möglich, sollten Sie den Akku aus dem alten Controller entfernen und dann den Akku in den neuen Controller einsetzen. Bei einigen Controller-Upgrades ist der Akku des alten Controllers jedoch nicht mit dem neuen Controller kompatibel. In diesen Fällen müssen Sie einen Akku zusammen mit Ihrem neuen Controller bestellen und den Akku vor Beginn dieser Aufgaben zur Verfügung haben.

- **Synchronous Mirroring und Asynchronous Mirroring**

Wenn Ihr Storage-Array an synchroner Spiegelung teilnimmt, werden nur iSCSI- oder Fibre Channel-Verbindungen zwischen dem primären Standort und dem Remote-Standort unterstützt. Wenn die Konfiguration der Host Interface Card (HIC) in Ihren neuen Controllern keine iSCSI- oder Fibre Channel-Verbindungen umfasst, wird Synchronous Mirroring nicht unterstützt.

Für das asynchrone Spiegeln können auf dem lokalen Storage-Array und dem Remote-Storage-Array unterschiedliche Firmware-Versionen ausgeführt werden. Die unterstützte minimale Firmware-Version ist die SANtricity-Firmware-Version 7.84.



Bei E4000-Controllern wird Spiegelung nur über Fibre-Channel-Verbindungen unterstützt.

- **Speicherobjektgrenzen**

Wenn Sie Ihre Controller von Midrange- auf Einstiegsmodelle ändern (z. B. 5x00-Modelle in 2x00-Modelle), unterstützt Ihre neue Storage-Array-Konfiguration in der Speicherverwaltungssoftware eine geringere Anzahl von Speicherobjekten (z. B. Volumes) als Ihre alte Konfiguration. Sie müssen sicherstellen, dass Ihre alte Konfiguration die Storage-Objektgrenzen nicht überschreitet.

Weitere Informationen finden Sie unter "[Hardware Universe](#)".

- **Upgrade auf neuere Modelle**

Wenn Sie die Controller austauschen, um ein Upgrade auf ein neues Modell durchzuführen, sollten Sie beachten, dass Ihr aktuelles Storage Array möglicherweise über Premiumfunktionen verfügt, die das neue Modell nicht unterstützen kann.

Beim Upgrade des E-Series Controllers sollten Sie alle Premium-Funktionen des Storage-Arrays deaktivieren, die auf den neuen Controllern nicht unterstützt werden.

- **Bandinterne Verwaltung mit dem Access Volume**

- Der E4000 unterstützt keine bandinterne Verwaltung mit dem Access Volume.

Heben Sie vor dem Upgrade auf E4000-Controller die Zuordnung des Access Volumes zu allen definierten Hosts und Host-Clustern auf.

Upgrade-Kompatibilität

Unterstützte Upgrade-Pfade für jedes Storage-Array-Modell prüfen.

E4000-Controller-Upgrade-Kompatibilität

Upgrade-Pfad	Batterie	Funktionsunterstützung	SAS-3 Shelves
Von E2800 bis E4000	Bestellen Sie eine neue Batterie.	<ul style="list-style-type: none">• E4000 unterstützt kein ARVM iSCSI• E4000 Baseboard-Port funktioniert nur iSCSI und kann nicht zu FC geändert werden• E4000 kann nur 300 Laufwerke unterstützen• E4000 kann nur 512 Volumes unterstützen• E4000 unterstützt keine SAS-Konfigurationen• E4000 unterstützt keine Remote Storage Volumes• Der E4000 unterstützt keine bandinterne Verwaltung mit dem Access Volume.	E4000 Controller müssen SAS-3-Shelves verwenden.

Upgrade-Pfad	Batterie	Funktionsunterstützung	SAS-3 Shelves
Von E5700 bis E4000	Bestellen Sie eine neue Batterie.	<ul style="list-style-type: none"> • E4000 unterstützt kein ARVM iSCSI • E4000 Baseboard-Port funktioniert nur iSCSI und kann nicht zu FC geändert werden • E4000 kann nur 300 Laufwerke unterstützen <ul style="list-style-type: none"> ◦ E5700 unterstützt bis zu 480 Laufwerke • E4000 kann nur 512 Volumes unterstützen <ul style="list-style-type: none"> ◦ E5700 unterstützt bis zu 2048 Volumes • Die Unterstützung von InfiniBand-Host-Schnittstellenkarten ist nicht verfügbar • E4000 unterstützt keine SAS-Konfigurationen • E4000 unterstützt keine Remote Storage Volumes • Der E4000 unterstützt keine bandinterne Verwaltung mit dem Access Volume. 	E4000 Controller müssen SAS-3-Shelves verwenden.

Upgrade-Kompatibilität für EF600 und EF300 Controller

Upgrade-Pfad	Batterie	Funktionsunterstützung	SAS-3 Shelves
Von EF600 bis EF600 mit einer anderen Host-Schnittstellenkarte	Verwenden Sie die alte Batterie wieder.	<ul style="list-style-type: none"> • Keine Unterstützung von Thin Provisioning Volumes • Keine Unterstützung für synchrones Spiegeln 	Für EF600 Controller müssen SAS-3-Shelves verwendet werden.
Von EF300 bis EF600	Verwenden Sie die alte Batterie wieder.	<ul style="list-style-type: none"> • Keine Unterstützung von Thin Provisioning Volumes • Keine Unterstützung für synchrones Spiegeln 	Für EF600 Controller müssen SAS-3-Shelves verwendet werden.

Kompatibilität bei älteren Controller-Upgrades

Upgrade-Pfad	Batterie	Lieferanten-ID	Funktionsunterstützung	SAS-3 Shelves
Von E2x00 bis E2x00	Verwenden Sie die alte Batterie wieder.	Weitere Schritte erforderlich.	Ältere Snapshots werden auf der E2700 nicht unterstützt.	E2800 Controller dürfen nicht in SAS-2 Shelves integriert werden.

Upgrade-Pfad	Batterie	Lieferanten-ID	Funktionsunterstützung	SAS-3 Shelves
Von E2x00 bis E5X00	Bestellen Sie eine neue Batterie.	Beim Upgrade der E2600 auf E5500 oder E5600 oder beim Upgrade der E2700 auf E5400 sind weitere Schritte erforderlich.	<ul style="list-style-type: none"> • Ältere Snapshots werden auf der E5500 oder der E5600 nicht unterstützt. • Ältere Remote Volume-Spiegelung (RVM) wird auf dem E5500 oder E5600 nicht mit iSCSI-HICs unterstützt. • Data Assurance wird von E5500 oder E5600 mit iSCSI-HICs nicht unterstützt. • E5700 Controller dürfen nicht in SAS-2 Shelves platziert werden. 	Die Controller E5400, E5500 und E5600 dürfen nicht in SAS-3-Shelves platziert werden.
Von E5X00 bis E2x00	Bestellen Sie eine neue Batterie.	Beim Upgrade des E5500 oder der E5600 auf das E2600 oder beim Upgrade des E5400 auf das E2700 System sind weitere Schritte erforderlich.	Ältere Snapshots werden auf der E2700 nicht unterstützt.	5400-, E5500- und E5600-Controller dürfen nicht in SAS-3-Shelves platziert werden.

Upgrade-Pfad	Batterie	Lieferanten-ID	Funktionsunterstützung	SAS-3 Shelves
Von E5X00 bis E5X00	Verwenden Sie die alte Batterie wieder.	Weitere Schritte erforderlich beim Upgrade von E5400 auf E5500 oder E5600.	<ul style="list-style-type: none"> • Ältere Snapshots werden auf der E5500 oder der E5600 nicht unterstützt. • Ältere Remote Volume-Spiegelung (RVM) wird auf der E5400 oder E5500 mit iSCSI-HICs nicht unterstützt. • Data Assurance wird auf der E5400 oder E5500 mit iSCSI-HICs nicht unterstützt. • E5700 Controller dürfen nicht in SAS-2 Shelves platziert werden. 	Die Controller E5400, E5500 und E5600 dürfen nicht in SAS-3-Shelves platziert werden.
Von EF5x0 bis EF540	Verwenden Sie die alte Batterie wieder.	Weitere Schritte sind beim Upgrade von der EF540 auf die EF550 oder EF560 erforderlich.	<ul style="list-style-type: none"> • Keine alten Snapshots für EF550/EF560. • Keine Data Assurance für EF550/EF560 mit iSCSI • EF570 Controller dürfen nicht in SAS-3 Shelves integriert werden. 	Die Controller EF540, EF550 und EF560 dürfen nicht in SAS-3-Shelves platziert werden.

SAS-Gehäuse

Die E5700 unterstützt DE5600 und DE6600 SAS-2 Gehäuse über ein Head Upgrade. Wenn ein E5700 Controller in SAS-2-Gehäusen installiert ist, werden die Unterstützung der Basis-Host-Ports deaktiviert.

SAS-2-Shelfs	SAS-3 Shelves
<p>SAS-2-Shelves umfassen die folgenden Modelle:</p> <ul style="list-style-type: none"> • DE1600, DE5600 und DE6600 Laufwerksfächern • E5400, E5500 und E5600 Controller-Laufwerksfächer • EF540, EF550 und EF560 Flash-Arrays • E2600 und E2700 Controller-Laufwerksfächer 	<p>SAS-3-Shelves umfassen die folgenden Modelle:</p> <ul style="list-style-type: none"> • E4000 Controller-Shelfs • EF600 Controller-Shelfs ¹ • EF300 Controller-Shelfs ¹ • E2800 Controller-Shelfs • E5700 Controller-Shelfs • DE212C, DE224C, DE460C Festplatten-Shelfs

Hinweise:

1. EF600 und EF300 Controller können nur SAS-3-Shelfs als Erweiterung verwenden.

Investitionsschutz durch SAS-2 zu SAS-3

Sie können Ihr SAS-2-System neu konfigurieren, damit Sie es hinter einem neuen SAS-3 Controller-Shelf (E57XX/EF570/E28XX) verwenden können.



Für diese Vorgehensweise ist eine FPVR (Feature Product Variance Request) erforderlich. Wenn Sie eine FPVR-Datei einreichen möchten, wenden Sie sich an Ihr Vertriebsteam.

Vorbereitung für das Upgrade der E-Series Controller

Bereiten Sie das Upgrade von Controllern vor, indem Sie den Laufwerkssicherheitsschlüssel (falls verwendet) speichern, die Seriennummer aufzeichnen, Supportdaten sammeln, bestimmte Funktionen deaktivieren (falls verwendet) und den Controller offline schalten.



Das Sammeln von Support-Daten kann vorübergehend Auswirkungen auf die Performance Ihres Storage Arrays haben.

Schritte

1. Stellen Sie sicher, dass das vorhandene Speicherarray auf die neueste Version des Betriebssystems (Controller-Firmware) aktualisiert wird, die für Ihre aktuellen Controller verfügbar ist. Wählen Sie im SANtricity System Manager im Menü:Support[Upgrade Center], um Ihren Software- und Firmware-Bestand anzuzeigen.



Wenn Sie ein Upgrade auf Controller durchführen, die SANtricity OS Version 8.50 unterstützen, müssen Sie nach der Installation die neuesten Versionen von SANtricity OS und den neuesten NVSRAM installieren und die neuen Controller einschalten. Wenn Sie dieses Upgrade nicht durchführen, können Sie das Speicher-Array möglicherweise nicht für den automatischen Lastausgleich (ALB) konfigurieren.

2. Wenn Sie über sichere Laufwerke verfügen und einen vollständigen Austausch des Controllers planen, führen Sie die entsprechenden Schritte für Ihren Sicherheitstyp (intern oder extern) und den Laufwerksstatus in der folgenden Tabelle durch. Wenn Sie nicht * mit sicheren Laufwerken installiert

haben, können Sie diesen Schritt überspringen und mit Schritt 3 unter der Tabelle fortfahren.



Für einige Schritte in der Tabelle sind Befehle der Befehlszeilenschnittstelle (CLI) erforderlich. Informationen über die Verwendung dieser Befehle finden Sie im ["Referenz für Befehlszeilenschnittstelle"](#).

Sicherheitstyp und Kontext	Schritte
Internes Verschlüsselungsmanagement, ein oder mehrere Laufwerke sind gesperrt	Exportieren Sie die interne Sicherheitsschlüsseldatei an einen bekannten Speicherort auf dem Management-Client (das System mit einem Browser, der für den Zugriff auf System Manager verwendet wird). Verwenden Sie die <code>export storageArray securityKey</code> CLI-Befehl. Sie müssen den Passphrase angeben, der mit dem Sicherheitsschlüssel verknüpft ist, und den Speicherort angeben, an dem der Schlüssel gespeichert werden soll.

Sicherheitstyp und Kontext	Schritte
<p>Externes Verschlüsselungsmanagement, alle Laufwerke gesperrt. Sie können vorübergehend auf das interne Verschlüsselungsmanagement für den Austausch des Controllers (empfohlen) umsteigen.</p>	<p>Führen Sie die folgenden Schritte in der Reihenfolge aus:</p> <ol style="list-style-type: none"> Notieren Sie die Adresse und die Portnummer des externen KMS-Servers. Wählen Sie in System Manager Menü:Einstellungen[System > Sicherheitsschlüsselverwaltung > Einstellungen für Key Management Server anzeigen/bearbeiten]. Stellen Sie sicher, dass die Client- und Server-Zertifikate auf Ihrem lokalen Host verfügbar sind, damit sich das Speicherarray und der Schlüsselverwaltungsserver nach Abschluss des Controller-Austauschs gegenseitig authentifizieren können. Verwenden Sie die <code>save storageArray keyManagementCertificate</code> CLI-Befehl zum Speichern der Zertifikate. Stellen Sie sicher, dass Sie den Befehl zweimal, einmal mit dem ausführen <code>certificateType</code> Parameter auf gesetzt <code>client</code>, Und der andere mit dem Parameter auf gesetzt <code>server</code>. Wechseln Sie zu internem Verschlüsselungsmanagement, indem Sie den ausführen <code>disable storageArray externalKeyManagement</code> CLI-Befehl. Exportieren Sie die interne Sicherheitsschlüsseldatei an einen bekannten Speicherort auf dem Management-Client (das System mit einem Browser, der für den Zugriff auf System Manager verwendet wird). Verwenden Sie die <code>export storageArray securityKey</code> CLI-Befehl. Sie müssen den Passphrase angeben, der mit dem Sicherheitsschlüssel verknüpft ist, und den Speicherort angeben, an dem der Schlüssel gespeichert werden soll.
<p>Externes Verschlüsselungsmanagement, alle Laufwerke gesperrt, Sie können vorübergehend nicht auf ein internes Verschlüsselungsmanagement für den Austausch des Controllers umsteigen.</p>	<p>Wenden Sie Sich An Den Kundendienst.</p>
<p>Externes Verschlüsselungsmanagement, teilweise Laufwerke gesperrt</p>	<p>Es sind keine weiteren Schritte erforderlich.</p>



Ihr Speicher-Array muss sich im optimalen Zustand befinden, um Client- und Serverzertifikate abzurufen. Wenn die Zertifikate nicht abgerufen werden können, müssen Sie eine neue CSR erstellen, die CSR signieren lassen und das Serverzertifikat vom externen Schlüsselverwaltungsserver (EKMS) herunterladen.

3. Notieren Sie die Seriennummer für Ihr Speicher-Array:

- a. Wählen Sie in System Manager Menü:Support[Support Center > Registerkarte Support Resources].
- b. Scrollen Sie nach unten zu **Detaillierte Speicher-Array-Informationen** und wählen Sie dann **Storage-Array-Profil**.

Der Bericht wird auf Ihrem Bildschirm angezeigt.

- c. Um die Seriennummer des Gehäuses unter dem Profil des Speicherarrays zu finden, geben Sie **Seriennummer** in das Textfeld **Suchen** ein, und klicken Sie dann auf **Suchen**.

Alle übereinstimmenden Begriffe werden hervorgehoben. Um alle Ergebnisse nacheinander durchzublätern, klicken Sie mit * Suchen*.

- d. Erstellen Sie einen Eintrag des Chassis Serial Number.

Sie benötigen diese Seriennummer, um die Schritte in auszuführen ["Führen Sie das Controller-Upgrade durch"](#).

4. Sie können Support-Daten über Ihr Storage Array über die grafische Benutzeroberfläche oder die CLI erfassen:

- Verwenden Sie System Manager, um ein Supportpaket Ihres Speicherarrays zu sammeln und zu speichern.
 - Wählen Sie in System Manager im Menü:Support[Support Center > Registerkarte Diagnose]. Wählen Sie dann **Support-Daten sammeln** und klicken Sie auf **Collect**.

Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert support-data.7z.

Wenn Ihr Regal Schubladen enthält, werden die Diagnosedaten für dieses Shelf in einer separaten Datei mit dem Namen gezippt archiviert tray-component-state-capture.7z.

- Verwenden Sie die CLI, um die auszuführen `save storageArray supportData` Befehl zum Sammeln umfassender Support-Daten zum Storage Array.

5. Vergewissern Sie sich, dass keine I/O-Vorgänge zwischen dem Storage-Array und allen verbundenen Hosts auftreten:

- a. Beenden Sie alle Prozesse, die die LUNs umfassen, die den Hosts vom Storage zugeordnet sind.
- b. Stellen Sie sicher, dass keine Applikationen Daten auf LUNs schreiben, die vom Storage den Hosts zugeordnet sind.
- c. Heben Sie die Bereitstellung aller Dateisysteme auf, die mit den Volumes im Array verbunden sind, auf.



Die genauen Schritte zur Stoerung von Host-I/O-Vorgängen hängen vom Host-Betriebssystem und der Konfiguration ab, die den Umfang dieser Anweisungen übersteigen. Wenn Sie nicht sicher sind, wie Sie I/O-Vorgänge für Hosts in Ihrer Umgebung anhalten, sollten Sie das Herunterfahren des Hosts in Betracht ziehen.



Möglicher Datenverlust — Wenn Sie diesen Vorgang während der I/O-Vorgänge fortsetzen, können Sie Daten verlieren.

6. Wenn das Speicher-Array an einer Spiegelungsbeziehung beteiligt ist, beenden Sie alle Host-I/O-Vorgänge auf dem sekundären Storage Array.
7. Wenn Sie eine asynchrone oder synchrone Spiegelung verwenden, löschen Sie alle gespiegelten Paare und deaktivieren Sie irgendwelche Spiegelbeziehungen über den System Manager oder das Array Management-Fenster.
8. Wenn ein Thin Provisioning-Volume auf dem Host als Thin Volume gemeldet wird und auf dem alten Array Firmware (ab Version 8.25 Firmware) ausgeführt wird, die die UNMAP-Funktion unterstützt, deaktivieren Sie Write Back Caching für alle Thin Volumes:
 - a. Wählen Sie im System Manager Menü:Storage[Volumes] aus.
 - b. Wählen Sie ein beliebiges Volume aus, und wählen Sie dann Menü:Mehr[Cache-Einstellungen ändern].

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

- c. Wählen Sie die Registerkarte **Basic** und deaktivieren Sie die Einstellungen für Lese-Cache und Schreib-Cache.
 - d. Klicken Sie Auf **Speichern**.
 - e. Warten Sie fünf Minuten, bis alle Daten im Cache-Speicher auf die Festplatte gespeichert werden.
9. Wenn die Security Assertion Markup Language (SAML) auf dem Controller aktiviert ist, wenden Sie sich an den technischen Support, um die SAML-Authentifizierung zu deaktivieren.



Nachdem SAML aktiviert ist, können Sie sie nicht über die SANtricity System Manager-Schnittstelle deaktivieren. Wenden Sie sich an den technischen Support, um Hilfe zu erhalten, wenn Sie die SAML-Konfiguration deaktivieren möchten.

10. Warten Sie, bis alle laufenden Vorgänge abgeschlossen sind, bevor Sie mit dem nächsten Schritt fortfahren.
 - a. Wählen Sie auf der Seite **Home** des System Managers die Option **laufenden Betrieb anzeigen**.
 - b. Vergewissern Sie sich, dass alle im Fenster **laufenden Betrieb** angezeigten Vorgänge abgeschlossen sind, bevor Sie fortfahren.
11. Schalten Sie das Controller-Laufwerksfach aus

Warten Sie, bis alle LEDs am Controller-Laufwerksfach dunkel werden.

12. Schalten Sie die Stromversorgung für jedes Laufwerksfach aus, das mit dem Controller-Laufwerksfach verbunden ist

Warten Sie zwei Minuten, bis alle Laufwerke heruntergefahren sind.

Was kommt als Nächstes?

Gehen Sie zu "[Controller entfernen](#)".

Entfernen Sie die E-Series Controller

Nach der Vorbereitung der Aktualisierung können Sie die Controller entfernen und gegebenenfalls die Batterie entfernen.

Schritt 1: Controller entfernen

Entfernen Sie den Controller-Behälter, damit Sie ihn mit einem neuen aktualisieren können. Sie müssen alle Kabel trennen und alle SFP-Transceiver entfernen. Anschließend können Sie den Controller-Behälter aus dem Controller-Regal schieben.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- Ein ESD-Armband oder andere antistatische Vorsichtsmaßnahmen treffen.
- Etiketten, um jedes Kabel zu identifizieren, das mit dem Controller-Behälter verbunden ist.

Über diese Aufgabe

Führen Sie für jeden Controller im Fach für das Controller-Laufwerk die folgenden Schritte aus

Wenn Sie Controller in einem Duplex-Controller-Laufwerksfach aktualisieren, wiederholen Sie alle Schritte, um den zweiten Controller-Behälter zu entfernen.

Schritte

1. Setzen Sie ein ESD-Armband an oder ergreifen Sie andere antistatische Vorsichtsmaßnahmen.
2. Beschriften Sie jedes Kabel, das am alten Controller-Behälter befestigt ist. Je nach HIC-Konfiguration können Sie möglicherweise einige Kabel wieder anschließen, nachdem Sie den Controller-Behälter ersetzt haben.
3. Trennen Sie alle Schnittstellen- und Ethernet-Kabel vom alten Controller-Behälter.

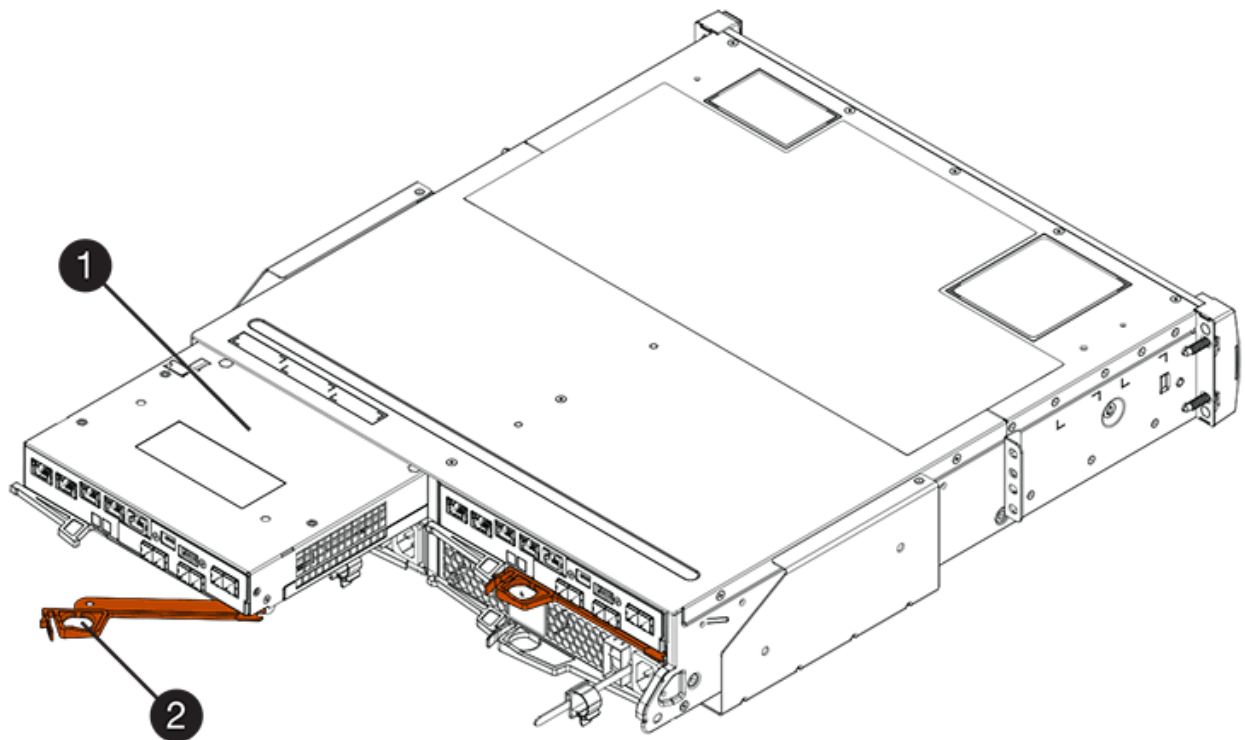
Wenn Glasfaserkabel vorhanden sind, können Sie den Controller-Behälter mit den beiden Freigabehebeln teilweise ausbauen. Durch das Öffnen dieser Freigabehebel lässt sich die Freigabelasche des Glasfaserkabels leichter herunterdrücken.



Um eine verminderte Leistung zu vermeiden, dürfen die Kabel nicht verdreht, gefaltet, gequetscht oder treten.

4. Wenn der alte Controller-Behälter eine Fibre-Channel-HIC oder eine InfiniBand-HIC enthält, entfernen Sie die SFP+-Transceiver (für Fibre Channel) oder Quad SFP (QSFP+) von der HIC und speichern Sie sie zur möglichen Wiederverwendung.
5. Controller A. entfernen
 - a. Entriegeln und drehen Sie die Entriegelungsgriffe heraus, um den Controller-Behälter zu lösen.
 - b. Ziehen Sie den Controller-Behälter mithilfe der Freigabegriffe und der Hände aus dem Controller-Laufwerksfach heraus

Die folgende Abbildung zeigt ein Beispiel für den allgemeinen Speicherort der Release-Griffe für Controller-Modelle. Controller Shelves und Controller-Laufwerksfächer verfügen über eine ähnliche Konfiguration für die Release-Griffe.



(1) *Controller-Behälter*

(2) *Cam Griff*

6. Stellen Sie den alten Controller-Behälter mit den Freigabehebeln auf eine flache, statische Oberfläche in der Nähe des Controller-Laufwerkfachs ein. Positionieren Sie den Controller-Behälter so, dass Sie auf die obere Abdeckung zugreifen können.
7. (Bedingt) Wenn Sie Controller in einem Duplex-Controller-Laufwerksfach aktualisieren, wiederholen Sie alle Schritte, um den zweiten Controller-Behälter zu entfernen.

Wenn Sie den Akku des alten Reglers in der neuen Steuerung verwenden möchten, gehen Sie zum nächsten Teil des Abschnitts; andernfalls gehen Sie zu ["Installieren Sie neue Controller"](#).

Schritt 2: Entfernen Sie den Akku

Entfernen Sie den Akku nur, wenn Sie beabsichtigen, den Akku aus dem alten Controller-Behälter im neuen Controller-Behälter zu verwenden.

Schritte

1. Drücken Sie die beiden Verriegelungsknöpfe der oberen Abdeckung am alten Controller-Behälter nach unten, und schieben Sie die obere Abdeckung nach hinten am Behälter.
2. Lösen Sie bei Ihrem Modell des Controller-Laufwerkfachs die Lasche, mit der der Akku am Controller-Aktivkohlebehälter befestigt ist, um den alten Akku freizugeben.
3. Entfernen Sie die Batterie, indem Sie sie zur Rückseite des alten Reglerkanisters schieben.

Was kommt als Nächstes?

Gehen Sie zu ["Installieren Sie neue Controller"](#).

Installation neuer E-Series Controller

Nachdem Sie die alten Controller entfernt haben, können Sie neue Controller in das Controller-Laufwerksfach installieren

Über diese Aufgabe

Führen Sie für jeden Controller im Fach für das Controller-Laufwerk die folgenden Schritte aus. Wenn Sie Controller in einem Duplex-Controller-Laufwerksfach aktualisieren, wiederholen Sie alle Schritte, um den zweiten Controller-Behälter zu installieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- Ein ESD-Armband oder andere antistatische Vorsichtsmaßnahmen treffen.
- Eine Batterie aus dem Original-Controller-Behälter oder ein neuer Akku, den Sie bestellt haben.
- Der neue Reglerbehälter.

Schritt 1: Batterie einbauen

Setzen Sie den Akku ein, den Sie aus dem ursprünglichen Controller-Behälter entfernt haben, oder einen neuen Akku, den Sie bestellt haben.

Schritte

1. Packen Sie den neuen Controller-Behälter aus, und stellen Sie ihn auf eine flache, statische Oberfläche, so dass die abnehmbare Abdeckung nach oben zeigt.
2. Drücken Sie die Abdeckungstaste nach unten, und schieben Sie die Abdeckung ab.
3. Richten Sie den Controller-Behälter so aus, dass der Steckplatz für die Batterie zu Ihnen zeigt.
4. Setzen Sie den Akku in den neuen Controller-Behälter ein.

Schieben Sie die Batterie in den Behälter, und achten Sie darauf, dass sie unterhalb der Niete an der Wand des neuen Kanisters bleibt.

- a. Halten Sie den Verriegelungsgriff in einem 45-Grad-Winkel, richten Sie die Stecker an der Unterseite der Batterie an den Anschlüssen am Behälter aus.
- b. Drücken Sie den Akku nach unten, bis er hörbar einrastet. Bewegen Sie den Verriegelungsgriff nach oben, um den Controller-Akku am Controller-Behälter zu befestigen.



Um sicherzustellen, dass der Controller-Akku korrekt in einem E5XX-Laufwerksfach eingesetzt wird, müssen Sie ihn möglicherweise herauschieben und erneut einsetzen. Es ist sicher, wenn Sie hören, dass es einrastet und wenn der Verriegelungsgriff sich nicht aus seiner aufrechten Position bewegt, wenn Sie ihn wackeln.

- c. Setzen Sie die obere Abdeckung des neuen Reglerkanisters wieder ein, indem Sie sie nach vorn schieben, bis die oberen Verriegelungsdeckel einrasten.

Wenn die Verriegelung einrastet, Haken unten an der Verriegelung in einen Metallschlitz am Gehäuse.

5. Drehen Sie den Controller-Behälter um, um zu bestätigen, dass der Akku ordnungsgemäß installiert ist.

Schritt 2: Installieren Sie den neuen Controller-Behälter

Setzen Sie den neuen Controller-Behälter in das Reglerregal ein.

Schritte

1. Schieben Sie den neuen Controller-Behälter vollständig in das Fach für das Controller-Laufwerk. Drehen Sie die Entriegelungsgriffe zur Mitte des Reglerbehälters, um ihn zu verriegeln.
2. Wenn Ihr neuer Controller-Behälter über eine Fibre-Channel-HIC oder eine InfiniBand-HIC verfügt, installieren Sie die SFP+-Transceiver (Fibre Channel) oder QSFP+-Transceiver (InfiniBand) in den Controller-Behälter und schließen Sie die Hostkabel wieder an.

Je nach den an Ihrem Upgrade beteiligten HICs können Sie SFP+ Transceiver oder QSFP+ Transceiver, die Sie aus Ihrem alten Controller-Behälter entfernt haben, wiederverwenden.

3. Schließen Sie alle Kabel wieder an das Controller-Laufwerksfach und die Laufwerksfächer an.

Wenn die Laufwerksverkabelung mit den alten Controllern identisch ist, können Sie die Etiketten, die Sie an den Kabeln angeschlossen haben, verwenden, um die Kabel ordnungsgemäß wiederherzustellen.

Was kommt als Nächstes?

Wenn die Laufwerksicherheit aktiviert ist, fahren Sie mit ["Entsperren von Laufwerken"](#) fort. Andernfalls gehen Sie zu ["Führen Sie das Controller-Upgrade durch"](#).

E-Series Laufwerke freischalten

Die Laufwerkssicherheitsfunktion für diese Controller sperrt die Laufwerke teilweise, extern oder intern. Wenn die Laufwerkssicherheitsfunktion aktiviert ist, müssen Sie diese Laufwerke manuell entsperren.

Befolgen Sie das entsprechende Verfahren für:

- [Internes Verschlüsselungsmanagement](#)
- [Externes Verschlüsselungskeymanagement](#)

Internes Verschlüsselungsmanagement

Führen Sie diese Schritte für das interne Verschlüsselungsmanagement aus, wenn alle Laufwerke gesperrt sind.

Über diese Aufgabe

Die neu getauschten Controller werden mit einem siebensegmentreichen Anzeigefeld von **L5** gesperrt. Diese Sperre tritt auf, wenn keine Laufwerke die Autocodierung (ACS) durchführen können. Nach dem Import des Sicherheitsschlüssels wird ACS die neuen Controller wieder aufgenommen und aktualisiert.



Wenn Sie Management-Port 1 nicht verwenden, versuchen Sie es mit anderen Standard-IP-Adressen: + Strg A Port 1: 169.254.128.101 + Strg A Port 2: 169.254.128.102 + Strg B Port 1: 169.254.128.101 + Strg B Port 2: 169.254.128.102

Schritte

1. Stellen Sie eine direkte, private ethernet-Verbindung zwischen dem Speicher-Array und dem Laptop oder

PC des SANtricity-Clients her. Dazu:

- a. Verwenden Sie ein RJ45-ethernet-Kabel, um den Laptop mit dem Verwaltungsport 1 an Controller A zu verbinden
 - b. Um die Verbindung abzuschließen, müssen Sie den Laptop möglicherweise einer IP-Adresse im selben Subnetz zuweisen wie Controller A. während der Controller-Sperrung wird Controller A standardmäßig auf die Managementadresse 169.254.128.101 gesetzt. Sie können den Laptop also einem Subnetz wie „169.254.128.201“ zuweisen.
2. Importieren Sie unter Verwendung der IP-Adresse 169.254.128.101 mit dem Benutzernamen **admin** und dem Passwort leer den internen Schlüssel mit dem `import storageArray securityKey file CLI`-Befehl, wobei der Sicherheitsschlüssel aus gespeichert ["Controller-Upgrades vorbereiten"](#) ist. Informationen zur Verwendung dieses Befehls finden Sie im ["Referenz für Befehlszeilenschnittstelle"](#).

Beispiel: `SMcli 169.254.128.101 -k -u admin -p "" -c "import storageArray securityKey file=\"Directory&FileName\" passPhrase=\"passPhraseString\";"`

Alternativ können Sie den internen Schlüssel über die Rest-API über den folgenden Aufruf importieren:
`/storage-systems/{system-id}/security-key/import`

Die Controller werden mit der Synchronisierung von Autocodes von den Laufwerken fortgesetzt und neu gestartet. Nach dem Neustart können die Controller über die ursprüngliche IP-Konfiguration aufgerufen werden.

Externes Verschlüsselungskeymanagement

Führen Sie diese Schritte für externes Verschlüsselungsmanagement aus, wenn alle Laufwerke gesperrt sind.

Über diese Aufgabe

Die neu getauschten Controller werden mit einem siebensegmentreichen Anzeigefeld von **L5** gesperrt. Diese Sperre tritt auf, wenn keine Laufwerke die Autocodierung (ACS) durchführen können. Nach dem Import des Sicherheitsschlüssels wird ACS die neuen Controller wieder aufgenommen und aktualisiert.

Schritte

1. Stellen Sie eine direkte, private ethernet-Verbindung zwischen dem Speicher-Array und dem Laptop oder PC des SANtricity-Clients her. Dazu:
 - a. Verwenden Sie ein RJ45-ethernet-Kabel, um den Laptop mit dem Verwaltungsport 1 an Controller A zu verbinden
 - b. Um die Verbindung abzuschließen, müssen Sie den Laptop möglicherweise einer IP-Adresse im selben Subnetz zuweisen wie Controller A. während der Controller-Sperrung wird Controller A standardmäßig auf die Managementadresse 169.254.128.101 gesetzt. Sie können den Laptop also einem Subnetz wie „169.254.128.201“ zuweisen.
2. ["Controller-Upgrades vorbereiten"](#) Importieren Sie den externen Schlüssel mit dem von gespeicherten Sicherheitsschlüssel in die IP-Adresse 169.254.128.101, wobei der Benutzername **admin** und das Passwort leer bleiben.

Beispiel: `SMcli 169.254.128.101 -k -u admin -p "" -c "import storageArray securityKey file=\"Directory&FileName\" passPhrase=\"passPhraseString\";"`

Alternativ können Sie den externen Schlüssel über die Rest-API über den folgenden Aufruf importieren:
`/storage-systems/{system-id}/security-key/import`

Die Controller werden mit der Synchronisierung von Autocodes von den Laufwerken fortgesetzt und neu gestartet. Nach dem Neustart können die Controller über die ursprüngliche IP-Konfiguration aufgerufen werden.

3. (Optional) bei Bedarf können die Laufwerke mit einem Rekeying neu coden, indem Sie die folgenden Schritte ausführen:

Beispiel: SMcli <original_controller_ip> -u admin -p "<original_array_password>"
-c "create storageArray securityKey" passPhrase="\passPhraseString\
file="\filename\";"

Abschließen des E-Series Controller-Upgrades

Führen Sie das Controller-Upgrade durch, indem Sie das Controller Shelf einschalten und die Controller-Softwareversion validieren. Anschließend können Sie Supportdaten erfassen und den Betrieb fortsetzen.

Wenn Sie Controller in einem Duplex-Controller-Laufwerksfach aktualisieren, wiederholen Sie alle Schritte, um das Upgrade für den zweiten Controller abzuschließen.


Schritt 1: Controller einschalten

Sie müssen das Controller-Shelf einschalten, um sicherzustellen, dass es ordnungsgemäß funktioniert.

Schritte

1. Schalten Sie den Netzschalter auf der Rückseite jedes Laufwerksfachs ein, das mit dem Controller-Laufwerksfach verbunden ist
2. Warten Sie zwei Minuten, bis die Laufwerke hochfahren.
3. Schalten Sie den Netzschalter auf der Rückseite des Controller-Laufwerksfachs ein
4. Warten Sie drei Minuten, bis der Einschaltvorgang abgeschlossen ist.
5. Wenn Sie einen vollständigen Controller-Austausch für E2800 oder E5700 Controller durchführen, fahren Sie je nach Sicherheitsszenario mit einem der folgenden Verfahren fort:

Den Austausch des Controllers abschließen	Verfahren und Voraussetzungen
Alle ungesicherten Laufwerke, weder externe noch interne Schlüsselverwaltung	Fahren Sie mit dem nächsten Schritt fort.

Den Austausch des Controllers abschließen	Verfahren und Voraussetzungen
Mischung aus gesicherten und ungesicherten Laufwerken, internes Schlüsselmanagement	<p>Sie müssen zunächst einen internen Sicherheitsschlüssel erstellen und dann den Sicherheitsschlüssel manuell importieren, um die gesicherten Laufwerke zu entsperren. Nachdem die Laufwerke entsperrt sind, können Sie auf die Laufwerke zugreifen.</p> <ol style="list-style-type: none"> Interner Sicherheitsschlüssel erstellen Der Controller kann durch internes Verschlüsselungsmanagement und ein oder mehrere gesicherte Laufwerke ausgetauscht werden Führen Sie den SMClient-Befehl aus, <code>set allDrives nativeState</code>. Warten Sie, bis beide Controller neu gebootet werden.
Alle gesicherten Laufwerke, internes Schlüsselmanagement	<p>Der Controller kann durch internes Verschlüsselungsmanagement und ein oder mehrere gesicherte Laufwerke ausgetauscht werden</p>
Mischung aus gesicherten und ungesicherten Laufwerken, External Key Management	<p>Fahren Sie mit dem nächsten Schritt fort.</p> <p>Nach dem Austausch des Controllers werden die Controller automatisch mit dem External Key Management Server resynchronisiert, sodass die Laufwerke entsperrt werden und auf sie zugegriffen werden kann.</p> <div data-bbox="873 1377 927 1434">  </div> <p>Wenn Sie einen Sperrcode für sieben Segmente erhalten 15 Nachdem Sie einen Controller-Austausch von gemischten gesicherten Laufwerken mit internem Verschlüsselungsmanagement durchgeführt haben, wenden Sie sich an den technischen Support.</p>

Den Austausch des Controllers abschließen	Verfahren und Voraussetzungen
Alle gesicherten Laufwerke, External Key Management, haben Sie vorübergehend zum internen Schlüsselmanagement für das Controller-Ersatzverfahren zurückgekehrt	<p>Sie müssen die gesicherten Laufwerke zuerst mithilfe des Verfahrens zur internen Schlüsselverwaltung entsperren. Nachdem die Laufwerke entsperrt sind, wechseln Sie zurück zur externen Schlüsselverwaltung, indem Sie einen neuen externen Sicherheitsschlüssel für das Speicherarray erstellen.</p> <ol style="list-style-type: none"> Der Controller kann durch internes Verschlüsselungsmanagement und ein oder mehrere gesicherte Laufwerke ausgetauscht werden Externen Sicherheitsschlüssel erstellen Führen Sie den SMClient-Befehl aus, <code>set allDrives nativeState</code>. Warten Sie, bis beide Controller neu gebootet werden.
Alle gesicherten Laufwerke, External Key Management, haben Sie nicht vorübergehend zur internen Schlüsselverwaltung für das Controller-Ersatzverfahren gewechselt	Controller-Swap mit externem Verschlüsselungsmanagement und allen gesicherten Laufwerken. Detaillierte Anweisungen finden Sie unter " Externes Verschlüsselungskeymanagement ".

Schritt 2: Überprüfen Sie den Status der Controller und Fächer

Sie können die LEDs und die Speicherverwaltungssoftware verwenden, um den Status Ihrer Controller und Fächer zu überprüfen.

Schritte

1. Schauen Sie sich die LEDs an Controller A an, um sicherzustellen, dass sie ordnungsgemäß gebootet werden.

Während des Neubootens werden die erforderlichen LEDs für den Host Link Service grün angezeigt.

Nachdem der Controller den Neustart erfolgreich abgeschlossen hat, können Sie den neuen Controller-Behälter mithilfe der Speicherverwaltungssoftware ermitteln.

2. Wenn eine der Service Action required LEDs des Controller-Laufwerksfachs *on* leuchtet oder wenn die LED für die Service-Aktion des Controllers *ON* leuchtet:
 - a. Prüfen Sie, ob der Controller-Behälter richtig eingesetzt wurde und alle Kabel richtig eingesetzt sind. Setzen Sie ggf. den Controller-Behälter wieder ein.
 - b. Überprüfen Sie die Action Action required LEDs des Controller-Laufwerksfachs und die Action-LED für den Controller-Service erneut. Wenn das Problem nicht behoben wird, wenden Sie sich an den technischen Support.
3. Wiederholen Sie für eine Duplexkonfiguration Schritt 1 bis Schritt 2 für Controller B
4. Überprüfen Sie mithilfe der LEDs und der Speicherverwaltungssoftware den Status aller Fächer im

Speicher-Array. Wenn eine Komponente einen Aufmerksamkeitsstatus benötigt, verwenden Sie den Recovery Guru, um Probleme zu beheben. Wenn das Problem nicht behoben wird, wenden Sie sich an den technischen Support.

Schritt 3: Validieren der Controller-Softwareversion

Sie müssen sicherstellen, dass Ihre neuen Controller mit dem richtigen Betriebssystem (Controller-Firmware) und NVSRAM ausgeführt werden.

Schritte

1. Wenn bei Ihrem Controller-Upgrade eine Protokolländerung (z. B. Fibre Channel zu iSCSI) vorgenommen wird und bereits Hosts für Ihr Storage Array definiert sind, verknüpfen Sie die neuen Host-Ports mit Ihren Hosts:

- a. Wählen Sie im System Manager Menü:Storage[Hosts] aus.
- b. Wählen Sie den Host aus, dem die Ports zugeordnet werden sollen, und klicken Sie dann auf **Einstellungen anzeigen/bearbeiten**.

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

- c. Klicken Sie auf die Registerkarte **Host Ports**.

Im Dialogfeld werden die aktuellen Host-Port-IDs angezeigt.

- d. Um die Informationen zur Host-Port-Kennung zu aktualisieren, die jedem Host zugeordnet sind, ersetzen Sie die Host-Port-IDs der alten Hostadapter durch die neuen Host-Port-IDs für den neuen Hostadapter.
- e. Wiederholen Sie Schritt d für jeden Host.
- f. Klicken Sie Auf **Speichern**.

Informationen über kompatible Hardware finden Sie im ["NetApp Interoperabilitätsmatrix"](#) Und das ["NetApp Hardware Universe"](#).

2. Wenn die Write Back-Cache-Speicherung für alle Thin-Volumes deaktiviert wurde, die sich auf den Headswap vorbereiten, aktivieren Sie das Write Back-Caching erneut.
 - a. Wählen Sie im System Manager Menü:Storage[Volumes] aus.
 - b. Wählen Sie ein beliebiges Volume aus, und wählen Sie dann Menü:Mehr[Cache-Einstellungen ändern].

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

- c. Wählen Sie die Registerkarte **Basic** und aktivieren Sie die Einstellungen für Lese-Caching und Schreib-Caching.
- d. Klicken Sie Auf **Speichern**.

3. Wenn SAML bei der Vorbereitung auf das Kopftausch deaktiviert wurde, aktivieren Sie SAML neu.
 - a. Wählen Sie im System Manager Menü:Einstellungen[Zugriffsverwaltung].
 - b. Wählen Sie die Registerkarte **SAML** aus, und befolgen Sie die Anweisungen auf der Seite.

4. Sie können Support-Daten über Ihr Storage Array über die grafische Benutzeroberfläche oder die CLI erfassen:

- Verwenden Sie System Manager, um ein Supportpaket Ihres Speicherarrays zu sammeln und zu speichern.
 - Wählen Sie in System Manager im Menü:Support[Support Center > Registerkarte Diagnose]. Wählen Sie dann **Support-Daten sammeln** und klicken Sie auf **Collect**.

Die Datei wird im Ordner Downloads für Ihren Browser mit dem Namen gespeichert support-data.7z.

Wenn Ihr Regal Schubladen enthält, werden die Diagnosedaten für dieses Shelf in einer separaten Datei mit dem Namen gezippt archiviert tray-component-state-capture.7z

- Verwenden Sie die CLI, um die auszuführen `save storageArray supportData` Befehl zum Sammeln umfassender Support-Daten zum Storage Array.



Das Sammeln von Support-Daten kann vorübergehend Auswirkungen auf die Performance Ihres Storage Arrays haben.

5. Benachrichtigen Sie den technischen Support von NetApp über die Änderungen, die Sie an der Konfiguration Ihres Storage-Arrays vorgenommen haben.

- Holen Sie sich die Seriennummer des in notierten Controller-Laufwerksfachs [Controller-Upgrades vorbereiten](#).
- Loggen Sie sich auf der NetApp Support Site unter ein "mysupport.netapp.com/eservice/assistant".
- Wählen Sie in der Dropdown-Liste unter **Kategorie 1** die Option **Produktregistrierung** aus.
- Geben Sie den folgenden Text in das Textfeld **Kommentare** ein und ersetzen Sie die Seriennummer Ihres Controller-Laufwerksfachs für die Seriennummer:

Please create alert against Serial Number: serial number. The alert name should be "E-Series Upgrade". The alert text should read as follows:

"Attention: The controllers in this system have been upgraded from the original configuration. Verify the controller configuration before ordering replacement controllers and notify dispatch that the system has been upgraded."

- Klicken Sie unten im Formular auf die Schaltfläche **Senden**.

Was kommt als Nächstes?

Das Controller Upgrade ist abgeschlossen und Sie können den normalen Betrieb wieder aufnehmen.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.