ASA r2 Dokumentation

ASA r2

NetApp
August 19, 2025

Inhalt

ASA r2 Dokumentation

Versionshinweise

Was ist neu in ONTAP 9.17.1 für ASA r2-Systeme

Informieren Sie sich über die neuen Funktionen in ONTAP 9.17.1 für ASA r2-Systeme.

SAN-Datenmigration

Aktualisieren	Beschreibung
"Unterstützung für die Datenmigration von einem Speichersystem eines Drittanbieters"	Die SAN-Datenmigration mit Foreign LUN Import (FLI) wird für ASA R2-Systeme unterstützt. Mit FLI können Sie Daten von einer LUN auf einem Speichersystem eines Drittanbieters auf ein ASA R2-System migrieren.

Datensicherung

Aktualisieren	Beschreibung
"Unterstützung für autonomen Ransomware-Schutz mit künstlicher Intelligenz (ARP/AI)"	ARP/AI kann auf ASA R2-Speichereinheiten aktiviert werden. ARP/AI bietet zusätzlichen Datenschutz, indem es potenzielle Ransomware-Angriffe ohne Lernphase erkennt und meldet.
"SnapMirror Active Sync-Unterstützung für NVMe-Protokolle"	SnapMirror Active Sync unterstützt VMware-Workloads mit NVMe/TCP- und NVMe/FC-Hostzugriff für ONTAP Cluster mit zwei Knoten. Die Unterstützung von VMware-Workloads für NVMe/TCP hängt von der Behebung der VMware-Fehler-ID TR1049746 ab.

Storage-Effizienz

Aktualisieren	Beschreibung
"Unterstützung für automatischen Workload-Ausgleich"	Um Leistung und Ressourcennutzung zu optimieren, werden Arbeitslasten automatisch zwischen den Knoten eines HA-Paares ausgeglichen.

Neuerungen in ONTAP 9.16.1 für ASA r2-Systeme

Erfahren Sie mehr über die neuen Funktionen in ONTAP 9.16.1 für ASA r2 Systeme.

Plattformen

Aktualisieren	Beschreibung
Plattformen	Die folgenden NetApp ASA r2-Systeme werden ab ONTAP 9.16.1 unterstützt. Diese Plattformen bieten eine einheitliche Hardware- und Softwarelösung, die eine vereinfachte Benutzererfahrung bietet, speziell für die Anforderungen von reinen SAN-Kunden. • ASA A50 • ASA A30 • ASA A20 • ASA C30

Datensicherung

Aktualisieren	Beschreibung
"Unterstützung der Verschlüsselungsmigration zwischen Schlüsselmanagern"	Wenn Sie vom integrierten ONTAP Schlüsselmanager zu einem externen Schlüsselmanager auf Cluster-Ebene wechseln, können Sie die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, um die Schlüssel problemlos von einem Schlüsselmanager auf den anderen zu migrieren.
"Unterstützung für hierarchische Consistency Groups"	Mithilfe von hierarchischen Konsistenzgruppen können Sie eine übergeordnete Konsistenzgruppe erstellen, die mehrere untergeordnete Konsistenzgruppen enthält. Dadurch wird die Datensicherung und das Management komplexer Datenstrukturen vereinfacht.

Protokollunterstützung

Aktualisieren	Beschreibung
"NVMe Unterstützung für symmetrisches aktiv/aktiv-Multipathing"	NVMe/FC und NVMe/TCP unterstützen jetzt symmetrische aktiv/aktiv-Architektur für Multipathing, sodass alle Pfade zwischen den Hosts und dem Storage aktiv/optimiert sind.

Storage-Effizienz

Aktualisieren	Beschreibung
"Unterstützung für eine automatische Ausbalancierung von Storage-Einheiten"	ONTAP balanciert die Storage-Einheiten automatisch über Ihre Storage-Verfügbarkeitszonen hinweg aus, um optimale Performance und Kapazitätsauslastung zu erzielen.
Der NVMe-Leerraum ist standardmäßig aktiviert	Space deallocation (auch „Hole Punching“ und „unmap“ genannt) ist standardmäßig für NVMe-Namespaces aktiviert. Space deallocation ermöglicht einem Host, nicht verwendete Blöcke aus Namespaces zu Zuordnung zu machen, um Speicherplatz zurückzugewinnen. Dadurch wird die gesamte Storage-Effizienz erheblich verbessert, insbesondere bei File-Systemen mit hohem Datenfluktuationsgrad.

Neuerungen in ONTAP 9.16.0 für ASA r2-Systeme

Erfahren Sie mehr über die neuen Funktionen in ONTAP 9.16.0 für ASA r2 Systeme.

Plattformen

Aktualisieren	Beschreibung
Plattformen	Die folgenden NetApp ASA r2-Systeme sind verfügbar. Diese Plattformen bieten eine einheitliche Hardware- und Softwarelösung, die eine vereinfachte Benutzererfahrung bietet, speziell für die Anforderungen von reinen SAN-Kunden. • ASA A1K • ASA A70 • ASA A90

System Manager

Aktualisieren	Beschreibung
"Optimierter Support für reine SAN-Kunden"	System Manager ist optimiert, um wichtige SAN-Funktionalität zu unterstützen, während gleichzeitig die Transparenz von Funktionen und Funktionen entfällt, die in SAN-Umgebungen nicht unterstützt werden.

Storage-Management

Aktualisieren	Beschreibung
"Vereinfachtes Storage-Management"	ASA r2-Systeme führen Storage-Einheiten mit Konsistenzgruppen ein, was das Storage-Management vereinfacht. • Eine *Storage unit* stellt Ihren SAN-Hosts Speicherplatz für Datenoperationen zur Verfügung. Eine Storage-Einheit bezieht sich auf eine LUN für SCSI-Hosts oder einen NVMe-Namespace für NVMe-Hosts. • *Eine Consistency Group* ist eine Sammlung von Speichereinheiten, die als eine Einheit verwaltet werden.

Datensicherheit

Aktualisieren	Beschreibung
"Onboard-Verschlüsselungsmanagement und Dual-Layer-Verschlüsselung"	ASA r2 Systeme unterstützen einen integrierten Schlüsselmanager und eine Dual-Layer-Verschlüsselung (Hardware und Software).

Änderungen an ONTAP-Limits und -Standardeinstellungen wirken sich auf ASA r2-Systeme aus

Erfahren Sie mehr über die Änderungen an Grenzwerten und Standardwerten für ASA r2-Systeme. NetApp bemüht sich darum, seinen Kunden die wichtigsten Änderungen bei Standard- und Grenzwertänderungen jeder ONTAP Version zu erläutern.

Änderungen an den ONTAP-Limits

Funktion	Begrenzungsänderung	In Freigabe geändert…
Nodes pro Cluster	Die maximale Anzahl an Nodes pro Cluster wurde von 2 auf 12 erhöht. Wenn Sie ONTAP 9.16.1 mit mehr als 2 Nodes in einem Cluster ausführen, können Sie nicht auf ONTAP 9.16.0 zurücksetzen.	ONTAP 9.16.1
Speichereinheiten	Die maximale Anzahl an Storage-Einheiten wird von 2500 pro HA-Paar auf 10,000 pro HA-Paar erhöht.	ONTAP 9.16.1

Los geht’s

Erfahren Sie mehr über ASA r2 Storage-Systeme

Die NetApp ASA r2 Systeme bieten eine einheitliche Hardware- und Softwarelösung, mit der eine vereinfachte Erfahrung speziell für die Anforderungen reiner SAN-Kunden erzielt wird.

Die folgenden ASA-Plattformen werden als ASA r2-Systeme klassifiziert:

- ASA A1K
- ASA A90
- ASA A70
- ASA A50
- ASA A30
- ASA A20
- ASA C30

ASA r2 Systeme unterstützen alle SAN-Protokolle (iSCSI, FC, NVMe/FC, NVMe/TCP). Die Protokolle iSCSI, FC, NVMe/FC und NVMe/TCP unterstützen die symmetrische aktiv/aktiv-Architektur für Multipathing, sodass alle Pfade zwischen Hosts und Storage aktiv/optimiert sind. Die iSCSI- und NVMe/TCP-Protokolle unterstützen direkte Pfade zwischen den Hosts und dem Storage.

Auf einem ASA r2 System sind ONTAP Software und System Manager optimiert, um die grundlegenden SAN-Funktionen zu unterstützen und gleichzeitig Funktionen zu entfernen, die in SAN-Umgebungen nicht unterstützt werden.

Bei ASA r2-Systemen werden Storage-Einheiten mit Konsistenzgruppen eingesetzt:

- Eine *Storage unit* stellt Ihren SAN-Hosts Speicherplatz für Datenoperationen zur Verfügung. Eine Storage-Einheit bezieht sich auf eine LUN für SCSI-Hosts oder einen NVMe-Namespace für NVMe-Hosts.
- *Eine Consistency Group* ist eine Sammlung von Speichereinheiten, die als eine Einheit verwaltet werden.

ASA r2-Systeme verwenden Speichereinheiten mit Konsistenzgruppen, um die Speicherverwaltung und den Datenschutz zu vereinfachen. Angenommen, Sie haben eine Datenbank, die aus 10 Speichereinheiten in einer Konsistenzgruppe besteht, und Sie müssen die gesamte Datenbank sichern. Anstatt jede Speichereinheit einzeln zu sichern, können Sie die gesamte Datenbank schützen, indem Sie die Konsistenzgruppe sichern.

Um Ihre Daten vor böswilligen Angriffen wie Diebstahl oder Ransomware zu schützen, unterstützen ASA r2-Systeme einen integrierten Schlüsselmanager, Dual-Layer-Verschlüsselung, Multi-Faktor-Authentifizierung und Multi-Admin-Verifizierung. Manipulationssichere Snapshots werden auch auf sekundären ASA r2-Systemen unterstützt.

ASA r2-Systeme unterstützen keine gemeinsame Verwendung von Clustern mit aktuellen ASA-, AFF- oder FAS-Systemen.

Finden Sie weitere Informationen

- Weitere Informationen zur Unterstützung und Einschränkungen von ASA r2-Systemen finden Sie im "NetApp Hardware Universe".

- Erfahren Sie mehr über "Den ASA r2 Systemen im Vergleich zu den ASA Systemen".
- Erfahren Sie mehr über die "NetApp ASA".

Schnellstart für ASA r2-Speichersysteme

Um Ihr ASA r2 System in Betrieb zu nehmen, installieren Sie Ihre Hardwarekomponenten, richten Ihren Cluster ein, richten den Datenzugriff von Ihren Hosts auf das Storage-System ein und stellen den Storage bereit.

1 **Installieren und richten Sie Ihre Hardware ein**

"Installieren und einrichten" Ihrem ASA r2 System installieren und dieses in Ihrer ONTAP Umgebung implementieren können.

2 **Richten Sie den Cluster ein**

Verwenden Sie System Manager, um Sie durch einen schnellen und einfachen Prozess zu führen"Richten Sie Ihren ONTAP-Cluster ein".

3 **Richten Sie den Datenzugriff ein**

"Verbinden Sie das ASA r2-System mit Ihren SAN-Clients".

4 **Bereitstellung von Storage**

"Bereitstellung von Storage" Um Ihren SAN-Clients Daten bereitzustellen.

Was kommt als Nächstes?

Sie können jetzt den System Manager verwenden, um Ihre Daten durch "Erstellen von Snapshots"zu schützen.

Installieren Sie Ihr ASA r2-System

Installations- und Setup-Workflow für ASA r2 Storage-Systeme

Zum Installieren und Konfigurieren des ASA r2 Systems überprüfen Sie die Hardwareanforderungen, bereiten den Standort vor, installieren und verkabeln die Hardwarekomponenten, schalten das System ein und richten den ONTAP-Cluster ein.

1 **"Überprüfen Sie die Anforderungen für die Hardwareinstallation"**

Überprüfen Sie die Hardwareanforderungen für die Installation Ihres ASA r2-Speichersystems.

2 **"Bereiten Sie die Installation des ASA r2-Speichersystems vor"**

Um die Installation Ihres ASA r2-Systems vorzubereiten, müssen Sie den Standort vorbereiten, die Umgebung

und die elektrischen Anforderungen prüfen und sicherstellen, dass genügend Rack-Platz vorhanden ist. Packen Sie dann das Gerät aus, vergleichen Sie dessen Inhalt mit dem Packzettel, und registrieren Sie die Hardware, um auf Support-Vorteile zuzugreifen.

3 **"Installieren Sie die Hardware für das ASA r2-Speichersystem"**

Um die Hardware zu installieren, installieren Sie die Schienenkits für Ihr Speichersystem und die Regale, und installieren und sichern Sie dann das Speichersystem im Schrank oder im Telco-Rack. Schieben Sie dann die Regale auf die Schienen. Schließen Sie schließlich die Kabelverwaltungsgeräte an der Rückseite des Speichersystems an, um die Kabelführung zu organisieren.

4 **"Die Controller und Storage Shelfs für das ASA r2 Storage-System verkabeln"**

Um die Hardware zu verkabeln, verbinden Sie zuerst die Storage Controller mit dem Netzwerk und anschließend die Controller mit den Storage-Shelfs.

5 **"Schalten Sie das ASA r2-Speichersystem ein"**

Schalten Sie vor dem Einschalten der Controller jedes NS224-Shelf ein und weisen Sie eine eindeutige Shelf-ID zu, damit jedes Shelf im Setup eindeutig identifiziert wird.

Installationsanforderungen für ASA r2-Speichersysteme

Überprüfen Sie die erforderlichen Geräte und die Vorsichtsmaßnahmen zum Anheben des ASA r2-Storage-Systems und der Storage-Shelfs.

Für die Installation erforderliche Ausrüstung

Zur Installation des ASA r2-Speichersystems benötigen Sie die folgenden Geräte und Tools.

- Zugriff auf einen Webbrowser zur Konfiguration des Speichersystems
- Band für elektrostatische Entladung (ESD)
- Taschenlampe
- Laptop oder Konsole mit USB-/serieller Verbindung
- Büroklammer oder Kugelschreiber mit schmaler Spitze zum Einstellen von Regalbehelf-IDs
- Kreuzschlitzschraubendreher #2

Vorsichtsmaßnahmen beim Anheben

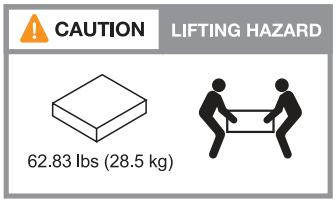
ASA r2 Storage-Systeme und Storage-Shelfs sind schwer. Gehen Sie beim Anheben und Bewegen dieser Gegenstände vorsichtig vor.

Gewichte des Storage-Systems

Treffen Sie die erforderlichen Vorsichtsmaßnahmen, wenn Sie Ihr ASA r2-Speichersystem bewegen oder anheben.

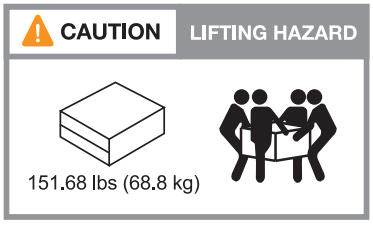
A1K

Ein ASA A1K Storage-System kann bis zu 28.5 kg (62.83 lbs) wiegen. Zum Anheben des Lagersystems zwei Personen oder einen Hydraulikhub verwenden.



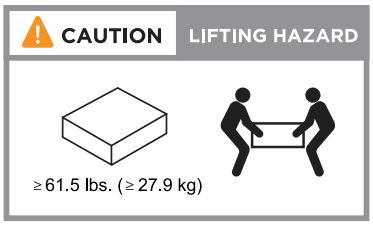
A70 und A90

Ein ASA A70 oder ASA A90 Storage-System kann bis zu 68.8 kg (151.68 lbs) wiegen. Zum Anheben des Lagersystems vier Personen oder einen Hydraulikhub verwenden.



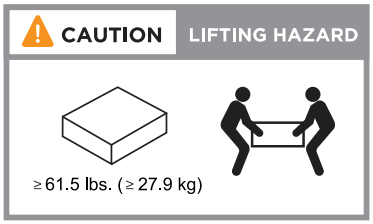
A20, A30 UND A50

Ein ASA A20, ASA A30 oder ASA A50 Storage-System kann bis zu 27.9 kg (61.5 lbs) wiegen. Zum Anheben des Lagersystems zwei Personen oder einen Hydraulikhub verwenden.



C30

Ein ASA C30 Storage-System kann bis zu 27.9 kg (61.5 lbs) wiegen. Zum Anheben des Lagersystems zwei Personen oder einen Hydraulikhub verwenden.

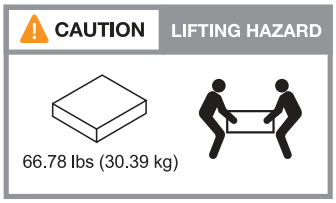


Gewicht des Lagerregals

Treffen Sie die erforderlichen Vorsichtsmaßnahmen, wenn Sie Ihr Regal bewegen oder anheben.

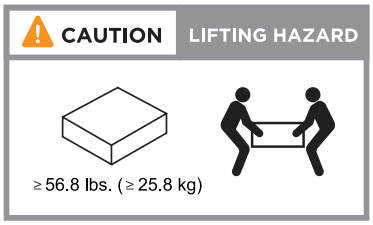
NS224-Shelf

Ein NS224-Einschub kann bis zu 30.29 kg (66.78 lbs) wiegen. Zum Anheben des Regals zwei Personen oder einen Hydraulikhub verwenden. Halten Sie alle Komponenten im Regal (vorne und hinten), um ein Ausbalancieren des Regalgewichts zu vermeiden.



NS224-Shelf mit NSM100B-Modulen

Ein NS224-Shelf mit NSM100B-Modulen kann bis zu 25.8 kg (56.8 lbs) wiegen. Zum Anheben des Regals zwei Personen oder einen Hydraulikhub verwenden. Halten Sie alle Komponenten im Regal (vorne und hinten), um ein Ausbalancieren des Regalgewichts zu vermeiden.



Verwandte Informationen

- "Sicherheitsinformationen und gesetzliche Hinweise"

Was kommt als Nächstes?

Nachdem Sie die Hardwareanforderungen überprüft haben, können Sie "Bereiten Sie die Installation Ihres ASA r2-Speichersystems vor".

Bereiten Sie die Installation eines ASA r2-Speichersystems vor

Bereiten Sie die Installation Ihres ASA r2-Speichersystems vor, indem Sie den Standort vorbereiten, die Kartons auspacken, den Inhalt der Kartons mit dem Packzettel vergleichen und das System registrieren, um auf die Supportvorteile zuzugreifen.

Schritt 1: Bereiten Sie den Standort vor

Um Ihr ASA r2-Speichersystem zu installieren, stellen Sie sicher, dass der Standort und der Schrank oder das Rack, den Sie verwenden möchten, den Spezifikationen für Ihre Konfiguration entsprechen.

Schritte

1. Mit "NetApp Hardware Universe" können Sie überprüfen, ob Ihr Standort die Umwelt- und elektrischen Anforderungen für Ihr Speichersystem erfüllt.
2. Stellen Sie sicher, dass Sie ausreichend Platz im Schrank oder Rack für Ihr Speichersystem, Ihre Regale und alle Switches haben:

A1K

- 4 HE in einer HA-Konfiguration
- 2 HE für jedes NS224 Storage-Shelf
- 1 HE für die meisten Switches

A70 und A90

- 4 HE in einer HA-Konfiguration
- 2 HE für jedes NS224 Storage-Shelf
- 1 HE für die meisten Switches

A20, A30 UND A50

- 2 HE für ein Storage-System
- 2 HE für jedes NS224 Storage-Shelf
- 1 HE für die meisten Switches

C30

- 2 HE für ein Storage-System
- 2 HE für jedes NS224 Storage-Shelf
- 1 HE für die meisten Switches

3. Installieren Sie alle erforderlichen Netzwerk-Switches.

   Installationsanweisungen und Kompatibilitätsinformationen finden Sie im "Switch-Dokumentation" "NetApp Hardware Universe" .

Schritt 2: Auspacken der Boxen

Nachdem Sie sichergestellt haben, dass der Standort und der Schrank oder das Rack, den Sie für Ihr ASA r2-Speichersystem verwenden möchten, die erforderlichen Spezifikationen erfüllen, packen Sie alle Kartons aus und vergleichen Sie den Inhalt mit den Artikeln auf dem Packzettel.

Schritte

1. Öffnen Sie sorgfältig alle Kartons und legen Sie den Inhalt in einer organisierten Art und Weise.
2. Vergleichen Sie den Inhalt, den Sie ausgepackt haben, mit der Liste auf dem Packzettel. Wenn Abweichungen auftreten, notieren Sie sie für weitere Maßnahmen.

   Sie können Ihre Packliste erhalten, indem Sie den QR-Code auf der Seite des Versandkartons scannen.

   Die folgenden Elemente sind einige der Inhalte, die Sie in den Feldern sehen können.

Hardware	* Kabel*	

• Blende • Storage-System • Schienensätze mit Anweisungen (optional) • Lagerregal (wenn Sie zusätzlichen Speicher bestellt haben)	• Management-Ethernet-Kabel (RJ-45-Kabel) • Netzwerkkabel • Stromkabel • Speicherkabel (wenn Sie zusätzlichen Speicher bestellt haben) • Serielles USB-C-Anschlusskabel	

Schritt 3: Registrieren Sie Ihr Storage-System

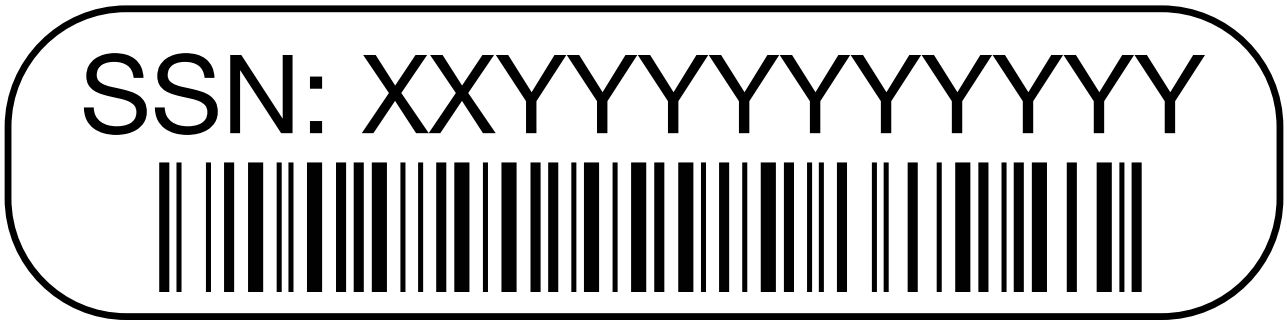
Nachdem Sie sichergestellt haben, dass Ihr Standort die Anforderungen für Ihre ASA r2 Storage-Systemspezifikationen erfüllt und überprüft haben, dass alle von Ihnen bestellten Teile vorhanden sind, sollten Sie Ihr System registrieren.

Schritte

1. Suchen Sie nach den Seriennummern für Ihr Storage-System.

   Die Seriennummern finden Sie an folgenden Stellen:

   - Auf dem Packzettel
   - In Ihrer Bestätigungs-E-Mail
   - Auf jedem Controller oder bei einigen Systemen auf dem Systemmanagementmodul jedes Controllers

2. Gehen Sie zum "NetApp Support-Website".
3. Ermitteln Sie, ob Sie Ihr Storage-System registrieren müssen:

Wenn Sie ein…	Führen Sie die folgenden Schritte aus…
Bestehender NetApp Kunde	a. Melden Sie sich mit Ihrem Benutzernamen und Passwort an. b. Wählen Sie **Systeme** > **Eigene Systeme**. c. Bestätigen Sie, dass die neue Seriennummer aufgeführt ist. d. Wenn die Seriennummer nicht aufgeführt ist, folgen Sie den Anweisungen für neue NetApp Kunden.

Wenn Sie ein…	Führen Sie die folgenden Schritte aus…
Neuer NetApp Kunde	a. Klicken Sie auf **Jetzt registrieren** und erstellen Sie ein Konto. b. Wählen Sie **Systeme** > **Systeme Registrieren**. c. Geben Sie die Seriennummer des Storage-Systems und die angeforderten Details ein. Nach der Registrierung können Sie die erforderliche Software herunterladen. Der Genehmigungsprozess kann bis zu 24 Stunden in Anspruch nehmen.

Was kommt als Nächstes?

Nachdem Sie die Installation Ihrer ASA r2-Hardware vorbereitet haben, können Sie "Installieren Sie die Hardware für Ihr ASA r2-Speichersystem".

Installieren Sie Ihr ASA r2-Speichersystem

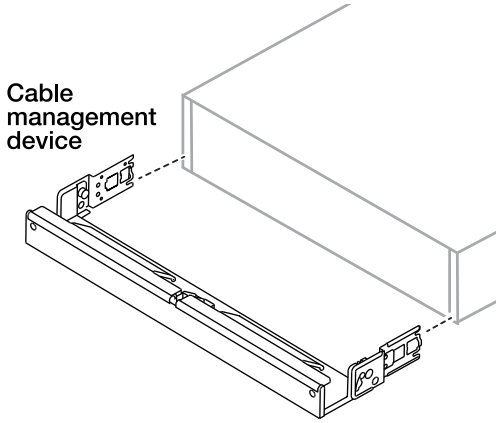
Nachdem Sie die Installation des ASA r2-Speichersystems vorbereitet haben, installieren Sie die Hardware für das System. Installieren Sie zunächst die Schienensätze. Installieren und sichern Sie dann Ihr Speichersystem in einem Schrank oder einem Telco-Rack.

Bevor Sie beginnen

- Stellen Sie sicher, dass die Anweisungen im Schienensatz enthalten sind.
- Beachten Sie die Sicherheitsbedenken im Zusammenhang mit dem Gewicht des Lagersystems und des Lagerregals.
- Stellen Sie fest, dass der Luftstrom durch das Speichersystem von der Vorderseite, an der die Blende oder die Endkappen installiert sind, einströmt und an der Rückseite, an der sich die Anschlüsse befinden, absaugt.

Schritte

1. Installieren Sie die Schienen-Kits für Ihr Speichersystem und die Lagerregale nach Bedarf gemäß den Anweisungen, die den Kits beiliegen.
2. Installieren und sichern Sie Ihr Speichersystem im Schrank oder im Telco-Rack:
   a. Positionieren Sie das Speichersystem auf den Schienen in der Mitte des Schranks oder des Telco-Racks, und stützen Sie das Speichersystem von unten ab, und schieben Sie es hinein.
   b. Stellen Sie sicher, dass die Führungsstifte am Schrank oder Telco-Rack sicher in die Führungsschlitze des Speichersystems passen.
   c. Befestigen Sie das Speichersystem mit den mitgelieferten Befestigungsschrauben am Schrank oder Telco-Rack.
3. Befestigen Sie die Blende an der Vorderseite des Speichersystems.
4. Wenn Ihr ASA r2-System mit einem Kabelverwaltungsgerät geliefert wurde, schließen Sie es an der Rückseite des Speichersystems an.



5. Installieren und befestigen Sie das Lagerregal:
   a. Positionieren Sie die Rückseite des Lagerregals auf den Schienen, und stützen Sie das Regal von unten ab, und schieben Sie es in den Schrank oder das Telco-Rack.

      Wenn Sie mehrere Storage-Shelfs installieren, platzieren Sie das erste Storage-Shelf direkt über den Controllern. Platzieren Sie das zweite Storage-Shelf direkt unter den Controllern. Wiederholen Sie dieses Muster für zusätzliche Storage-Shelfs.

   b. Befestigen Sie den Aufbewahrungs-Shelf mit den mitgelieferten Befestigungsschrauben am Schrank oder Telco-Rack.

Was kommt als Nächstes?

Nachdem Sie die Hardware für Ihr ASA r2-System installiert haben, können Sie "Verkabeln Sie die Controller und Storage Shelfs für Ihr ASA r2 System".

Verkabeln Sie die Hardware für Ihr ASA r2 Storage-System

Nachdem Sie die Rack-Hardware für das ASA r2 Storage-System installiert haben, installieren Sie die Netzwerkkabel für die Controller und verbinden Sie die Kabel zwischen den Controllern und Storage-Shelfs.

Bevor Sie beginnen

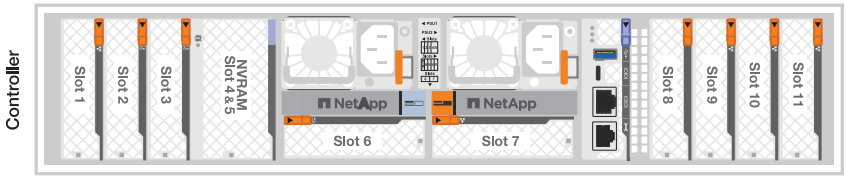
Wenden Sie sich an Ihren Netzwerkadministrator, um Informationen über das Anschließen des Speichersystems an die Netzwerk-Switches zu erhalten.

Über diese Aufgabe

- Diese Verfahren zeigen gängige Konfigurationen. Die jeweilige Verkabelung hängt von den für das Speichersystem bestellten Komponenten ab. Ausführliche Informationen zur Konfiguration und zur Steckplatzpriorität finden Sie unter "NetApp Hardware Universe".
- Die Verfahren zur Verkabelung von Cluster/HA und Host-Netzwerk zeigen gemeinsame Konfigurationen.

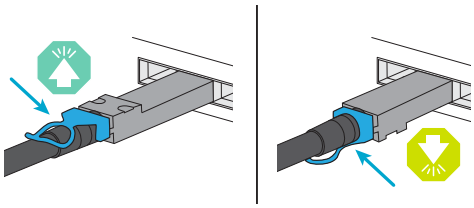
  Wenn Ihre Konfiguration in den Verkabelungsverfahren nicht angezeigt wird, gehen Sie zu "NetApp Hardware Universe" für umfassende Konfigurations- und Steckplatzprioritätsinformationen, um Ihr Speichersystem richtig zu verkabeln.

- Wenn Sie ein ASA A1K-, ASA A70- oder ASA A90-Speichersystem haben, sind die E/A-Steckplätze von 1 bis 11 nummeriert.



- Die Verkabelungsgrafiken haben Pfeilsymbole, die die richtige Ausrichtung (nach oben oder unten) des Kabelsteckers zeigen, wenn ein Anschluss in einen Anschluss eingesetzt wird.

  Wenn Sie den Anschluss einsetzen, sollten Sie das Gefühl haben, dass er einrasten kann. Wenn Sie nicht das Gefühl haben, dass er klickt, entfernen Sie ihn, drehen Sie ihn um und versuchen Sie es erneut.



- Wenn Sie eine Verkabelung zu einem optischen Switch vornehmen, stecken Sie den optischen Transceiver in den Controller-Port, bevor Sie ihn mit dem Switch-Port verbinden.

Schritt 1: Cluster/HA-Verbindungen verkabeln

Verkabeln Sie die Controller mit dem ONTAP-Cluster. Dieses Verfahren hängt von Ihrem Speichersystemmodell und Ihrer I/O-Modulkonfiguration ab.

Der Cluster-Interconnect-Verkehr und der HA Traffic nutzen dieselben physischen Ports.

A1K

Erstellen Sie die ONTAP-Cluster-Verbindungen. Bei Clustern ohne Switch verbinden Sie die Controller miteinander. Verbinden Sie bei geswitchten Clustern die Controller mit den Cluster-Netzwerk-Switches.

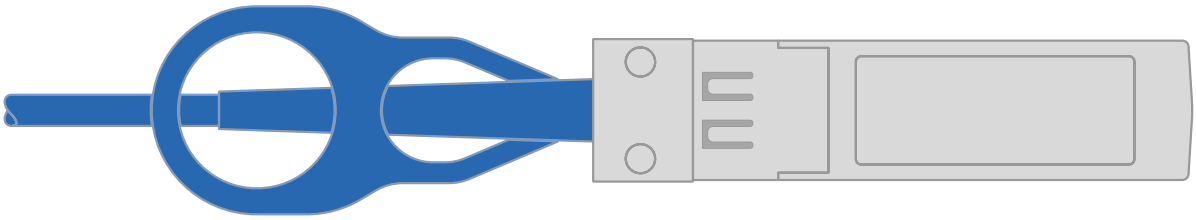
Cluster-Verkabelung ohne Switch

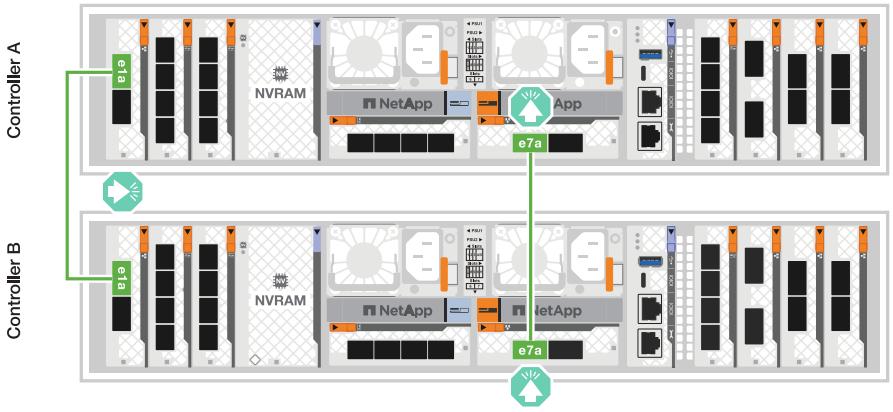
Verwenden Sie das Cluster/HA-Verbindungskabel, um die Ports e1a mit e1a und die Ports e7a mit e7a zu verbinden.

Schritte

1. Schließen Sie den Port e1a an Controller A an den Port e1a an Controller B. an
2. Verbinden Sie Port e7a an Controller A mit Port e1a an Controller B.

Cluster/HA Verbindungskabel





Switch-Cluster-Verkabelung

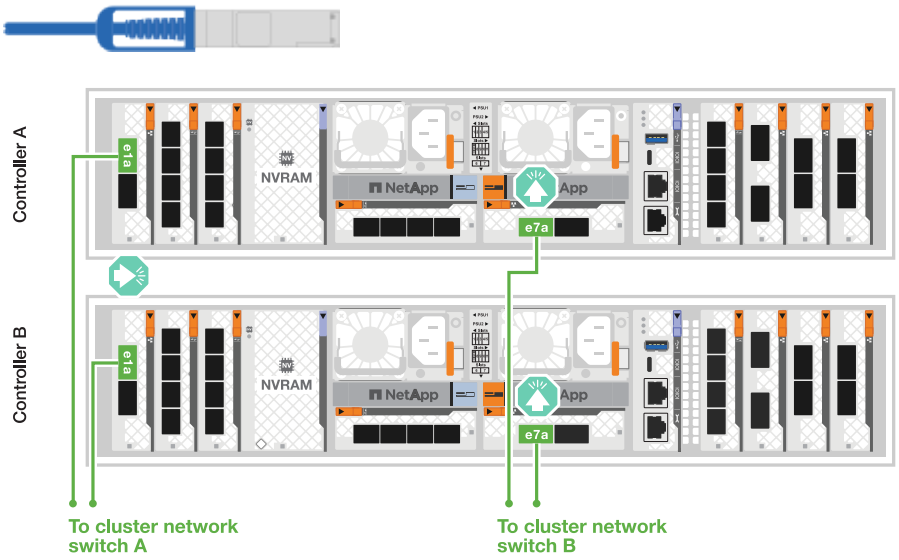
Verwenden Sie das 100-GbE-Kabel, um die Ports e1a an e1a und die Ports e7a an e7a anzuschließen.

Switched-Cluster-Konfigurationen werden ab 9.16.1 unterstützt.

Schritte

1. Verbinden Sie Port e1a an Controller A und Port e1a an Controller B mit Cluster-Netzwerk-Switch A.
2. Verbinden Sie Port e7a an Controller A und Port e7a an Controller B mit Cluster-Netzwerk-Switch B.

100-GbE-Kabel



A70 und A90

Erstellen Sie die ONTAP-Cluster-Verbindungen. Bei Clustern ohne Switch verbinden Sie die Controller miteinander. Verbinden Sie bei geswitchten Clustern die Controller mit den Cluster-Netzwerk-Switches.

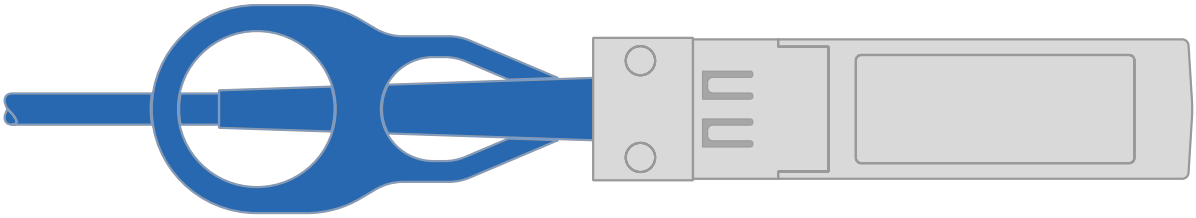
Cluster-Verkabelung ohne Switch

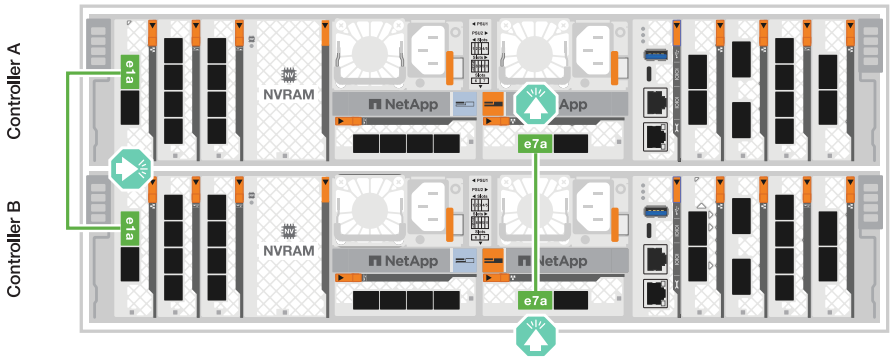
Verwenden Sie das Cluster/HA-Verbindungskabel, um die Ports e1a mit e1a und die Ports e7a mit e7a zu verbinden.

Schritte

1. Schließen Sie den Port e1a an Controller A an den Port e1a an Controller B. an
2. Verbinden Sie Port e7a an Controller A mit Port e1a an Controller B.

Cluster/HA Verbindungskabel





Switch-Cluster-Verkabelung

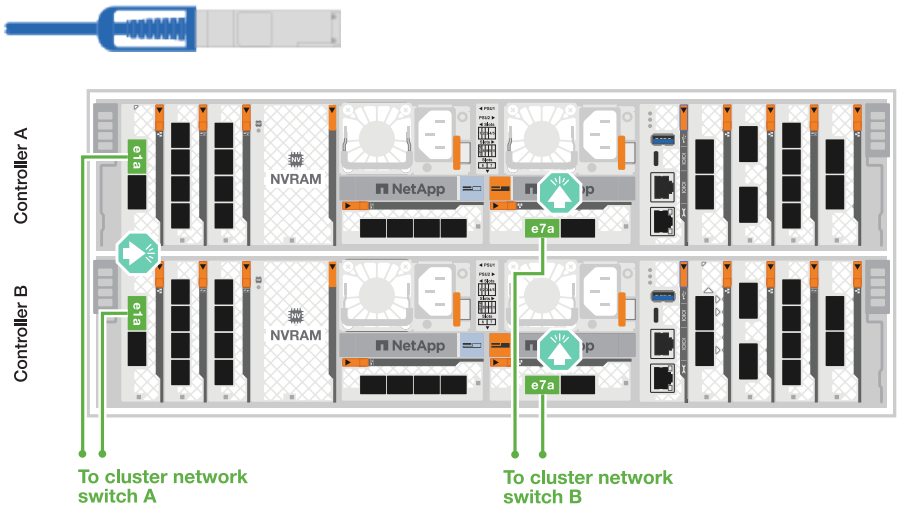
Verwenden Sie das 100-GbE-Kabel, um die Ports e1a an e1a und die Ports e7a an e7a anzuschließen.

Switched-Cluster-Konfigurationen werden ab 9.16.1 unterstützt.

Schritte

1. Verbinden Sie Port e1a an Controller A und Port e1a an Controller B mit Cluster-Netzwerk-Switch A.
2. Verbinden Sie Port e7a an Controller A und Port e7a an Controller B mit Cluster-Netzwerk-Switch B.

100-GbE-Kabel



A20, A30 UND A50

Erstellen Sie die ONTAP-Cluster-Verbindungen. Bei Clustern ohne Switch verbinden Sie die Controller miteinander. Verbinden Sie bei geswitchten Clustern die Controller mit den Cluster-Netzwerk-Switches.

Cluster-Verkabelung ohne Switches

Verbinden Sie die Controller miteinander, um die ONTAP-Cluster-Verbindungen zu erstellen.

ASA A30 und ASA A50 mit zwei 40/100-GbE-I/O-Modulen mit 2 Ports

Schritte

1. Verbinden Sie die Cluster/HA Interconnect-Verbindungen:

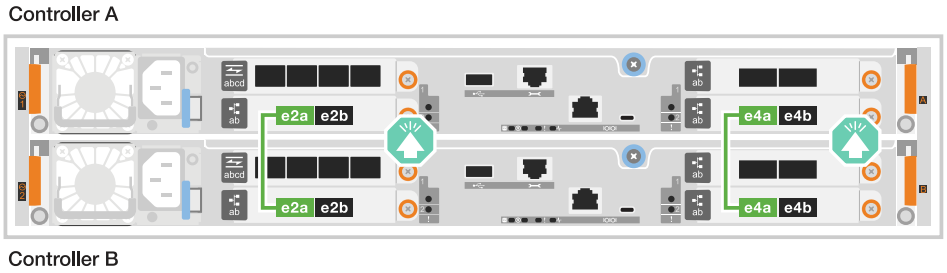
> Der Cluster-Interconnect-Verkehr und der HA Traffic nutzen dieselben physischen Ports (auf den I/O-Modulen in den Steckplätzen 2 und 4). Die Ports sind 40/100 GbE.

a. Controller A-Port e2a an Controller B-Port e2a anschließen.

b. Verbinden Sie den Controller A-Port e4a mit dem Controller B-Port e4a.

> Die I/O-Modulports e2b und e4b sind nicht verwendet und stehen für die Host-Netzwerk-Konnektivität zur Verfügung.

100 GbE Cluster/HA Interconnect-Kabel



ASA A30 und ASA A50 mit einem 40/100-GbE-I/O-Modul mit 2 Anschlüssen

Schritte

1. Verbinden Sie die Cluster/HA Interconnect-Verbindungen:

> Der Cluster-Interconnect-Verkehr und der HA-Verkehr teilen sich dieselben physischen Ports (auf dem I/O-Modul in Steckplatz 4). Die Ports sind 40/100 GbE.

a. Verbinden Sie den Controller A-Port e4a mit dem Controller B-Port e4a.

b. Verbinden Sie den Controller A-Port e4b mit dem Controller B-Port e4b.

100 GbE Cluster/HA Interconnect-Kabel

Controller A

Controller B

ASA A20 mit einem 10/25-GbE-I/O-Modul mit 2 Ports

Schritte

1. Verbinden Sie die Cluster/HA Interconnect-Verbindungen:

> Der Cluster-Interconnect-Verkehr und der HA-Verkehr teilen sich dieselben physischen Ports (auf dem I/O-Modul in Steckplatz 4). Die Ports sind 10/25 GbE.

a. Verbinden Sie den Controller A-Port e4a mit dem Controller B-Port e4a.

b. Verbinden Sie den Controller A-Port e4b mit dem Controller B-Port e4b.

25 GbE Cluster/HA Interconnect-Kabel

Controller A

Controller B

Switch-Cluster-Verkabelung

Verbinden Sie die Controller mit den Cluster-Netzwerk-Switches, um die ONTAP-Cluster-Verbindungen zu erstellen.

ASA A30 oder ASA A50 mit zwei 40/100-GbE-I/O-Modulen mit 2 Ports

Schritte

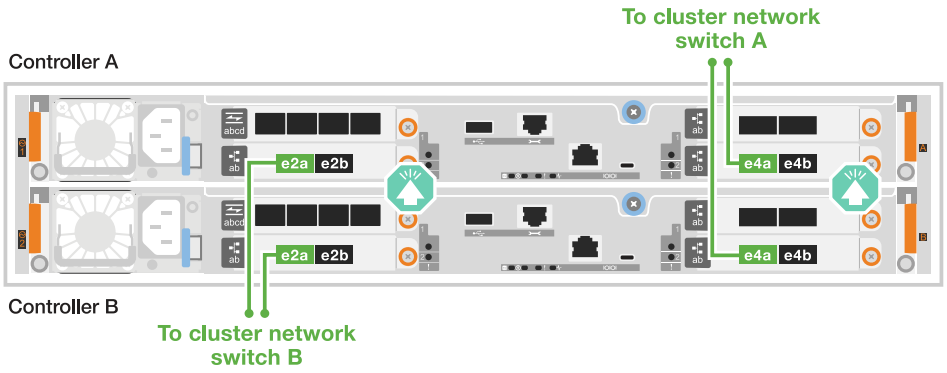
1. Verkabeln der Cluster/HA Interconnect-Verbindungen:

> Der Cluster-Interconnect-Verkehr und der HA Traffic nutzen dieselben physischen Ports (auf den I/O-Modulen in den Steckplätzen 2 und 4). Die Ports sind 40/100 GbE.

a. Verbinden Sie Port e4a des Controllers A mit dem Cluster-Netzwerk-Switch A.
b. Verbinden Sie Port e2a von Controller A mit Cluster-Netzwerk-Switch B.
c. Verbinden Sie Port e4a des Controllers B mit dem Cluster-Netzwerk-Switch A.
d. Verbinden Sie Port e2a des Controllers B mit dem Cluster-Netzwerk-Switch B.

> Die I/O-Modulports e2b und e4b sind nicht verwendet und stehen für die Host-Netzwerk-Konnektivität zur Verfügung.

40/100 GbE Cluster/HA Interconnect-Kabel



ASA A30 oder ASA A50 mit einem 40/100-GbE-I/O-Modul mit 2 Anschlüssen

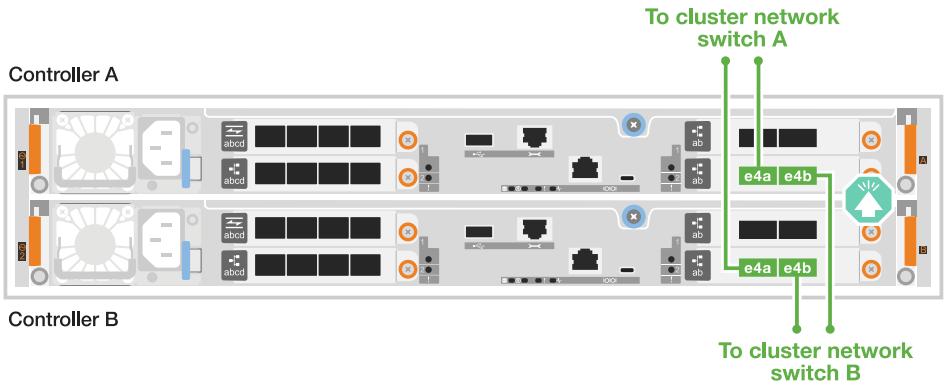
Schritte

1. Verkabeln Sie die Controller mit den Cluster-Netzwerk-Switches:

> Der Cluster-Interconnect-Verkehr und der HA-Verkehr teilen sich dieselben physischen Ports (auf dem I/O-Modul in Steckplatz 4). Die Ports sind 40/100 GbE.

a. Verbinden Sie Port e4a des Controllers A mit dem Cluster-Netzwerk-Switch A.
b. Verbinden Sie Port e4b von Controller A mit Cluster-Netzwerk-Switch B.
c. Verbinden Sie Port e4a des Controllers B mit dem Cluster-Netzwerk-Switch A.
d. Verbinden Sie Port e4b des Controllers B mit dem Cluster-Netzwerk-Switch B.

40/100 GbE Cluster/HA Interconnect-Kabel



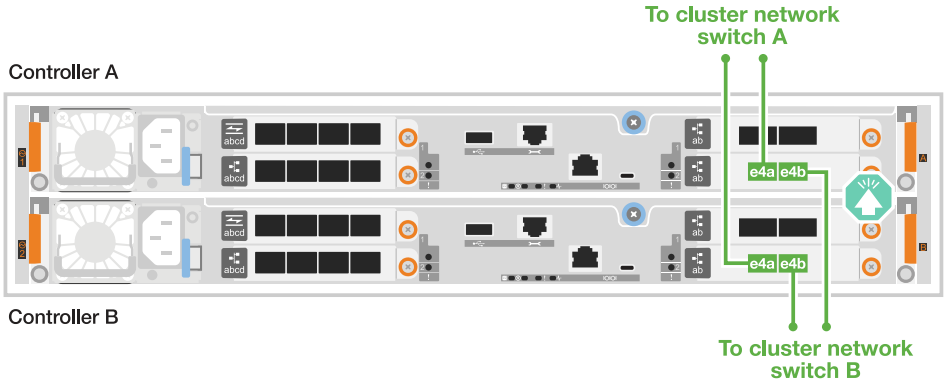
ASA A20 mit einem 10/25-GbE-I/O-Modul mit 2 Ports

1. Verkabeln Sie die Controller mit den Cluster-Netzwerk-Switches:

   Der Cluster-Interconnect-Verkehr und der HA-Verkehr teilen sich dieselben physischen Ports (auf dem I/O-Modul in Steckplatz 4). Die Ports sind 10/25 GbE.

   a. Verbinden Sie Port e4a des Controllers A mit dem Cluster-Netzwerk-Switch A.
   b. Verbinden Sie Port e4b von Controller A mit Cluster-Netzwerk-Switch B.
   c. Verbinden Sie Port e4a des Controllers B mit dem Cluster-Netzwerk-Switch A.
   d. Verbinden Sie Port e4b des Controllers B mit dem Cluster-Netzwerk-Switch B.

   10/25 GbE Cluster/HA Interconnect-Kabel



C30

Erstellen Sie die ONTAP-Cluster-Verbindungen. Bei Clustern ohne Switch verbinden Sie die Controller miteinander. Verbinden Sie bei geswitchten Clustern die Controller mit den Cluster-Netzwerk-Switches.

Cluster-Verkabelung ohne Switches

Verbinden Sie die Controller miteinander, um die ONTAP-Cluster-Verbindungen zu erstellen.

ASA C30 mit zwei 2-Port 40/100 GbE I/O-Modulen

Schritte

1. Verkabeln der Cluster/HA Interconnect-Verbindungen:

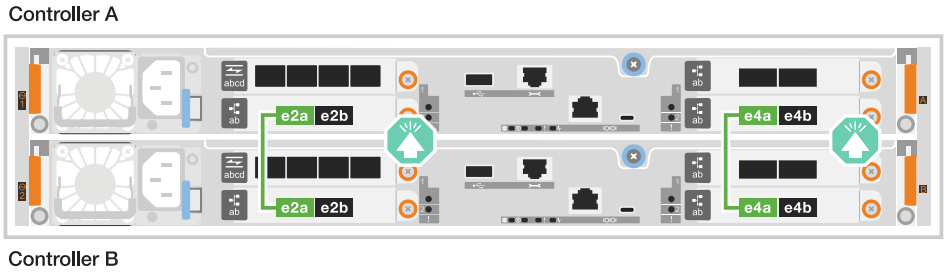
> Der Cluster-Interconnect-Verkehr und der HA Traffic nutzen dieselben physischen Ports (auf den I/O-Modulen in den Steckplätzen 2 und 4). Die Ports sind 40/100 GbE.

a. Controller A-Port e2a an Controller B-Port e2a anschließen.

b. Verbinden Sie den Controller A-Port e4a mit dem Controller B-Port e4a.

> Die I/O-Modulports e2b und e4b sind nicht verwendet und stehen für die Host-Netzwerk-Konnektivität zur Verfügung.

100 GbE Cluster/HA Interconnect-Kabel



ASA C30 mit einem 40/100-GbE-I/O-Modul mit 2 Ports

Schritte

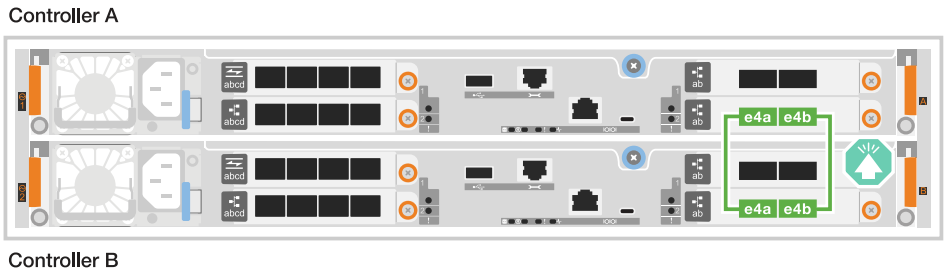
1. Verkabeln der Cluster/HA Interconnect-Verbindungen:

> Der Cluster-Interconnect-Verkehr und der HA-Verkehr teilen sich dieselben physischen Ports (auf dem I/O-Modul in Steckplatz 4). Die Ports sind 40/100 GbE.

   a. Verbinden Sie den Controller A-Port e4a mit dem Controller B-Port e4a.

   b. Verbinden Sie den Controller A-Port e4b mit dem Controller B-Port e4b.

100 GbE Cluster/HA Interconnect-Kabel



Switch-Cluster-Verkabelung

Verbinden Sie die Controller mit den Cluster-Netzwerk-Switches, um die ONTAP-Cluster-Verbindungen zu erstellen.

ASA C30 mit zwei 2-Port 40/100 GbE I/O-Modulen

Schritte

1. Verkabeln der Cluster/HA Interconnect-Verbindungen:

> Der Cluster-Interconnect-Verkehr und der HA Traffic nutzen dieselben physischen Ports (auf den I/O-Modulen in den Steckplätzen 2 und 4). Die Ports sind 40/100 GbE.

a. Verbinden Sie Port e4a des Controllers A mit dem Cluster-Netzwerk-Switch A.

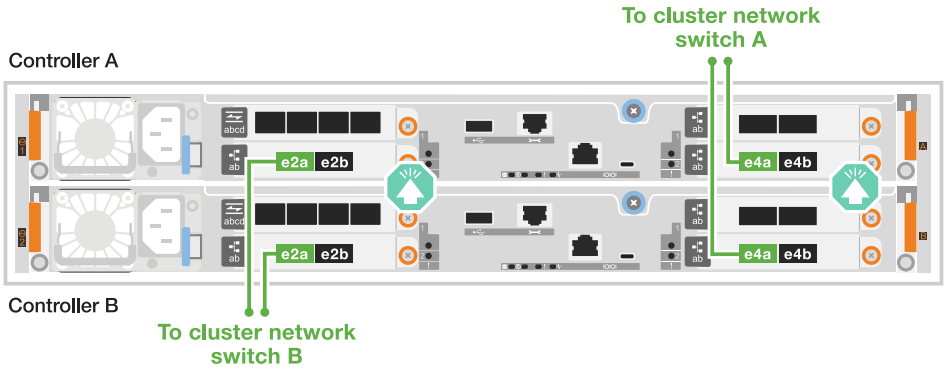
b. Verbinden Sie Port e2a von Controller A mit Cluster-Netzwerk-Switch B.

c. Verbinden Sie Port e4a des Controllers B mit dem Cluster-Netzwerk-Switch A.

d. Verbinden Sie Port e2a des Controllers B mit dem Cluster-Netzwerk-Switch B.

> Die I/O-Modulports e2b und e4b sind nicht verwendet und stehen für die Host-Netzwerk-Konnektivität zur Verfügung.

40/100 GbE Cluster/HA Interconnect-Kabel



ASA C30 mit einem 40/100-GbE-I/O-Modul mit 2 Ports

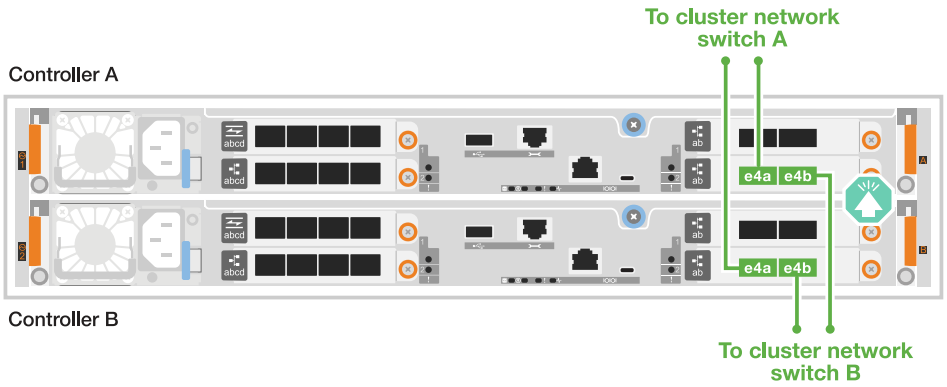
Schritte

1. Verbinden Sie die Controller mit den Cluster-Netzwerk-Switches:

> Der Cluster-Interconnect-Verkehr und der HA-Verkehr teilen sich dieselben physischen Ports (auf dem I/O-Modul in Steckplatz 4). Die Ports sind 40/100 GbE.

a. Verbinden Sie Port e4a des Controllers A mit dem Cluster-Netzwerk-Switch A.
b. Verbinden Sie Port e4b von Controller A mit Cluster-Netzwerk-Switch B.
c. Verbinden Sie Port e4a des Controllers B mit dem Cluster-Netzwerk-Switch A.
d. Verbinden Sie Port e4b des Controllers B mit dem Cluster-Netzwerk-Switch B.

40/100 GbE Cluster/HA Interconnect-Kabel



Schritt 2: Verkabeln Sie die Host-Netzwerkverbindungen

Verbinden Sie die Controller mit Ihrem Host-Netzwerk.

Dieses Verfahren hängt von Ihrem Speichersystemmodell und Ihrer I/O-Modulkonfiguration ab.

A1K

Verbinden Sie die Ethernet-Modulports mit Ihrem Hostnetzwerk.

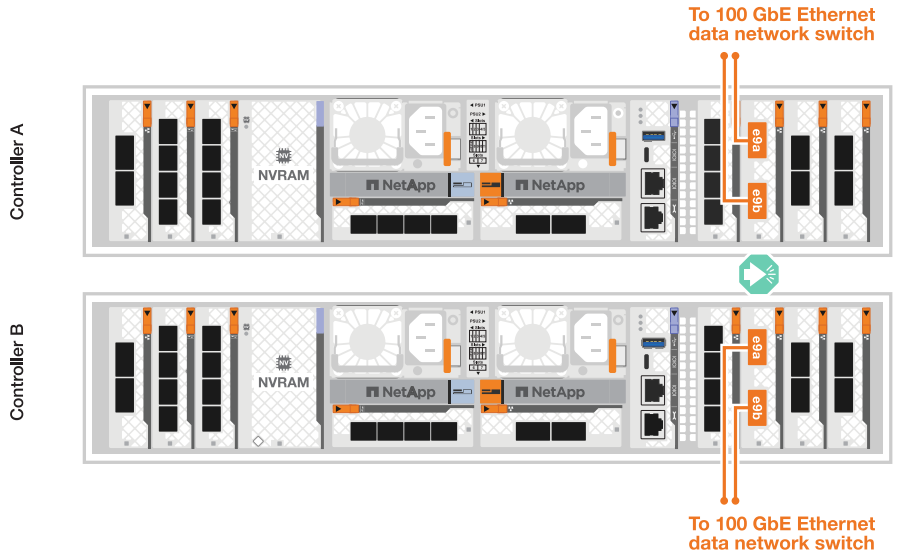
Im Folgenden finden Sie einige typische Beispiele für eine Verkabelung im Host-Netzwerk. Informationen zu Ihrer spezifischen Systemkonfiguration finden Sie unter "NetApp Hardware Universe" .

Schritte

1. Verbinden Sie die Ports e9a und e9b mit dem Ethernet-Datennetzwerk-Switch.

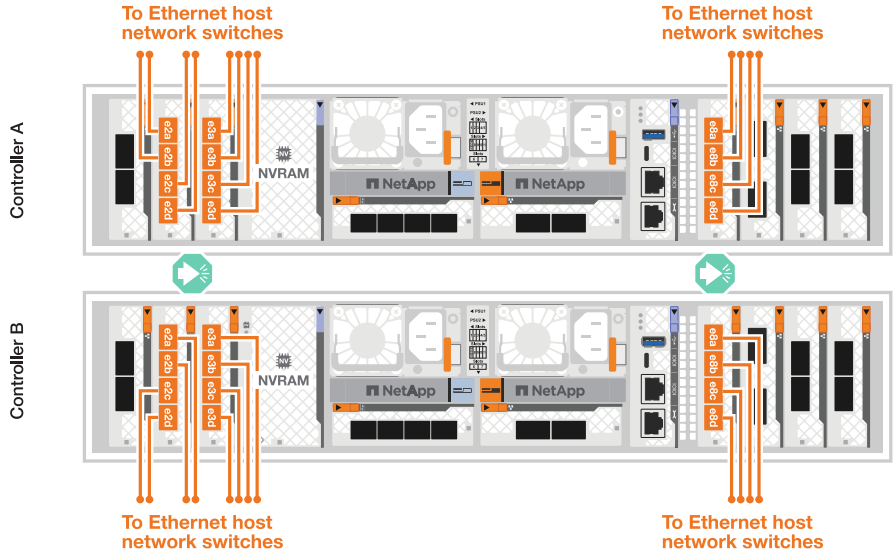
> Verwenden Sie für maximale Systemperformance für Cluster- und HA-Datenverkehr die Ports e1b und e7b nicht für Host-Netzwerkverbindungen. Verwenden Sie eine separate Hostkarte, um die Leistung zu maximieren.

100-GbE-Kabel



2. Verbinden Sie Ihre 10/25 GbE Host-Netzwerk-Switches.

10/25 GbE Host



A70 und A90

Verbinden Sie die Ethernet-Modulports mit Ihrem Hostnetzwerk.

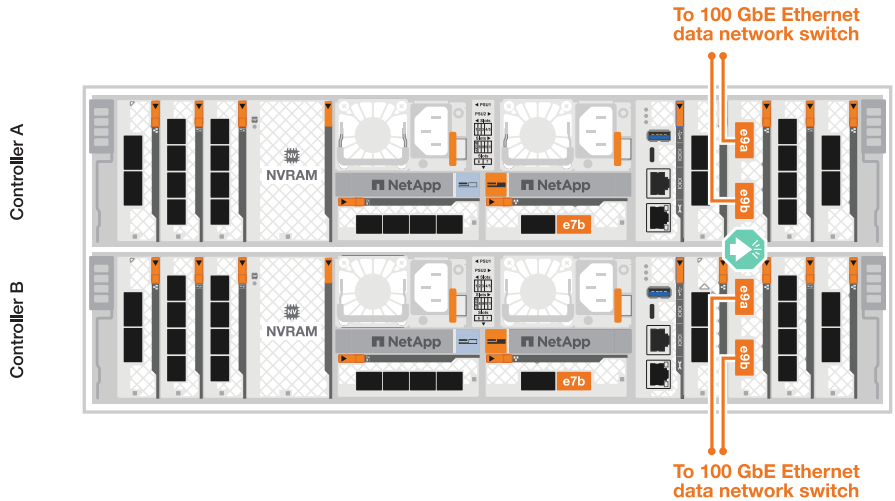
Im Folgenden finden Sie einige typische Beispiele für eine Verkabelung im Host-Netzwerk. Informationen zu Ihrer spezifischen Systemkonfiguration finden Sie unter "NetApp Hardware Universe" .

Schritte

1. Verbinden Sie die Ports e9a und e9b mit dem Ethernet-Datennetzwerk-Switch.

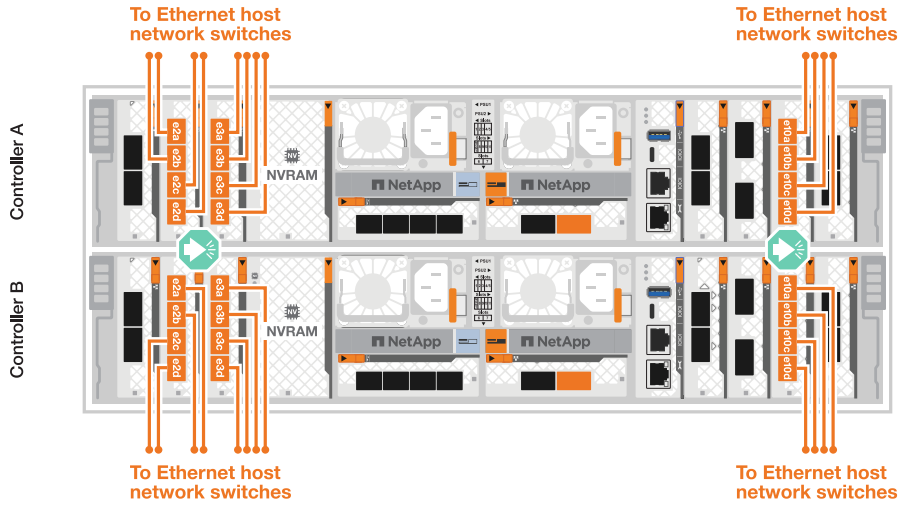
> Verwenden Sie für maximale Systemperformance für Cluster- und HA-Datenverkehr die Ports e1b und e7b nicht für Host-Netzwerkverbindungen. Verwenden Sie eine separate Hostkarte, um die Leistung zu maximieren.

100-GbE-Kabel



2. Verbinden Sie Ihre 10/25 GbE Host-Netzwerk-Switches.

4 Ports, 10/25 GbE Host



A20, A30 UND A50

Verbinden Sie die Ethernet-Modulports oder die Fibre-Channel-Modulports (FC) mit Ihrem Hostnetzwerk.

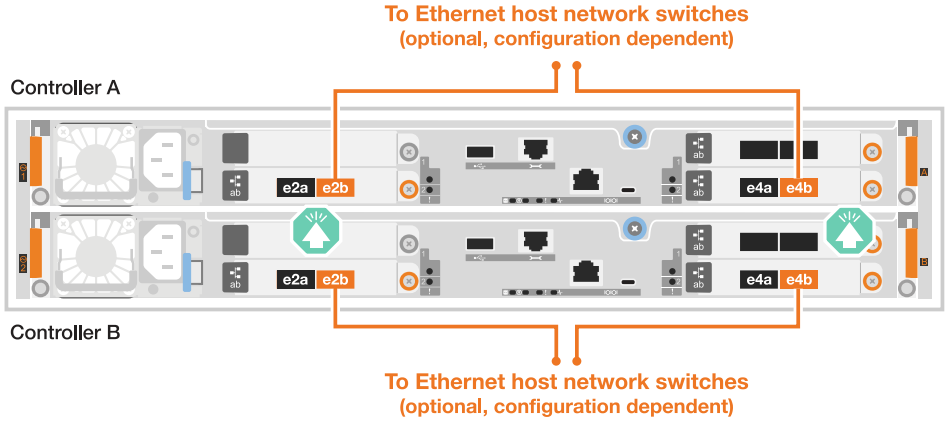
Ethernet-Host-Verkabelung

ASA A30 und ASA A50 mit zwei 40/100-GbE-I/O-Modulen mit 2 Ports

Verbinden Sie an jedem Controller die Ports e2b und e4b mit den Ethernet-Host-Netzwerk-Switches.

Die Ports an E/A-Modulen in Steckplatz 2 und 4 sind 40/100 GbE (Host-Konnektivität ist 40/100 GbE).

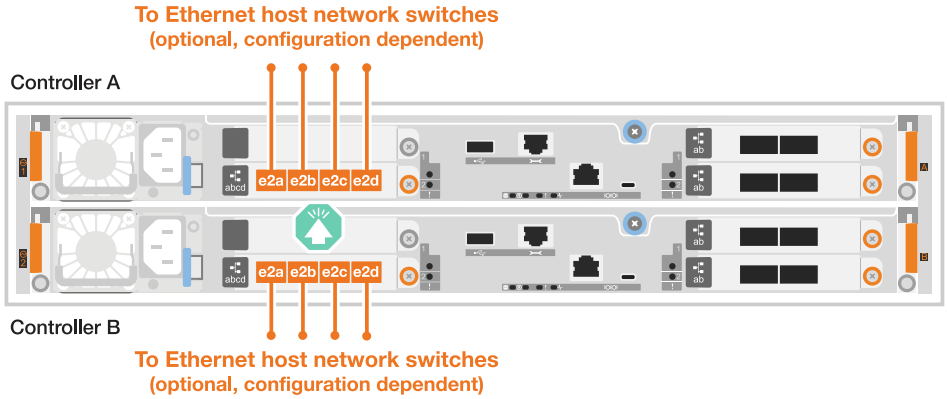
40/100-GbE-Kabel



ASA A20, A30 und A50 mit einem 4-Port 10/25 GbE I/O-Modul

Verbinden Sie auf jedem Controller die Ports e2a, e2b, e2c und e2d mit den Ethernet-Host-Netzwerk-Switches.

10/25-GbE-Kabel

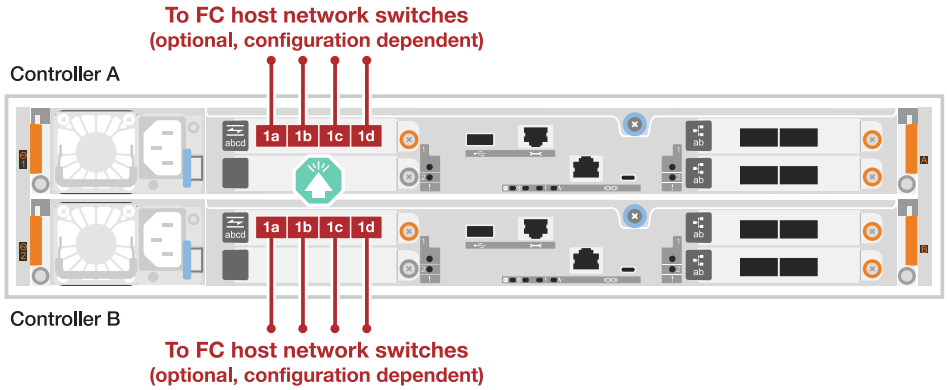


FC-Hostverkabelung

ASA A20, A30 und A50 mit einem 4-Port 64 Gb/s FC I/O-Modul

Verbinden Sie auf jedem Controller die Ports 1a, 1b, 1c und 1d mit den FC-Host-Netzwerk-Switches.

64 Gbit/s FC-Kabel



C30

Verbinden Sie die Ethernet-Modulports oder die Fibre-Channel-Modulports (FC) mit Ihrem Hostnetzwerk.

Ethernet-Host-Verkabelung

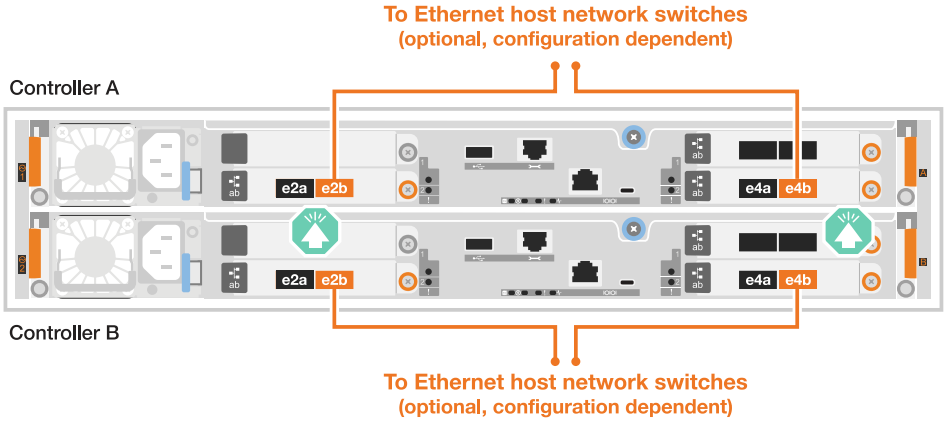
ASA C30 mit zwei 2-Port 40/100 GbE I/O-Modulen

Schritte

1. Verbinden Sie an jedem Controller die Ports e2b und e4b mit den Ethernet-Host-Netzwerk-Switches.

> Die Ports an E/A-Modulen in Steckplatz 2 und 4 sind 40/100 GbE (Host-Konnektivität ist 40/100 GbE).

40/100-GbE-Kabel

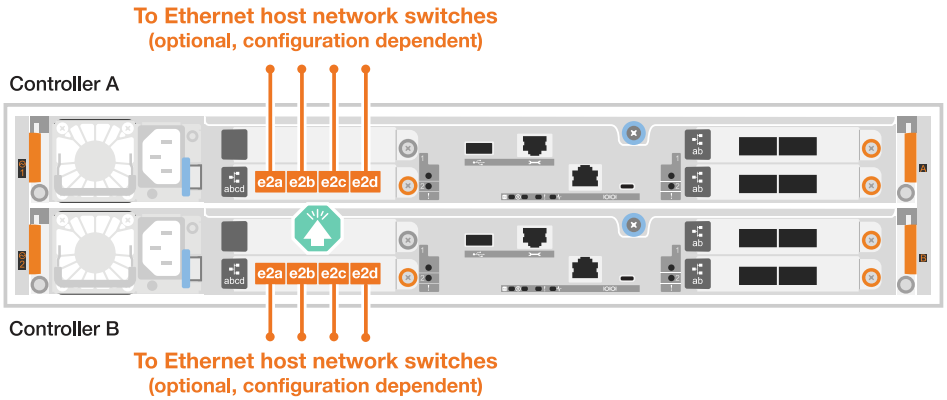


ASA C30 mit einem 10/25-GbE-I/O-Modul mit 4 Ports

Schritte

1. Verkabeln Sie bei jedem Controller die Ports e2a, e2b, e2c und e2d mit den Ethernet-Host-Netzwerk-Switches.

10/25-GbE-Kabel

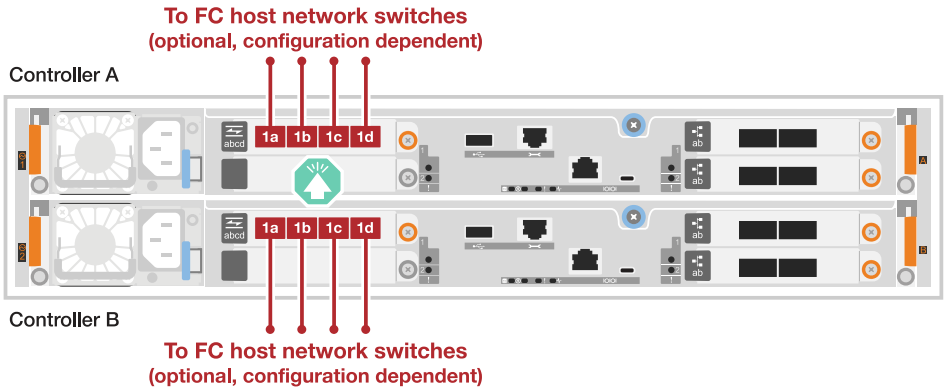


ASA C30 mit einem 4-Port 64 Gb/s FC I/O-Modul

Schritte

1. Verkabeln Sie an jedem Controller die Ports 1a, 1b, 1c und 1d mit den FC-Host-Netzwerk-Switches.

64 Gbit/s FC-Kabel



Schritt 3: Verkabelung der Management-Netzwerkverbindungen

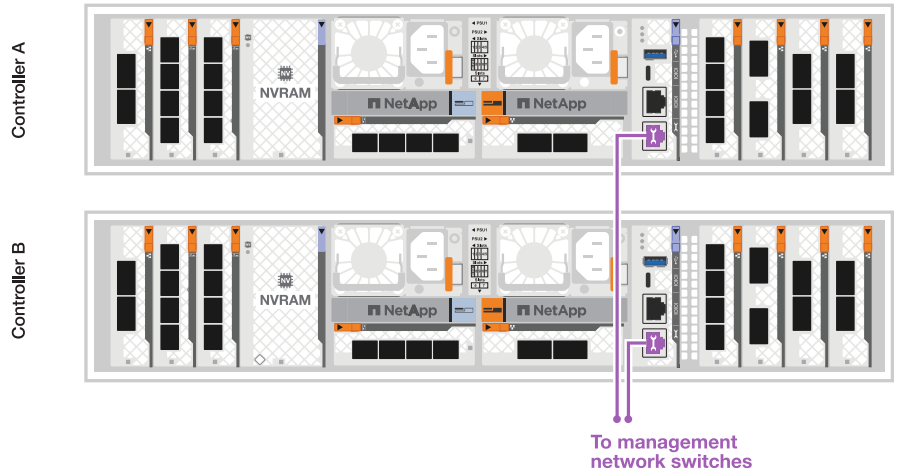
Verbinden Sie die Controller mit dem Managementnetzwerk.

Informationen zum Anschließen des Speichersystems an die Management-Netzwerk-Switches erhalten Sie von Ihrem Netzwerkadministrator.

A1K

Verwenden Sie die 1000BASE-T RJ-45-Kabel, um die Management-Ports (Schraubenschlüssel) an den einzelnen Controllern mit den Managementnetzwerk-Switches zu verbinden.

- 1000BASE-T RJ-45 KABEL*

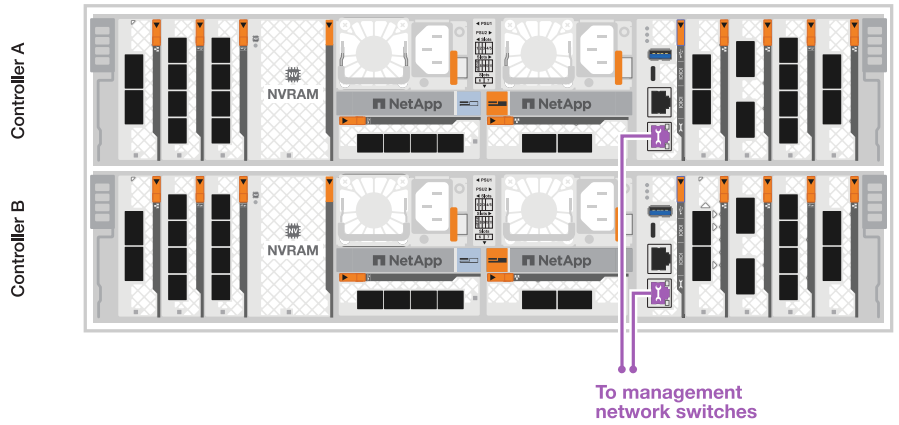


Stecken Sie die Netzkabel noch nicht ein.

A70 und A90

Verwenden Sie die 1000BASE-T RJ-45-Kabel, um die Management-Ports (Schraubenschlüssel) an den einzelnen Controllern mit den Managementnetzwerk-Switches zu verbinden.

- 1000BASE-T RJ-45 KABEL*

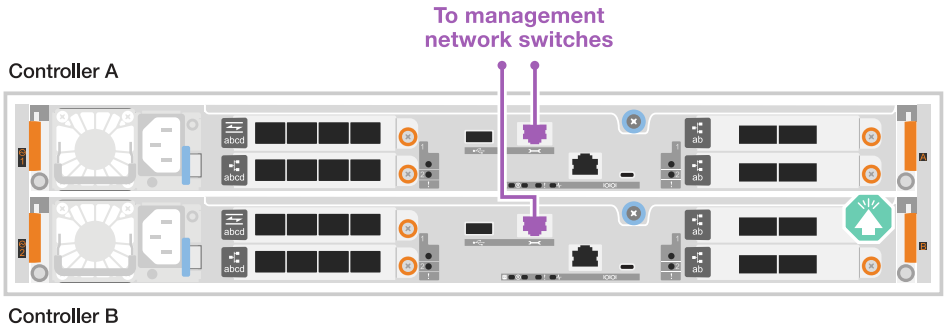


Stecken Sie die Netzkabel noch nicht ein.

A20, A30 UND A50

Verbinden Sie die Management-Ports (Schraubenschlüssel) an den einzelnen Controllern mit den Managementnetzwerk-Switches.

- 1000BASE-T RJ-45 KABEL*

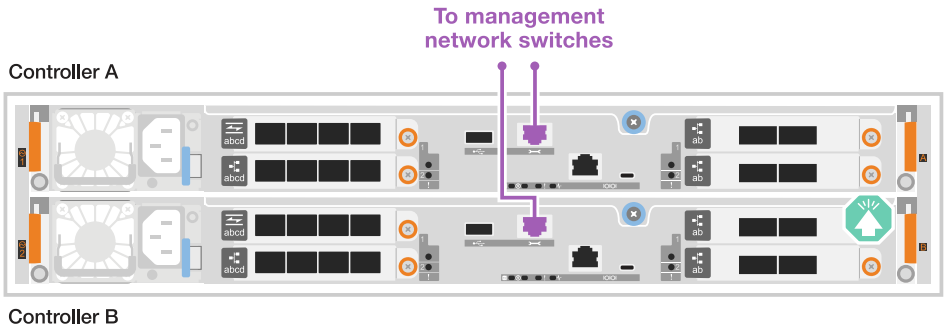


Stecken Sie die Netzkabel noch nicht ein.

C30

Verbinden Sie die Management-Ports (Schraubenschlüssel) an den einzelnen Controllern mit den Managementnetzwerk-Switches.

- 1000BASE-T RJ-45 KABEL*



Stecken Sie die Netzkabel noch nicht ein.

Schritt 4: Verkabeln Sie die Shelf-Verbindungen

Die folgenden Verkabelungsverfahren zeigen, wie Sie Ihre Controller mit einem Storage Shelf verbinden.

Die maximale Anzahl der unterstützten Einschübe für Ihr Speichersystem und alle Verkabelungsoptionen, wie "NetApp Hardware Universe"z. B. optische und Switch-Attached, finden Sie unter .

A1K

Die AFF A1K Speichersysteme unterstützen NS224-Shelves mit dem Modul NSM100 oder NSM100B. Die Hauptunterschiede zwischen den Modulen sind:

- NSM100-Regalmodule verwenden die integrierten Ports e0a und e0b.
- NSM100B-Shelf-Module verwenden die Ports e1a und e1b in Steckplatz 1.

Das folgende Verkabelungsbeispiel zeigt NSM100-Module in den NS224-Schränken, wenn auf die Anschlüsse der Regalmodule verwiesen wird.

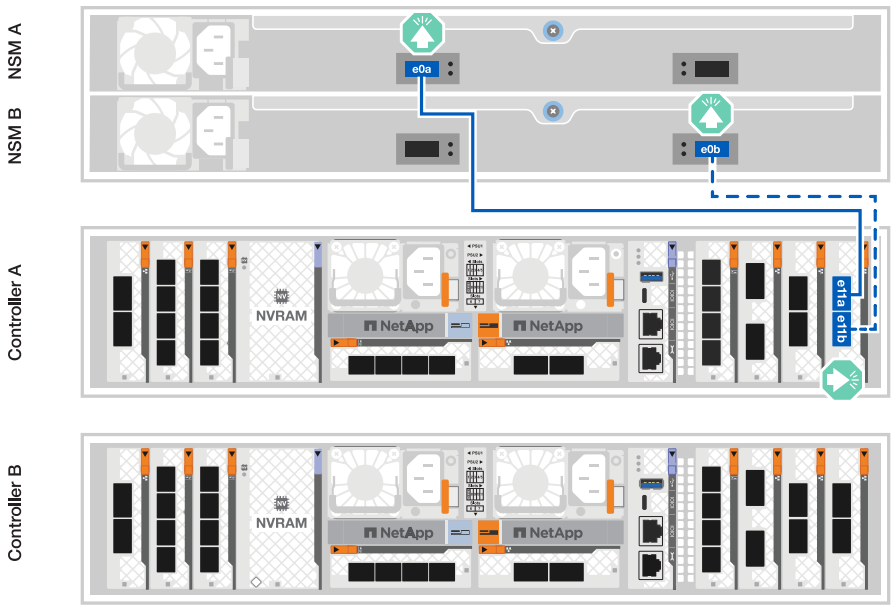
Wählen Sie eine der folgenden Verkabelungsoptionen, die Ihrem Setup entsprechen.

Option 1: Ein NS224 Storage-Shelf

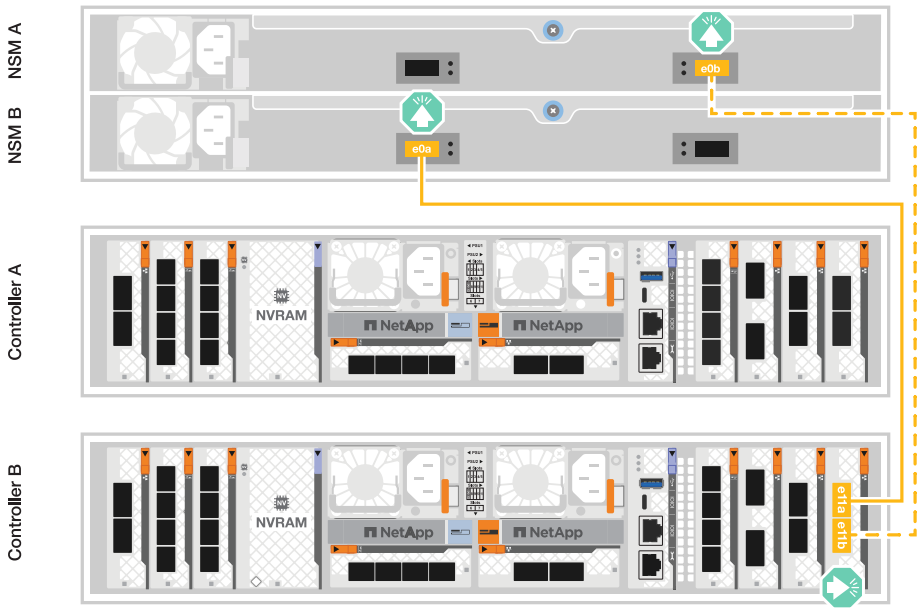
Verbinden Sie jeden Controller mit den NSM-Modulen im NS224-Shelf. Die Grafik zeigt die Verkabelung von den einzelnen Controllern: Die Verkabelung von Controller A wird blau und die Verkabelung von Controller B gelb dargestellt.

Schritte

1. Verbinden Sie auf Controller A die folgenden Ports:
   a. Verbinden Sie Port e11a mit NSM A Port e0a.
   b. Verbinden Sie Port e11b mit Port NSM B Port e0b.



2. Verbinden Sie an Controller B die folgenden Ports:
   a. Verbinden Sie Port e11a mit NSM B Port e0a.
   b. Verbinden Sie Port e11b mit NSM A Port e0b.

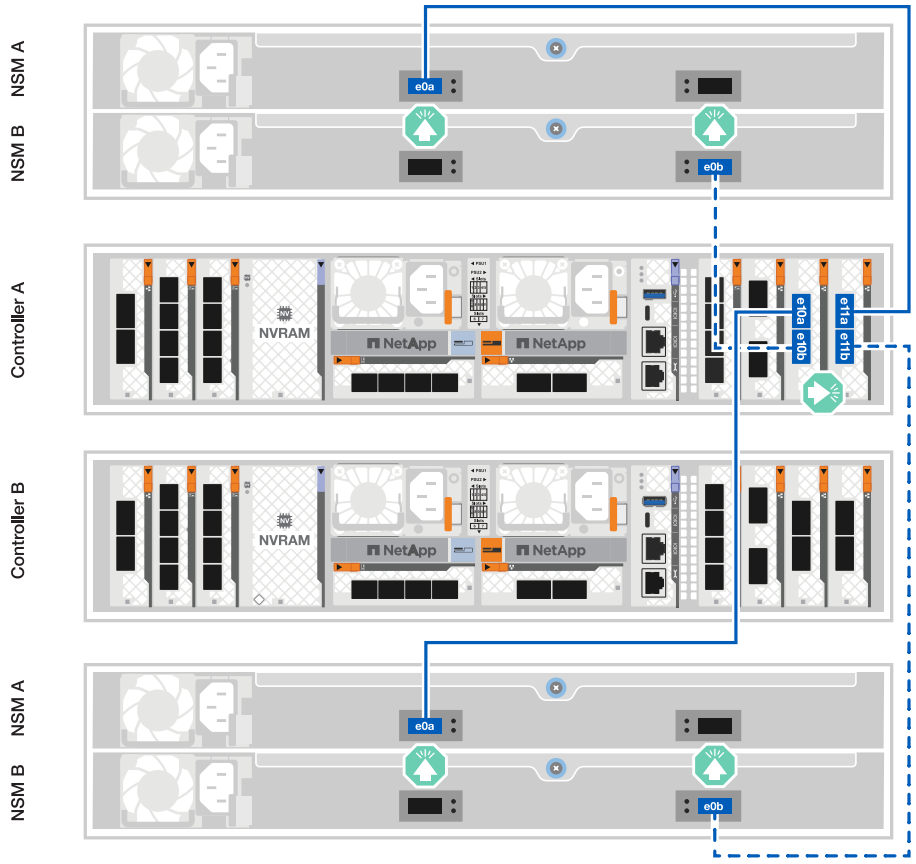


Option 2: Zwei NS224 Storage-Shelfs

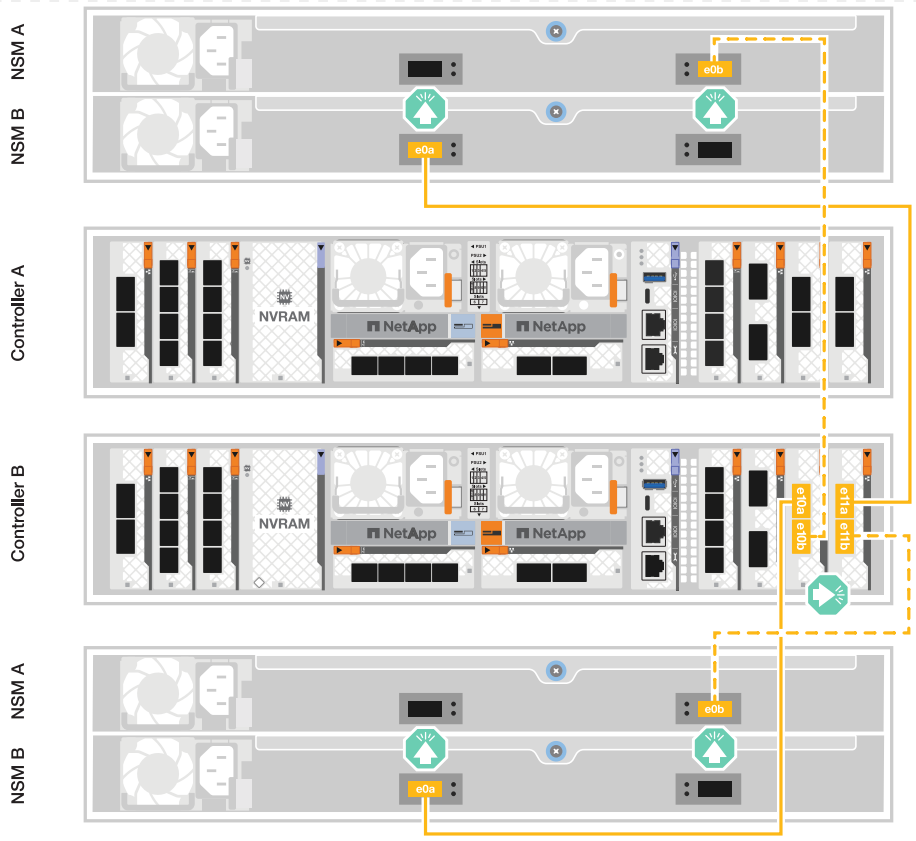
Verbinden Sie jeden Controller mit den NSM-Modulen beider NS224-Shelfs. Die Grafik zeigt die Verkabelung von den einzelnen Controllern: Die Verkabelung von Controller A wird blau und die Verkabelung von Controller B gelb dargestellt.

Schritte

1. Verbinden Sie auf Controller A die folgenden Ports:
   a. Verbinden Sie Port e11a mit Shelf 1 NSM A Port e0a.
   b. Verbinden Sie den Port e11b mit dem Shelf 2 NSM B-Port e0b.
   c. Verbinden Sie Port e10a mit Shelf 2 NSM A Port E0a.
   d. Verbinden Sie Port e10b mit Shelf 1 NSM A Port e0b.



2. Verbinden Sie an Controller B die folgenden Ports:
   a. Verbinden Sie Port e11a mit Shelf 1 NSM B Port e0a.
   b. Verbinden Sie Port e11b mit Shelf 2 NSM A Port e0b.
   c. Verbinden Sie Port e10a mit Shelf 2 NSM B Port e0a.
   d. Verbinden Sie Port e10b mit Shelf 1 NSM A Port e0b.



A70 und A90

Die Speichersysteme AFF A70 und 90 unterstützen NS224-Shelves mit dem Modul NSM100 oder NSM100B. Die Hauptunterschiede zwischen den Modulen sind:

- NSM100-Regalmodule verwenden die integrierten Ports e0a und e0b.
- NSM100B-Shelf-Module verwenden die Ports e1a und e1b in Steckplatz 1.

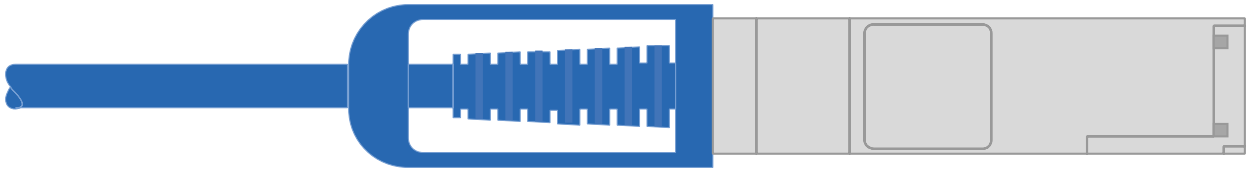
Das folgende Verkabelungsbeispiel zeigt NSM100-Module in den NS224-Schränken, wenn auf die Anschlüsse der Regalmodule verwiesen wird.

Wählen Sie eine der folgenden Verkabelungsoptionen, die Ihrem Setup entsprechen.

Option 1: Ein NS224 Storage-Shelf

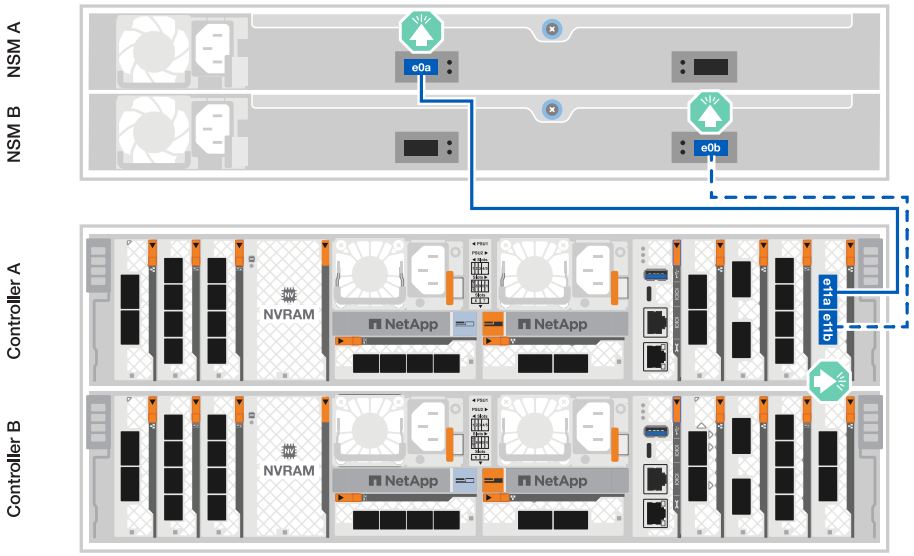
Verbinden Sie jeden Controller mit den NSM-Modulen im NS224-Shelf. Die Grafik zeigt die Verkabelung von den einzelnen Controllern: Die Verkabelung von Controller A wird blau und die Verkabelung von Controller B gelb dargestellt.

100 GbE QSFP28 Kupferkabel

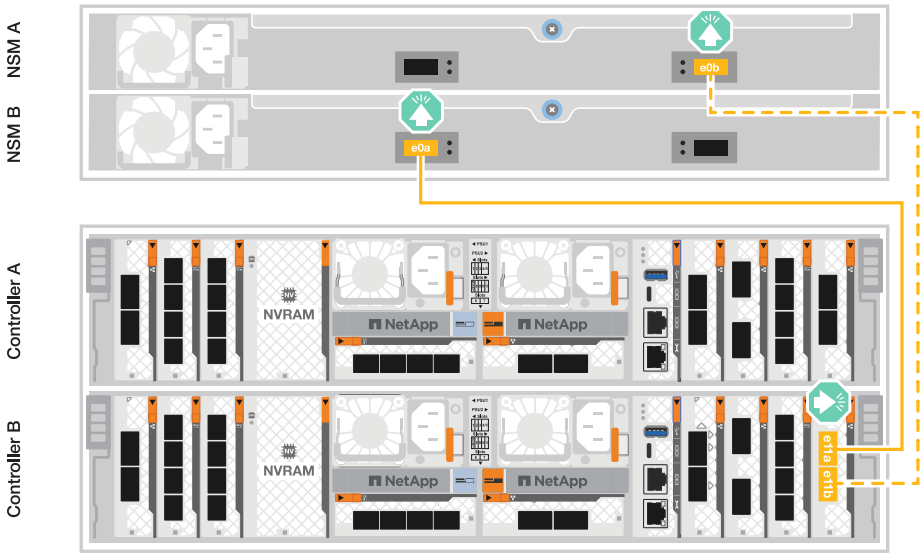


Schritte

1. Verbinden Sie den Controller A-Port e11a mit dem NSM A-Port e0a.
2. Verbinden Sie den Controller A-Port e11b mit dem Port NSM B Port e0b.



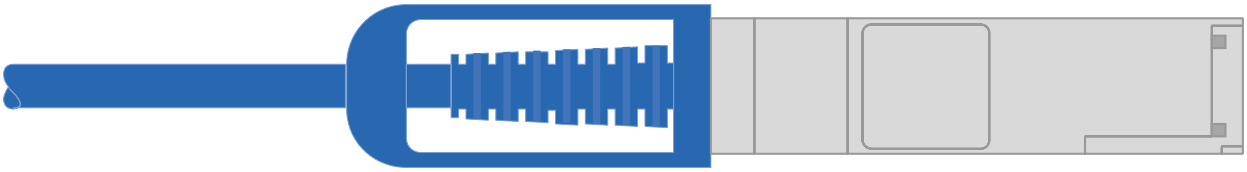
3. Verbinden Sie den Port e11a von Controller B mit dem Port e0a von NSM B.
4. Verbinden Sie den Port e11b des Controllers B mit dem Port e0b des NSM A.


NSM A
NSM B
Controller A
Controller B
e0b
e0a
NVRAM
NetApp
NetApp
NVRAM
NetApp
NetApp
e11a
e11b

Option 2: Zwei NS224 Storage-Shelfs

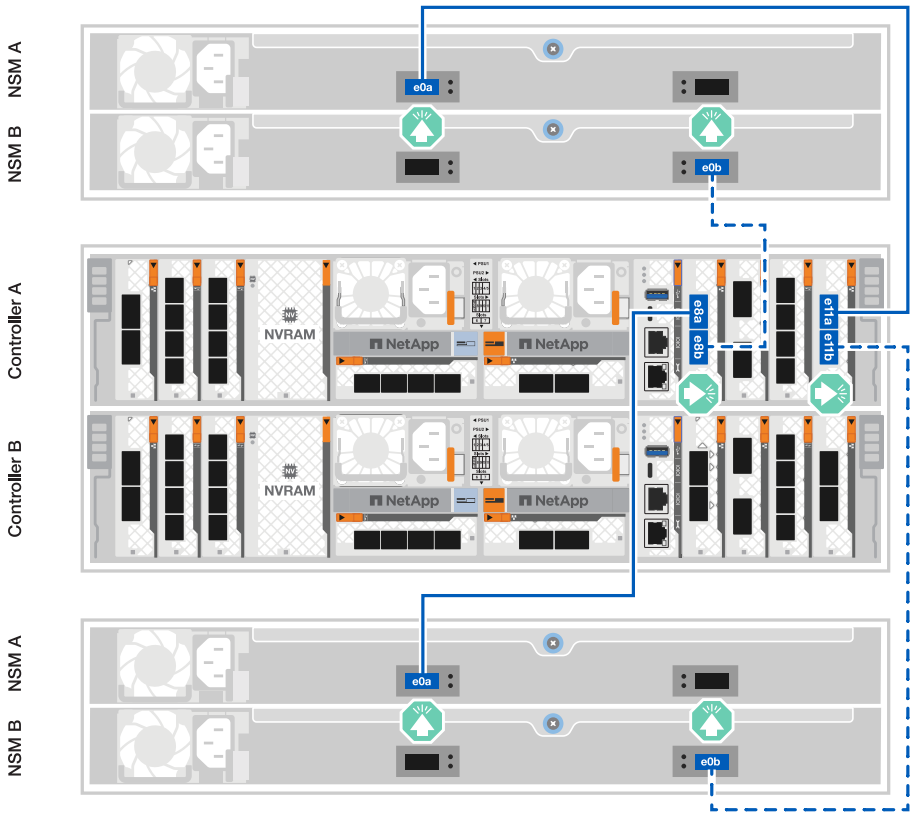
Verbinden Sie jeden Controller mit den NSM-Modulen beider NS224-Shelfs. Die Grafik zeigt die Verkabelung von den einzelnen Controllern: Die Verkabelung von Controller A wird blau und die Verkabelung von Controller B gelb dargestellt.

100 GbE QSFP28 Kupferkabel



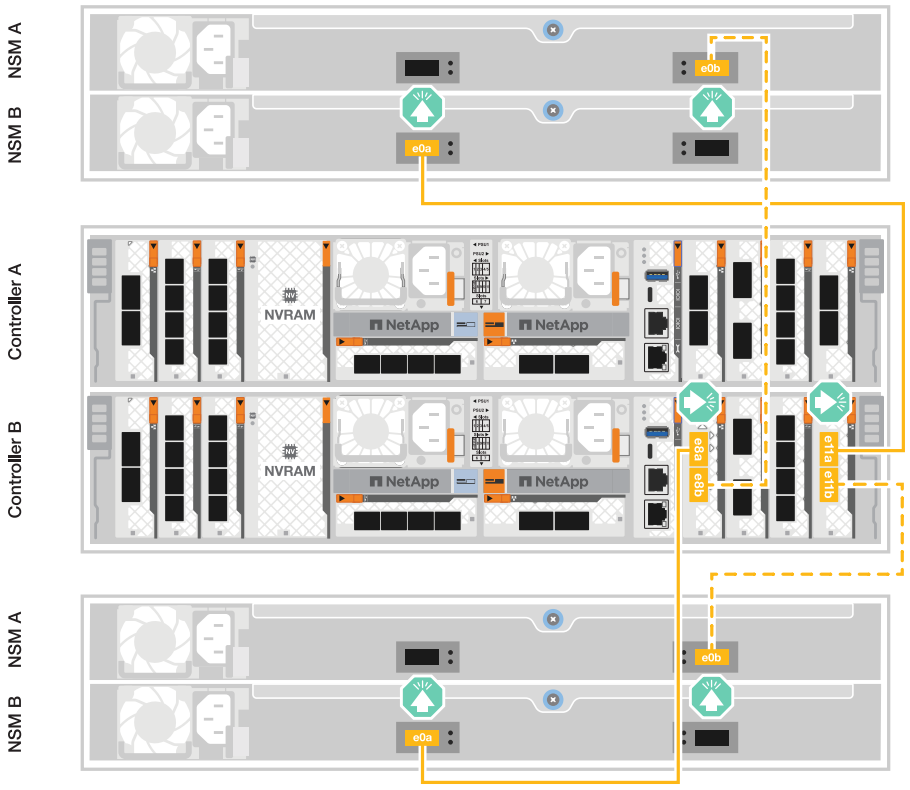
Schritte

1. Verbinden Sie auf Controller A die folgenden Ports:
   a. Verbinden Sie Port e11a mit Shelf 1, NSM A Port e0a.
   b. Verbinden Sie den Port e11b mit Shelf 2, den NSM B Port e0b.
   c. Verbinden Sie Port e8a mit Shelf 2, NSM A Port e0a.
   d. Verbinden Sie Port e8b mit Shelf 1, NSM B Port e0b.



2. Verbinden Sie an Controller B die folgenden Ports:
   a. Verbinden Sie Port e11a mit Shelf 1, NSM B Port e0a.
   b. Verbinden Sie Port e11b mit Shelf 2, NSM A Port e0b.
   c. Verbinden Sie Port e8a mit Shelf 2, NSM B Port e0a.

d. Verbinden Sie Port e8b mit Shelf 1, NSM A Port e0b.



A20, A30 UND A50

Die Verkabelung des NS224-Regals zeigt NSM100B-Module anstelle von NSM100-Modulen. Die Verkabelung ist unabhängig vom Typ der verwendeten NSM-Module gleich, lediglich die Portnamen unterscheiden sich:

- NSM100B-Module verwenden die Ports e1a und e1b auf einem E/A-Modul in Steckplatz 1.
- NSM100-Module verwenden integrierte (Onboard-)Ports e0a und e0b.

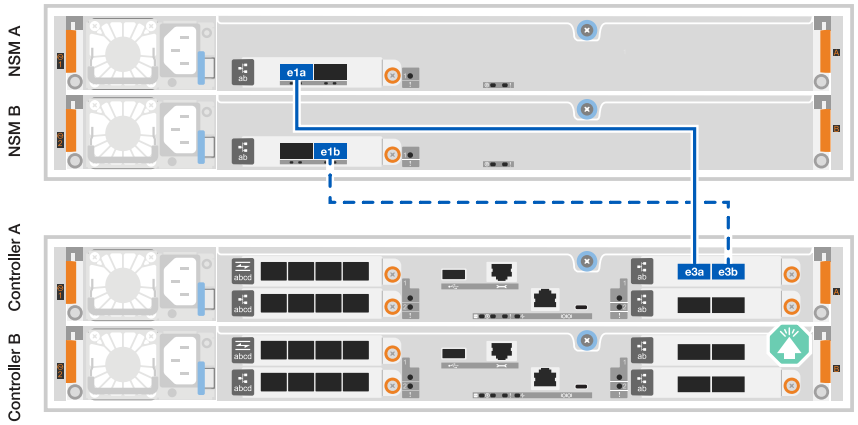
Sie verkabeln jeden Controller mit jedem NSM-Modul im NS224-Regal mithilfe der Speicherkabel, die mit Ihrem Speichersystem geliefert wurden. Dabei kann es sich um den folgenden Kabeltyp handeln:

100 GbE QSFP28 Kupferkabel

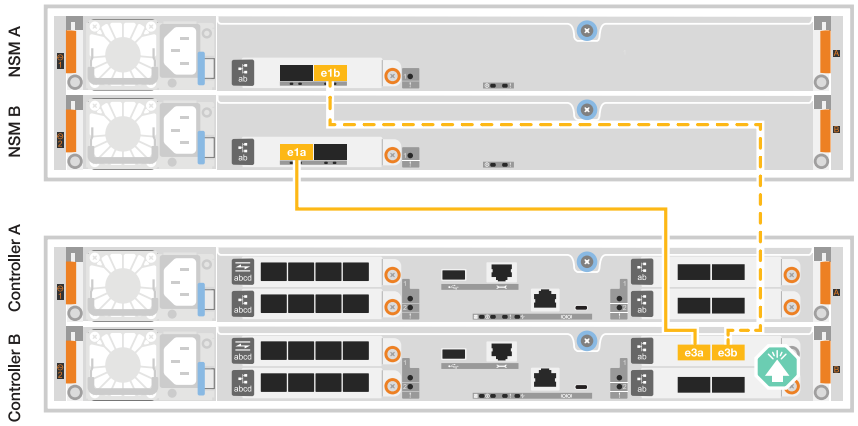
Die Grafik zeigt die Verkabelung von Controller A blau und Controller B gelb.

Schritte

1. Controller A mit dem Shelf verbinden:
   a. Verbinden Sie den Controller A-Port e3a mit dem NSM A-Port e1a.
   b. Den Controller A-Port e3b mit dem NSM B-Port e1b verbinden.



2. Controller B mit dem Shelf verbinden:
   a. Verbinden Sie den Port e3a von Controller B mit dem Port e1a von NSM B.
   b. Verbinden Sie den Port e3b des Controllers B mit dem Port e1b des NSM A.



C30

Die Verkabelung des NS224-Regals zeigt NSM100B-Module anstelle von NSM100-Modulen. Die Verkabelung ist unabhängig vom Typ der verwendeten NSM-Module gleich, lediglich die Portnamen unterscheiden sich:

- NSM100B-Module verwenden die Ports e1a und e1b auf einem E/A-Modul in Steckplatz 1.
- NSM100-Module verwenden integrierte (Onboard-)Ports e0a und e0b.

Sie verkabeln jeden Controller mit jedem NSM-Modul im NS224-Regal mithilfe der Speicherkabel, die mit Ihrem Speichersystem geliefert wurden. Dabei kann es sich um den folgenden Kabeltyp handeln:

100 GbE QSFP28 Kupferkabel

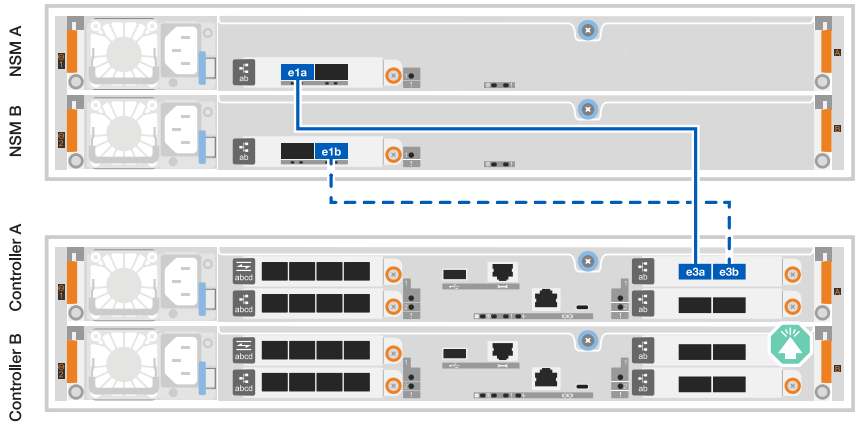
Die Grafik zeigt die Verkabelung von Controller A blau und Controller B gelb.

Schritte

1. Controller A mit dem Shelf verbinden:

a. Verbinden Sie den Controller A-Port e3a mit dem NSM A-Port e1a.

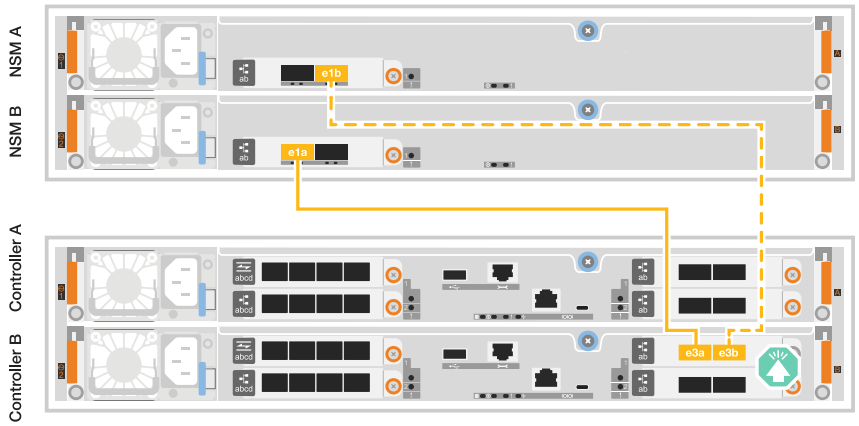
b. Den Controller A-Port e3b mit dem NSM B-Port e1b verbinden.



2. Controller B mit dem Shelf verbinden:

a. Verbinden Sie den Port e3a von Controller B mit dem Port e1a von NSM B.

b. Verbinden Sie den Port e3b des Controllers B mit dem Port e1b des NSM A.



Was kommt als Nächstes?

Nachdem Sie die Speicher-Controller mit Ihrem Netzwerk verbunden und dann die Controller mit Ihren Speicher-Shelfs verbunden haben, Sie "Schalten Sie das ASA r2-Speichersystem ein".

Schalten Sie das ASA r2-Speichersystem ein

Nachdem Sie die Rack-Hardware für das ASA r2 Storage-System installiert und die Kabel für die Controller und Storage Shelfs installiert haben, sollten Sie die Storage-Shelfs und Controller einschalten.

Schritt 1: Schalten Sie das Shelf ein und weisen Sie die Shelf-ID zu

Jedes Shelf wird durch eine eindeutige Shelf-ID unterschieden. Diese ID stellt sicher, dass das Shelf innerhalb Ihrer Storage-System-Einrichtung unterscheidbar ist.

Über diese Aufgabe

- Gültige Shelf-ID: 01 bis 99.

  Bei internen, in die Controller integrierten Shelfs (Storage) wird Ihnen eine feste Shelf-ID mit der Nummer 00 zugewiesen.

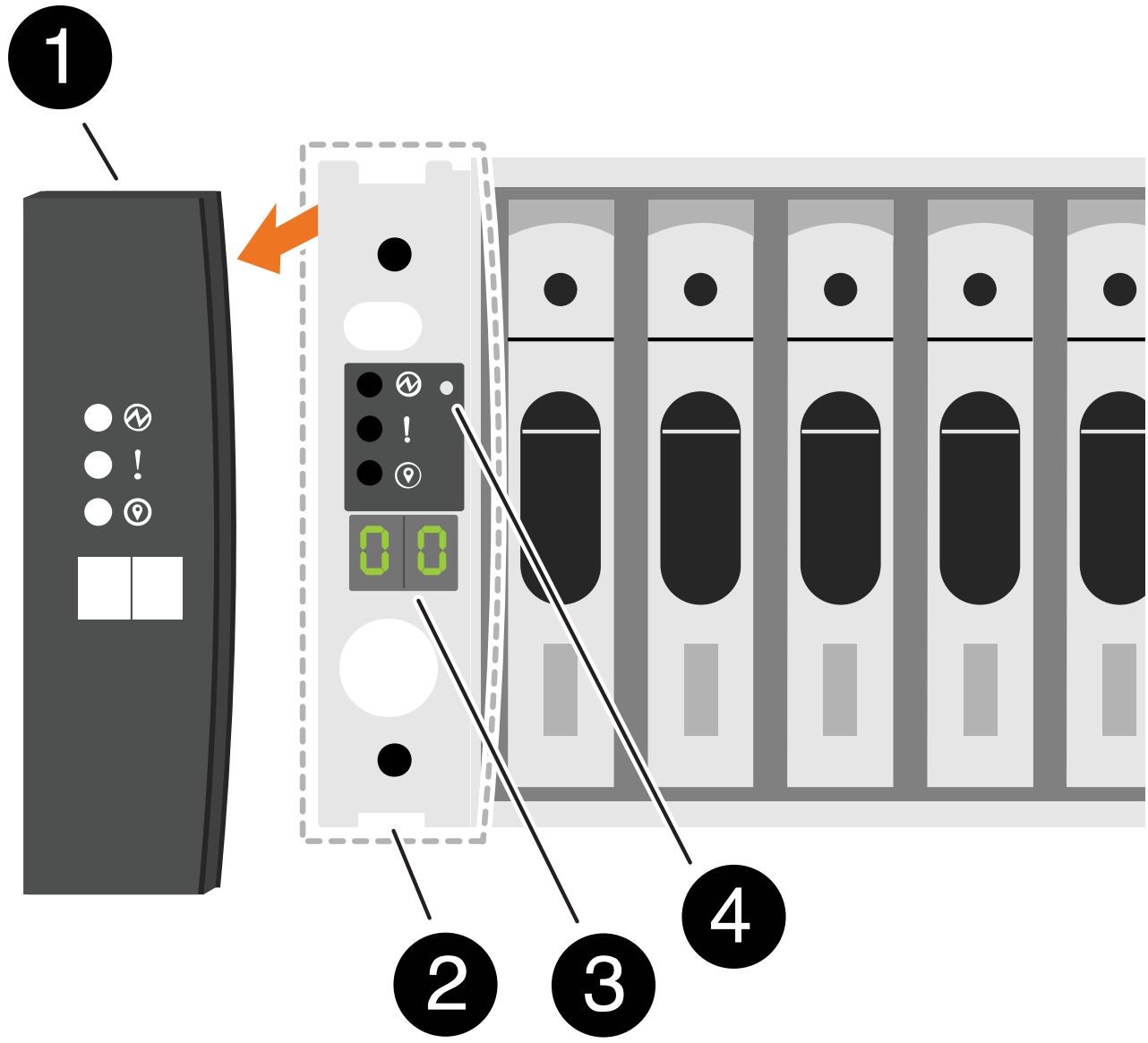
- Sie müssen ein Shelf aus- und wieder einschalten (trennen Sie beide Netzkabel, warten Sie die entsprechende Zeit und schließen Sie sie dann wieder an), damit die Shelf-ID wirksam wird.

Schritte

1. Schalten Sie das Shelf ein, indem Sie die Netzkabel zuerst an das Shelf anschließen, sie mit der Netzkabelhalterung sichern und dann die Netzkabel an die Stromversorgung an verschiedenen Stromkreisen anschließen.

   Das Shelf wird eingeschaltet und startet automatisch, wenn es an die Stromversorgung angeschlossen ist.

2. Entfernen Sie die linke Endkappe, um auf die Shelf-ID-Taste hinter der Frontplatte zuzugreifen.



1	Einlegeboden-Endkappe
2	Ablagefaceplate
3	Shelf-ID-Nummer
4	Shelf-ID-Taste

3. Ändern Sie die erste Nummer der Shelf-ID:

   a. Führen Sie das gerade gebogene Ende eines Büroklammer oder eines Kugelschreibers mit schmaler Spitze in das kleine Loch ein, um die Shelf-ID-Taste zu drücken.

   b. Halten Sie die erste Shelf-ID-Taste gedrückt, bis die erste Ziffer auf der digitalen Anzeige blinkt, und lassen Sie dann die Taste los.

      Es kann bis zu 15 Sekunden dauern, bis die Ziffer blinkt. Dadurch wird der Programmiermodus für die Shelf-ID aktiviert.

      > Wenn das Blinken der ID länger als 15 Sekunden dauert, halten Sie die Shelf-ID-Taste erneut gedrückt und vergewissern Sie sich, dass sie vollständig gedrückt wird.

   c. Drücken Sie die Shelf-ID-Taste und lassen Sie sie los, um die Nummer vorzurücken, bis Sie die gewünschte Zahl von 0 auf 9 erreichen.

      Jede Presse- und Freigabedauer kann eine Sekunde lang sein.

   Die erste Ziffer blinkt weiterhin.

4. Ändern Sie die zweite Nummer der Shelf-ID:

   a. Halten Sie die Taste gedrückt, bis die zweite Ziffer auf der digitalen Anzeige blinkt.

      Es kann bis zu drei Sekunden dauern, bis die Ziffer blinkt.

   Die erste Ziffer auf dem digitalen Display hört auf zu blinken.

   a. Drücken Sie die Shelf-ID-Taste und lassen Sie sie los, um die Nummer vorzurücken, bis Sie die gewünschte Zahl von 0 auf 9 erreichen.

      Die zweite Ziffer blinkt weiterhin.

5. Sperren Sie die gewünschte Ziffer und beenden Sie den Programmiermodus, indem Sie die Shelf-ID-Taste gedrückt halten, bis die zweite Ziffer nicht mehr blinkt.

   Es kann bis zu drei Sekunden dauern, bis die Ziffer nicht mehr blinkt.

   Beide Ziffern auf der digitalen Anzeige beginnen zu blinken, und die gelbe LED beginnt nach ca. fünf Sekunden zu leuchten, sodass Sie darauf informiert werden, dass die ausstehende Shelf-ID noch nicht wirksam wurde.

6. Schalten Sie das Shelf mindestens 10 Sekunden aus und wieder ein, damit die Shelf-ID übernommen wird.
   a. Ziehen Sie das Netzkabel aus beiden Netzteilen auf dem Shelf ab.
   b. Warten Sie 10 Sekunden.
   c. Schließen Sie die Netzkabel wieder an die Shelf-Netzteile an, um den aus- und Wiedereinschalten zu beenden.

      Ein Netzteil wird eingeschaltet, sobald das Netzkabel angeschlossen ist. Seine zweifarbige LED sollte grün leuchten.
7. Die linke Endkappe austauschen.

Schritt 2: Schalten Sie die Controller ein

Nachdem Sie Ihre Storage Shelfs eingeschaltet und ihnen eindeutige IDs zugewiesen haben, schalten Sie die Storage Controller ein.

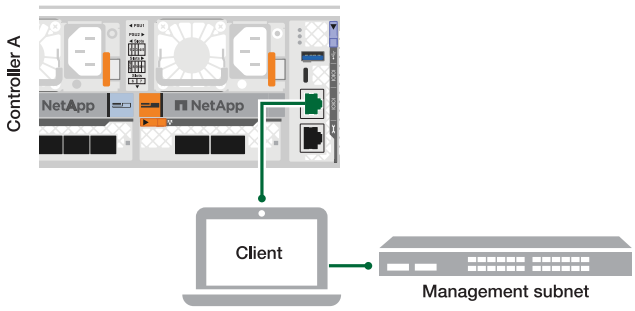
Schritte

1. Schließen Sie den Laptop an den seriellen Konsolenport an. Auf diese Weise können Sie die Boot-Sequenz überwachen, wenn die Controller eingeschaltet werden.
   a. Stellen Sie den seriellen Konsolenport am Laptop auf 115,200 Baud mit N-8-1 ein.

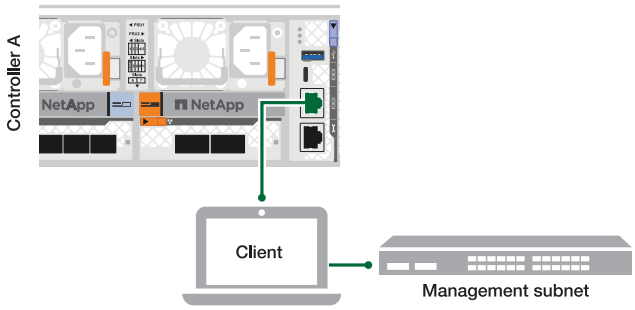
      Anweisungen zum Konfigurieren des seriellen Konsolenports finden Sie in der Online-Hilfe Ihres Laptops.

   b. Schließen Sie das Konsolenkabel an den Laptop an und verbinden Sie den seriellen Konsolenport am Controller mithilfe des Konsolenkabels, das mit dem Storage-System geliefert wurde.
   c. Schließen Sie den Laptop an den Switch im Management-Subnetz an.

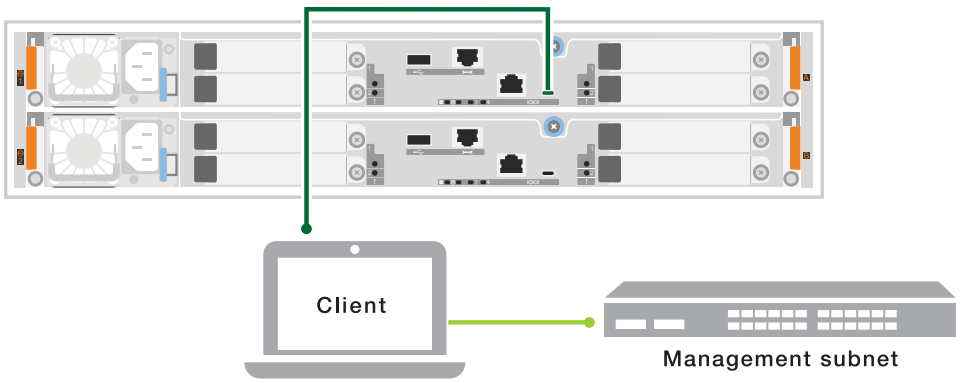
A1K



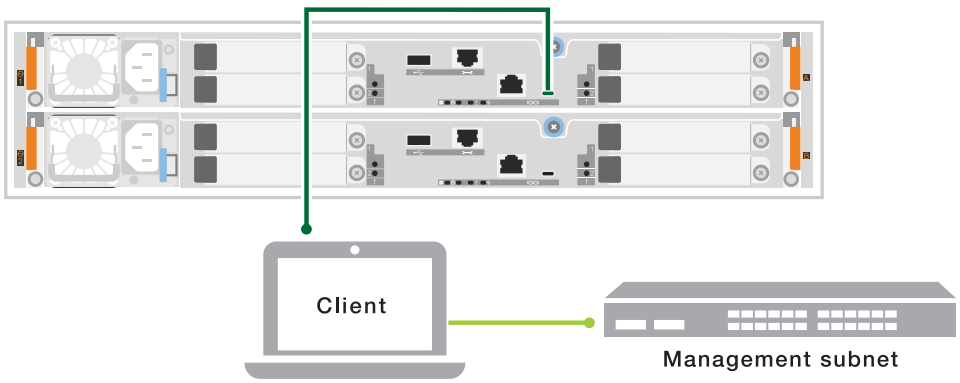
A70 und A90



A20, A30 UND A50



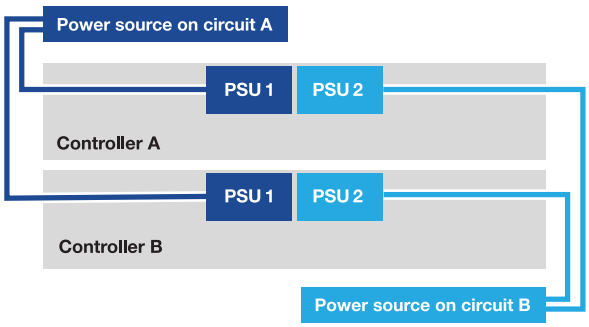
C30



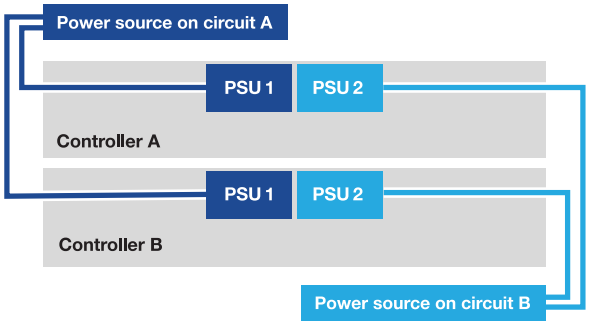
2. Weisen Sie dem Laptop eine TCP/IP-Adresse zu, die sich im Management-Subnetz befindet.
3. Schließen Sie die Stromkabel an die Controller-Netzteile an, und schließen Sie sie dann an Stromquellen

auf verschiedenen Stromkreisen an.

A1K



A70 und A90



A20, A30 UND A50

C30

- Das System startet den Startvorgang. Die Startsequenz kann bis zu acht Minuten dauern.
- Während des Startvorgangs beobachten Sie, wie die LEDs blinken und die Lüfter sich einschalten und damit signalisieren, dass die Controller hochfahren.
- Beachten Sie, dass die Lüfter beim ersten Start möglicherweise ein hohes Geräusch erzeugen. Das Lüftergeräusch während des Startvorgangs ist normal.
- Bei den Speichersystemen ASA A20, A30, A50 und ASA C30 leuchtet die Shelf-ID-Anzeige an der Vorderseite des Systemgehäuses nicht.

4. Sichern Sie die Netzkabel mit dem Sicherungsgerät an jedem Netzteil.

Was kommt als Nächstes?

Nachdem Sie Ihr ASA r2-Speichersystem eingeschaltet haben, können Sie "Richten Sie einen ONTAP ASA r2-Cluster ein".

Richten Sie Ihr ASA r2-System ein

Richten Sie einen ONTAP-Cluster auf Ihrem ASA r2 Storage-System ein

ONTAP System Manager führt Sie durch einen schnellen und einfachen Workflow zur Einrichtung eines ONTAP ASA r2 Clusters.

Während der Cluster-Einrichtung wird Ihre standardmäßige Virtual Machine (VM) für den Datenspeicher erstellt. Optional können Sie das Domain Name System (DNS) zum Auflösen von Hostnamen aktivieren, das Cluster so einstellen, dass es das Network Time Protocol (NTP) für die Zeitsynchronisierung verwendet und die Verschlüsselung von Daten im Ruhezustand aktiviert.

Bevor Sie beginnen

Stellen Sie die folgenden Informationen zusammen:

- Cluster-Management-IP-Adresse

  Die Cluster-Management-IP-Adresse ist eine eindeutige IPv4-Adresse für die Cluster-Managementoberfläche, die vom Cluster-Administrator für den Zugriff auf die Admin-Storage-VM und das Management des Clusters verwendet wird. Sie können diese IP-Adresse vom Administrator beziehen, der für das Zuweisen von IP-Adressen in Ihrem Unternehmen verantwortlich ist.

- Netzwerk-Subnetzmaske

  Während der Cluster-Einrichtung empfiehlt ONTAP eine Reihe von Netzwerkschnittstellen, die für die jeweilige Konfiguration geeignet sind. Sie können die Empfehlung bei Bedarf anpassen.

- IP-Adresse des Netzwerk-Gateways
- Partner-Node-IP-Adresse
- DNS-Domain-Namen
- IP-Adressen des DNS-Namensservers
- IP-Adressen des NTP-Servers
- Daten-Subnetzmaske

Schritte

1. Ermitteln Sie das Cluster-Netzwerk
   a. Verbinden Sie Ihren Laptop mit dem Management-Switch, und greifen Sie auf die Netzwerkcomputer und -Geräte zu.
   b. Öffnen Sie Den Datei-Explorer.
   c. Wählen Sie **Netzwerk** aus, klicken Sie mit der rechten Maustaste und wählen Sie **Aktualisieren** aus.
   d. Wählen Sie ein ONTAP-Symbol aus, und akzeptieren Sie alle auf dem Bildschirm angezeigten Zertifikate.

      System Manager wird geöffnet.

2. Erstellen Sie unter **Passwort** ein sicheres Passwort für das Admin-Konto.

   Das Passwort muss mindestens acht Zeichen lang sein und mindestens einen Buchstaben und eine Ziffer enthalten.

3. Geben Sie das Passwort zur Bestätigung erneut ein und wählen Sie dann **Weiter**.
4. Geben Sie unter **Netzwerkadressen** einen Namen für das Speichersystem ein oder übernehmen Sie den Standardnamen.

   Wenn Sie den Standardnamen des Speichersystems ändern, muss der neue Name mit einem Buchstaben beginnen und darf weniger als 44 Zeichen enthalten. Sie können einen Punkt (.), Bindestrich (-) oder Unterstrich (_) im Namen verwenden.

5. Geben Sie die Cluster-Management-IP-Adresse, Subnetzmaske, Gateway-IP-Adresse und die IP-Adresse des Partner-Knotens ein, und wählen Sie dann **Weiter** aus.
6. Wählen Sie unter **Network Services** die gewünschten Optionen aus, um **das Domain Name System (DNS) zum Auflösen von Hostnamen** zu verwenden und **das Network Time Protocol (NTP) zu verwenden, um die Uhrzeiten zu synchronisieren**.

   Wenn Sie den DNS verwenden möchten, geben Sie die DNS-Domain und die Namensserver ein. Wenn Sie NTP verwenden möchten, geben Sie die NTP-Server ein, und wählen Sie dann **Weiter**.

7. Geben Sie unter **Verschlüsselung** eine Passphrase für den Onboard Key Manager (OKM) ein.

   Standardmäßig ist die Verschlüsselung von Daten im Ruhezustand mit einem Onboard Key Manager (OKM) ausgewählt. Wenn Sie einen externen Schlüsselmanager verwenden möchten, aktualisieren Sie die Auswahl.

   Optional können Sie nach Abschluss der Cluster-Einrichtung Ihr Cluster für die Verschlüsselung konfigurieren.

8. Wählen Sie **Initialisieren**.

   Nach dem Setup werden Sie zur Management-IP-Adresse des Clusters umgeleitet.

9. Wählen Sie unter **Netzwerk Protokolle konfigurieren**.

Um IP zu konfigurieren (iSCSI und NVMe/TCP), gehen Sie folgendermaßen vor:	**So konfigurieren Sie FC und NVMe/FC:**
a. Wählen Sie **IP**, und wählen Sie dann **IP-Schnittstellen konfigurieren**. b. Wählen Sie **Subnetz hinzufügen**. c. Geben Sie einen Namen für das Subnetz ein, und geben Sie dann die Subnetz-IP-Adressen ein. d. Geben Sie die Subnetzmaske ein, und geben Sie optional ein Gateway ein; wählen Sie dann **Add** aus. e. Wählen Sie das soeben erstellte Subnetz aus, und wählen Sie dann **Speichern**. f. Wählen Sie **Speichern**.	a. Wählen Sie **FC**, und wählen Sie dann **Configure FC Interfaces** und/oder **Configure NVMe/FC Interfaces** aus. b. Wählen Sie die FC- und/oder NVMe/FC-Ports aus, und wählen Sie dann **Save**.

10. Optional können "Active IQ Config Advisor"Sie die Konfiguration herunterladen und ausführen.

    ActiveIQ Config Advisor ist ein Tool für NetApp Systeme, das auf häufig auftretende Konfigurationsfehler prüft.

Was kommt als Nächstes?

Sie können "Richten Sie den Datenzugriff ein"Ihre SAN-Clients auf Ihr ASA r2-System übertragen.

SAN-Hostkonfiguration mit ASA r2-Systemen

ASA r2-Systeme befolgen dieselben Empfehlungen und Richtlinien für die SAN-Host-Konfiguration wie alle anderen ONTAP-Systeme.

Es wird empfohlen, zwei oder mehr Switches zu verwenden, um das Speichersystem mit einem oder mehreren SAN-Hosts zu verbinden. Bei iSCSI-Konfigurationen wird die Netzwerktopologie, die Ihre Hosts, Switches und Speichersysteme verbindet, als *Network* bezeichnet. Für FC- und FC-NVMe-Konfigurationen wird dieselbe Netzwerktopologie als „*Fabric*“ bezeichnet.

Es werden mehrere Netzwerk- oder Multi-Fabric-Konfigurationen (Konfigurationen mit zwei oder mehr Switches) empfohlen, da diese für Redundanz auf Switch- und Storage-Ebene sorgen. Diese Redundanz macht Ihr Storage-System fehlertoleranter und unterstützt einen unterbrechungsfreien Betrieb.

Die folgende Abbildung zeigt ein Beispiel einer FC-Konfiguration mit mehreren Hosts, die zwei Fabrics für den Zugriff auf ein einzelnes HA-Paar verwenden. Die FC-Ziel-Port-Nummern (0c, 0d, 1a, 1b) sind ebenfalls Beispiele. Die tatsächlichen Port-Nummern variieren je nach Plattformmodell und ob Sie Erweiterungsadapter verwenden.

Erfahren Sie mehr über "SAN-Konfiguration für iSCSI-Hosts". Erfahren Sie mehr über "SAN-Konfiguration für FC- und FC/NVMe-Hosts".

Zoning-Empfehlung für FC-Hosts

Konfigurieren Sie die FC-Hosts für das Zoning. ASA r2-Systeme folgen denselben Empfehlungen und Richtlinien für das FC-Host-Zoning wie alle anderen ONTAP-Systeme.

Eine Zone ist eine logische Gruppierung von einem oder mehreren Ports innerhalb einer Fabric. Damit Geräte einander erkennen, Sitzungen miteinander aufbauen und kommunizieren können, müssen beide Ports über eine gemeinsame Zonenmitgliedschaft verfügen.

Erfahren Sie mehr über "FC-/FC-NVMe-Zoning".

Aktivieren Sie den Datenzugriff von SAN-Hosts auf Ihr ASA r2 Storage-System

Um den Datenzugriff einzurichten, sollten Sie sicherstellen, dass die kritischen Parameter und Einstellungen auf Ihrem SAN-Client für den ordnungsgemäßen Betrieb mit ONTAP korrekt konfiguriert sind. Wenn Sie Storage für Ihre VMware-Umgebung bereitstellen, sollten Sie OTV 10.3 installieren, um Ihren ASA r2-Speicher einfach zu verwalten.

Richten Sie den Datenzugriff von SAN-Hosts ein

Die für die Einrichtung des Datenzugriffs auf Ihrem ASA r2-System über Ihre SAN-Hosts erforderliche Konfiguration variiert je nach Host-Betriebssystem und Protokoll. Die richtige Konfiguration ist für die beste Performance und ein erfolgreiches Failover von großer Bedeutung.

"VMware vSphere SCSI-Clients""VMware vSphere NVMe Clients""Andere SAN-Clients"Informationen zur ordnungsgemäßen Konfiguration Ihrer Hosts für die Verbindung mit Ihrem ASA r2-System finden Sie in der Dokumentation zu ONTAP-SAN-Hosts für und.

Migrieren Sie virtuelle VMware-Maschinen

Wenn Sie Ihren VM-Workload von einem ASA Storage-System auf ein ASA r2 Storage-System migrieren müssen, empfiehlt NetApp die Verwendung "VMware vSphere vMotion" für eine Live-Migration Ihrer Daten ohne Unterbrechungen.

Verwandte Informationen

- Erfahren Sie mehr über "die Vorteile der Verwendung von ONTAP für vSphere" .
- Erfahren Sie mehr über"VMware Live Site Recovery mit ONTAP" .
- Erfahren Sie mehr über"Kontinuierliche Verfügbarkeitslösungen für vSphere-Umgebungen" .

Migrieren Sie Daten aus einem Speichersystem eines Drittanbieters

Ab ONTAP 9.17.1 können Sie mit Foreign LUN Import (FLI) Daten von einer LUN auf einem Drittanbieter-Speichersystem auf ein ASA R2-System migrieren. Durch die Verwendung von FLI für Ihre Datenmigration können Sie das Risiko von Datenverlust und Ausfallzeiten während des Migrationsprozesses minimieren.

FLI unterstützt sowohl Online- als auch Offline-Migrationen. Bei einer Online-Migration bleibt das Client-System online, während Daten vom Drittanbieter-Speichersystem auf das ONTAP -Speichersystem kopiert werden. Online-Migrationen werden von Windows-, Linux- und ESXi-Hostbetriebssystemen unterstützt. Bei einer Offline-Migration wird das Client-System offline genommen, die LUN-Daten werden vom Drittanbieter-Speichersystem auf das ONTAP -Speichersystem kopiert und anschließend wieder online geschaltet.

- Erfahren Sie, wie Sie eine "FLI Offline-Migration" .
- Erfahren Sie, wie Sie eine "FLI Online-Migrationen" .

Konfigurieren Sie Ihr ASA r2-System als Storage-Provider in Ihrer VMware-Umgebung

Mit ONTAP Tools für VMware können Sie Ihr ASA r2 System problemlos als Storage-Anbieter in Ihrer VMware Umgebung einrichten.

ONTAP Tools for VMware vSphere ist ein Satz von Tools, die in Verbindung mit der virtuellen VMware vCenter Server-Appliance (vCSA) für ein einfaches Management von Virtual Machines auf Ihren VMware ESXi-Hosts eingesetzt werden können.

ASA r2-Systeme werden von und höher unterstützt"ONTAP Tools für VMware vSphere 10.3".

Erfahren Sie, wie Sie Folgendes tun können, "Implementieren Sie ONTAP-Tools für VMware" und verwenden Sie es dann, um Folgendes zu tun:

- "Fügen Sie vCenter Server-Instanzen hinzu"
- "Konfigurieren Sie die ESXi-Hosteinstellungen"
- "Ermitteln Sie Ihr ASA r2 Storage-System und Ihre Hosts"

Was kommt als Nächstes?

Sie sind bereit"Bereitstellung von Storage", Ihren SAN-Hosts das Lesen und Schreiben von Daten auf Speichereinheiten zu ermöglichen.

Nutzen Sie ONTAP für das Datenmanagement

ASA r2 Storage-System – Video-Demos

Sehen Sie sich kurze Videos an, die zeigen, wie Sie mit ONTAP System Manager häufige Aufgaben auf ASA r2 Storage-Systemen schnell und einfach ausführen.

Konfigurieren Sie SAN-Protokolle auf Ihrem ASA r2-System

"Video-Transkript"

Stellen Sie SAN Storage auf Ihrem ASA r2-System bereit

"Video-Transkript"

Replizieren Sie Daten von einem ASA r2 System auf einen Remote-Cluster

"Video-Transkript"

Managen Sie Ihren Storage

Stellen Sie ONTAP SAN-Storage auf den ASA r2-Systemen bereit

Wenn Sie Storage bereitstellen, ermöglichen Sie Ihren SAN-Hosts, Daten von ASA r2 Storage-Systemen zu lesen und auf diese zu schreiben. Um Speicher bereitzustellen, erstellen Sie mit ONTAP System Manager Speichereinheiten, fügen Hostinitiatoren hinzu und ordnen den Host einer Speichereinheit zu. Außerdem müssen Sie Schritte auf dem Host durchführen, um Lese-/Schreibvorgänge zu ermöglichen.

Erstellen von Speichereinheiten

Auf einem ASA r2-System stellt eine Storage-Einheit Ihren SAN-Hosts Speicherplatz für Datenoperationen zur Verfügung. Eine Storage-Einheit bezieht sich auf eine LUN für SCSI-Hosts oder einen NVMe-Namespace für NVMe-Hosts. Wenn Ihr Cluster zur Unterstützung von SCSI-Hosts konfiguriert ist, werden Sie aufgefordert, eine LUN zu erstellen. Wenn das Cluster zur Unterstützung von NVMe Hosts konfiguriert ist, werden Sie aufgefordert, einen NVMe Namespace zu erstellen. Eine ASA r2-Speichereinheit hat eine maximale Kapazität von 128 TB.

Im "NetApp Hardware Universe" finden Sie die aktuellen Storage-Grenzwerte für ASA r2 Systeme.

Host-Initiatoren werden der Speichereinheit als Teil der Erstellung der Speichereinheit hinzugefügt und zugeordnet. Sie können "Fügen Sie Host-Initiatoren hinzu" "Karte"sie auch an Ihre Speichereinheiten übertragen, nachdem die Speichereinheiten erstellt wurden.

Schritte

1. Wählen Sie im System Manager **Storage** und anschließend aus 

.
2. Geben Sie einen Namen für die neue Speichereinheit ein.
3. Geben Sie die Anzahl der Einheiten ein, die Sie erstellen möchten.

   Wenn Sie mehr als eine Speichereinheit erstellen, wird jede Einheit mit derselben Kapazität, demselben

Host-Betriebssystem und derselben Host-Zuordnung erstellt.

4. Geben Sie die Kapazität der Speichereinheit ein, und wählen Sie dann das Host-Betriebssystem aus.
5. Akzeptieren Sie die automatisch ausgewählte **Host-Zuordnung**, oder wählen Sie eine andere Host-Gruppe für die zuzuordnende Speichereinheit aus.

   Host Mapping bezieht sich auf die Hostgruppe, der die neue Speichereinheit zugeordnet wird. Wenn für den Hosttyp, den Sie für Ihre neue Speichereinheit ausgewählt haben, eine bereits vorhandene Hostgruppe vorhanden ist, wird die vorhandene Hostgruppe automatisch für Ihre Hostzuordnung ausgewählt. Sie können die Host-Gruppe akzeptieren, die automatisch für Ihre Host-Zuordnung ausgewählt ist, oder Sie können eine andere Host-Gruppe auswählen.

   Wenn keine Host-Gruppe für Hosts vorhanden ist, die auf dem angegebenen Betriebssystem ausgeführt werden, erstellt ONTAP automatisch eine neue Host-Gruppe.

6. Wenn Sie einen der folgenden Schritte ausführen möchten, wählen Sie **Weitere Optionen** und führen Sie die erforderlichen Schritte aus.

Option	Schritte
Ändern Sie die standardmäßige QoS-Richtlinie (Quality of Service) Wenn die Standard-QoS-Richtlinie zuvor nicht auf der Storage Virtual Machine (VM) festgelegt wurde, auf der die Speichereinheit erstellt wird, ist diese Option nicht verfügbar.	a. Wählen Sie unter **Speicher und Optimierung** neben **Quality of Service (QoS)** die Option ⌄. b. Wählen Sie eine vorhandene QoS-Richtlinie aus.

Option	Schritte
Neue QoS-Richtlinie erstellen	a. Wählen Sie unter **Speicher und Optimierung** neben **Quality of Service (QoS)** die Option ⌄ . b. Wählen Sie **neue Richtlinie definieren**. c. Geben Sie einen Namen für die neue QoS-Richtlinie ein. d. Legen Sie eine QoS-Grenze, eine QoS-Garantie oder beides fest. i. Geben Sie unter **Limit** optional eine maximale Durchsatzgrenze, eine maximale IOPS-Grenze oder beides ein. Die Festlegung eines maximalen Durchsatzes und IOPS für eine Speichereinheit schränkt ihre Auswirkungen auf die Systemressourcen ein, sodass sie die Performance kritischer Workloads nicht beeinträchtigt. ii. Geben Sie optional unter **Guarantee** einen minimalen Durchsatz, ein Minimum an IOPS oder beides ein. Durch die Festlegung eines minimalen Durchsatzes und IOPS für eine Storage-Einheit wird sichergestellt, dass unabhängig von der Nachfrage durch konkurrierende Workloads minimale Performance-Ziele erfüllt werden. e. Wählen Sie **Hinzufügen**.
Ändern Sie das Standard-Performance-Service-Level. ASA r2-Systeme bieten zwei Leistungsstufen. Der Standard-Performance-Level ist **Extreme**, das höchste verfügbare Level. Sie können das Leistungsniveau auf **Leistung** senken.	a. Wählen Sie unter **Speicher und Optimierung** neben dem **Performance Service Level** die Option ⌄. b. Wählen Sie * Leistung*.
Fügen Sie einen neuen SCSI-Host hinzu	a. Wählen Sie unter **Host Information SCSI** für das Verbindungsprotokoll aus. b. Wählen Sie das Host-Betriebssystem aus. c. Wählen Sie unter **Host Mapping New Hosts** aus. d. Wählen Sie **FC** oder **iSCSI**. e. Wählen Sie vorhandene Host-Initiatoren aus, oder wählen Sie **Add Initiator**, um einen neuen Host-Initiator hinzuzufügen. Ein Beispiel für einen gültigen FC-WWPN ist „01:02:03:04:0a:0b:0c:0d“. Beispiele für gültige iSCSI-Initiatornamen sind „iqn.1995-08.com.example:string"“ und „eui.0123456789abcdef“.

Option	Schritte
Erstellen Sie eine neue SCSI-Host-Gruppe	a. Wählen Sie unter **Host Information SCSI** für das Verbindungsprotokoll aus. b. Wählen Sie das Host-Betriebssystem aus. c. Wählen Sie unter **Host Mapping Neue Host-Gruppe** aus. d. Geben Sie einen Namen für die Host-Gruppe ein, und wählen Sie dann die Hosts aus, die der Gruppe hinzugefügt werden sollen.
Hinzufügen eines neuen NVMe-Subsystems	a. Wählen Sie unter **Host Information NVMe** für das Verbindungsprotokoll aus. b. Wählen Sie das Host-Betriebssystem aus. c. Wählen Sie unter **Host Mapping New NVMe Subsystem** aus. d. Geben Sie einen Namen für das Subsystem ein, oder übernehmen Sie den Standardnamen. e. Geben Sie einen Namen für den Initiator ein. f. Wenn Sie die bandinterne Authentifizierung oder Transport Layer Security (TLS) aktivieren möchten, wählen Sie ; und dann Ihre Optionen aus. Die in-Band-Authentifizierung ermöglicht eine sichere bidirektionale und unidirektionale Authentifizierung zwischen den NVMe Hosts und dem ASA r2 System. TLS verschlüsselt alle Daten, die zwischen Ihren NVMe/TCP-Hosts und Ihrem ASA r2-System über das Netzwerk gesendet werden. g. Wählen Sie **Add Initiator**, um weitere Initiatoren hinzuzufügen. Die Host-NQN sollte als <nqn.yyyy-mm> formatiert werden, gefolgt von einem vollständig qualifizierten Domänennamen. Das Jahr muss mindestens 1970 Jahre entsprechen. Die maximale Gesamtlänge sollte 223 betragen. Ein Beispiel für einen gültigen NVMe-Initiator ist nqn.2014-08.com.example:string

7. Wählen Sie **Hinzufügen**.

Was kommt als Nächstes?

Die Speichereinheiten werden erstellt und den Hosts zugeordnet. Sie können jetzt "Erstellen von Snapshots"die Daten auf Ihrem ASA r2-System sichern.

Finden Sie weitere Informationen

Erfahren Sie mehr über "So verwenden ASA r2-Systeme Storage Virtual Machines".

Fügen Sie Host-Initiatoren hinzu

Sie können Ihrem ASA r2-System jederzeit neue Hostinitiatoren hinzufügen. Initiatoren stellen die Hosts für den Zugriff auf Speichereinheiten und die Durchführung von Datenoperationen zur Verfügung.

Bevor Sie beginnen

Wenn Sie die Hostkonfiguration während des Hinzufügens der Hostinitiatoren auf ein Zielcluster replizieren möchten, muss sich Ihr Cluster in einer Replikationsbeziehung befinden. Optional können Sie "Erstellen Sie eine Replikationsbeziehung"nach dem Hinzufügen Ihres Hosts.

Fügen Sie Host-Initiatoren für SCSI- oder NVMe-Hosts hinzu.

SCSI-Hosts

Schritte

1. Wählen Sie **Host**.
2. Wählen Sie **SCSI**, und wählen Sie dann + Add.
3. Geben Sie den Hostnamen ein, wählen Sie das Host-Betriebssystem aus und geben Sie eine Hostbeschreibung ein.
4. Wenn Sie die Hostkonfiguration auf einen Zielcluster replizieren möchten, wählen Sie **Replicate Host Configuration** aus, und wählen Sie dann den Zielcluster aus.

   Ihr Cluster muss sich in einer Replikationsbeziehung befinden, um die Hostkonfiguration replizieren zu können.

5. Fügen Sie neue oder vorhandene Hosts hinzu.

Fügen Sie neue Hosts hinzu	Fügen Sie vorhandene Hosts hinzu
a. Wählen Sie **Neue Hosts**. b. Wählen Sie **FC** oder **iSCSI** aus, und wählen Sie dann die Host-Initiatoren aus. c. Wählen Sie optional **Configure Host Proximity**. Durch das Konfigurieren der Host-Nähe kann ONTAP den Controller identifizieren, der dem Host am nächsten ist, um den Datenpfad zu optimieren und die Latenz zu verringern. Dies gilt nur, wenn Sie Daten an einem Remote-Standort repliziert haben. Wenn Sie keine Snapshot-Replikation eingerichtet haben, müssen Sie diese Option nicht auswählen. d. Wenn Sie neue Initiatoren hinzufügen müssen, wählen Sie **Initiatoren hinzufügen** aus.	a. Wählen Sie **existing Hosts**. b. Wählen Sie den Host aus, den Sie hinzufügen möchten. c. Wählen Sie **Hinzufügen**.

6. Wählen Sie **Hinzufügen**.

Was kommt als Nächstes?

Ihre SCSI-Hosts werden Ihrem ASA r2-System hinzugefügt, und Sie können Ihre Hosts Ihren Speichereinheiten zuordnen.

NVMe-Hosts

Schritte

1. Wählen Sie **Host**.
2. Wählen Sie **NVMe** aus, und wählen Sie dann + Add.
3. Geben Sie einen Namen für das NVMe-Subsystem ein, wählen Sie das Host-Betriebssystem aus und geben Sie eine Beschreibung ein.
4. Wählen Sie **Add Initiator**.

Was kommt als Nächstes?

Ihre NVMe Hosts werden Ihrem ASA r2 System hinzugefügt, und Sie können Ihre Hosts Ihren Storage-Einheiten zuordnen.

Ordnen Sie die Speichereinheit einem Host zu

Nachdem Sie die ASA r2 Storage-Einheiten erstellt und Host-Initiatoren hinzugefügt haben, müssen Sie Ihre Hosts den Storage-Einheiten zuordnen, um mit der Datenbereitstellung zu beginnen. Speichereinheiten werden Hosts im Rahmen der Erstellung der Speichereinheit zugeordnet. Sie können vorhandene Storage-Einheiten jederzeit neuen oder bestehenden Hosts zuordnen.

Schritte

1. Wählen Sie **Speicher**.
2. Bewegen Sie den Mauszeiger über den Namen der zu zuordnungsenden Speichereinheit.
3. Wählen Sie ⋮; und dann **Zuordnung zu Hosts**.
4. Wählen Sie die Hosts aus, die der Speichereinheit zugeordnet werden sollen, und wählen Sie dann **Karte**.

Was kommt als Nächstes?

Die Speichereinheit wird Ihren Hosts zugeordnet, und Sie können den Bereitstellungsprozess auf Ihren Hosts abschließen.

Vollständige Host-seitige Bereitstellung

Nachdem Sie die Speichereinheiten erstellt, die Hostinitiatoren hinzugefügt und die Speichereinheiten zugeordnet haben, müssen Sie auf den Hosts Schritte ausführen, bevor sie Daten auf dem ASA r2-System lesen und schreiben können.

Schritte

1. Bei FC und FC/NVMe sollten Sie Ihre FC-Switches mit WWPN Zone.

   Verwenden Sie eine Zone pro Initiator und schließen Sie alle Ziel-Ports in jeder Zone an.

2. Entdecken Sie die neue Speichereinheit.
3. Initialisieren Sie die Speichereinheit und ein CREATE-Dateisystem.
4. Überprüfen Sie, ob Ihr Host Daten auf der Speichereinheit lesen und schreiben kann.

Was kommt als Nächstes?

Sie haben den Bereitstellungsprozess abgeschlossen und können mit der Datenbereitstellung beginnen. Sie können jetzt "Erstellen von Snapshots"die Daten auf Ihrem ASA r2-System sichern.

Finden Sie weitere Informationen

Weitere Informationen zur Konfiguration auf Hostseite finden Sie im "ONTAP SAN-Host-Dokumentation" für Ihren spezifischen Host.

Klonen von Daten auf ASA r2 Storage-Systemen

Das Klonen von Daten erstellt mithilfe von ONTAP System Manager Kopien von Storage-Einheiten und Konsistenzgruppen auf dem ASA r2 System, die sich zur Entwicklung von Applikationen, für Tests, Backups, Datenmigration oder andere administrative Funktionen

einsetzen lassen.

Storage-Einheiten klonen

Wenn Sie eine Storage-Einheit klonen, erstellen Sie auf Ihrem ASA r2-System eine neue Storage-Einheit, die eine zeitpunktgenaue, beschreibbare Kopie der geklonten Storage-Einheit ist.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Bewegen Sie den Mauszeiger über den Namen der Speichereinheit, die Sie klonen möchten.
3. Wählen Sie ⋮; und dann **Clone**.
4. Übernehmen Sie den Standardnamen für die neue Speichereinheit, die als Klon erstellt werden soll, oder geben Sie einen neuen ein.
5. Wählen Sie das Host-Betriebssystem aus.

   Standardmäßig wird ein neuer Snapshot für den Klon erstellt.

6. Wenn Sie einen vorhandenen Snapshot verwenden, eine neue Host-Gruppe erstellen oder einen neuen Host hinzufügen möchten, wählen Sie **Weitere Optionen**.

Option	Schritte
Verwenden Sie einen vorhandenen Snapshot	a. Wählen Sie unter **Snapshot to Clone Use an existing snaphot** aus. b. Wählen Sie den Snapshot aus, den Sie für den Klon verwenden möchten.
Erstellen Sie eine neue Hostgruppe	a. Wählen Sie unter **Host Mapping New Host Group** aus. b. Geben Sie einen Namen für die neue Host-Gruppe ein, und wählen Sie dann die Host-Initiatoren aus, die in die Gruppe aufgenommen werden sollen.
Fügen Sie einen neuen Host hinzu	a. Wählen Sie unter **Host Mapping New Hosts** aus. b. Geben Sie den A-Namen für den neuen Host ein, und wählen Sie dann **FC** oder **iSCSI** aus. c. Wählen Sie die Host-Initiatoren aus der Liste der vorhandenen Initiatoren aus, oder wählen Sie **Add**, um neue Initiatoren für den Host hinzuzufügen.

7. Wählen Sie **Clone**.

Was kommt als Nächstes?

Sie haben eine neue Storage-Einheit erstellt, die mit der von Ihnen geklonten Storage-Einheit identisch ist. Sie können die neue Speichereinheit jetzt nach Bedarf verwenden.

Klonen von Konsistenzgruppen

Wenn Sie eine Konsistenzgruppe klonen, erstellen Sie eine neue Konsistenzgruppe, die in der Struktur, den Storage-Einheiten und den Daten der von Ihnen geklonten Konsistenzgruppe identisch ist. Verwenden Sie einen Konsistenzgruppenklon, um Applikationstests durchzuführen oder Daten zu migrieren. Angenommen, Sie müssen einen Produktions-Workload aus einer Konsistenzgruppe migrieren. Sie können die Konsistenzgruppe klonen, um eine Kopie Ihres Produktions-Workloads zu erstellen, die als Backup gewartet werden soll, bis die Migration abgeschlossen ist.

Der Klon wird aus einem Snapshot der zu klonenden Konsistenzgruppe erstellt. Der für den Klon verwendete Snapshot wird zu dem Zeitpunkt erstellt, zu dem der Klonprozess standardmäßig initiiert wird. Sie können das Standardverhalten ändern, um einen vorhandenen Snapshot zu verwenden.

Im Rahmen des Klonens werden Zuordnungen von Storage-Einheiten kopiert. Snapshot-Richtlinien werden im Rahmen des Klonprozesses nicht kopiert.

Sie können Klone von Konsistenzgruppen erstellen, die lokal auf Ihrem ASA r2-System gespeichert sind, oder von Konsistenzgruppen, die an Remote-Standorte repliziert wurden.

Klonen mit lokalem Snapshot

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Bewegen Sie den Mauszeiger über die Konsistenzgruppe, die Sie klonen möchten.
3. Wählen Sie ⋮, und wählen Sie dann **Clone**.
4. Geben Sie einen Namen für einen Konsistenzgruppenklon ein, oder übernehmen Sie den Standardnamen.
5. Wählen Sie das Host-Betriebssystem aus.
6. Wenn Sie den Clone von der Quell-Consistency Group trennen und Speicherplatz zuweisen möchten, wählen Sie **Split Clone** aus.
7. Wenn Sie einen vorhandenen Snapshot verwenden möchten, erstellen Sie eine neue Host-Gruppe oder fügen Sie einen neuen Host für den Klon hinzu, wählen Sie **Weitere Optionen**.

Option	Schritte
Verwenden Sie einen vorhandenen Snapshot	a. Wählen Sie unter **Snapshot to Clone** die Option **Use an existing Snapshot** aus. b. Wählen Sie den Snapshot aus, den Sie für den Klon verwenden möchten.
Erstellen Sie eine neue Hostgruppe	a. Wählen Sie unter **Host Mapping New Host Group** aus. b. Geben Sie einen Namen für die neue Host-Gruppe ein, und wählen Sie dann die Host-Initiatoren aus, die in die Gruppe aufgenommen werden sollen.
Fügen Sie einen neuen Host hinzu	a. Wählen Sie unter **Host Mapping New Hosts** aus. b. Geben Sie den Namen des neuen Hostnamens ein, und wählen Sie dann **FC** oder **iSCSI**. c. Wählen Sie die Host-Initiatoren aus der Liste der vorhandenen Initiatoren aus, oder wählen Sie **Add Initiator**, um neue Initiatoren für den Host hinzuzufügen.

8. Wählen Sie **Clone**.

Klonen mit Remote-Snapshot

Schritte

1. Wählen Sie in System Manager **Schutz > Replikation** aus.
2. Bewegen Sie den Mauszeiger über die **Quelle**, die Sie klonen möchten.
3. Wählen Sie ⋮, und wählen Sie dann **Clone**.
4. Wählen Sie das Quell-Cluster und die Storage-VM aus und geben Sie dann einen Namen für die

neue Konsistenzgruppe ein, oder übernehmen Sie den Standardnamen.

5. Wählen Sie den zu klonenden Snapshot aus, und wählen Sie dann **Clone** aus.

Was kommt als Nächstes?

Sie haben von Ihrem Remote-Standort aus eine Konsistenzgruppe geklont. Die neue Konsistenzgruppe ist lokal auf Ihrem ASA r2 System verfügbar und kann nach Bedarf verwendet werden.

Was kommt als Nächstes?

Zum Schutz der Daten sollten Sie "Erstellen von Snapshots"die geklonte Konsistenzgruppe verwenden.

Teilen Sie den Klon der Konsistenzgruppe auf

Wenn Sie einen Konsistenzgruppenklon aufteilen, trennen Sie den Klon von der Quell-Konsistenzgruppe und weisen dem Klon Speicherplatz zu. Der Klon wird zu einer eigenständigen Konsistenzgruppe, die unabhängig von der Konsistenzgruppe der Quelle verwendet werden kann.

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Bewegen Sie den Mauszeiger über den zu teilenden Konsistenzgruppenklon.
3. Wählen Sie **Clone teilen**.
4. Wählen Sie **Split**.

Ergebnis

Der Klon ist von der Quell-Konsistenzgruppe getrennt, und der Festplattenspeicher des Klons wird zugewiesen.

Verwalten von Hostgruppen

Erstellen Sie Hostgruppen auf Ihrem ASA R2-System

Auf einem ASA r2-System ist eine *Host-Gruppe* der Mechanismus, der verwendet wird, um Hosts Zugriff auf Speichereinheiten zu gewähren. Eine Host-Gruppe bezieht sich auf eine Initiatorgruppe für SCSI-Hosts oder auf ein NVMe-Subsystem für NVMe-Hosts. Ein Host kann nur die Speichereinheiten sehen, die den Host-Gruppen zugeordnet sind, zu denen er gehört. Wenn eine Hostgruppe einer Speichereinheit zugeordnet ist, können die Hosts, die Mitglieder der Gruppe sind, die Speichereinheit mounten (Verzeichnisse und Dateistrukturen erstellen).

Hostgruppen werden automatisch oder manuell erstellt, wenn Sie Ihre Speichereinheiten erstellen. Sie können optional die folgenden Schritte ausführen, um Hostgruppen vor oder nach der Erstellung der Speichereinheit zu erstellen.

Schritte

1. Wählen Sie im System Manager **Host** aus.
2. Wählen Sie die Hosts aus, die Sie der Host-Gruppe hinzufügen möchten.

   Nachdem Sie den ersten Host ausgewählt haben, wird die Option zum Hinzufügen zu einer Host-Gruppe über der Liste der Hosts angezeigt.

3. Wählen Sie **zu Host-Gruppe hinzufügen**.
4. Suchen Sie nach der Hostgruppe, der Sie den Host hinzufügen möchten, und wählen Sie sie aus.

Was kommt als Nächstes?

Sie haben eine Hostgruppe erstellt und können nun "ordnen Sie es einer Speichereinheit zu" .

Löschen einer Hostgruppe auf Ihrem ASA R2-System

Auf einem ASA R2-System dient eine Hostgruppe dazu, Hosts Zugriff auf Speichereinheiten zu gewähren. Eine Hostgruppe bezeichnet eine igroup für SCSI-Hosts oder ein NVMe-Subsystem für NVMe-Hosts. Ein Host kann nur die Speichereinheiten sehen, die den zugehörigen Hostgruppen zugeordnet sind. Sie können eine Hostgruppe löschen, wenn die Hosts in der Gruppe keinen Zugriff mehr auf die zugeordneten Speichereinheiten haben sollen.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie unter **Host-Zuordnung** die Host-Gruppe aus, die Sie löschen möchten.
3. Wählen Sie **Zugeordneter Speicher**.
4. Wählen Sie **Mehr** und dann **Löschen**.
5. Wählen Sie zur Bestätigung, dass Sie fortfahren möchten, und wählen Sie dann **Löschen**.

Was kommt als Nächstes?

Die Hostgruppe wird gelöscht. Die Hosts in der Gruppe haben keinen Zugriff mehr auf die Speichereinheiten, die der Hostgruppe zugeordnet waren.

Verwaltung von Storage-Einheiten

Ändern Sie die Speichereinheiten auf ASA r2-Speichersystemen

Zum Optimieren der Performance auf Ihrem ASA r2 System müssen Sie möglicherweise Ihre Storage-Einheiten anpassen, um deren Kapazität zu erhöhen, QoS-Richtlinien zu aktualisieren oder die Hosts zu ändern, die den Einheiten zugeordnet sind. Wenn beispielsweise ein neuer, kritischer Applikations-Workload zu einer vorhandenen Storage-Einheit hinzugefügt wird, müssen Sie möglicherweise die Richtlinie zur Quality of Service (QoS), die auf die Storage-Einheit angewendet wird, ändern, um das Performance-Level zu unterstützen, das für die neue Applikation erforderlich ist.

Erhöhte Kapazität

Vergrößern Sie eine Speichereinheit, bevor sie die volle Kapazität erreicht, um einen Verlust des Datenzugriffs zu verhindern, der auftreten kann, wenn der beschreibbare Speicherplatz der Speichereinheit nicht mehr verfügbar ist. Die Kapazität einer Speichereinheit kann auf 128 TB erhöht werden, was der von ONTAP maximal zulässigen Größe entspricht.

Ändern von Host-Zuordnungen

Ändern Sie die Hosts, die einer Speichereinheit zugeordnet sind, um den Workload-Ausgleich oder die Neukonfiguration der Systemressourcen zu unterstützen.

QoS-Richtlinie ändern

Die Richtlinien zur Quality of Service (QoS) garantieren, dass die Performance bei kritischen Workloads nicht durch konkurrierende Workloads beeinträchtigt wird. Mithilfe von QoS-Richtlinien können Sie einen QoS Throughput *Limit* und einen QoS Throughput *guarantee* festlegen.

- QoS-Durchsatzbegrenzung

  Der QoS Throughput *Limit* begrenzt die Auswirkungen eines Workloads auf Systemressourcen, indem der Durchsatz des Workloads auf eine maximale Anzahl an IOPS oder MB/s bzw. IOPS und MB/s begrenzt wird.

- QoS-Durchsatzgarantie

  Der QoS Throughput *guarantee* sorgt dafür, dass kritische Workloads unabhängig von der Anforderung durch konkurrierende Workloads Mindestdurchsatzziele erfüllen, indem sichergestellt wird, dass der Durchsatz für den kritischen Workload nicht unter eine Mindestanzahl an IOPS oder MB/s bzw. IOPS und MB/s fällt.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Bewegen Sie den Mauszeiger über den Namen der Speichereinheit, die Sie bearbeiten möchten.
3. Wählen Sie ⋮; und dann **Bearbeiten**.
4. Aktualisieren Sie die Parameter der Speichereinheit nach Bedarf, um die Kapazität zu erhöhen, die QoS-Richtlinie zu ändern und die Host-Zuordnung zu aktualisieren.

Was kommt als Nächstes?

Wenn Sie die Größe der Speichereinheit erhöht haben, müssen Sie die Speichereinheit auf dem Host erneut scannen, damit der Host die Änderung der Größe erkennen kann.

Verschieben Sie Speichereinheiten auf ASA r2-Speichersystemen

Wenn in einer Storage-Verfügbarkeitszone der Speicherplatz knapp ist, können Sie Storage-Einheiten auf eine andere Storage-Verfügbarkeitszone verschieben, um die Storage-Auslastung im Cluster auszugleichen.

Sie können eine Storage-Einheit verschieben, während die Storage-Einheit online ist und Daten bereitstellt. Der Verschiebungsvorgang ist unterbrechungsfrei.

Bevor Sie beginnen

- Sie müssen ONTAP 9.16.1 oder höher ausführen.
- Der Cluster muss aus vier oder mehr Nodes bestehen.

Schritte

1. Wählen Sie im System Manager **Storage** aus, und wählen Sie dann die zu verschiebende Speichereinheit aus.
2. Wählen Sie ⋮; und dann **move**.
3. Wählen Sie die Speicherverfügbarkeitszone aus, in die die Speichereinheit verschoben werden soll, und wählen Sie dann **move**.

Löschen Sie Speichereinheiten auf ASA r2-Speichersystemen

Löschen Sie eine Speichereinheit, wenn Sie die in der Einheit enthaltenen Daten nicht mehr verwalten müssen. Durch Löschen von nicht mehr benötigten Speichereinheiten können Sie Speicherplatz für andere Hostanwendungen freigeben.

Bevor Sie beginnen

Wenn sich die zu löschende Speichereinheit in einer Konsistenzgruppe befindet, die sich in der Replikationsbeziehung befindet, müssen Sie "Entfernen Sie die Speichereinheit aus der Konsistenzgruppe"sie vor dem Löschen unbedingt löschen.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Bewegen Sie den Mauszeiger über den Namen der zu löschenden Speichereinheit.
3. Wählen Sie ⋮; und dann **Löschen**.
4. Bestätigen Sie, dass der Löschvorgang nicht rückgängig gemacht werden kann.
5. Wählen Sie **Löschen**.

Was kommt als Nächstes?

Sie können den Speicherplatz, "Vergrößern Sie die Größe"der von der gelöschten Speichereinheit zu den Speichereinheiten freigegeben wird, die zusätzliche Kapazität benötigen, verwenden.

ASA r2 Storage-Grenzwerte

Für optimale Performance, Konfiguration und Support sollten Sie die ASA r2 Storage-Grenzwerte kennen.

ASA r2-Systeme unterstützen Folgendes:

Maximale Anzahl von Knoten pro Cluster	12
Maximale Anzahl von Speichereinheiten pro Cluster	30.000
Maximale Speichereinheitsgröße	128 TB
Maximale Größe der Speicherverfügbarkeitszone	2 PB

Finden Sie weitere Informationen

Eine vollständige Liste der aktuellen ASA r2-Speicherlimits finden Sie unter "NetApp Hardware Universe".

Sichern Sie Ihre Daten

Erstellen Sie Snapshots für die Sicherung Ihrer Daten auf ASA r2 Storage-Systemen

Um Daten auf Ihrem ASA r2-System zu sichern, müssen Sie einen Snapshot erstellen. Mit ONTAP System Manager können Sie einen manuellen Snapshot einer einzelnen Storage-Einheit erstellen oder eine Konsistenzgruppe erstellen und automatische

Snapshots mehrerer Storage-Einheiten gleichzeitig planen.

Schritt 1: Optional: Erstellen Sie eine Konsistenzgruppe

Eine Konsistenzgruppe ist eine Sammlung von Speichereinheiten, die als eine Einheit gemanagt werden. Erstellen von Konsistenzgruppen zur Vereinfachung des Storage-Managements und der Datensicherung bei Applikations-Workloads über mehrere Storage-Einheiten hinweg Angenommen, Sie haben eine Datenbank, die aus 10 Speichereinheiten in einer Konsistenzgruppe besteht, und Sie müssen die gesamte Datenbank sichern. Anstatt jede Storage-Einheit zu sichern, können Sie die gesamte Datenbank sichern, indem Sie der Konsistenzgruppe einfach Snapshot-Datenschutz hinzufügen.

Erstellen Sie eine Konsistenzgruppe mit neuen Speichereinheiten oder erstellen Sie eine Konsistenzgruppe mit vorhandenen Speichereinheiten.

Wenn Sie eine Konsistenzgruppe mit neuen Storage-Einheiten erstellen, können Sie jeder Storage-Einheit eine unterschiedliche Kapazität zuweisen, das Standard-Service-Level für die Performance ändern und bis zu fünf untergeordnete Konsistenzgruppen erstellen. Wenn Sie eine Konsistenzgruppe mit vorhandenen Speichereinheiten erstellen, können Sie bereits verwendete Speichereinheiten hinzufügen.

Neue Speichereinheiten verwenden

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Wählen Sie + Add; und dann **mit neuen Speichereinheiten**.
3. Geben Sie einen Namen für die neue Speichereinheit, die Anzahl der Einheiten und die Kapazität pro Einheit ein.

   Wenn Sie mehr als eine Einheit erstellen, wird jede Einheit standardmäßig mit derselben Kapazität und demselben Host-Betriebssystem erstellt. Optional können Sie jeder Einheit eine andere Kapazität zuweisen.

4. Wenn Sie einen der folgenden Schritte ausführen möchten, wählen Sie **Weitere Optionen** und führen Sie die erforderlichen Schritte aus.

Option	Schritte
Weisen Sie jeder Speichereinheit eine andere Kapazität zu	Wählen Sie **eine andere Kapazität hinzufügen**.
Ändern Sie das Standard-Performance-Service-Level	Wählen Sie unter **Performance Service Level** einen anderen Service Level aus.
Erstellen einer untergeordneten Konsistenzgruppe	Wählen Sie **untergeordnete Consistency Group hinzufügen**.

5. Wählen Sie das Host-Betriebssystem und die Host-Zuordnung aus.
6. Wählen Sie **Hinzufügen**.

Was kommt als Nächstes?

Sie haben eine Konsistenzgruppe erstellt, die die Speichereinheiten enthält, die Sie schützen möchten. Sie können jetzt einen Snapshot erstellen.

Nutzung vorhandener Storage-Einheiten

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Wählen Sie + Add; und dann **mit vorhandenen Speichereinheiten**.
3. Geben Sie einen Namen für die Konsistenzgruppe ein, suchen Sie dann nach, und wählen Sie die Speichereinheiten aus, die in die Konsistenzgruppe aufgenommen werden sollen.
4. Wählen Sie **Hinzufügen**.

Was kommt als Nächstes?

Sie haben eine Konsistenzgruppe erstellt, die die Speichereinheiten enthält, die Sie schützen möchten. Sie können jetzt einen Snapshot erstellen.

Schritt 2: Erstellen Sie einen Snapshot

Ein Snapshot ist eine lokale, schreibgeschützte Kopie Ihrer Daten, mit der Sie Storage-Einheiten zu einem bestimmten Zeitpunkt wiederherstellen können.

Snapshots können nach Bedarf erstellt werden, oder sie können automatisch in regelmäßigen Abständen auf Basis eines erstellt werden"snapshot Richtlinie und Zeitplan". Die Snapshot-Richtlinie und der Zeitplan legen fest, wann die Snapshots erstellt werden sollen, wie viele Kopien beibehalten werden sollen, wie sie benannt werden und wie sie für die Replikation beschriftet werden sollen. Beispielsweise erstellt ein System jeden Tag um 12:10 Uhr einen Snapshot, behält die beiden neuesten Kopien bei, benennt sie „täglich“ (angehängt mit einem Zeitstempel) und kennzeichnet sie zur Replizierung „täglich“.

Snapshot-Typen

Sie können einen On-Demand-Snapshot einer einzelnen Speichereinheit oder einer Konsistenzgruppe erstellen. Sie können automatische Snapshots einer Konsistenzgruppe erstellen, die mehrere Speichereinheiten enthält. Sie können keine automatischen Snapshots einer einzelnen Speichereinheit erstellen.

- On-Demand-Snapshots

  Ein On-Demand-Snapshot einer Speichereinheit kann jederzeit erstellt werden. Die Speichereinheit muss kein Mitglied einer Consistency Group sein, die durch einen On-Demand-Snapshot geschützt werden soll. Wenn Sie einen On-Demand-Snapshot einer Speichereinheit erstellen, die Mitglied einer Konsistenzgruppe ist, werden die anderen Speichereinheiten der Konsistenzgruppe nicht in den On-Demand-Snapshot aufgenommen. Wenn Sie einen On-Demand-Snapshot einer Konsistenzgruppe erstellen, werden alle Speichereinheiten in der Konsistenzgruppe in den Snapshot aufgenommen.

- Automatisierte Snapshots

  Automatisierte Snapshots werden mit Snapshot-Richtlinien erstellt. Um eine Snapshot-Richtlinie auf eine Speichereinheit für die automatische Snapshot-Erstellung anzuwenden, muss die Speichereinheit Mitglied einer Konsistenzgruppe sein. Wenn Sie eine Snapshot-Richtlinie auf eine Konsistenzgruppe anwenden, werden alle Speichereinheiten in der Konsistenzgruppe durch automatische Snapshots geschützt.

Erstellen Sie einen Snapshot einer Konsistenzgruppe oder einer Speichereinheit.

Snapshot einer Konsistenzgruppe

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Bewegen Sie den Mauszeiger über den Namen der Konsistenzgruppe, die Sie schützen möchten.
3. Wählen Sie ⋮ ; und dann **protect**.
4. Wenn Sie einen sofortigen Snapshot nach Bedarf erstellen möchten, wählen Sie unter **lokaler Schutz Jetzt Snapshot hinzufügen** aus.

   Der lokale Schutz erstellt den Snapshot auf demselben Cluster, das die Speichereinheit enthält.

   a. Geben Sie einen Namen für den Snapshot ein, oder übernehmen Sie den Standardnamen, und geben Sie optional eine SnapMirror-Bezeichnung ein.

      Das SnapMirror-Label wird vom entfernten Ziel verwendet.

5. Wenn Sie automatisierte Snapshots mithilfe einer Snapshot-Richtlinie erstellen möchten, wählen Sie **Snapshots planen**.

   a. Wählen Sie eine Snapshot-Richtlinie aus.

      Akzeptieren Sie die standardmäßige Snapshot-Richtlinie, wählen Sie eine vorhandene Richtlinie aus, oder erstellen Sie eine neue Richtlinie.

Option	Schritte
Wählen Sie eine vorhandene Snapshot-Richtlinie aus	Wählen Sie ⌄ neben der Standardrichtlinie aus, und wählen Sie dann die vorhandene Richtlinie aus, die Sie verwenden möchten.
Neue Snapshot-Richtlinie erstellen	i. Wählen Sie + Add ; und geben Sie dann die Snapshot Policy-Parameter ein. ii. Wählen Sie **Richtlinie hinzufügen**.

6. Wenn Sie Ihre Snapshots auf einen Remote-Cluster replizieren möchten, wählen Sie unter **Remote-Schutz auf einen Remote-Cluster replizieren**.

   a. Wählen Sie das Quell-Cluster und die Storage-VM aus, und wählen Sie dann die Replizierungsrichtlinie aus.

      Die erste Datenübertragung für die Replikation wird standardmäßig sofort gestartet.

7. Wählen Sie **Speichern**.

Momentaufnahme der Speichereinheit

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Bewegen Sie den Mauszeiger über den Namen der Speichereinheit, die Sie schützen möchten.
3. Wählen Sie ⋮ ; und dann **protect**. Wenn Sie einen sofortigen Snapshot nach Bedarf erstellen möchten, wählen Sie unter **lokaler Schutz Jetzt Snapshot hinzufügen** aus.

Der lokale Schutz erstellt den Snapshot auf demselben Cluster, das die Speichereinheit enthält.

4. Geben Sie einen Namen für den Snapshot ein, oder übernehmen Sie den Standardnamen, und geben Sie optional eine SnapMirror-Bezeichnung ein.

   Das SnapMirror-Label wird vom entfernten Ziel verwendet.

5. Wenn Sie automatisierte Snapshots mithilfe einer Snapshot-Richtlinie erstellen möchten, wählen Sie **Snapshots planen**.

   a. Wählen Sie eine Snapshot-Richtlinie aus.

      Akzeptieren Sie die standardmäßige Snapshot-Richtlinie, wählen Sie eine vorhandene Richtlinie aus, oder erstellen Sie eine neue Richtlinie.

Option	Schritte
Wählen Sie eine vorhandene Snapshot-Richtlinie aus	Wählen Sie ⌄ neben der Standardrichtlinie aus, und wählen Sie dann die vorhandene Richtlinie aus, die Sie verwenden möchten.
Neue Snapshot-Richtlinie erstellen	i. Wählen Sie + Add ; und geben Sie dann die Snapshot Policy-Parameter ein. ii. Wählen Sie **Richtlinie hinzufügen**.

6. Wenn Sie Ihre Snapshots auf einen Remote-Cluster replizieren möchten, wählen Sie unter **Remote-Schutz auf einen Remote-Cluster replizieren**.

   a. Wählen Sie das Quell-Cluster und die Storage-VM aus, und wählen Sie dann die Replizierungsrichtlinie aus.

      Die erste Datenübertragung für die Replikation wird standardmäßig sofort gestartet.

7. Wählen Sie **Speichern**.

Was kommt als Nächstes?

Nachdem Ihre Daten nun durch Snapshots geschützt sind, sollten Sie "Richten Sie die Snapshot-Replikation ein"Ihre Konsistenzgruppen für das Backup und Disaster Recovery an einen geografisch Remote Standort kopieren.

Erstellen Sie eine Intercluster-Speicher-VM-Peer-Beziehung auf ASA R2-Speichersystemen

Eine Peer-Beziehung definiert Netzwerkverbindungen, die Clustern und virtuellen Speichermaschinen (VMs) den sicheren Datenaustausch ermöglichen. Erstellen Sie Peer-Beziehungen zwischen Speicher-VMs auf verschiedenen Clustern, um Datenschutz und Notfallwiederherstellung mit SnapMirror zu ermöglichen.

"Erfahren Sie mehr über Peer-Beziehungen" .

Bevor Sie beginnen

Sie müssen eine Cluster-Peer-Beziehung zwischen dem lokalen und dem Remote-Cluster hergestellt haben,

bevor Sie eine Speicher-VM-Peer-Beziehung erstellen können. "Erstellen einer Cluster-Peer-Beziehung" falls Sie dies nicht bereits getan haben.

Schritte

1. Wählen Sie im System Manager **Schutz > Übersicht**.
2. Wählen Sie unter **Storage-VM-Peers** die Option **Einen Storage-VM-Peer hinzufügen** aus.
3. Wählen Sie die Speicher-VM auf dem lokalen Cluster und dann die Speicher-VM auf dem Remote-Cluster aus.
4. Wählen Sie **Einen Speicher-VM-Peer hinzufügen**.

Replizieren von Snapshots von ASA r2 Storage-Systemen zu einem Remote-Cluster

Die Snapshot-Replizierung ist ein Prozess, bei dem Konsistenzgruppen auf Ihrem ASA r2-System an einen geografischen Standort kopiert werden. Nach der ersten Replikation werden Änderungen an Consistency Groups basierend auf einer Replikationsrichtlinie an den Remote-Standort kopiert. Replizierte Konsistenzgruppen können für Disaster Recovery oder Datenmigration verwendet werden.

> ⓘ Die Snapshot Replizierung für ein ASA r2 Storage-System wird nur von einem anderen ASA r2 Storage-System unterstützt. Sie können keine Snapshots von einem ASA r2-System auf ein aktuelles ASA-, AFF- oder FAS-System oder von einem aktuellen ASA-, AFF- oder FAS-System auf ein ASA r2-System replizieren.

Um die Snapshot-Replikation einzurichten, müssen Sie eine Replikationsbeziehung zwischen Ihrem ASA r2-System und dem Remote-Standort herstellen. Die Replikationsbeziehung wird durch eine Replikationsrichtlinie geregelt. Während der Cluster-Einrichtung wird eine Standardrichtlinie zur Replizierung aller Snapshots erstellt. Sie können die Standardrichtlinie verwenden oder optional eine neue Richtlinie erstellen.

Schritt: Erstellen einer Cluster-Peer-Beziehung

Bevor Sie Ihre Daten schützen können, indem Sie sie auf ein Remote-Cluster replizieren, müssen Sie eine Cluster-Peer-Beziehung zwischen dem lokalen und dem Remote-Cluster erstellen.

Bevor Sie beginnen

Die Voraussetzungen für Cluster-Peering sind für ASA R2-Systeme dieselben wie für andere ONTAP Systeme. "Überprüfen der Voraussetzungen für Cluster-Peering" .

Schritte

1. Wählen Sie im lokalen Cluster im System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie unter **Intercluster Settings** neben **Cluster Peers** die Option , und wählen Sie dann **Cluster Peer hinzufügen** aus.
3. Wählen Sie **Lauch Remote-Cluster** aus; dadurch wird eine Passphrase generiert, die Sie zur Authentifizierung beim Remote-Cluster verwenden werden.
4. Nachdem die Passphrase für den Remote-Cluster generiert wurde, fügen Sie sie unter **Passphrase** auf dem lokalen Cluster ein.
5. Wählen Sie + Add ; und geben Sie dann die IP-Adresse der Intercluster-Netzwerkschnittstelle ein.
6. Wählen Sie **Initiate Cluster Peering** aus.

Was kommt als Nächstes?

Sie haben einen lokalen ASA r2-Cluster mit einem Remote-Cluster erreicht. Sie können jetzt eine Replikationsbeziehung erstellen.

Schritt 2: Erstellen Sie optional eine Replikationsrichtlinie

Die Snapshot-Replikationsrichtlinie legt fest, wann Aktualisierungen am ASA r2-Cluster am Remote-Standort repliziert werden.

Schritte

1. Wählen Sie in System Manager **Schutz > Richtlinien** aus, und wählen Sie dann **Replikationsrichtlinien** aus.
2. Wählen Sie + Add.
3. Geben Sie einen Namen für die Replikationsrichtlinie ein, oder akzeptieren Sie den Standardnamen, und geben Sie dann eine Beschreibung ein.
4. Wählen Sie den Bereich **Policy** aus.

   Wenn Sie die Replikationsrichtlinie auf den gesamten Cluster anwenden möchten, wählen Sie **Cluster** aus. Wenn die Replikationsrichtlinie nur auf die Speichereinheiten in einer bestimmten Speicher-VM angewendet werden soll, wählen Sie **Speicher-VM** aus.

5. Wählen Sie die Option **Policy type** aus.

Option	Schritte
Kopieren Sie die Daten nach dem Schreiben auf die Quelle an den Remote-Standort.	a. Wählen Sie **Asynchron**. b. Akzeptieren Sie unter **Transfer Snapshots from source** den Standard-Übertragungszeitplan oder wählen Sie einen anderen aus. c. Wählen Sie diese Option aus, um alle Snapshots zu übertragen oder Regeln zu erstellen, um festzulegen, welche Snapshots übertragen werden sollen. d. Aktivieren Sie optional die Netzwerkkomprimierung.
Schreiben Sie Daten gleichzeitig an die Quell- und Remote-Standorte.	a. Wählen Sie * Synchron*.

6. Wählen Sie **Speichern**.

Was kommt als Nächstes?

Sie haben eine Replikationsrichtlinie erstellt und sind nun bereit, eine Replikationsbeziehung zwischen Ihrem ASA r2-System und Ihrem Remote-Standort zu erstellen.

Finden Sie weitere Informationen

Erfahren Sie mehr über "Storage VMs für den Client-Zugriff".

Schritt 3: Erstellen einer Replikationsbeziehung

Eine Snapshot-Replikationsbeziehung stellt eine Verbindung zwischen Ihrem ASA r2-System und einem Remote-Standort her, sodass Sie Consistency Groups auf ein Remote-Cluster replizieren können. Replizierte

Konsistenzgruppen können für Disaster Recovery oder Datenmigration verwendet werden.

Wenn Sie Ihre Replizierungsbeziehung einrichten, können Sie zum Schutz vor Ransomware-Angriffen auswählen, um Ziel-Snapshots zu sperren. Gesperrte Snapshots können nicht versehentlich oder böswillig gelöscht werden. Sie können gesperrte Snapshots verwenden, um Daten wiederherzustellen, wenn eine Storage-Einheit durch einen Ransomware-Angriff kompromittiert wird.

Bevor Sie beginnen

Wenn Sie Ihre Ziel-Snapshots sperren möchten, müssen Sie dies "Initialisieren Sie die Snapshot-Compliance-Uhr" vor dem Erstellen der Replikationsbeziehung tun.

Erstellen Sie eine Replikationsbeziehung mit oder ohne gesperrte Ziel-Snapshots.

Mit gesperrten Snapshots

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Wählen Sie eine Konsistenzgruppe aus.
3. Wählen Sie ⋮; und dann **protect**.
4. Wählen Sie unter **Remote Protection Replicate to a Remote Cluster** aus.
5. Wählen Sie die **Replikationsrichtlinie** aus.

   Sie müssen eine *Vault* Replikationsrichtlinie auswählen.

6. Wählen Sie **Zieleinstellungen**.
7. Wählen Sie **Ziel-Snapshots sperren, um das Löschen zu verhindern**
8. Geben Sie den maximalen und minimalen Aufbewahrungszeitraum für Daten ein.
9. Um den Start der Datenübertragung zu verzögern, deaktivieren Sie **Transfer sofort starten**.

   Die erste Datenübertragung beginnt standardmäßig sofort.

10. Um den Standard-Übertragungszeitplan zu überschreiben, wählen Sie optional **Zieleinstellungen** und dann **Übertragungszeitplan überschreiben**.

    Ihr Transferplan muss mindestens 30 Minuten betragen, um unterstützt zu werden.

11. Wählen Sie **Speichern**.

Ohne gesperrte Snapshots

Schritte

1. Wählen Sie in System Manager **Schutz > Replikation** aus.
2. Wählen Sie diese Option aus, um die Replikationsbeziehung mit dem lokalen Ziel oder der lokalen Quelle zu erstellen.

Option	Schritte
Lokale Ziele	a. Wählen Sie **Lokale Ziele**, und wählen Sie dann Replicate. b. Suchen Sie die Quell-Konsistenzgruppe, und wählen Sie sie aus. Die Konsistenzgruppe „*Source*“ bezieht sich auf die Konsistenzgruppe in Ihrem lokalen Cluster, die Sie replizieren möchten.

Option	Schritte
Lokale Quellen	a. Wählen Sie **Lokale Quellen**, und wählen Sie dann Replicate. b. Suchen Sie die Quell-Konsistenzgruppe, und wählen Sie sie aus. Die Konsistenzgruppe „*Source*“ bezieht sich auf die Konsistenzgruppe in Ihrem lokalen Cluster, die Sie replizieren möchten. c. Wählen Sie unter **Replikationsziel** den zu replizierenden Cluster aus, und wählen Sie dann die Speicher-VM aus.

3. Wählen Sie eine Replikationsrichtlinie aus.
4. Um den Start der Datenübertragung zu verzögern, wählen Sie **Zieleinstellungen** und deaktivieren Sie dann **Transfer sofort starten**.

   Die erste Datenübertragung beginnt standardmäßig sofort.
5. Um den Standard-Übertragungszeitplan zu überschreiben, wählen Sie optional **Zieleinstellungen** und dann **Übertragungszeitplan überschreiben**.

   Ihr Transferplan muss mindestens 30 Minuten betragen, um unterstützt zu werden.
6. Wählen Sie **Speichern**.

Was kommt als Nächstes?

Nachdem Sie nun eine Replikationsrichtlinie und -Beziehung erstellt haben, beginnt Ihr erster Datentransfer wie in Ihrer Replikationsrichtlinie definiert. Sie können optional Ihren Replikations-Failover testen, um sicherzustellen, dass ein erfolgreicher Failover auftreten kann, wenn Ihr ASA r2-System offline geht.

Schritt 4: Testen des Replikations-Failovers

Überprüfen Sie optional, ob Sie Daten von replizierten Speichereinheiten auf einem Remote-Cluster erfolgreich bereitstellen können, wenn das Quell-Cluster offline ist.

Schritte

1. Wählen Sie in System Manager **Schutz > Replikation** aus.
2. Bewegen Sie den Mauszeiger über die Replikationsbeziehung, die Sie testen möchten, und wählen Sie dann ⋮.
3. Wählen Sie **Failover testen**.
4. Geben Sie die Failover-Informationen ein, und wählen Sie dann **Failover testen**.

Was kommt als Nächstes?

Da Ihre Daten jetzt mit Snapshot-Replizierung für Disaster Recovery gesichert sind, sollten Sie "Verschlüsselung von Daten im Ruhezustand"sie nicht mehr lesen können, wenn eine Festplatte in Ihrem ASA r2 System neu zugewiesen, zurückgegeben, verlegt oder gestohlen wird.

Richten Sie SnapMirror Active Sync ein

SnapMirror Active Sync-Setup-Workflow

Der Datenschutz von ONTAP SnapMirror Active Sync ermöglicht die Weiterführung von Geschäftsdiensten auch bei einem vollständigen Standortausfall und unterstützt Anwendungen beim transparenten Failover mithilfe einer sekundären Kopie. Mit SnapMirror Active Sync sind keine manuellen Eingriffe oder benutzerdefinierten Skripts erforderlich, um ein Failover auszulösen.

Während sich die Verfahren des System Managers zum Konfigurieren von SnapMirror Active Sync auf ASA R2-Systemen von denen auf NetApp FAS, AFF und ASA -Systemen mit der einheitlichen ONTAP Persönlichkeit unterscheiden, sind die Anforderungen, die Architektur und der Betrieb von SnapMirror Active Sync dieselben.

"Erfahren Sie mehr über SnapMirror Active Sync" .

"Erfahren Sie mehr über Disaster Recovery mit SnapMirror Active Sync auf Ihrem ASA R2-System"

Auf ASA R2-Systemen unterstützt SnapMirror Active Sync symmetrische Aktiv/Aktiv-Konfigurationen. In einer symmetrischen Aktiv/Aktiv-Konfiguration können beide Standorte für aktive E/A auf den lokalen Speicher zugreifen.

Erfahren Sie mehr über "symmetrische Aktiv/Aktiv-Konfigurationen" .

1. **Bereiten Sie die Konfiguration der aktiven SnapMirror -Synchronisierung vor.**

Zu "Bereiten Sie die Konfiguration von SnapMirror Active Sync vor" Sie sollten auf Ihrem ASA R2-System die Konfigurationsvoraussetzungen überprüfen, die Unterstützung für Ihre Host-Betriebssysteme bestätigen und sich über Objektbeschränkungen im Klaren sein, die sich auf bestimmte Konfigurationen auswirken könnten.

2. **Bestätigen Sie Ihre Clusterkonfiguration.**

Bevor Sie SnapMirror Active Sync konfigurieren, sollten Sie "Bestätigen Sie, dass Ihre ASA R2-Cluster in den richtigen Peering-Beziehungen stehen und andere Konfigurationsanforderungen erfüllen" .

3. **Installieren Sie ONTAP Mediator.**

Mit ONTAP Mediator oder ONTAP Cloud Mediator können Sie den Zustand Ihres Clusters überwachen und die Geschäftskontinuität sicherstellen. Wenn Sie ONTAP Mediator verwenden, müssen Sie "Installieren Sie es" auf Ihrem Host. Wenn Sie ONTAP Cloud Mediator verwenden, können Sie diesen Schritt überspringen.

4. **Konfigurieren Sie ONTAP Mediator oder ONTAP Cloud Mediator mit selbstsignierten Zertifikaten.**

Sie müssen "ONTAP Mediator oder ONTAP Cloud Mediator konfigurieren" bevor Sie es mit SnapMirror Active Sync zur Clusterüberwachung verwenden können.

5. **Konfigurieren Sie die aktive Synchronisierung von SnapMirror .**

"Konfigurieren Sie SnapMirror Active Sync" um eine Kopie Ihrer Daten an einem sekundären Standort zu erstellen und Ihren Hostanwendungen im Katastrophenfall ein automatisches und transparentes Failover zu ermöglichen.

Bereiten Sie die Konfiguration von SnapMirror Active Sync auf ASA R2-Systemen vor

Zur Vorbereitung der Konfiguration von SnapMirror Active Sync auf Ihrem ASA R2-System sollten Sie die Konfigurationsvoraussetzungen überprüfen, die Unterstützung für die Betriebssysteme Ihres Hosts bestätigen und sich über Objektbeschränkungen im Klaren sein, die sich auf bestimmte Konfigurationen auswirken können.

Schritte

1. Überprüfen Sie die SnapMirror Active Sync "Voraussetzungen" .
2. "Stellen Sie sicher, dass Ihre Host-Betriebssysteme unterstützt werden" für SnapMirror Active Sync.
3. Überprüfen Sie die "Objektgrenzen" das könnte Ihre Konfiguration beeinträchtigen.
4. Überprüfen Sie die Hostprotokollunterstützung für SnapMirror Active Sync auf Ihrem ASA R2-System.

   Die Unterstützung für SnapMirror Active Sync auf ASA R2-Systemen variiert je nach ONTAP -Version und Hostprotokoll.

Beginnend mit ONTAP…	SnapMirror Active Sync unterstützt …
9.17.1	• iSCSI • FC • NVMe/FC • NVMe/TCP
9.16.0	• iSCSI • FC

NVMe-Protokollbeschränkungen mit SnapMirror Active Sync auf ASA R2-Systemen

Bevor Sie SnapMirror Active Sync auf einem ASA R2-System mit NVMe-Hosts konfigurieren, sollten Sie sich bestimmter Einschränkungen des NVMe-Protokolls bewusst sein.

Alle NVMe-Speichereinheiten im NVMe-Subsystem müssen Mitglieder derselben Konsistenzgruppe sein und alle Teil derselben SnapMirror Active-Sync-Beziehung sein.

Die Protokolle NVMe/FC und NVMe/TCP werden mit SnapMirror Active Sync wie folgt unterstützt:

- Nur auf 2-Knoten-Clustern
- Nur auf ESXi-Hosts
- Nur bei symmetrischen Aktiv/Aktiv-Konfigurationen

  Asymmetrische Aktiv/Aktiv-Konfigurationen werden bei NVMe-Hosts nicht unterstützt.

SnapMirror Active Sync mit NVMe unterstützt Folgendes nicht:

- Subsysteme, die mehr als einer Konsistenzgruppe zugeordnet sind

  Einer Konsistenzgruppe können mehrere Subsysteme zugeordnet werden, jedes Subsystem kann jedoch nur einer Konsistenzgruppe zugeordnet werden.

- Erweiterung von Konsistenzgruppen in einer SnapMirror Active Sync-Beziehung
- Zuordnen von NVMe-Speichereinheiten, die sich nicht in einer SnapMirror Active Sync-Beziehung befinden, zu replizierten Subsystemen
- Entfernen einer Speichereinheit aus einer Konsistenzgruppe
- Änderung der Geometrie der Konsistenzgruppe
- "Microsoft Offloaded Data Transfer (ODX)"

Was kommt als Nächstes?

Nachdem Sie die notwendigen Vorbereitungen zur Aktivierung von SnapMirror Active Sync abgeschlossen haben, sollten Sie "Bestätigen Sie Ihre Clusterkonfiguration" .

Bestätigen Sie Ihre ASA R2-Clusterkonfiguration, bevor Sie SnapMirror Active Sync konfigurieren

SnapMirror Active Sync nutzt Peering-Cluster, um Ihre Daten im Falle eines Failovers zu schützen. Bevor Sie SnapMirror Active Sync konfigurieren, sollten Sie sicherstellen, dass Ihre ASA R2-Cluster in einer unterstützten Peering-Beziehung stehen und weitere Konfigurationsanforderungen erfüllen.

Schritte

1. Bestätigen Sie, dass zwischen den Clustern eine Cluster-Peering-Beziehung besteht.

   > Der Standard-IP-Bereich wird von SnapMirror Active Sync für Cluster-Peer-Beziehungen benötigt. Ein benutzerdefinierter IP-Bereich wird nicht unterstützt.

   "Erstellen einer Cluster-Peer-Beziehung" .

2. Bestätigen Sie, dass zwischen den virtuellen Speichermaschinen (VMs) auf jedem Cluster eine Peer-Beziehung besteht.

   "Erstellen einer Intercluster-Speicher-VM-Peer-Beziehung" .

3. Bestätigen Sie, dass auf jedem Knoten im Cluster mindestens ein LIF erstellt wird.

   "Erstellen eines LIF"

4. Bestätigen Sie, dass die erforderlichen Speichereinheiten erstellt und Hostgruppen zugeordnet wurden.

   "Erstellen Sie eine Speichereinheit" Und "Ordnen Sie die Speichereinheit einer Hostgruppe zu" .

5. Scannen Sie den Anwendungshost erneut, um neue Speichereinheiten zu erkennen.

Was kommt als Nächstes?

Nachdem Sie Ihre Clusterkonfiguration bestätigt haben, können Sie "ONTAP Mediator installieren" .

Installieren Sie ONTAP Mediator auf ASA R2-Systemen

Um ONTAP Mediator für Ihr ASA R2-System zu installieren, sollten Sie dasselbe Verfahren befolgen, das Sie zur Installation von ONTAP Mediator für alle anderen ONTAP Systeme verwenden.

Die Installation von ONTAP Mediator umfasst die Vorbereitung der Installation, die Aktivierung des Zugriffs auf Repositorys, das Herunterladen des ONTAP Mediator-Pakets, die Überprüfung der Codesignatur, die Installation des Pakets auf dem Host und die Durchführung von Aufgaben nach der Installation.

Um ONTAP Mediator zu installieren, folgen Sie "dieser Workflow"

Wie es weiter geht

Nachdem ONTAP Mediator installiert ist, sollten Sie "Konfigurieren Sie ONTAP Mediator mit selbstsignierten Zertifikaten" .

Konfigurieren Sie ONTAP Mediator oder ONTAP Cloud Mediator mit selbstsignierten Zertifikaten auf ASA R2-Systemen

Sie müssen ONTAP Mediator oder ONTAP Cloud Mediator konfigurieren, bevor Sie SnapMirror Active Sync zur Clusterüberwachung nutzen können. ONTAP Mediator und ONTAP Cloud Mediator bieten beide einen persistenten und abgeschirmten Speicher für Hochverfügbarkeits-Metadaten (HA), die von den ONTAP Clustern in einer SnapMirror Active Sync-Beziehung verwendet werden. Darüber hinaus bieten beide Mediatoren eine synchrone Knotenzustandsabfragefunktion zur Unterstützung der Quorumbestimmung und dienen als Ping-Proxy zur Controller-Aktivitätserkennung.

Bevor Sie beginnen

- Wenn Sie ONTAP Cloud Mediator verwenden, überprüfen Sie, ob Ihr ASA r2-System die erforderlichen "Voraussetzungen" .

Schritte

1. Wählen Sie im System Manager **Schutz > Übersicht**.
2. Wählen Sie im rechten Bereich neben **Mediatoren** ⋮ ; wählen Sie dann **Mediator hinzufügen**.
3. Wählen Sie den **Mediatortyp** aus.
4. Geben Sie für einen **Cloud**-Mediator die Organisations-ID, die Client-ID und das Client-Geheimnis ein. Geben Sie für einen **On-Premises**-Mediator die IP-Adresse, den Port, den Mediator-Benutzernamen und das Mediator-Passwort ein.
5. Wählen Sie den Cluster-Peer aus der Liste der berechtigten Cluster-Peers aus oder wählen Sie **Cluster-Peer hinzufügen**, um einen neuen hinzuzufügen.
6. Kopieren Sie den Inhalt der `intermediate.crt` Datei und fügen Sie sie in das Feld **Zertifikat** ein, oder wählen Sie **Importieren**, um zum `intermediate.crt` Datei und importieren Sie die Zertifikatsinformationen.
7. Wählen Sie **Hinzufügen**.

Was kommt als Nächstes?

Nachdem Sie den Mediator initialisiert haben, können Sie "Konfigurieren Sie SnapMirror Active Sync" um eine Kopie Ihrer Daten an einem sekundären Standort zu erstellen und Ihren Hostanwendungen im Katastrophenfall ein automatisches und transparentes Failover zu ermöglichen.

Konfigurieren Sie SnapMirror Active Sync auf ASA R2-Systemen

Konfigurieren Sie SnapMirror Active Sync, um eine Kopie Ihrer Daten an einem sekundären Standort zu erstellen und Ihren Hostanwendungen im Katastrophenfall ein automatisches und transparentes Failover zu ermöglichen.

Auf ASA R2-Systemen unterstützt SnapMirror Active Sync symmetrische Aktiv/Aktiv-Konfigurationen. In einer symmetrischen Aktiv/Aktiv-Konfiguration können beide Standorte für aktive E/A auf den lokalen Speicher zugreifen.

Wenn Sie das iSCSI- oder FC-Protokoll verwenden und ONTAP Tools für VMware Sphere nutzen, können Sie optional "Verwenden Sie ONTAP Tools für VM Ware, um SnapMirror Active Sync zu konfigurieren" .

Bevor Sie beginnen

"Erstellen einer Konsistenzgruppe" am primären Standort mit neuen Speichereinheiten. Wenn Sie eine nicht einheitliche symmetrische Aktiv/Aktiv-Konfiguration erstellen möchten, erstellen Sie auch am sekundären Standort eine Konsistenzgruppe mit neuen Speichereinheiten.

Erfahren Sie mehr über "ungleichmäßig" symmetrische Aktiv/Aktiv-Konfigurationen.

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Bewegen Sie den Mauszeiger über den Namen der Konsistenzgruppe, die Sie mit SnapMirror Active Sync schützen möchten.
3. Wählen ⋮ und wählen Sie dann **Schützen**.
4. Wählen Sie unter **Remote Protection Replicate to a Remote Cluster** aus.
5. Wählen Sie einen vorhandenen Cluster-Peer aus oder wählen Sie „Einen neuen hinzufügen“ aus.
6. Wählen Sie die Speicher-VM aus.
7. Wählen Sie als Replikationsrichtlinie **AutomatedFailOverDuplex** aus.
8. Wenn Sie eine nicht einheitliche symmetrische Aktiv/Aktiv-Konfiguration erstellen, wählen Sie **Zieleinstellungen** aus und geben Sie dann den Namen der neuen Zielkonsistenzgruppe ein, die Sie erstellen, bevor Sie mit diesem Verfahren beginnen.
9. Wählen Sie **Speichern**.

Ergebnis

SnapMirror Active Sync ist zum Schutz Ihrer Daten konfiguriert, sodass Sie im Katastrophenfall den Betrieb mit einem Recovery Point Objective (RPO) und einem Recovery Time Objective (RTO) von nahezu null fortsetzen können.

Verwalten Sie die aktive Synchronisierung von SnapMirror

Führen Sie ein geplantes Failover von ASA R2-Clustern in einer SnapMirror Active Sync-Beziehung durch

SnapMirror Active Sync bietet kontinuierliche Verfügbarkeit für geschäftskritische Anwendungen, indem es eine Kopie Ihrer Daten an einem sekundären Standort erstellt und Ihren Host-Anwendungen im Notfall ein automatisches und transparentes Failover

ermöglicht. Möglicherweise müssen Sie ein geplantes Failover Ihrer SnapMirror Active Sync-Verbindung durchführen, um den Failover-Prozess zu testen oder Wartungsarbeiten am primären Standort durchzuführen.

Bevor Sie beginnen

- Die aktive Synchronisierungsbeziehung von SnapMirror muss synchronisiert sein.
- Sie können kein geplantes Failover einleiten, wenn gerade ein unterbrechungsfreier Vorgang, beispielsweise das Verschieben einer Speichereinheit, ausgeführt wird.
- ONTAP Mediator oder ONTAP Cloud Mediator müssen konfiguriert, verbunden und im Quorum sein.

Schritte

1. Wählen Sie **Schutz > Replikation**.
2. Wählen Sie die SnapMirror Active Sync-Beziehung aus, für die Sie ein Failover durchführen möchten.
3. Wählen ⋮ ; wählen Sie dann **Failover**.

Was kommt als Nächstes

Verwenden Sie die `snapmirror failover show` Befehl in der ONTAP -Befehlszeilenschnittstelle (CLI), um den Status des Failovers zu überwachen.

Stellen Sie die SnapMirror Active Sync-Beziehung nach einem ungeplanten Failover Ihrer ASA R2-Cluster wieder her

Ein automatisches ungeplantes Failover (AUFO) erfolgt, wenn der primäre Cluster ausfällt oder isoliert ist. Der Mediator erkennt das Failover und führt ein automatisches ungeplantes Failover zum sekundären Cluster aus. Der sekundäre Cluster wird zum primären Cluster konvertiert und beginnt mit der Bereitstellung von Clients.

Bevor Sie beginnen

- Die aktive Synchronisierungsbeziehung von SnapMirror muss synchronisiert sein.
- Sie können kein geplantes Failover einleiten, wenn gerade ein unterbrechungsfreier Vorgang, beispielsweise das Verschieben einer Speichereinheit, ausgeführt wird.
- Der ONTAP Mediator muss konfiguriert, verbunden und im Quorum sein.

Schritte

1. Wählen Sie **Schutz > Replikation**.
2. Wählen Sie die SnapMirror Active Sync-Beziehung aus, die Sie wiederherstellen möchten.
3. Warten Sie, bis der Beziehungsstatus **InSync** anzeigt.
4. Wählen ⋮ ; wählen Sie dann **Failover**, um den Betrieb auf dem ursprünglichen primären Cluster fortzusetzen.

Was kommt als Nächstes

Um den Verlust von E/A-Pfaden zu Ihren Hosts zu verhindern, müssen Sie die Hostpfade nach der Wiederaufnahme des Betriebs auf dem primären Cluster erneut scannen.

Stellen Sie Daten auf ASA r2 Storage-Systemen wieder her

Daten in einer durch Snapshots geschützten Konsistenzgruppe oder Storage-Einheit

können bei Verlust oder Beschädigung wiederhergestellt werden.

Stellen Sie eine Konsistenzgruppe wieder her

Durch das Wiederherstellen einer Konsistenzgruppe werden die Daten in allen Speichereinheiten der Konsistenzgruppe durch die Daten aus einem Snapshot ersetzt. Änderungen an den Speichereinheiten, die nach dem Erstellen des Snapshots vorgenommen wurden, werden nicht wiederhergestellt.

Sie können eine Konsistenzgruppe aus einem lokalen oder Remote-Snapshot wiederherstellen.

Wiederherstellen von einem lokalen Snapshot

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Doppelklicken Sie auf die Konsistenzgruppe mit den wiederherzustellenden Daten.

   Die Seite mit den Details der Konsistenzgruppe wird geöffnet.
3. Wählen Sie **Snapshots**.
4. Wählen Sie den Snapshot aus, den Sie wiederherstellen möchten, und wählen Sie dann ⋮.
5. Wählen Sie **Restore Consistency Group aus diesem Snapshot** aus und wählen Sie dann **Restore** aus.

Wiederherstellen von einem Remote-Snapshot

Schritte

1. Wählen Sie in System Manager **Schutz > Replikation** aus.
2. Wählen Sie **Lokale Ziele**.
3. Wählen Sie die **Quelle** aus, die Sie wiederherstellen möchten, und wählen Sie dann ⋮.
4. Wählen Sie **Wiederherstellen**.
5. Wählen Sie den Cluster, die Storage-VM und die Konsistenzgruppe aus, auf der Sie Daten wiederherstellen möchten.
6. Wählen Sie den Snapshot aus, aus dem Sie wiederherstellen möchten.
7. Wenn Sie dazu aufgefordert werden, geben Sie „Restore“ ein, und wählen Sie dann **Restore**.

Ergebnis

Die Konsistenzgruppe wird auf den Zeitpunkt des für die Wiederherstellung verwendeten Snapshots zurückgesetzt.

Wiederherstellung einer Speichereinheit

Durch das Wiederherstellen einer Speichereinheit werden alle Daten in der Speichereinheit durch die Daten aus einem Snapshot ersetzt. Änderungen an der Speichereinheit, die nach der Erstellung des Snapshots vorgenommen wurden, werden nicht wiederhergestellt.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Doppelklicken Sie auf die Speichereinheit, die die Daten enthält, die Sie wiederherstellen möchten.

Die Seite mit den Details der Speichereinheit wird geöffnet.

3. Wählen Sie **Snapshots**.
4. Wählen Sie den Snapshot aus, den Sie wiederherstellen möchten.
5. Wählen Sie ⋮; und dann **Restore**.
6. Wählen Sie **Use this Snapshot to restore the Storage unit** aus, und wählen Sie dann **Restore** aus.

Ergebnis

Die Speichereinheit wird bis zum Zeitpunkt des für die Wiederherstellung verwendeten Snapshots wiederhergestellt.

Management von ONTAP Consistency Groups auf ASA r2-Storage-Systemen

Eine Konsistenzgruppe ist eine Sammlung von Speichereinheiten, die als eine Einheit gemanagt werden. Verwenden Sie Konsistenzgruppen für vereinfachtes Storage-Management. Angenommen, Sie haben eine Datenbank, die aus 10 Speichereinheiten in einer Konsistenzgruppe besteht, und Sie müssen die gesamte Datenbank sichern. Anstatt jede Storage-Einheit zu sichern, können Sie die gesamte Datenbank sichern, indem Sie der Konsistenzgruppe einfach Snapshot-Datenschutz hinzufügen. Das Backup der Storage-Einheiten als Konsistenzgruppe anstatt einzeln sorgt auch für ein konsistentes Backup aller Einheiten, während ein individueller Backup der Einheiten potenziell Inkonsistenzen verursachen kann.

Ab ONTAP 9.16.1 können Sie mit System Manager hierarchische Konsistenzgruppen auf Ihrem ASA r2-System erstellen. In einer hierarchischen Struktur werden eine oder mehrere Konsistenzgruppen unter einer übergeordneten Konsistenzgruppe als untergeordnete Elemente konfiguriert.

Hierarchische Konsistenzgruppen ermöglichen es Ihnen, individuelle Snapshot-Richtlinien auf jede untergeordnete Konsistenzgruppe anzuwenden und die Snapshots aller untergeordneten Konsistenzgruppen als eine Einheit auf ein Remote-Cluster zu replizieren, indem Sie das übergeordnete Objekt replizieren. Dadurch wird die Datensicherung und das Management komplexer Datenstrukturen vereinfacht. Beispiel: Angenommen, Sie erstellen eine übergeordnete Konsistenzgruppe mit dem Namen, `SVM1_app` die zwei untergeordnete Konsistenzgruppen enthält: `SVM1app_data` Für Applikationsdaten und `SVM1app_logs` Anwendungsprotokolle. Snapshots von `SVM1app_data` werden alle 15 Minuten erstellt und stündlich erstellt `SVM1app_logs`. Die übergeordnete Konsistenzgruppe `SVM1_app`, verfügt über eine SnapMirror-Richtlinie, die die Snapshots sowohl von als auch `SVM1app_logs` alle 24 Stunden in einem Remote Cluster repliziert `SVM1app_data`. Die übergeordnete Konsistenzgruppe `SVM1_app` wird als eine einzelne Einheit gemanagt, die untergeordneten Konsistenzgruppen werden als separate Einheiten gemanagt.

Fügen Sie einer Konsistenzgruppe Snapshot Datensicherung hinzu

Wenn Sie einer Konsistenzgruppe Snapshot-Datenschutz hinzufügen, werden lokale Snapshots der Konsistenzgruppe in regelmäßigen Abständen basierend auf einem vordefinierten Zeitplan erstellt.

Sie können Snapshots verwenden"Daten wiederherstellen", die verloren gehen oder beschädigt sind.

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Bewegen Sie den Mauszeiger über die Konsistenzgruppe, die Sie schützen möchten.

3. Wählen Sie ⋮; und dann **Bearbeiten**.
4. Wählen Sie unter **lokaler Schutz Snapshots planen**.
5. Wählen Sie eine Snapshot-Richtlinie aus.

   Akzeptieren Sie die standardmäßige Snapshot-Richtlinie, wählen Sie eine vorhandene Richtlinie aus, oder erstellen Sie eine neue Richtlinie.

Option	Schritte
Wählen Sie eine vorhandene Snapshot-Richtlinie aus	Wählen Sie ⌄ neben der Standardrichtlinie aus, und wählen Sie dann die vorhandene Richtlinie aus, die Sie verwenden möchten.
Neue Snapshot-Richtlinie erstellen	a. Wählen Sie + Add ;, und geben Sie den neuen Richtliniennamen ein. b. Wählen Sie den Richtlinienumfang aus. c. Wählen Sie unter **Zeitpläne** + Add . d. Wählen Sie den Namen aus, der unter **Terminplanname** angezeigt wird; Wählen Sie anschließend ⌄. e. Wählen Sie den Richtlinienzeitplan aus. f. Geben Sie unter **Maximum Snapshots** die maximale Anzahl der Snapshots ein, die Sie von der Konsistenzgruppe behalten möchten. g. Optional unter **SnapMirror Label** ein SnapMirror Label eingeben. h. Wählen Sie **Speichern**.

6. Wählen Sie **Bearbeiten**.

Wie es weiter geht

Nachdem Ihre Daten nun durch Snapshots geschützt sind, sollten Sie "Richten Sie die Snapshot-Replikation ein"Ihre Konsistenzgruppen für das Backup und Disaster Recovery an einen geografisch Remote Standort kopieren.

Entfernen Sie die Snapshot-Datensicherung aus einer Konsistenzgruppe

Wenn Sie den Snapshot-Datenschutz aus einer Konsistenzgruppe entfernen, werden die Snapshots für alle Speichereinheiten in der Konsistenzgruppe deaktiviert.

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Halten Sie den Mauszeiger über die Konsistenzgruppe, die Sie nicht mehr schützen möchten.
3. Wählen Sie ⋮; und dann **Bearbeiten**.
4. Deaktivieren Sie unter **lokaler Schutz** die Option Snapshots planen.
5. Wählen Sie **Bearbeiten**.

Ergebnis

Snapshots werden für keine der Speichereinheiten in der Konsistenzgruppe erstellt.

Fügen Sie einer Konsistenzgruppe Speichereinheiten hinzu

Erweitern Sie die von einer Konsistenzgruppe gemanagte Speichermenge, indem Sie der Konsistenzgruppe Speichereinheiten hinzufügen.

Sie können der Konsistenzgruppe vorhandene Storage-Einheiten hinzufügen oder neue Storage-Einheiten erstellen, die der Konsistenzgruppe hinzugefügt werden sollen.

Vorhandene Speichereinheiten hinzufügen

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Halten Sie den Mauszeiger über die Konsistenzgruppe, die Sie erweitern möchten.
3. Wählen Sie ⋮; und dann **Expand**.
4. Wählen Sie **mit vorhandenen Speichereinheiten**.
5. Wählen Sie die Speichereinheiten aus, die der Consistency Group hinzugefügt werden sollen, und wählen Sie dann **Expand** aus.

Fügen Sie neue Speichereinheiten hinzu

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Halten Sie den Mauszeiger über die Konsistenzgruppe, die Sie erweitern möchten.
3. Wählen Sie ⋮; und dann **Expand**.
4. Wählen Sie **mit neuen Speichereinheiten**.
5. Geben Sie die Anzahl der Einheiten, die Sie erstellen möchten, sowie die Kapazität pro Einheit ein.

   Wenn Sie mehrere Einheiten erstellen, wird jede Einheit mit derselben Kapazität und demselben Host-Betriebssystem erstellt. Um jeder Einheit eine andere Kapazität zuzuweisen, wählen Sie **eine andere Kapazität hinzufügen**, um jeder Einheit eine andere Kapazität zuzuweisen.

6. Wählen Sie **Erweitern**.

Was kommt als Nächstes

Nachdem Sie eine neue Speichereinheit erstellt haben, sollten Sie "Fügen Sie Host-Initiatoren hinzu"und "Ordnen Sie die neu erstellte Speichereinheit einem Host zu". Durch das Hinzufügen von Hostinitiatoren können Hosts auf die Speichereinheiten zugreifen und Datenvorgänge durchführen. Durch das Zuordnen einer Speichereinheit zu einem Host kann die Speichereinheit mit der Bereitstellung von Daten für den Host beginnen, dem sie zugeordnet ist.

Was kommt als Nächstes?

Vorhandene Snapshots der Konsistenzgruppe enthalten keine neu hinzugefügten Speichereinheiten. Sie sollten "Erstellen Sie einen sofortigen Snapshot"Ihrer Konsistenzgruppe angehören, um Ihre neu hinzugefügten Speichereinheiten zu schützen, bis der nächste geplante Snapshot automatisch erstellt wird.

Entfernen einer Speichereinheit aus einer Konsistenzgruppe

Sie sollten eine Speichereinheit aus einer Konsistenzgruppe entfernen, wenn Sie die Speichereinheit löschen möchten, wenn Sie sie als Teil einer anderen Konsistenzgruppe verwalten möchten oder wenn Sie die darin enthaltenen Daten nicht mehr schützen müssen. Durch das Entfernen einer Speichereinheit aus einer

Konsistenzgruppe wird die Beziehung zwischen der Speichereinheit und der Konsistenzgruppe unterbrochen, aber die Speichereinheit wird nicht gelöscht.

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Doppelklicken Sie auf die Konsistenzgruppe, aus der Sie eine Speichereinheit entfernen möchten.
3. Wählen Sie im Abschnitt **Übersicht** unter **Speichereinheiten** die Speichereinheit aus, die Sie entfernen möchten, und wählen Sie dann **aus Konsistenzgruppe entfernen** aus.

Ergebnis

Die Speichereinheit ist nicht mehr Mitglied der Konsistenzgruppe.

Wie es weiter geht

Wenn Sie mit dem Datenschutz für die Speichereinheit fortfahren möchten, fügen Sie die Speichereinheit einer anderen Konsistenzgruppe hinzu.

Konvertieren einer vorhandenen Konsistenzgruppe in eine übergeordnete Konsistenzgruppe

Speichereinheiten können keiner übergeordneten Konsistenzgruppe direkt zugeordnet werden. Wenn Sie eine vorhandene Konsistenzgruppe in ein übergeordnetes Objekt konvertieren, wird eine neue untergeordnete Konsistenzgruppe erstellt und die Speichereinheiten, die zur konvertierten Konsistenzgruppe gehören, werden in die neue untergeordnete Konsistenzgruppe verschoben.

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Halten Sie den Mauszeiger über die Konsistenzgruppe, die Sie in eine übergeordnete Konsistenzgruppe konvertieren möchten.
3. Wählen Sie ⋮; und wählen Sie dann **heraufstufen zur übergeordneten Konsistenzgruppe** aus.
4. Geben Sie einen Namen für die übergeordnete Konsistenzgruppe ein, oder übernehmen Sie den Standardnamen, und wählen Sie dann den Komponententyp der Konsistenzgruppe aus.
5. Wählen Sie **Hochstufen**.

Was kommt als Nächstes?

Sie können zusätzliche untergeordnete Konsistenzgruppen unter der übergeordneten Konsistenzgruppe erstellen. Sie können auch "Richten Sie die Snapshot-Replikation ein"die übergeordnete Konsistenzgruppe für Backup und Disaster Recovery an einen geografisch Remote Standort kopieren.

Erstellen einer untergeordneten Konsistenzgruppe

Durch das Erstellen von untergeordneten Konsistenzgruppen können Sie individuelle Snapshot-Richtlinien auf jedes untergeordnete Element anwenden, während Sie eine Replikationsrichtlinie auf alle untergeordneten Konsistenzgruppen auf der übergeordneten Ebene anwenden.

Sie können eine untergeordnete Konsistenzgruppe aus einer neuen oder einer vorhandenen Konsistenzgruppe erstellen.

Aus einer neuen Konsistenzgruppe

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Halten Sie den Mauszeiger über die übergeordnete Konsistenzgruppe, der Sie eine untergeordnete Konsistenzgruppe hinzufügen möchten.
3. Wählen Sie ⋮; und dann **Add a New child Consistency Group**.
4. Geben Sie einen Namen für die untergeordnete Konsistenzgruppe ein, oder übernehmen Sie den Standardnamen, und wählen Sie dann den Komponententyp der Konsistenzgruppe aus.
5. Wählen Sie diese Option aus, um der untergeordneten Konsistenzgruppe vorhandene Speichereinheiten hinzuzufügen oder neue Speichereinheiten zu erstellen.

   Wenn Sie neue Speichereinheiten erstellen, geben Sie die Anzahl der Einheiten, die Sie erstellen möchten, sowie die Kapazität pro Einheit ein, und geben Sie dann die Hostinformationen ein.

   Wenn Sie mehr als eine Speichereinheit erstellen, wird jede Einheit mit derselben Kapazität und demselben Host-Betriebssystem erstellt. Um jeder Einheit eine andere Kapazität zuzuweisen, wählen Sie **eine andere Kapazität hinzufügen**.

6. Wählen Sie **Hinzufügen**.

Aus einer vorhandenen Konsistenzgruppe

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Wählen Sie die vorhandene Konsistenzgruppe aus, die Sie als untergeordnete Konsistenzgruppe erstellen möchten.
3. Wählen Sie ⋮; dann **move unter different Consistency Group**.

   Wenn die Konsistenzgruppe, die Sie als bereits untergeordnetes Element einer anderen Konsistenzgruppe verwenden möchten, müssen Sie sie von der vorhandenen übergeordneten Konsistenzgruppe entfernen, bevor Sie sie in eine neue übergeordnete Konsistenzgruppe verschieben können.

4. Geben Sie einen neuen Namen für die untergeordnete Konsistenzgruppe ein, oder übernehmen Sie den Standardnamen, und wählen Sie dann den Komponententyp der Konsistenzgruppe aus.
5. Wählen Sie die vorhandene Konsistenzgruppe aus, die Sie als übergeordnete Konsistenzgruppe festlegen möchten, oder wählen Sie aus, um eine neue übergeordnete Konsistenzgruppe zu erstellen.

   Wenn Sie auswählen, eine neue übergeordnete Konsistenzgruppe zu erstellen, geben Sie einen Namen für die übergeordnete Konsistenzgruppe ein, oder übernehmen Sie den Standardnamen, und wählen Sie dann den Komponententyp der Konsistenzgruppe aus.

6. Wählen Sie **Verschieben**.

Wie es weiter geht

Nachdem Sie eine untergeordnete Konsistenzgruppe erstellt haben, können Sie "Anwenden einzelner Snapshot-Schutzrichtlinien"jeder untergeordneten Konsistenzgruppe angehören. Sie können auch "Richten Sie eine Replikationsrichtlinie ein" auf der übergeordneten Konsistenzgruppe die Snapshots aller untergeordneten Konsistenzgruppen als eine Einheit auf ein Remote-Cluster replizieren.

Stufen Sie eine übergeordnete Konsistenzgruppe auf eine einzelne Konsistenzgruppe zurück

Wenn Sie eine übergeordnete Konsistenzgruppe zu einer einzelnen Konsistenzgruppe *herunterstufen*, werden die Speichereinheiten der zugeordneten untergeordneten Konsistenzgruppen zur übergeordneten Konsistenzgruppe hinzugefügt. Die untergeordneten Konsistenzgruppen werden gelöscht, und das übergeordnete Objekt wird dann als einzelne Konsistenzgruppe gemanagt.

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Bewegen Sie den Mauszeiger über die übergeordnete Konsistenzgruppe, die Sie herunterstufen möchten.
3. Wählen Sie ⋮; und dann **auf eine einzige Consistency Group zurückstufen**.
4. Wählen Sie **Zurückstufen**

Was kommt als Nächstes?

"Fügen Sie eine Snapshot-Richtlinie hinzu" In die heruntergestufte Konsistenzgruppe, um die Speichereinheiten zu schützen, die zuvor von den untergeordneten Konsistenzgruppen verwaltet wurden.

Trennen Sie eine untergeordnete Konsistenzgruppe von einer übergeordneten Konsistenzgruppe

Wenn Sie eine untergeordnete Konsistenzgruppe von einer übergeordneten Konsistenzgruppe trennen, wird die untergeordnete Konsistenzgruppe aus der übergeordneten Konsistenzgruppe entfernt und als einzelne Konsistenzgruppe gemanagt. Die auf das übergeordnete Element angewendete Replikationsrichtlinie wird nicht mehr auf die getrennte untergeordnete Konsistenzgruppe angewendet.

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Wählen Sie die übergeordnete Konsistenzgruppe aus.
3. Wählen Sie über der untergeordneten Konsistenzgruppe aus, die Sie entfernen möchten.
4. Wählen Sie ⋮; und dann **von übergeordnetem Element trennen**.
5. Geben Sie einen neuen Namen für die Konsistenzgruppe ein, die Sie entfernen, oder akzeptieren Sie den Standardnamen, und wählen Sie dann den Applikationstyp für die Konsistenzgruppe aus.
6. Wählen Sie * Trennen*.

Was kommt als Nächstes?

"Richten Sie eine Replikationsrichtlinie ein" So replizieren Sie die Snapshots der getrennten untergeordneten Konsistenzgruppe in ein Remote-Cluster als eine einzige Konsistenzgruppe.

Löschen einer Konsistenzgruppe

Wenn Sie die Mitglieder einer Konsistenzgruppe nicht mehr als eine Einheit verwalten müssen, können Sie die Konsistenzgruppe löschen. Nach dem Löschen einer Konsistenzgruppe bleiben die zuvor in der Gruppe enthaltenen Speichereinheiten auf dem Cluster aktiv.

Bevor Sie beginnen

Wenn die Konsistenzgruppe, die Sie löschen möchten, sich in einer Replizierungsbeziehung befindet, müssen Sie die Beziehung unterbrechen, bevor Sie die Konsistenzgruppe löschen. Nach dem Löschen einer Replikationskonsistenzgruppe bleiben die Speichereinheiten, die sich in der Konsistenzgruppe befanden, im Cluster aktiv und die replizierten Kopien bleiben im Remote-Cluster erhalten.

Schritte

1. Wählen Sie in System Manager **Schutz > Consistency Groups** aus.
2. Halten Sie den Mauszeiger über die Konsistenzgruppe, die Sie löschen möchten.
3. Wählen Sie ⋮; und dann **Löschen**.
4. Akzeptieren Sie die Warnung, und wählen Sie dann **Löschen**.

Was kommt als Nächstes?

Nachdem Sie eine Konsistenzgruppe gelöscht haben, sind die Speichereinheiten, die zuvor in der Konsistenzgruppe vorhanden waren, nicht mehr durch Snapshots geschützt. Ziehen Sie in Betracht, diese Storage-Einheiten einer anderen Konsistenzgruppe hinzuzufügen, um sie vor Datenverlust zu schützen.

Management von ONTAP Datensicherungsrichtlinien und Zeitplänen auf ASA r2 Storage-Systemen

Verwenden Sie Snapshot-Richtlinien, um die Daten in Ihren Konsistenzgruppen nach einem automatisierten Zeitplan zu schützen. Verwenden Sie Richtlinienzeitpläne in den Snapshot-Richtlinien, um zu bestimmen, wie oft Snapshots erstellt werden.

Erstellen Sie einen neuen Zeitplan für Schutzrichtlinien

Ein Zeitplan für Schutzrichtlinien legt fest, wie oft eine Snapshot-Richtlinie ausgeführt wird. Sie können Schichtpläne erstellen, die in regelmäßigen Intervallen ausgeführt werden, basierend auf einer Anzahl von Tagen, Stunden oder Minuten. Sie können beispielsweise einen Zeitplan erstellen, der jede Stunde oder nur einmal pro Tag ausgeführt wird. Sie können auch Zeitpläne erstellen, die zu bestimmten Zeiten an bestimmten Tagen der Woche oder des Monats ausgeführt werden. Sie können beispielsweise einen Zeitplan erstellen, der um 12:15am Uhr am 20. Eines jeden Monats ausgeführt wird.

Bei der Definition verschiedener Sicherungsrichtlinien-Zeitpläne erhalten Sie die Flexibilität, die Häufigkeit von Snapshots für verschiedene Applikationen zu erhöhen oder zu verringern. So können Sie für Ihre kritischen Workloads ein höheres Maß an Sicherheit und ein geringeres Risiko von Datenverlust erzielen, als für weniger kritische Workloads erforderlich wäre.

Schritte

1. Wählen Sie **Schutz > Richtlinien** und dann **Zeitplan**.
2. Wählen Sie + Add.
3. Geben Sie einen Namen für den Zeitplan ein, und wählen Sie dann die Zeitplanparameter aus.
4. Wählen Sie **Speichern**.

Was kommt als Nächstes?

Nachdem Sie nun einen neuen Richtlinienzeitplan erstellt haben, können Sie den neu erstellten Zeitplan innerhalb Ihrer Richtlinien verwenden, um festzulegen, wann Snapshots erstellt werden.

Erstellen einer Snapshot-Richtlinie

Eine Snapshot-Richtlinie definiert, wie oft Snapshots erstellt werden, wie viele Snapshots maximal zulässig sind und wie lange Snapshots aufbewahrt werden.

Schritte

1. Wählen Sie in System Manager **Schutz > Richtlinien** aus, und wählen Sie dann **Snapshot-Richtlinien** aus.

2. Wählen Sie + Add .
3. Geben Sie einen Namen für die Snapshot-Richtlinie ein.
4. Wählen Sie **Cluster**, um die Richtlinie auf den gesamten Cluster anzuwenden. Wählen Sie **Storage VM** aus, um die Richtlinie auf eine einzelne Storage-VM anzuwenden.
5. Wählen Sie **Add a schedule** aus, und geben Sie anschließend den Zeitplan für die Snapshot-Policy ein.
6. Wählen Sie **Richtlinie hinzufügen**.

Was kommt als Nächstes?

Nachdem Sie jetzt eine Snapshot-Richtlinie erstellt haben, können Sie sie auf eine Konsistenzgruppe anwenden. Snapshots werden von der Konsistenzgruppe auf Grundlage der Parameter erstellt, die Sie in Ihrer Snapshot-Richtlinie festgelegt haben.

Wenden Sie eine Snapshot-Richtlinie auf eine Konsistenzgruppe an

Wenden Sie eine Snapshot-Richtlinie auf eine Konsistenzgruppe an, um Snapshots der Konsistenzgruppe automatisch zu erstellen, aufzubewahren und zu kennzeichnen.

Schritte

1. Wählen Sie in System Manager **Schutz > Richtlinien** aus, und wählen Sie dann **Snapshot-Richtlinien** aus.
2. Bewegen Sie den Mauszeiger über den Namen der Snapshot-Richtlinie, die Sie anwenden möchten.
3. Wählen Sie ⋮; und dann **Apply**.
4. Wählen Sie die Consistency Groups aus, auf die Sie die Snapshot Policy anwenden möchten, und wählen Sie dann **Apply** aus.

Was kommt als Nächstes?

Nachdem Ihre Daten nun durch Snapshots geschützt sind, sollten Sie "Richten Sie eine Replikationsbeziehung ein"Ihre Konsistenzgruppen für das Backup und Disaster Recovery an einen geografisch Remote Standort kopieren.

Bearbeiten, löschen oder deaktivieren Sie eine Snapshot-Richtlinie

Bearbeiten Sie eine Snapshot-Richtlinie, um den Richtliniennamen, die maximale Anzahl an Snapshots oder das SnapMirror-Label zu ändern. Löschen Sie eine Richtlinie, um sie mit den zugehörigen Backup-Daten aus dem Cluster zu entfernen. Deaktivieren Sie eine Richtlinie, um die Erstellung oder Übertragung von Snapshots, die von der Richtlinie festgelegt wurden, vorübergehend zu beenden.

Schritte

1. Wählen Sie in System Manager **Schutz > Richtlinien** aus, und wählen Sie dann **Snapshot-Richtlinien** aus.
2. Bewegen Sie den Mauszeiger über den Namen der Snapshot-Richtlinie, die Sie bearbeiten möchten.
3. Wählen Sie ⋮; und dann **Bearbeiten**, **Löschen** oder **Deaktivieren**.

Ergebnis

Sie haben die Snapshot-Richtlinie geändert, gelöscht oder deaktiviert.

Bearbeiten Sie eine Replikationsrichtlinie

Bearbeiten Sie eine Replikationsrichtlinie, um die Richtlinienbeschreibung, den Übertragungszeitplan und die

Regeln zu ändern. Sie können die Richtlinie auch bearbeiten, um die Netzwerkkomprimierung zu aktivieren oder zu deaktivieren.

Schritte

1. Wählen Sie im System Manager **Schutz > Richtlinien** aus.
2. Wählen Sie **Replikationsrichtlinien** aus.
3. Bewegen Sie den Mauszeiger über die Replikationsrichtlinie, die Sie bearbeiten möchten, und wählen Sie dann ⋮.
4. Wählen Sie **Bearbeiten**.
5. Aktualisieren Sie die Richtlinie, und wählen Sie dann **Speichern**.

Ergebnis

Sie haben die Replikationsrichtlinie geändert.

Datensicherung

Verschlüsselung von Daten im Ruhezustand auf ASA r2 Storage-Systemen

Wenn Daten im Ruhezustand verschlüsselt werden, sind sie auch dann nicht lesbar, wenn ein Storage-Medium einem anderen Zweck zugewiesen, zurückgegeben, verlegt oder gestohlen wird. Sie können ONTAP System Manager zur Verschlüsselung Ihrer Daten auf Hardware- und Softwareebene für einen Dual-Layer-Schutz verwenden.

NetApp Storage Encryption (NSE) unterstützt Hardwareverschlüsselung über Self-Encrypting Drives (SEDs). SEDs verschlüsseln Daten beim Schreiben. Jede SED enthält einen eindeutigen Verschlüsselungsschlüssel. Verschlüsselte Daten, die auf der SED gespeichert sind, können ohne den SED-Verschlüsselungsschlüssel nicht gelesen werden. Knoten, die versuchen, von einer SED zu lesen, müssen authentifiziert werden, um auf den Verschlüsselungsschlüssel der SED zuzugreifen. Knoten werden authentifiziert, indem ein Authentifizierungsschlüssel von einem Schlüsselmanager abgerufen und dann der SED den Authentifizierungsschlüssel vorgelegt wird. Wenn der Authentifizierungsschlüssel gültig ist, gibt die SED dem Knoten seinen Verschlüsselungsschlüssel für den Zugriff auf die darin enthaltenen Daten.

ⓘ In ASA r2-Systemen werden SEDs nur für NVMe-Protokolle unterstützt.

Verwenden Sie den integrierten Schlüsselmanager von ASA r2 oder einen externen Schlüsselmanager, um Ihren Nodes Authentifizierungsschlüssel bereitzustellen.

Neben NSE können Sie auch Softwareverschlüsselung aktivieren, um Ihre Daten um eine weitere Sicherheitsebene zu erweitern.

Schritte

1. Wählen Sie im System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** unter **Verschlüsselung Konfigurieren** aus.
3. Konfigurieren Sie den Schlüsselmanager.

Option	Schritte
Konfigurieren Sie den Onboard Key Manager	a. Wählen Sie **Onboard Key Manager**, um die Schlüsselserver hinzuzufügen. b. Geben Sie eine Passphrase ein.
Konfigurieren Sie einen externen Schlüsselmanager	a. Wählen Sie **External Key Manager**, um die Schlüsselserver hinzuzufügen. b. Wählen Sie + Add diese Option aus, um die Schlüsselserver hinzuzufügen. c. Fügen Sie die CA-Zertifikate des KMIP-Servers hinzu. d. Fügen Sie die KMIP-Client-Zertifikate hinzu.

4. Wählen Sie **Dual-Layer-Verschlüsselung**, um die Softwareverschlüsselung zu aktivieren.
5. Wählen Sie **Speichern**.

Was kommt als Nächstes?

Nachdem Sie nun Ihre Daten im Ruhezustand verschlüsselt haben, können Sie jetzt mit dem "Verschlüsseln Sie alle über das Netzwerk gesendeten Daten"NVMe-/TCP-Protokoll zwischen Ihrem NVMe-/TCP-Host und Ihrem ASA r2-System wechseln.

Migrieren Sie die ONTAP Datenverschlüsselung zwischen Schlüsselmanagern in Ihrem ASA r2 System

Sie können Ihre Datenschlüssel entweder über den integrierten ONTAP Schlüsselmanager auf Ihrem ASA r2 System oder über einen externen Schlüsselmanager (oder beides) managen. Externe Schlüsselmanager können nur auf Ebene der Storage-VM aktiviert werden. Auf ONTAP Cluster-Ebene können Sie entweder den Onboard-Schlüsselmanager oder einen externen Schlüsselmanager aktivieren.

Wenn Sie Ihren Schlüsselmanager im…	Sie können…
Nur Cluster-Ebene	Entweder dem Onboard-Schlüsselmanager oder einem externen Schlüsselmanager
Nur SVM-Ebene	Nur ein externer Schlüsselmanager

Wenn Sie Ihren Schlüsselmanager im…	Sie können…
Auf Cluster- und SVM-Ebene	Eine der folgenden Kombinationen von Schlüsselmanagern: • Option 1 Cluster-Ebene: Onboard-Schlüsselmanager SVM-Ebene: Externer Schlüsselmanager • Option 2 Cluster-Ebene: Externer Schlüsselmanager SVM-Ebene: Externer Schlüsselmanager

Migrieren Sie Schlüssel zwischen Schlüsselmanagern auf ONTAP-Cluster-Ebene

Ab ONTAP 9.16.1 können Sie die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, um Schlüssel zwischen Schlüsselmanagern auf Cluster-Ebene zu migrieren.

Von Onboard zu extern

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Erstellen Sie eine inaktive externe Schlüsselmanager-Konfiguration:

```
security key-manager external create-config
```

3. Wechseln Sie zum externen Schlüsselmanager:

```
security key-manager keystore enable -vserver <svm_name> -type KMIP
```

4. Löschen Sie die Onboard-Schlüsselmanager-Konfiguration:

```
security key-manager keystore delete-config -vserver <svm_name>
-type OKM
```

5. Legen Sie die Berechtigungsebene auf admin fest:

```
set -privilege admin
```

Von extern zu Onboard

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Erstellen einer inaktiven Onboard-Schlüsselmanager-Konfiguration:

```
security key-manager onboard create-config
```

3. Aktivieren der Onboard-Konfiguration für Verschlüsselungsmanagement:

```
security key-manager keystore enable -vserver <svm_name> -type OKM
```

4. Löschen Sie die externe Schlüsselmanager-Konfiguration

```
security key-manager keystore delete-config -vserver <svm_name>
-type KMIP
```

5. Legen Sie die Berechtigungsebene auf admin fest:

```
set -privilege admin
```

Schlüsselmanagement auf ONTAP-Cluster- und Storage-VM-Ebene migrieren

Mithilfe der ONTAP Befehlszeilenschnittstelle (CLI) können Sie Schlüssel zwischen dem Schlüsselmanager auf Cluster-Ebene und einem Schlüsselmanager auf Storage-VM-Ebene migrieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Migrieren der Schlüssel:

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<svm_name>
```

3. Legen Sie die Berechtigungsebene auf admin fest:

```
set -privilege admin
```

Schutz vor Ransomware-Angriffen

Erstellen Sie manipulationssichere Snapshots zum Schutz vor Ransomware-Angriffen auf ASA R2-Speichersysteme

Um besser gegen Ransomware-Angriffe zu schützen, replizieren Sie Snapshots in ein Remote-Cluster und sperren Sie dann die Ziel-Snapshots, damit sie manipulationssicher sind. Gesperrte Snapshots können nicht versehentlich oder böswillig gelöscht werden. Sie können gesperrte Snapshots verwenden, um Daten wiederherzustellen, wenn ein Storage-Gerät jemals durch einen Ransomware-Angriff kompromittiert wurde.

Initialisieren Sie die SnapLock Compliance-Uhr

Bevor Sie manipulationssichere Snapshots erstellen können, müssen Sie die SnapLock Compliance Uhr auf Ihren lokalen und Ziel-Clustern initialisieren.

Schritte

1. Wählen Sie **Cluster > Übersicht**.
2. Wählen Sie im Abschnitt **Knoten** die Option **SnapLock Compliance-Uhr initialisieren** aus.
3. Wählen Sie **Initialisieren**.
4. Vergewissern Sie sich, dass die Compliance-Uhr initialisiert ist.
   a. Wählen Sie **Cluster > Übersicht**.
   b. Wählen Sie im Abschnitt **Knoten** die Option ; und wählen Sie dann **SnapLock Compliance Uhr**.

Was kommt als Nächstes?

Nachdem Sie die SnapLock Compliance-Uhr auf Ihren lokalen und Ziel-Clustern initialisiert haben, sind Sie bereit zu "Erstellen Sie eine Replikationsbeziehung mit gesperrten Snapshots".

Aktivieren Sie autonomen Ransomware-Schutz mit KI auf Ihren ASA R2-Speichersystemen

Ab ONTAP 9.17.1 können Sie die Daten Ihres ASA r2-Systems mit Autonomous Ransomware Protection mit künstlicher Intelligenz (ARP/AI) schützen. ARP/AI erkennt potenzielle Ransomware-Bedrohungen schnell, erstellt automatisch einen ARP-Snapshot zum Schutz Ihrer Daten und zeigt im System Manager eine Warnmeldung an, um Sie auf verdächtige Aktivitäten aufmerksam zu machen.

Ab ONTAP 9.17.1 verbessert ARP die Cyber-Resilienz durch die Einführung eines Machine-Learning-Modells für Anti-Ransomware-Analysen, das sich ständig weiterentwickelnde Formen von Ransomware mit einer Genauigkeit von 98 % in SAN-Umgebungen erkennt. Das Machine-Learning-Modell von ARP wird vor und nach einem simulierten Ransomware-Angriff anhand eines großen Datensatzes vortrainiert. Dieses ressourcenintensive Training erfolgt außerhalb von ONTAP, und das daraus resultierende vortrainierte Modell ist im Lieferumfang von ONTAP enthalten. Dieses Modell ist weder über die CLI noch über die API zugänglich oder modifizierbar. Daher ist ARP/AI sofort nach der Aktivierung aktiv; es gibt keine "Lernphase" .

> Kein System zur Erkennung oder Prävention von Ransomware kann einen vollständigen Schutz vor einem Ransomware-Angriff garantieren. Obwohl ein Angriff möglicherweise unentdeckt bleibt, fungiert ARP/AI als wichtige zusätzliche Verteidigungsebene, falls Antivirensoftware einen Angriff nicht erkennt.

Über diese Aufgabe

ARP/AI-Unterstützung ist im Lieferumfang enthalten "ONTAP One-Lizenz" .

Nachdem Sie ARP/AI aktiviert haben, sollten Sie "Aktivieren Sie automatische Updates für Ihre Sicherheitsdateien" um automatisch neue Sicherheitsupdates zu erhalten.

Aktivieren Sie ARP/AI auf allen Speichereinheiten in einer SVM

Sie können ARP/AI standardmäßig auf allen in einer Storage Virtual Machine (SVM) erstellten Speichereinheiten aktivieren. Das bedeutet, dass ARP/AI für alle neuen Speichereinheiten in der SVM automatisch aktiviert ist. Sie können ARP/AI auch auf vorhandene Speichereinheiten in der SVM anwenden.

Schritte

1. Wählen Sie im System Manager **Cluster > Storage-VMs** aus.
2. Wählen Sie die Speicher-VM aus, auf der Sie ARP/AI aktivieren möchten.
3. Wählen Sie im Abschnitt **Sicherheit** neben **Anti-Ransomware** ; wählen Sie dann **Anti-Ransomware-**

Einstellungen bearbeiten.

4. Wählen Sie **Anti-Ransomware aktivieren**.

   Dadurch wird ARP/AI standardmäßig auf allen zukünftigen Speichereinheiten aktiviert, die auf der ausgewählten Speicher-VM erstellt werden.

5. Um ARP auf vorhandene Speichereinheiten auf der ausgewählten Speicher-VM anzuwenden, wählen Sie **Diese Änderung auf alle zutreffenden vorhandenen Speichereinheiten auf dieser Speicher-VM anwenden**.
6. Wählen Sie **Speichern**.

Ergebnis

Alle neuen Speichereinheiten, die Sie auf der SVM erstellen, sind standardmäßig vor Ransomware-Angriffen geschützt und verdächtige Aktivitäten werden Ihnen im System Manager gemeldet.

Aktivieren Sie ARP/AI auf bestimmten Speichereinheiten in einer SVM

Wenn Sie ARP/AI nicht auf allen Speichereinheiten in einer SVM aktivieren möchten, können Sie die spezifischen Einheiten auswählen, die aktiviert werden sollen.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie die Speichereinheiten aus, für die Sie ARP/AI aktivieren möchten.
3. Wählen ⋮ ; wählen Sie dann **Anti-Ransomware aktivieren**.
4. Wählen Sie **Aktivieren**.

Ergebnis

Die von Ihnen ausgewählten Speichereinheiten sind vor Ransomware-Angriffen geschützt und verdächtige Aktivitäten werden Ihnen im System Manager gemeldet.

Ändern Sie die Aufbewahrungsfristen für ARP/AI-Snapshots auf ASA R2-Speichersystemen

Wenn Autonomous Ransomware Protection mit Künstlicher Intelligenz (ARP/AI) ungewöhnliche Aktivitäten auf einer oder mehreren Ihrer ASA r2-Systemspeichereinheiten erkennt, erstellt es automatisch einen ARP-Snapshot, um die Daten der Speichereinheit zu schützen. Abhängig von Ihrer Speicherkapazität und den geschäftlichen Anforderungen an Ihre Daten können Sie die standardmäßige Aufbewahrungsdauer für ARP-Snapshots verlängern oder verkürzen. Beispielsweise können Sie die Aufbewahrungsdauer für geschäftskritische Anwendungen verlängern, um bei Bedarf längere Aufbewahrungsfristen für die Datenwiederherstellung zu haben, oder die Aufbewahrungsdauer für nicht-kritische Anwendungen verkürzen, um Speicherplatz zu sparen.

Die standardmäßige Aufbewahrungsdauer für den ARP-Snapshot variiert je nach der Aktion, die Sie als Reaktion auf die abnormale Aktivität ergreifen.

Wenn Sie diese Aktion ausführen …	ARP-Snapshots werden standardmäßig aufbewahrt für…
Als falsch positiv markieren	12 Stunden
Als potenziellen Ransomware-Angriff markieren	7 Tage
Ergreifen Sie keine sofortigen Maßnahmen	10 Tage

Die Standardaufbewahrungsfristen können über die ONTAP Befehlszeilenschnittstelle (CLI) geändert werden. Siehe "Optionen für automatische ONTAP -Snapshots ändern" für Schritte zum Ändern der Standardaufbewahrungsdauer.

Reagieren Sie auf autonomen Ransomware-Schutz mit KI-Warnungen auf ASA R2-Speichersystemen

Wenn der autonome Ransomware-Schutz mit künstlicher Intelligenz (ARP/AI) ungewöhnliche Aktivitäten auf einer oder mehreren Ihrer ASA r2-Systemspeichereinheiten erkennt, wird eine Warnung im System Manager-Dashboard angezeigt. Sie sollten die Warnung anzeigen, die Aktivität überprüfen und gegebenenfalls Maßnahmen ergreifen, um eine potenzielle Bedrohung Ihrer Daten zu verhindern.

Wenn eine ARP/AI-Warnmeldung angezeigt wird, sollten Sie vor dem Ergreifen von Maßnahmen die Integrität der Daten auf dem Speichergerät mit einem entsprechenden Anwendungsintegritätsprüfer überprüfen. Durch die Überprüfung der Datenintegrität des Speichergeräts können Sie feststellen, ob die Aktivität akzeptabel ist oder ob es sich um einen potenziellen Ransomware-Angriff handelt.

Wenn die abnormale Aktivität … ist.	Dann tun Sie Folgendes …
Akzeptabel	Markieren Sie die Aktivität als falsch-positiv.
Ein potenzieller Ransomware-Angriff	Markieren Sie die Aktivität als potenziellen Ransomware-Angriff.
Unbestimmt	Ergreifen Sie keine sofortigen Maßnahmen. Überwachen Sie den Speicher bis zu 7 Tage lang. Wenn der Speicher weiterhin normal funktioniert, markieren Sie die Aktivität als falsch positiv. Wenn der Speicher weiterhin ungewöhnliche Aktivitäten aufweist, markieren Sie die Aktivität als potenziellen Ransomware-Angriff.

Schritte

1. Wählen Sie in System Manager **Dashboard** aus.

   Wenn ARP auf einer oder mehreren Speichereinheiten eine ungewöhnliche Aktivität festgestellt hat, wird unter **Warnungen** eine Meldung angezeigt.

2. Wählen Sie die Warnmeldung aus.
3. Wählen Sie unter **Ereignisübersicht** die Meldung **Warnungen** aus, die die Anzahl der Speichereinheiten mit abnormaler Aktivität angibt.
4. Wählen Sie unter **Speichereinheiten mit ungewöhnlicher Aktivität** die Speichereinheit aus.
5. Wählen Sie **Sicherheit**.

Bei ungewöhnlichen Aktivitäten auf dem Speichergerät wird unter **Anti-Ransomware** eine Meldung angezeigt.

6. Wählen Sie **Aktion auswählen**.
7. Wählen Sie **Als falsch-positiv markieren** oder **Als potenziellen Ransomware-Angriff markieren**.

Autonomen Ransomware-Schutz mit KI auf Ihren ASA R2-Speichersystemen pausieren oder fortsetzen

Ab ONTAP 9.17.1 können Sie Autonomous Ransomware Protection mit künstlicher Intelligenz (ARP/AI) nutzen, um die Daten auf Ihrem ASA r2-System zu schützen. Bei einem ungewöhnlichen Workload-Ereignis können Sie die ARP/AI-Analyse vorübergehend aussetzen, um Fehlalarme bei Ransomware-Angriffen zu verhindern. Nach Abschluss des Workload-Ereignisses können Sie die ARP/AI-Analyse fortsetzen.

ARP/AI pausieren

Bevor Sie mit einem ungewöhnlichen Workload-Ereignis beginnen, müssen Sie die ARP/AI-Analyse möglicherweise vorübergehend aussetzen, um falsch positive Erkennungen von Ransomware-Angriffen zu verhindern.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie die Speichereinheiten aus, für die Sie ARP/AI pausieren möchten.
3. Wählen Sie **Anti-Ransomware pausieren**.

Ergebnis

Die ARP/AI-Analyse wird für die ausgewählten Speichereinheiten angehalten und Ihnen werden im System Manager keine verdächtigen Aktivitäten gemeldet, bis Sie ARP/AI wieder aufnehmen.

ARP/AI fortsetzen

Wenn Sie ARP/AI während einer ungewöhnlichen Arbeitslast anhalten, sollten Sie es nach Abschluss der Arbeitslast fortsetzen, um Ihre Daten vor Ransomware-Angriffen zu schützen.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie die Speichereinheiten aus, für die Sie ARP/AI fortsetzen möchten.
3. Wählen Sie **Anti-Ransomware fortsetzen**.

Ergebnis

Die Analyse potenzieller Ransomware-Angriffe wird fortgesetzt und verdächtige Aktivitäten werden Ihnen im System Manager gemeldet.

Sichere NVMe-Verbindungen auf Ihren ASA r2 Storage-Systemen

Bei Verwendung des NVMe-Protokolls können Sie die in-Band-Authentifizierung konfigurieren, um die Datensicherheit zu erhöhen. Die in-Band-Authentifizierung ermöglicht eine sichere bidirektionale und unidirektionale Authentifizierung zwischen den NVMe Hosts und dem ASA r2 System. Die in-Band-Authentifizierung ist für alle NVMe-

Hosts verfügbar. Bei Verwendung des NVMe/TCP-Protokolls können Sie die Datensicherheit weiter erhöhen, indem Sie TLS (Transport Layer Security) für die Verschlüsselung aller Daten konfigurieren, die zwischen Ihren NVMe/TCP-Hosts und Ihrem ASA r2-System über das Netzwerk übertragen werden.

Schritte

1. Wählen Sie **Hosts** aus, und wählen Sie dann **NVMe** aus.
2. Wählen Sie + Add .
3. Geben Sie den Hostnamen ein, und wählen Sie dann das Host-Betriebssystem aus.
4. Geben Sie eine Hostbeschreibung ein, und wählen Sie dann die Speicher-VM aus, die mit dem Host verbunden werden soll.
5. Wählen Sie neben dem Hostnamen aus.
6. Wählen Sie **bandinterne Authentifizierung** aus.
7. Wenn Sie das NVMe/TCP-Protokoll verwenden, wählen Sie **benötigt Transport Layer Security (TLS)** aus.
8. Wählen Sie **Hinzufügen**.

Ergebnis

Die Sicherheit Ihrer Daten wird durch die in-Band-Authentifizierung und/oder TLS erhöht.

Sichere IP-Verbindungen auf Ihren ASA r2-Storage-Systemen

Wenn Sie das IP-Protokoll auf Ihrem ASA r2-System verwenden, können Sie die IP-Sicherheit (IPsec) konfigurieren, um Ihre Datensicherheit zu erhöhen. IPsec ist ein Internetstandard, der Verschlüsselung von Daten während der Übertragung, Authentifizierung für den Datenverkehr zwischen den Netzwerkendpunkten auf IP-Ebene und Schutz vor Replay- und böswilligen man-in-the-Middle-Angriffen auf Ihre Daten bietet.

Für ASA r2-Systeme ist IPsec für iSCSI- und NVMe/TCP-Hosts verfügbar.

Auf bestimmten ASA r2-Systemen können mehrere kryptografische Vorgänge, wie z. B. Verschlüsselungs- und Integritätsprüfungen, auf eine unterstützte NIC-Karte (Network Interface Controller) ausgelagert werden. Der Durchsatz für auf die NIC-Karte ausgelagerte Vorgänge beträgt etwa 5 % oder weniger. Dies kann die Leistung und den Durchsatz des durch IPsec geschützten Netzwerkverkehrs erheblich verbessern.

Die folgenden NIC-Karten werden für die Hardwareauslagerung auf den folgenden ASA r2-Systemen unterstützt:

Unterstützte NIC-Karte	ASA r2-Systeme
X50131A – (2P, 40 G/100 G/200 G/400 G Ethernet-Controller)	• ASA A1K • ASA A90 • ASA A70

Unterstützte NIC-Karte	ASA r2-Systeme
X60132A – (4p, 10G/25G Ethernet-Controller)	• ASA A50 • ASA A30 • ASA A20

Was kommt als Nächstes?

"Konfigurieren Sie die IP-Sicherheit für das ONTAP-Netzwerk"

Administration und Überwachung

Upgrade und Wiederherstellung von ONTAP

Führen Sie ein Upgrade von ONTAP auf ASA r2 Storage-Systemen durch

Wenn Sie Ihre ONTAP Software auf Ihrem ASA r2 System aktualisieren, können Sie von neuen und verbesserten ONTAP Funktionen profitieren, mit denen Sie Kosten senken, kritische Workloads beschleunigen, die Sicherheit erhöhen und den Umfang der für Ihr Unternehmen verfügbaren Datensicherung erweitern können.

ONTAP Software-Upgrades für ASA r2 Systeme befolgen denselben Prozess wie Upgrades anderer ONTAP Systeme. Wenn Sie über einen aktiven SupportEdge-Vertrag für den digitalen Berater von Active IQ (auch als digitaler Berater bekannt) verfügen, sollten Sie "Bereiten Sie das Upgrade mit Upgrade Advisor vor". Upgrade Advisor bietet intelligente Funktionen, mit denen Sie die Unsicherheit und Risiken minimieren können, indem Sie den Cluster bewerten und einen konfigurationsspezifischen Upgrade-Plan erstellen. Wenn Sie keinen aktiven SupportEdge-Vertrag für Active IQ Digital Advisor haben, sollten Sie dies "Vorbereitung auf das Upgrade ohne Upgrade Advisor"tun.

Nach der Vorbereitung auf das Upgrade wird empfohlen, Upgrades mit durchzuführen"Automatisierte unterbrechungsfreie Upgrades (ANDU) von System Manager". ANDU nutzt die Hochverfügbarkeits-(HA-)Failover-Technologie von ONTAP, um sicherzustellen, dass Cluster während des Upgrades Daten weiterhin ohne Unterbrechung bereitstellen.

Erfahren Sie mehr über "Upgrades für die ONTAP Software".

ONTAP auf ASA R2-Speichersystemen zurücksetzen

ONTAP -Software-Reverts für ASA R2-Systeme folgen demselben Prozess wie Reverts für andere ONTAP Systeme.

Das Zurücksetzen eines ONTAP -Clusters ist störend. Sie müssen den Cluster für die Dauer des Zurücksetzens offline nehmen. Sie sollten einen Produktionscluster nicht ohne Unterstützung durch den technischen Support zurücksetzen. Sie können einen neuen oder Testcluster ohne Unterstützung zurücksetzen. Wenn das Zurücksetzen eines neuen oder Testsystems fehlschlägt oder erfolgreich abgeschlossen wird, Sie aber mit der Cluster-Leistung in Ihrer Produktionsumgebung nicht zufrieden sind, wenden Sie sich an den technischen Support.

"Einen ONTAP Cluster zurücksetzen" .

Rückgängigmachen der Anforderungen für ASA R2-Systeme

Bei bestimmten ASA R2-Clusterkonfigurationen müssen Sie bestimmte Maßnahmen ergreifen, bevor Sie mit der Wiederherstellung der ONTAP -Software beginnen.

Zurücksetzen von ONTAP 9.17.1

Wenn Sie von ONTAP 9.17.1 auf einem ASA R2-System zurückkehren, sollten Sie vor Beginn der Rücksetzung die folgenden Aktionen ausführen:

"Automatischer Workload-Ausgleich"wird standardmäßig 14 Tage nach dem Upgrade auf ONTAP 9.17.1 oder der Initialisierung eines neuen ONTAP 9.17.1 ASA r2-Clusters aktiviert. Sie können auf Ihrem ASA R2-System nicht von ONTAP 9.17.1 zurückkehren, nachdem die automatische Neuverteilung der Arbeitslast aktiviert wurde.

Wenn Sie…	Bevor Sie zurückkehren, sollten Sie …
Hierarchische Konsistenzgruppen in einer SnapMirror Active Sync-Beziehung	Entfernen Sie die SnapMirror Active Sync-Beziehung
Aktive Importbeziehungen	Löschen der aktiven Importbeziehungen
Anti-Ransomware-Schutz aktiviert	Deaktivieren Sie den Anti-Ransomware-Schutz

Aktualisieren der Firmware auf ASA r2-Speichersystemen

ONTAP lädt automatisch Firmware- und Systemdateien auf Ihrem ASA r2-System herunter und aktualisiert diese standardmäßig. Wenn Sie die Möglichkeit haben möchten, empfohlene Updates vor dem Herunterladen und Installieren anzuzeigen, können Sie ONTAP System Manager verwenden, um automatisierte Updates zu deaktivieren oder Aktualisierungsparameter zu bearbeiten, um Ihnen Benachrichtigungen über verfügbare Updates anzuzeigen, bevor eine Aktion durchgeführt wird.

Aktivieren Sie automatische Updates

Empfohlene Updates für Speicher-Firmware, SP/BMC-Firmware und Systemdateien werden automatisch heruntergeladen und standardmäßig auf Ihrem ASA r2-System installiert. Wenn automatische Updates deaktiviert wurden, können Sie sie aktivieren, um das Standardverhalten wiederherzustellen.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie unter **Softwareupdates** die Option **Aktivieren** aus.
3. Lesen Sie die EULA.
4. Akzeptieren Sie die Standardeinstellung „Benachrichtigung über empfohlene Updates anzeigen“. Wählen Sie optional „Automatisch aktualisieren“ oder „Automatisch verwerfen“ für empfohlene Updates aus.
5. Wählen Sie diese Option, um zu bestätigen, dass Ihre Aktualisierungsänderungen auf alle aktuellen und zukünftigen Aktualisierungen angewendet werden.
6. Wählen Sie **Speichern**.

Ergebnis

Empfohlene Aktualisierungen werden automatisch heruntergeladen und auf Ihrem ASA r2-System installiert, basierend auf Ihrer Auswahl für das Update.

Deaktivieren Sie automatische Updates

Deaktivieren Sie automatische Updates, wenn Sie die Möglichkeit haben möchten, empfohlene Updates vor der Installation anzuzeigen. Wenn Sie automatische Updates deaktivieren, müssen Sie Firmware- und Systemdateiaktualisierungen manuell durchführen.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie unter **Softwareupdates** die Option **Deaktivieren** aus.

Ergebnis

Automatische Updates sind deaktiviert. Sie sollten regelmäßig nach empfohlenen Updates suchen und entscheiden, ob Sie eine manuelle Installation durchführen möchten.

Automatische Updates anzeigen

Zeigen Sie eine Liste der Firmware- und Systemdatei-Updates an, die auf das Cluster heruntergeladen wurden und für die automatische Installation geplant sind. Zeigen Sie auch Updates an, die zuvor automatisch installiert wurden.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie neben **Software-Updates** → und wählen Sie dann **Alle automatischen Updates anzeigen**.

Automatische Aktualisierungen bearbeiten

Sie können festlegen, dass empfohlene Updates für Storage-Firmware, SP/BMC Firmware und Ihre Systemdateien automatisch heruntergeladen und auf dem Cluster installiert werden. Alternativ können Sie festlegen, dass empfohlene Updates automatisch verworfen werden. Wenn Sie die Installation oder das Entlassen von Updates manuell steuern möchten, wählen Sie die Option, um benachrichtigt zu werden, wenn eine empfohlene Aktualisierung verfügbar ist. Sie können dann manuell auswählen, um sie zu installieren oder zu schließen.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie neben **Software-Updates** → und wählen Sie dann **Alle anderen Updates** aus.
3. Aktualisieren Sie die Auswahl für automatische Aktualisierungen.
4. Wählen Sie **Speichern**.

Ergebnis

Automatische Aktualisierungen werden basierend auf Ihrer Auswahl geändert.

Aktualisieren Sie die Firmware manuell

Wenn Sie die Möglichkeit haben möchten, empfohlene Updates vor dem Herunterladen und Installieren anzuzeigen, können Sie automatische Updates deaktivieren und Ihre Firmware manuell aktualisieren.

Schritte

1. Laden Sie die Firmware-Aktualisierungsdatei auf einen Server oder lokalen Client herunter.
2. Wählen Sie im System Manager **Cluster > Übersicht** und dann **Alle anderen Updates**.
3. Wählen Sie unter **Manuelle Updates** die Option **Firmware-Dateien hinzufügen** und anschließend **Vom Server herunterladen** oder **Vom lokalen Client hochladen**.
4. Installieren Sie die Firmware-Update-Datei.

Ergebnis

Ihre Firmware wird aktualisiert.

Management des Client-Zugriffs auf Storage-VMs auf ASA r2 Storage-Systemen

Storage-Einheiten eines ASA r2-Systems befinden sich in Storage Virtual Machines (VMs). Storage-VMs dienen der Bereitstellung von Daten für Ihre SAN-Clients. Erstellen Sie mit ONTAP System Manager eine LIF (Netzwerkschnittstelle) für Ihre SAN-Clients, um eine Storage-VM anzuschließen und auf Daten in den Storage-Einheiten zuzugreifen. Optional können Sie Subnetze zur Vereinfachung der LIF-Erstellung und IPspaces verwenden, um Ihren Storage VMs ihren eigenen sicheren Storage, die Administration und das Routing bereitzustellen.

Erstellen einer Storage-VM

Während der Cluster-Einrichtung wird Ihre standardmäßige Virtual Machine (VM) für den Datenspeicher erstellt. Alle neuen Storage-Einheiten werden innerhalb Ihrer Standard-Storage-VM erstellt, es sei denn, Sie erstellen und wählen eine andere Storage-VM aus. Vielleicht möchten Sie eine zusätzliche Storage-VM erstellen, um Ihre Storage-Einheiten für verschiedene Applikationen, Abteilungen oder Clients zu trennen. Vielleicht möchten Sie beispielsweise eine Storage-VM für Ihre Entwicklungsumgebung und eine andere Storage-VM für die Produktionsumgebung erstellen oder eine Storage-VM für die Finanzabteilung und eine andere Storage-VM für die Marketingabteilung erstellen.

Schritte

1. Wählen Sie **Cluster > Storage VMs**.
2. Wählen Sie + Add.
3. Geben Sie einen Namen für die Storage-VM ein, oder übernehmen Sie den Standardnamen.
4. Wählen Sie unter **Configure protocols** die Protokolle für die Storage VM aus.

   Wählen Sie **IP** für iSCSI und NVMe/TCP aus. Wählen Sie **FC** für Fibre Channel oder NVMe/FC.
5. Wählen Sie unter **Storage VM Administration Manage Administrator Account** aus, und geben Sie anschließend den Benutzernamen und das Passwort für das Administratorkonto ein.
6. Fügen Sie eine Netzwerkschnittstelle für die Storage-VM hinzu.
7. Wählen Sie **Speichern**.

Was kommt als Nächstes?

Sie haben eine Storage-VM erstellt. Sie können nun die Storage-VM für "Bereitstellung von Storage"verwenden.

Erstellen von IPspaces

Ein IPspace ist ein eindeuiger IP-Adressbereich, in dem sich Storage-VMs befinden. Wenn Sie IPspaces erstellen, ermöglichen Sie Ihren Storage-VMs ihren eigenen sicheren Storage, ihre Administration und ihr eigenes sicheres Routing. Außerdem können Clients in administrativ getrennten Netzwerkdomänen überlappende IP-Adressen aus demselben IP-Adressensubnetz verwenden.

Sie müssen einen IPspace erstellen, bevor Sie ein Subnetz erstellen können.

Schritte

1. Wählen Sie **Netzwerk > Übersicht**.
2. Wählen Sie unter **IPspaces** die Option + Add.
3. Geben Sie einen Namen für die IP-Adresse ein, oder übernehmen Sie den Standardnamen.

   Der IPspace-Name kann nicht „all“ sein, da „all“ ein systemreservierter Name ist.

4. Wählen Sie **Speichern**.

Was kommt als Nächstes?

Nachdem Sie nun einen IPspace erstellt haben, können Sie ihn zum Erstellen eines Subnetzes verwenden.

Subnetze erstellen

Ein Subnetz ermöglicht es Ihnen, bestimmte Blöcke von IPv4- oder IPv6-Adressen zuzuweisen, die beim Erstellen einer LIF (Netzwerkschnittstelle) verwendet werden sollen. Ein Subnetz vereinfacht die LIF-Erstellung, da Sie in der Lage sind, den Subnetznamen anstelle einer bestimmten IP-Adresse und Netzwerkmaske für jede LIF anzugeben.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Der "Broadcast-Domäne" und IP-Bereich, in dem Sie das Subnetz hinzufügen möchten, muss bereits vorhanden sein.

Schritte

1. Wählen Sie **Netzwerk > Übersicht**.
2. Wählen Sie **Subnetze** aus, und wählen Sie dann + Add.
3. Geben Sie den Subnetznamen ein.

   Alle Subnetznamen müssen innerhalb eines IPspaces eindeutig sein.

4. Geben Sie die Subnetz-IP-Adresse und die Subnetzmaske ein.
5. Geben Sie den IP-Adressbereich für das Subnetz an.

   Wenn Sie den IP-Adressbereich für das Subnetz angeben, überlappen Sie IP-Adressen nicht mit anderen Subnetzen. Netzwerkprobleme können auftreten, wenn sich Subnetz-IP-Adressen überlappen und unterschiedliche Subnetze oder Hosts versuchen, dieselbe IP-Adresse zu verwenden.

6. Wählen Sie die Broadcast-Domäne für das Subnetz aus.
7. Wählen Sie **Hinzufügen**.

Was kommt als Nächstes?

Sie haben ein Subnetz erstellt, mit dem Sie nun die Erstellung Ihrer LIFs vereinfachen können.

LIF erstellen (Netzwerkschnittstelle)

Eine LIF (Netzwerkschnittstelle) ist eine IP-Adresse, die einem physischen oder logischen Port zugeordnet ist. Erstellen Sie LIFs an den Ports, die Sie für den Datenzugriff verwenden möchten. Storage-VMs stellen Daten über ein oder mehrere LIFs für Clients bereit. Bei einem Komponentenausfall kann eine LIF ein Failover durchführen oder zu einem anderen physischen Port migriert werden, sodass die Netzwerkkommunikation nicht unterbrochen wird.

Auf einem ASA r2 System können Sie IP-, FC- und NVMe/FC-LIFs erstellen. Eine IP-Daten-LIF kann standardmäßig sowohl iSCSI- als auch NVMe/TCP-Datenverkehr verarbeiten. Für den FC- und NVMe/FC-Datenverkehr müssen getrennte Daten-LIFs erstellt werden.

Wenn Sie den automatischen iSCSI-LIF-Failover aktivieren möchten, müssen Sie eine IP LIF für reinen iSCSI-Datenverkehr erstellen. Wenn automatisches iSCSI-LIF-Failover aktiviert ist, wird im Falle eines Storage-Failovers die IP-iSCSI-LIF automatisch vom Home Node oder Port des Node bzw. Ports des Home Ports zu seinem HA-Partnerknoten bzw. -Port migriert und nach Abschluss des Failovers wieder aufgenommen. Wenn der Port für eine IP-iSCSI-LIF nicht mehr funktionsfähig ist, wird die LIF automatisch zu einem ordnungsgemäßen Port im aktuellen Home Node und anschließend zurück zu seinem ursprünglichen Port migriert, sobald der Port wieder funktionsfähig ist.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Der zugrunde liegende physische oder logische Netzwerkport muss im Administratorstatus konfiguriert worden `up` sein.
- Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, muss das Subnetz bereits vorhanden sein.
- Ein LIF, die Intracluster-Datenverkehr zwischen Nodes verarbeiten, sollte sich nicht im selben Subnetz wie ein LIF-Handling-Datenverkehr oder eine LIF mit Datenverkehr befinden.

Schritte

1. Wählen Sie **Netzwerk > Übersicht**.
2. Wählen Sie **Netzwerkschnittstellen** aus, und wählen Sie dann + Add.
3. Wählen Sie den Schnittstellentyp und das Protokoll aus und anschließend die Storage-VM aus.
4. Geben Sie einen Namen für das LIF ein, oder übernehmen Sie den Standardnamen.
5. Wählen Sie den Startknoten für die Netzwerkschnittstelle aus, und geben Sie dann die IP-Adresse und die Subnetzmaske ein.
6. Wählen Sie **Speichern**.

Ergebnis

Sie haben eine LIF für den Datenzugriff erstellt.

Was kommt als Nächstes?

Sie können die ONTAP -Befehlszeilenschnittstelle (CLI) verwenden, um ein reines iSCSI-LIF mit automatischem Failover zu erstellen.

Erstellen einer benutzerdefinierten iSCSI-only-LIF-Dienstrichtlinie

Wenn Sie nur iSCSI-LIFs mit automatischem LIF-Failover erstellen möchten, müssen Sie zuerst eine benutzerdefinierte nur iSCSI-LIF-Dienstrichtlinie erstellen.

Sie müssen die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, um die benutzerdefinierte Servicerichtlinie zu erstellen.

Schritt

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Erstellen Sie eine benutzerdefinierte iSCSI-only-LIF-Dienstrichtlinie:

```
network interface service-policy create -vserver <SVM_name> -policy
<service_policy_name> -services data-core,data-iscsi
```

3. Überprüfen Sie, ob die Servicerichtlinie erstellt wurde:

```
network interface service-policy show -policy <service_policy_name>
```

4. Setzen Sie die Berechtigungsstufe auf „Administrator“ zurück:

```
set -privilege admin
```

Erstellen Sie nur iSCSI-LIFs mit automatischem LIF-Failover

Wenn auf der SVM iSCSI-LIFs vorhanden sind, die nicht für automatischen LIF-Failover aktiviert sind, werden die neu erstellten LIFs auch nicht für automatischen LIF-Failover aktiviert. Wenn der automatische LIF-Failover nicht aktiviert ist und ein Failover-Ereignis tritt, werden die iSCSI LIFs nicht migriert.

Bevor Sie beginnen

Sie müssen eine benutzerdefinierte iSCSI-only-LIF-Dienstrichtlinie erstellt haben.

Schritte

1. Erstellen Sie nur iSCSI-LIFs mit automatischem LIF-Failover:

```
network interface create -vserver <SVM_name> -lif <iscsi_lif_name>
-service-policy <service_policy_name> -home-node <home_node> -home-port
<port_name> -address <ip_address> -netmask <netmask> -failover-policy
sfo-partner-only -status-admin up
```

   - Es wird empfohlen, auf jedem Knoten zwei iSCSI-LIFs zu erstellen, eines für Fabric A und eines für Fabric B. Dies sorgt für Redundanz und Lastausgleich für Ihren iSCSI-Verkehr. Im folgenden Beispiel werden insgesamt vier iSCSI-LIFs erstellt, zwei auf jedem Knoten und eines für jedes Fabric.

```
network interface create -vserver svm1 -lif iscsi-lif-01a -service
-policy custom-data-iscsi -home-node node1 -home-port e2b -address
<node01-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-01b -service
-policy custom-data-iscsi -home-node node1 -home-port e4b -address
<node01-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02a -service
-policy custom-data-iscsi -home-node node2 -home-port e2b -address
<node02-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02b -service
-policy custom-data-iscsi -home-node node2 -home-port e4b -address
<node02-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up
```

- Wenn Sie VLANs verwenden, passen Sie die `home-port` Parameter, um die VLAN-Port-Informationen für das jeweilige iSCSI-Fabric einzuschließen, zum Beispiel `-home-port e2b-<iSCSI-A-VLAN>` für iSCSI Fabric A und `-home-port e4b-<iSCSI-B-VLAN>` .
- Wenn Sie Schnittstellengruppen (ifgroups) mit VLANs verwenden, passen Sie die `home-port` Parameter, um den entsprechenden VLAN-Port einzuschließen, z. B. `-home-port a0a-<iSCSI-A-VLAN>` für iSCSI Fabric A und `-home-port a0a-<iSCSI-B-VLAN>` für iSCSI-Fabric B, wobei `a0a` ist die ifgroup und a0a-<iSCSI-A-VLAN> und a0a-<iSCSI-B-VLAN> sind die jeweiligen VLAN-Ports für das iSCSI A-Fabric und das iSCSI B-Fabric.

2. Überprüfen Sie, ob die iSCSI-LIFs erstellt wurden:

```
network interface show -lif iscsi*
```

Ändern einer LIF (Netzwerkschnittstellen)

LIFs können bei Bedarf deaktiviert oder umbenannt werden. Sie können auch die LIF-IP-Adresse und die Subnetzmaske ändern.

Schritte

1. Wählen Sie **Netzwerk > Übersicht** und dann **Netzwerkschnittstellen**.
2. Bewegen Sie den Mauszeiger über die Netzwerkschnittstelle, die Sie bearbeiten möchten, und wählen Sie dann ⋮.
3. Wählen Sie **Bearbeiten**.
4. Sie können die Netzwerkschnittstelle deaktivieren, die Netzwerkschnittstelle umbenennen, die IP-Adresse ändern oder die Subnetzmaske ändern.

5. Wählen Sie **Speichern**.

Ergebnis

Ihr LIF wurde geändert.

Managen Sie Cluster-Netzwerke auf ASA r2 Storage-Systemen

Mit ONTAP System Manager können Sie eine grundlegende Storage-Netzwerkadministration auf Ihrem ASA r2 System durchführen. Sie können beispielsweise eine Broadcast-Domäne hinzufügen oder Ports einer anderen Broadcast-Domäne neu zuweisen.

Fügen Sie eine Broadcast-Domäne hinzu

Verwenden Sie Broadcast-Domänen, um das Management Ihres Cluster-Netzwerks zu vereinfachen, indem Sie Netzwerkports gruppieren, die zum gleichen Layer-2-Netzwerk gehören. Storage Virtual Machines (VMs) können dann die Ports in der Gruppe für Daten- oder Managementdatenverkehr verwenden.

Während des Cluster-Setups werden die „Standard“-Broadcast-Domäne und die „Cluster“ Broadcast-Domäne erstellt. Die „Standard“-Broadcast-Domäne enthält Ports, die sich im „Standard“-IPspace befinden. Diese Ports werden hauptsächlich zum Bereitstellen von Daten genutzt. Auch Cluster-Management- und Node-Management-Ports befinden sich in dieser Broadcast-Domäne. Die Broadcast-Domain „Cluster“ enthält Ports die sich im „Cluster“ IPspace befinden. Diese Ports werden für die Cluster-Kommunikation verwendet und umfassen alle Cluster-Ports aus allen Nodes im Cluster.

Sie können zusätzliche Broadcast-Domänen erstellen, nachdem das Cluster initialisiert wurde. Wenn Sie eine Broadcast-Domäne erstellen, wird automatisch eine Failover-Gruppe erstellt, die dieselben Ports enthält.

Über diese Aufgabe

Die maximale Übertragungseinheit (MTU) der Ports, die einer Broadcast-Domäne hinzugefügt wurden, wird auf den in der Broadcast-Domäne eingestellten MTU-Wert aktualisiert.

Schritte

1. Wählen Sie im System Manager **Netzwerk > Übersicht** aus.
2. Wählen Sie unter **Broadcast** Domains die Option + Add.
3. Geben Sie einen Namen für die Broadcast-Domäne ein, oder akzeptieren Sie den Standardnamen.

   Alle Broadcast-Domain-Namen müssen innerhalb eines IPspaces eindeutig sein.

4. Wählen Sie den IPspace für die Broadcast-Domäne aus.

   Wenn Sie keinen IPspace-Namen angeben, wird die Broadcast-Domain im „Standard“-IPspace erstellt.

5. Geben Sie die maximale Übertragungseinheit (MTU) ein.

   MTU ist das größte Datenpaket, das in Ihrer Broadcast-Domäne akzeptiert werden kann.

6. Wählen Sie die gewünschten Ports aus, und wählen Sie dann **Speichern**.

Ergebnis

Sie haben eine neue Broadcast-Domäne hinzugefügt.

Weisen Sie Ports einer anderen Broadcast-Domäne neu zu

Ports können nur zu einer Broadcast-Domäne gehören. Wenn Sie die Broadcast-Domäne ändern möchten, zu der ein Port gehört, müssen Sie den Port seiner vorhandenen Broadcast-Domäne einer neuen Broadcast-Domäne zuweisen.

Schritte

1. Wählen Sie im System Manager **Netzwerk > Übersicht** aus.
2. Wählen Sie unter **Broadcast Domains** neben dem Domainnamen aus, und wählen Sie dann **Bearbeiten**.
3. Heben Sie die Auswahl der Ethernet-Ports auf, die Sie einer anderen Domäne neu zuweisen möchten.
4. Wählen Sie die Broadcast-Domain aus, der Sie den Port neu zuweisen möchten, und wählen Sie dann **Neu zuweisen** aus.
5. Wählen Sie **Speichern**.

Ergebnis

Sie haben Ports einer anderen Broadcast-Domäne neu zugewiesen.

Erstellen Sie eine VLAN

Ein VLAN besteht aus Switch-Ports, die zu einer Broadcast-Domäne zusammengefasst sind. Mithilfe von VLANs können Sie die Sicherheit erhöhen, Probleme isolieren und verfügbare Pfade innerhalb Ihrer IP-Netzwerkinfrastruktur einschränken.

Bevor Sie beginnen

Die im Netzwerk implementierten Switches müssen entweder den IEEE 802.1Q Standards entsprechen oder über eine anbieterspezifische Implementierung von VLANs verfügen.

Über diese Aufgabe

- Ein VLAN kann nicht auf einem Port der Schnittstellengruppe erstellt werden, der keine Mitgliedsports enthält.
- Wenn Sie ein VLAN zum ersten Mal über einen Port konfigurieren, könnte der Port ausfallen, was zu einer vorübergehenden Trennung des Netzwerks führt. Nachfolgende VLAN-Erweiterungen zum selben Port wirken sich nicht auf den Portstatus aus.
- Sie sollten kein VLAN auf einer Netzwerkschnittstelle mit derselben Kennung wie das native VLAN des Switches erstellen. Wenn beispielsweise die Netzwerkschnittstelle e0b auf nativem VLAN 10 ist, sollten Sie keine VLAN e0b-10 auf dieser Schnittstelle erstellen.

Schritte

1. Wählen Sie im System Manager **Netzwerk > Ethernet-Ports** aus, und wählen Sie dann + VLAN.
2. Wählen Sie den Knoten und die Broadcast-Domäne für das VLAN aus.
3. Wählen Sie den Port für das VLAN aus.

   Das VLAN kann nicht mit einem Port verbunden werden, der eine Cluster-LIF hostet, oder mit den dem Cluster-IPspace zugewiesenen Ports.

4. Geben Sie eine VLAN-ID ein.

5. Wählen Sie **Speichern**.

Ergebnis

Sie haben ein VLAN erstellt, um die Sicherheit zu erhöhen, Probleme zu isolieren und die verfügbaren Pfade innerhalb Ihrer IP-Netzwerkinfrastruktur einzuschränken.

Überwachung der Nutzung und Erhöhung der Kapazität

Überwachung der Performance von Clustern und Speichereinheiten auf ASA r2-Storage-Systemen

Überwachen Sie mit ONTAP System Manager die Gesamt-Performance Ihres Clusters und die Performance bestimmter Storage-Einheiten, um zu bestimmen, wie Latenz, IOPS und Durchsatz sich auf Ihre geschäftskritischen Applikationen auswirken. Die Performance kann über verschiedene Zeiträume von einer Stunde bis zu einem Jahr überwacht werden.

Nehmen wir zum Beispiel an, eine geschäftskritische Applikation hat eine hohe Latenz und einen niedrigen Durchsatz. Wenn Sie die Cluster-Performance der letzten fünf Arbeitstage anzeigen, bemerken Sie einen Performance-Abfall zur gleichen Zeit am Tag. Anhand dieser Informationen können Sie ermitteln, ob die kritische Anwendung im Wettbewerb um Clusterressourcen steht, wenn im Hintergrund ein nicht kritischer Prozess ausgeführt wird. Anschließend können Sie Ihre QoS-Richtlinie ändern, um die Auswirkungen des nicht kritischen Workloads auf Systemressourcen zu begrenzen und sicherzustellen, dass Ihre kritische Workload die minimalen Durchsatzziele erfüllt.

Überwachen Sie die Cluster-Performance

Mithilfe von Cluster-Performance-Kennzahlen können Sie bestimmen, ob Sie Workloads verlagern müssen, um die Latenz zu minimieren sowie die IOPS und den Durchsatz Ihrer kritischen Applikationen zu maximieren.

Schritte

1. Wählen Sie in System Manager **Dashboard** aus.
2. Unter **Performance** sehen Sie die Latenz, IOPS und den Durchsatz für den Cluster nach Stunde, Tag, Woche, Monat oder Jahr.
3. Wählen Sie diese Option, um die Leistungsdaten herunterzuladen.

Was kommt als Nächstes?

Analysieren Sie mithilfe Ihrer Cluster-Performance-Kennzahlen, ob Sie Ihre QoS-Richtlinien ändern oder andere Anpassungen an den Applikations-Workloads vornehmen müssen, um die Cluster-Performance insgesamt zu maximieren.

Überwachung der Leistung der Speichereinheit

Verwenden Sie Performance-Kennzahlen der Storage-Einheit, um den Einfluss spezifischer Applikationen auf Latenz, IOPS und Durchsatz zu bestimmen.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie die zu überwachende Speichereinheit aus, und wählen Sie dann **Übersicht**.

3. Unter **Performance** sehen Sie die Latenz, IOPS und den Durchsatz für die Speichereinheit nach Stunde, Tag, Woche, Monat oder Jahr.
4. Wählen Sie  diese Option, um die Leistungsdaten herunterzuladen.

Was kommt als Nächstes?

Analysieren Sie mithilfe Ihrer Performance-Kennzahlen der Storage-Einheiten, ob Sie die QoS-Richtlinien, die Ihren Storage-Einheiten zugewiesen sind, ändern müssen, um die Latenz zu verringern und die IOPS und den Durchsatz zu maximieren.

Überwachung der Auslastung von Clustern und Speichereinheiten auf ASA r2-Storage-Systemen

Mit ONTAP System Manager überwachen Sie Ihre Storage-Auslastung, um sicherzustellen, dass Sie die Storage-Kapazität haben, die Sie für aktuelle und zukünftige Workloads benötigen.

Überwachen der Cluster-Auslastung

Überwachen Sie regelmäßig den von Ihrem Cluster verbrauchten Storage, um sicherzustellen, dass Sie bei Bedarf bereit sind, die Cluster-Kapazität zu erweitern, bevor der Speicherplatz knapp wird.

Schritte

1. Wählen Sie in System Manager **Dashboard** aus.
2. Unter **Capacity** sehen Sie die Menge des physisch belegten Speicherplatzes und die Menge des verfügbaren Speicherplatzes auf Ihrem Cluster.

   Das Datenreduzierungsverhältnis stellt den durch Storage-Effizienz eingesparten Speicherplatz dar.

Was kommt als Nächstes?

Wenn der Speicherplatz des Clusters knapp "Fügen Sie neue Laufwerke hinzu"ist oder nicht über die Kapazität verfügt, um zukünftigen Anforderungen gerecht zu werden, sollten Sie Ihr ASA r2 System einplanen, um Ihre Storage-Kapazität zu erhöhen.

Überwachung der Storage-Verfügbarkeitszonen-Auslastung

Jedes HA-Paar in einem ASA r2-System verwendet einen gemeinsamen Storage-Pool, der als „ Storage Availability Zone_“ bezeichnet wird. Die Storage-Verfügbarkeitszone hat Zugriff auf alle verfügbaren Festplatten im Storage-System und ist für beide Nodes im HA-Paar sichtbar.

Wenn Ihr Cluster 4 oder mehr Nodes enthält, können Sie die Menge des Speicherplatzes anzeigen, der von der Storage-Verfügbarkeitszone für jedes HA-Paar verwendet wird. Diese Metrik ist für 2-Node-Cluster nicht verfügbar.

Schritte

1. Wählen Sie im System Manager **Cluster** aus, und wählen Sie dann **Übersicht** aus.

   Für jedes HA-Paar im Cluster wird eine Zusammenfassung der Storage-Verfügbarkeitszone-Auslastung angezeigt.

2. Wenn Sie detailliertere Metriken benötigen, wählen Sie eine bestimmte Storage-Verfügbarkeit aus.

Unter **Übersicht** werden die Kapazität der Speicherverfügbarkeitszone, der genutzte Speicherplatz und das Datenreduzierungsverhältnis angezeigt.

Unter **Speichereinheiten** wird eine Liste aller Speichereinheiten in der Lagerverfügbarkeitszone angezeigt.

Was kommt als Nächstes?

Wenn die Storage-Verfügbarkeitszone knapp ist, sollten Sie eine andere Storage-Verfügbarkeitszone einplanen"Speichereinheiten verschieben", um die Storage-Auslastung im Cluster auszugleichen.

Überwachung der Auslastung der Speichereinheiten

Überwachen Sie den Storage-Verbrauch einer Storage-Einheit, um proaktiv die Größe der Storage-Einheit ganz nach Ihren Bedürfnissen zu erweitern.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie die zu überwachende Speichereinheit aus, und wählen Sie dann **Übersicht**.
3. Sehen Sie sich unter **Speicher** Folgendes an:
   - Größe der Speichereinheit
   - Menge des belegten Speicherplatzes
   - Datenreduzierungsquote

     Das Datenreduzierungsverhältnis stellt den durch Storage-Effizienz eingesparten Speicherplatz dar
   - Verwendeter Snapshot

     Der von Snapshots verwendete Snapshot stellt die Größe des von Snapshots verwendeten Speichers dar.

Was kommt als Nächstes?

Wenn sich die Speicherkapazität Ihrer Speichereinheit nähert, sollten Sie "Ändern Sie die Speichereinheit"sie vergrößern.

Erhöhen Sie die Storage-Kapazität auf ASA r2 Storage-Systemen

Fügen Sie zu einem Node oder Shelf Laufwerke hinzu, um die Storage-Kapazität Ihres ASA r2 Systems zu erhöhen.

Verwenden Sie NetApp Hardware Universe, um die Installation eines neuen Laufwerks vorzubereiten

Bevor Sie ein neues Laufwerk an einem Node oder Shelf installieren, verwenden Sie den NetApp Hardware Universe, um sicherzustellen, dass das hinzuzufügende Laufwerk von Ihrer ASA r2-Plattform unterstützt wird, und um den richtigen Steckplatz für das neue Laufwerk zu ermitteln. Die richtigen Steckplätze zum Hinzufügen von Laufwerken variieren je nach Plattformmodell und ONTAP-Version. In einigen Fällen müssen Sie in der Folge Laufwerke zu bestimmten Steckplätzen hinzufügen.

Schritte

1. Gehen Sie zum "NetApp Hardware Universe".
2. Wählen Sie unter **Produkte** Ihre Hardwarekonfigurationen aus.

3. Wählen Sie Ihre ASA r2-Plattform aus.
4. Wählen Sie Ihre ONTAP-Version aus, und wählen Sie dann **Ergebnisse anzeigen**.
5. Wählen Sie unter der Grafik **Klicken Sie hier, um alternative Ansichten zu sehen**; wählen Sie dann die Ansicht, die Ihrer Konfiguration entspricht.
6. Überprüfen Sie anhand der Konfigurationsansicht, ob das neue Laufwerk unterstützt wird und ob der richtige Steckplatz für die Installation vorhanden ist.

Ergebnis

Sie haben bestätigt, dass Ihr neues Laufwerk unterstützt wird, und Sie kennen den passenden Steckplatz für die Installation.

Installieren Sie ein neues Laufwerk auf dem ASA r2

Die Mindestanzahl der Laufwerke, die Sie in einem einzigen Verfahren hinzufügen sollten, beträgt sechs. Das Hinzufügen eines einzigen Laufwerks kann zu einer Performance-Verringerung führen.

Über diese Aufgabe

Wiederholen Sie die Schritte in diesem Verfahren für jedes Laufwerk.

Schritte

1. Richtig gemahlen.
2. Entfernen Sie vorsichtig die Blende von der Vorderseite der Plattform.
3. Setzen Sie das neue Laufwerk in den richtigen Steckplatz ein.
   a. Setzen Sie den neuen Antrieb mit beiden Händen ein, indem Sie den Nockengriff in die offene Position bringen.
   b. Drücken Sie, bis das Laufwerk stoppt.
   c. Schließen Sie den Nockengriff, so dass der Antrieb fest in der Mittelebene sitzt und der Griff einrastet.

      Schließen Sie den Nockengriff langsam, damit er korrekt an der Antriebsfläche ausgerichtet ist.
4. Vergewissern Sie sich, dass die Aktivitäts-LED (grün) des Laufwerks leuchtet.
   - WENN die LED konstant leuchtet, wird das Laufwerk mit Strom versorgt.
   - Wenn die LED blinkt, wird das Laufwerk mit Strom versorgt und E/A wird ausgeführt. Die LED blinkt auch, wenn die Laufwerksfirmware aktualisiert wird.

     Die Laufwerk-Firmware wird automatisch (unterbrechungsfrei) auf neuen Laufwerken aktualisiert, die keine aktuellen Firmware-Versionen aufweisen.
5. Wenn der Node für die automatische Laufwerkszuweisung konfiguriert ist, können Sie warten, bis ONTAP die neuen Laufwerke einem Node automatisch zuweist. Ist der Node nicht für die automatische Laufwerkszuweisung konfiguriert oder ist er vorzuziehen, können Sie die Laufwerke manuell zuweisen.

   Die neuen Laufwerke werden erst erkannt, wenn sie einem Node zugewiesen sind.

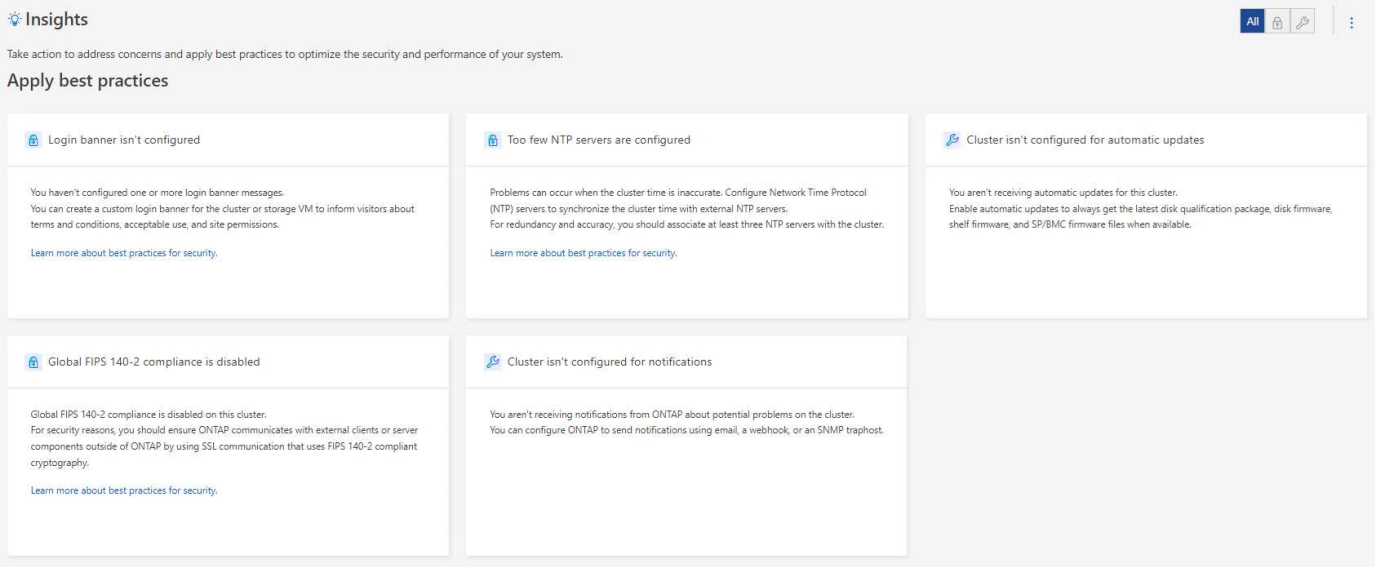
Was kommt als Nächstes?

Nachdem die neuen Laufwerke erkannt wurden, überprüfen Sie, ob sie hinzugefügt wurden und ihre Eigentumsrechte korrekt angegeben wurden.

ASA r2 Storage-System bietet Einblick in Cluster-Sicherheit und -Performance

Zeigen Sie *Insights* im ONTAP-System-Manager an, um Best Practices und Konfigurationsänderungen zu ermitteln, die Sie auf Ihrem ASA r2-System implementieren können, um Clustersicherheit und -Leistung zu optimieren.

Angenommen, Sie haben für das Cluster NTP-Server (Network Time Protocol) konfiguriert. Sie wissen jedoch nicht, dass für ein optimales Cluster-Zeitmanagement weniger als die empfohlene Anzahl von NTP-Servern erforderlich ist. Damit Sie Probleme vermeiden können, die bei ungenauer Cluster-Zeit auftreten können, werden Sie von Insights benachrichtigt, dass zu wenige NTP-Server konfiguriert sind, und Sie haben die Möglichkeit, mehr über dieses Problem zu erfahren, das Problem zu beheben oder es zu schließen.



Schritte

1. Wählen Sie im System Manager **Insights** aus.
2. Besprechen Sie die Empfehlungen.

Wie es weiter geht

Führen Sie alle erforderlichen Aktionen durch, um Best Practices zu implementieren und die Sicherheit und Performance des Clusters zu optimieren.

Anzeigen von Clusterereignissen und -Jobs auf ASA r2-Speichersystemen

Verwenden Sie ONTAP System Manager, um eine Liste der Fehler oder Warnmeldungen anzuzeigen, die in Ihrem System aufgetreten sind, sowie empfohlene Korrekturmaßnahmen. Sie können auch Systemauditprotokolle und eine Liste von Jobs anzeigen, die aktiv, abgeschlossen oder fehlgeschlagen sind.

Schritte

1. Wählen Sie im System Manager **Ereignisse & Jobs** aus.

2. Anzeigen von Clusterereignissen und -Jobs

Um dies anzuzeigen…	Tun Sie das…
Cluster-Ereignisse	Wählen Sie **Events**, und wählen Sie dann **Event Log**.
Vorschläge von Active IQ	Wählen Sie **Ereignisse** und dann **Active IQ Suggestions**.
Systemmeldungen	a. Wählen Sie **System Alerts**. b. Wählen Sie die Systemwarnung aus, für die Sie Maßnahmen ergreifen möchten. c. Bestätigen oder unterdrücken Sie die Warnmeldung.
Cluster-Jobs	Wählen Sie **Jobs**.
Prüfprotokolle	Wählen Sie **Audit-Protokolle**.

Senden von E-Mail-Benachrichtigungen für Cluster-Ereignisse und Prüfprotokolle

Konfigurieren Sie das System so, dass eine Benachrichtigung an bestimmte E-Mail-Adressen gesendet wird, wenn ein Clusterereignis- oder Überwachungsprotokolleintrag vorhanden ist.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie neben **Benachrichtigungsverwaltung** ⋮.
3. Um ein Ereignisziel zu konfigurieren, wählen Sie **Ereignisziele anzeigen** und dann **Ereignisziele**. Wählen Sie zum Konfigurieren eines Überwachungsprotokollziels **Überwachungsziele anzeigen** aus, und wählen Sie dann **Überwachungsziele** aus.
4. Wählen Sie + Add.
5. Geben Sie die Zielinformationen ein, und wählen Sie dann **Hinzufügen**.

Ergebnis

Die von Ihnen hinzugefügte E-Mail-Adresse erhält nun die angegebenen E-Mail-Benachrichtigungen für Clusterereignisse und Prüfprotokolle.

Managen von Nodes

Hinzufügen von ASA r2-Nodes zu einem ONTAP-Cluster

Ab ONTAP 9.16.1 unterstützen ASA r2 Storage-Systeme bis zu 12 Nodes pro Cluster. Nachdem die neuen Nodes eines HA-Paars verkabelt und eingeschaltet wurden, müssen Sie sie mit dem Cluster verbinden.

Bevor Sie beginnen

Stellen Sie die folgenden Informationen zusammen:

- Die Node-IP-Adresse
- Die IP-Adresse der Intercluster-Netzwerkschnittstelle
- Die Subnetz-Maske des Intercluster-Netzwerks
- Das Intercluster Netzwerk-Gateway
- Wenn Sie den Onboard Key Manager (OKM) konfigurieren möchten, benötigen Sie die OKM-Passphrase.

Schritte

1. Wählen Sie im System Manager **Cluster > Übersicht** aus.
2. Wählen Sie ⋮ neben dem Knoten, dem Sie beitreten möchten, und wählen Sie dann **Knoten hinzufügen**
3. Geben Sie die IP-Adresse für jeden Node ein.
4. Geben Sie die IP-Adresse, die Subnetzmaske und das Gateway der Intercluster-Netzwerkschnittstelle ein.
5. Wenn Sie den Onboard Key Manager (OKM) konfigurieren möchten, geben Sie die OKM-Passphrase ein.

   Konfigurieren des Onboard-Schlüsselmanagers für die Verschlüsselung ist standardmäßig ausgewählt.

6. Wählen Sie **Hinzufügen**.

Ergebnis

Das neue HA-Paar wird mit dem Cluster verbunden.

Was kommt als Nächstes?

Nachdem Sie dem Cluster das neue HA-Paar hinzugefügt haben, können Sie "Aktivieren Sie den Datenzugriff über Ihre SAN-Hosts"sie den neuen Nodes hinzufügen.

Starten Sie einen Node auf einem ASA r2-Speichersystem neu

Möglicherweise müssen Sie einen Node aus Wartungsgründen, zur Fehlerbehebung, zu Softwareupdates oder aus anderen administrativen Gründen neu booten. Beim Neustart eines Node führt der HA-Partner automatisch eine Übernahme aus. Der Partner-Node führt dann ein automatisches Giveback durch, nachdem der neu gebootete Node wieder online geschaltet wurde.

Schritte

1. Wählen Sie im System Manager **Cluster > Übersicht** aus.
2. Wählen Sie ⋮ neben dem Knoten, den Sie neu starten möchten, und wählen Sie dann **Neustart**.
3. Geben Sie den Grund für das Neustarten des Knotens ein, und wählen Sie dann **Neustart** aus.

   Der von Ihnen eingegebene Grund für das Neubooten wird im Systemauditprotokoll aufgezeichnet.

Was kommt als Nächstes?

Während des Neubootens des Node führt der HA-Partner einen Takeover aus, sodass der Datenservice nicht unterbrochen wird. Nach Abschluss des Neubootens führt der HA-Partner ein Giveback durch.

Benennen Sie einen Knoten in einem ASA r2-Speichersystem um

Sie können ONTAP System Manager verwenden, um einen Knoten auf dem ASA r2-System umzubenennen. Möglicherweise müssen Sie einen Node umbenennen, um ihn an die Namenskonventionen Ihres Unternehmens oder aus anderen administrativen Gründen anzupassen.

Schritte

1. Wählen Sie im System Manager **Cluster > Übersicht** aus.
2. Wählen Sie ⋮ neben dem Knoten, den Sie umbenennen möchten, und wählen Sie dann **Umbenennen**.
3. Geben Sie den neuen Namen für den Knoten ein, und wählen Sie dann **Umbenennen**.

Ergebnis

Der neue Name wird auf den Node angewendet.

Neuverteilung der Arbeitslasten zwischen Knoten auf ASA R2-Speichersystemen

Ab ONTAP 9.17.1 gleicht ONTAP die Workloads automatisch zwischen den Knoten eines ASA R2-System-HA-Paares aus, um optimale Leistung zu erzielen. Steigt beispielsweise die Auslastung eines Knotens auf 70 %, während die des HA-Partners nur 30 % beträgt, verschiebt ONTAP die Workloads automatisch, sodass die Auslastung der einzelnen Knoten besser ausgeglichen wird. Da die Knoten des HA-Paares dieselbe Storage Availability Zone nutzen, erfolgt die Workload-Neuverteilung kopierfrei und ohne Auswirkungen auf die Leistung.

Ändern des Standardauswertungszeitraums für die automatische Neuverteilung der Arbeitslast

Die automatische Lastverteilung wird standardmäßig 14 Tage nach dem Upgrade auf ONTAP 9.17.1 oder der Initialisierung eines neuen ONTAP 9.17.1 ASA r2-Clusters aktiviert. Über die ONTAP -Befehlszeilenschnittstelle (CLI) können Sie den Standard-Evaluierungszeitraum Ihren betrieblichen Anforderungen entsprechend verlängern oder verkürzen.

> ⓘ Sie können auf Ihrem ASA R2-System nicht von ONTAP 9.17.1 zurückkehren, nachdem die automatische Neuverteilung der Arbeitslast aktiviert wurde.

Schritte

1. Überprüfen Sie die Anzahl der verbleibenden Tage des Evaluierungszeitraums:

```
placement rebalance config show -fields evaluation-window
```

2. Ändern Sie den Bewertungszeitraum für die Neugewichtung:

```
placement rebalance config modify -evaluation-window
<number_of_evaluation_days>
```

Im folgenden Beispiel wird der verbleibende Auswertungszeitraum auf 10 Tage festgelegt.

```
placement rebalance config modify -evaluation-window 10
```

Ändern der Einstellung für die automatische Neuverteilung der Arbeitslast

Die automatische Neuverteilung der Workloads wird standardmäßig 14 Tage nach dem Upgrade auf ONTAP 9.17.1 oder der Initialisierung eines neuen ONTAP 9.17.1 ASA r2-Clusters aktiviert. Sie können die Standardeinstellung ändern, um die automatische Neuverteilung der Workloads zu deaktivieren oder sie auf einen empfohlenen Status zu setzen, um unausgeglichene Workloads zu kennzeichnen, ohne sie automatisch zu verschieben.

Schritt

1. Überprüfen Sie den aktuell auf Ihren Knoten eingestellten Neuausgleichsmodus:

```
placement rebalance config show -fields mode
```

2. Ändern Sie die Einstellung für die automatische Neuverteilung der Arbeitslast:

```
placement rebalance config modify -mode <disabled|advisory|automated>
```

3. Überprüfen Sie, ob der Neuausgleichsmodus geändert wurde:

```
placement rebalance config show -fields mode
```

Manuelles Auslösen einer Neuverteilung der Arbeitslast

Wenn Sie die automatische Neuverteilung der Arbeitslast deaktiviert haben, können Sie sie dennoch manuell auslösen. Dies ist nützlich, wenn Sie die Arbeitslasten nach einer Phase manueller Anpassungen neu verteilen möchten oder wenn Sie den Neuverteilungsmodus auf „Beratend“ gesetzt haben und basierend auf den Arbeitslast-Flags Maßnahmen ergreifen möchten.

Schritte

1. Überprüfen Sie den aktuell auf Ihren Knoten eingestellten Neuausgleichsmodus:

```
placement rebalance config show -fields mode
```

2. Wenn der Rebalancing-Modus nicht auf **beratend** eingestellt ist, stellen Sie ihn auf **beratend** ein:

```
placement rebalance config modify -mode advisory
```

3. Lösen Sie manuell eine Neuverteilung der Arbeitslast aus:

```
balanced-placement rebalance execute
```

4. Zeigen Sie den Status des Neuausgleichsvorgangs an:

```
placement rebalance config show-evaluation
```

Was kommt als Nächstes?

Wenn Sie den Rebalancing-Modus auf **automatisch** oder **deaktiviert** einstellen möchten, können Sie dies tun, indem Sie die `placement rebalance config modify` Befehl.

Managen von Benutzerkonten und Rollen auf ASA r2 Storage-Systemen

Mit System Manager können Sie den Active Directory-Domänencontroller-Zugriff sowie die LDAP- und SAML-Authentifizierung für Ihre Benutzerkonten konfigurieren. Erstellen Sie Benutzerkontorollen, um bestimmte Funktionen zu definieren, die Benutzer, die den Rollen zugewiesen sind, auf dem Cluster ausführen können.

Konfigurieren Sie den Zugriff auf den Active Directory-Domänencontroller

Konfigurieren Sie den Active Directory (AD) Domain Controller-Zugriff auf das Cluster oder die Storage-VM, damit Sie den Zugriff auf das AD-Konto aktivieren können.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** unter **Active Directory Konfigurieren** aus.

Was kommt als Nächstes?

Sie können nun den AD-Kontozugriff auf Ihrem ASA r2-System aktivieren.

LDAP konfigurieren

Konfigurieren Sie einen LDAP-Server (Lightweight Directory Access Protocol) zur zentralen Verwaltung von Benutzerinformationen für die Authentifizierung.

Bevor Sie beginnen

Sie müssen eine Zertifikatsignierungsanforderung erstellt und ein digitales Zertifikat für einen CA-signierten Server hinzugefügt haben.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** neben **LDAP** die Option ⚙.
3. Geben Sie den erforderlichen LDAP-Server und die Verbindungsinformationen ein, und wählen Sie dann **Speichern**.

Was kommt als Nächstes?

Sie können jetzt LDAP für Benutzerinformationen und Authentifizierung verwenden.

Konfigurieren Sie die SAML-Authentifizierung

Die SAML-Authentifizierung (Security Assertion Markup Language) ermöglicht die Authentifizierung von Benutzern durch einen sicheren Identitätsanbieter (Secure Identity Provider, IdP) anstelle von direkten Dienstanbietern wie Active Directory und LDAP.

Bevor Sie beginnen

- Der IdP, den Sie für die Remote-Authentifizierung verwenden möchten, muss konfiguriert werden.

  Informationen zur Konfiguration finden Sie in der IdP-Dokumentation.

- Sie müssen die URI des IdP haben.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie unter **Sicherheit** neben **SAML-Authentifizierung** die Option ⚙ .
3. Wählen Sie **SAML-Authentifizierung aktivieren**.
4. Geben Sie die IdP-URL und die IP-Adresse des Hostsystems ein, und wählen Sie dann **Speichern**.

   In einem Bestätigungsfenster werden die Metadateninformationen angezeigt, die automatisch in die Zwischenablage kopiert wurden.

5. Wechseln Sie zum angegebenen IdP-System, und kopieren Sie dann die Metadaten aus der Zwischenablage, um die Systemmetadaten zu aktualisieren.
6. Kehren Sie zum Bestätigungsfenster im System Manager zurück; wählen Sie dann **I have configured the IdP with the Host URI or metadata** aus.
7. Wählen Sie **Abmelden**, um die SAML-basierte Authentifizierung zu aktivieren.

   Das IdP-System zeigt einen Authentifizierungsbildschirm an.

Was kommt als Nächstes?

Sie können jetzt die SAML-Authentifizierung für Ihre Benutzerkonten verwenden.

Erstellen von Benutzerkontorollen

Rollen für Cluster-Administratoren und Storage-VM-Administratoren werden automatisch erstellt, wenn das Cluster initialisiert wird. Erstellen Sie zusätzliche Benutzerkontorollen, um bestimmte Funktionen zu definieren, die Benutzer, die den Rollen zugewiesen sind, auf Ihrem Cluster ausführen können.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** neben **Benutzer und Rollen** die Option →.
3. Wählen Sie unter **Rollen** die Option + Add .
4. Wählen Sie die Rollenattribute aus.

   Um mehrere Attribute hinzuzufügen, wählen Sie + Add .

5. Wählen Sie **Speichern**.

Ergebnis

Ein neues Benutzerkonto wird erstellt und steht für die Verwendung auf Ihrem ASA r2-System zur Verfügung.

Erstellen Sie ein Administratorkonto

Erstellen Sie ein Administrator-Benutzerkonto, mit dem der Account-Benutzer basierend auf der dem Konto zugewiesenen Rolle bestimmte Aktionen für den Cluster ausführen kann. Um die Kontosicherheit zu verbessern, richten Sie bei der Erstellung des Kontos eine Multi-Faktor-Authentifizierung (MFA) ein.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** neben **Benutzer und Rollen** die Option →.
3. Wählen Sie unter **Benutzer** die Option + Add.
4. Geben Sie einen Benutzernamen ein, und wählen Sie dann eine Rolle aus, die dem Benutzer zugewiesen werden soll.
5. Wählen Sie die Benutzeranmeldemethode und die Authentifizierungsmethode aus.
6. Um MFA zu aktivieren, wählen Sie + Add ; und wählen Sie dann eine sekundäre Anmeldemethode und Authentifizierungsmethode aus
7. Geben Sie ein Kennwort für den Benutzer ein.
8. Wählen Sie **Speichern**.

Ergebnis

Ein neues Administratorkonto wird erstellt und steht für den ASA r2-Cluster zur Verfügung.

Managen von Sicherheitszertifikaten auf ASA r2-Speichersystemen

Verwenden Sie digitale Sicherheitszertifikate, um die Identität von Remote-Servern zu überprüfen.

Online Certificate Status Protocol (OCSP) validiert den Status von digitalen Zertifikatsanforderungen von ONTAP-Diensten mithilfe von SSL- und TLS-Verbindungen (Transport Layer Security).

Generieren Sie eine Anforderung zum Signieren eines Zertifikats

Erstellen Sie eine Zertifikatsignierungsanforderung (CSR), um einen privaten Schlüssel zu erstellen, mit dem ein öffentliches Zertifikat erstellt werden kann.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie unter **Security** neben **Certificates** die Option →; und wählen Sie dann + Generate CSR.
3. Geben Sie den allgemeinen Namen des Studienteilnehmers ein, und wählen Sie dann das Land aus.
4. Wenn Sie die GSR-Standardwerte ändern möchten, wählen Sie Erweiterte Tastenverwendung oder fügen Sie alternative Namen für ↙↗ More optionsdas Thema hinzu, wählen Sie ; und dann die gewünschten Aktualisierungen vornehmen.

5. Wählen Sie **Erzeugen**.

Ergebnis

Sie haben eine CSR erstellt, mit der Sie ein öffentliches Zertifikat erstellen können.

Fügen Sie eine vertrauenswürdige Zertifizierungsstelle hinzu

ONTAP bietet einen Standardsatz vertrauenswürdiger Stammzertifikate für Anwendungen, die TLS (Transport Layer Security) verwenden. Sie können bei Bedarf weitere vertrauenswürdige Zertifizierungsstellen hinzufügen.

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie unter **Sicherheit** neben **Zertifikate** die Option →.
3. Wählen Sie **Vertrauenswürdige Zertifizierungsstellen**.
4. Geben Sie die Zertifikatdetails ein oder importieren Sie + Add sie, und wählen Sie dann .

Ergebnis

Sie haben Ihrem ASA r2-System eine neue vertrauenswürdige Zertifizierungsstelle hinzugefügt.

Erneuern oder Löschen einer vertrauenswürdigen Zertifizierungsstelle

Vertrauenswürdige Zertifizierungsstellen müssen jährlich erneuert werden. Wenn Sie ein abgelaufenes Zertifikat nicht erneuern möchten, sollten Sie es löschen.

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie unter **Sicherheit** neben **Zertifikate** die Option →.
3. Wählen Sie **Vertrauenswürdige Zertifizierungsstellen**.
4. Wählen Sie die Zertifizierungsstelle aus, die Sie erneuern oder löschen möchten.
5. Erneuern oder löschen Sie die Zertifizierungsstelle.

Um die Zertifizierungsstelle zu erneuern, gehen Sie folgendermaßen vor:	Gehen Sie folgendermaßen vor, um die Zertifizierungsstelle zu löschen:
a. Wählen Sie ⋮; und dann **erneuern**. b. Geben Sie die Zertifikatinformationen ein oder importieren Sie sie, und wählen Sie dann **Renew** aus.	a. Wählen Sie ⋮; und dann **Löschen**. b. Bestätigen Sie, dass Sie löschen möchten, und wählen Sie dann **Löschen**.

Ergebnis

Sie haben eine vorhandene vertrauenswürdige Zertifizierungsstelle auf Ihrem ASA r2-System erneuert oder gelöscht.

Fügen Sie ein Client/Server-Zertifikat oder lokale Zertifizierungsstellen hinzu

Fügen Sie ein Client/Server-Zertifikat oder lokale Zertifizierungsstellen hinzu, um sichere Webdienste zu ermöglichen.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie unter **Sicherheit** neben **Zertifikate** die Option →.
3. Wählen Sie **Client/Server-Zertifikate** oder **Local Certificate Authorities** aus.
4. Fügen Sie die Zertifikatinformationen hinzu, und wählen Sie dann + Add.

Ergebnis

Sie haben Ihrem ASA r2-System ein neues Client/Server-Zertifikat oder lokale Behörden hinzugefügt.

Erneuern oder löschen Sie ein Client/Server-Zertifikat oder lokale Zertifizierungsstellen

Client/Server-Zertifikate und lokale Zertifizierungsstellen müssen jährlich erneuert werden. Wenn Sie ein abgelaufenes Zertifikat oder eine lokale Zertifizierungsstelle nicht erneuern möchten, sollten Sie diese löschen.

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie unter **Sicherheit** neben Zertifikate die Option →.
3. Wählen Sie **Client/Server-Zertifikate** oder **Lokale Zertifizierungsstellen** aus.
4. Wählen Sie das Zertifikat aus, das Sie erneuern oder löschen möchten.
5. Erneuern oder löschen Sie die Zertifizierungsstelle.

Um die Zertifizierungsstelle zu erneuern, gehen Sie folgendermaßen vor:	Gehen Sie folgendermaßen vor, um die Zertifizierungsstelle zu löschen:
a. Wählen Sie ⋮; und dann **erneuern**. b. Geben Sie die Zertifikatinformationen ein oder importieren Sie sie, und wählen Sie dann **Renew** aus.	Wählen Sie ⋮; und dann **Löschen**.

Ergebnis

Sie haben ein vorhandenes Client/Server-Zertifikat oder eine lokale Zertifizierungsstelle auf Ihrem ASA r2-System erneuert oder gelöscht.

Überprüfen Sie die Hostkonnektivität auf Ihrem ASA r2-Speichersystem

Wenn bei den Host-Datenvorgängen ein Problem auftritt, können Sie mithilfe von ONTAP System Manager überprüfen, ob die Verbindung zwischen dem Host und dem ASA r2 Storage-System aktiv ist.

Schritte

1. Wählen Sie im System Manager **Host** aus.

   Der Host-Konnektivitätsstatus wird neben dem Namen der Host-Gruppe wie folgt angezeigt:

- **OK**: Zeigt an, dass alle Initiatoren mit beiden Knoten verbunden sind.
- **Teilweise verbunden**: Zeigt an, dass einige der Initiatoren nicht mit beiden Knoten verbunden sind.
- **Keine Verbindung**: Zeigt an, dass keine Initiatoren verbunden sind.

Was kommt als Nächstes?

Aktualisieren Sie Ihren Host, um Verbindungsprobleme zu beheben. ONTAP überprüft den Verbindungsstatus alle 15 Minuten erneut.

Wartung Ihres ASA r2 Storage-Systems

Unter "ASA r2 Wartungsdokumentation" erfahren Sie, wie Sie Wartungsverfahren für Ihre ASA r2-Systemkomponenten durchführen.

Weitere Informationen .

ASA r2 für ONTAP Power User

Vergleichen Sie ASA r2 Systeme mit anderen ONTAP Systemen

ASA R2-Systeme bieten eine Hardware- und Softwarelösung für reine SAN-Umgebungen auf Basis von All-Flash-Plattformen. ASA R2-Systeme unterscheiden sich von anderen ONTAP Systemen (ASA, AFF und FAS) in der Implementierung der ONTAP Persönlichkeit, der Speicherschicht und der unterstützten Protokolle.

Die folgenden ASA-Plattformen werden als ASA r2-Systeme klassifiziert:

- ASA A1K
- ASA A90
- ASA A70
- ASA A50
- ASA A30
- ASA A20
- ASA C30

Persönlichkeitsunterschiede

Auf einem ASA r2 System wird die ONTAP Software optimiert, um wichtige SAN-Funktionen zu unterstützen und gleichzeitig die Sichtbarkeit und Verfügbarkeit von nicht-SAN-bezogenen Funktionen zu beschränken. Beispielsweise zeigt System Manager, der auf einem ASA r2 System ausgeführt wird, keine Optionen zum Erstellen von Home Directorys für NAS-Clients an. Diese optimierte Version von ONTAP wird als *ASA r2 Personality* bezeichnet. ONTAP auf ASA Systemen wird als *ASA ONTAP Personality* identifiziert. ONTAP auf AFF und FAS ONTAP Systemen wird als „*Unified ONTAP Personality*“ bezeichnet. Die Unterschiede zwischen den ONTAP-Persönlichkeiten werden in der ONTAP-Befehlsreferenz (man-Pages), in der REST-API-Spezifikation und ggf. in EMS-Meldungen erwähnt.

Sie können die Persönlichkeit Ihres ONTAP-Speichers vom System Manager oder von der ONTAP-CLI überprüfen.

- Wählen Sie im Menü System Manager **Cluster > Übersicht**.
- Geben Sie über die CLI Folgendes ein: `san config show`

Die Persönlichkeit Ihres ONTAP Storage-Systems kann nicht geändert werden.

Unterschiede der Speicherebenen

ASA r2-Systeme verwenden eine vereinfachte Speicherschicht, die sich von der Speicherschicht unterscheidet, die von FAS, AFF und ASA Systemen verwendet wird.

FAS, AFF und ASA -Systeme

Die Speicherschicht für FAS -, AFF- und ASA -Systeme verwendet Aggregate als Basisspeichereinheit. Ein Aggregat besitzt einen bestimmten Satz der im Speichersystem verfügbaren Festplatten. Das Aggregat weist

den Speicherplatz auf den zugehörigen Festplatten Volumes für LUNs und Namespaces zu. Mit diesen Systemen können ONTAP Benutzer Aggregate, Volumes, LUNs und Namespaces erstellen und ändern.

ASA r2-Systeme

Anstelle von Aggregaten verwendet die Speicherebene in ASA r2-Systemen Speicherverfügbarkeitszonen. Eine Speicherverfügbarkeitszone ist ein gemeinsamer Speicherpool, der beiden Knoten eines HA-Paares zur Verfügung steht. Beide Knoten im HA-Paar haben Zugriff auf alle verfügbaren Festplatten in ihrer gemeinsamen Speicherverfügbarkeitszone. Beispielsweise gibt es in einem ASA r2-System- ONTAP Cluster mit zwei Knoten eine Speicherverfügbarkeitszone, auf die beide Knoten im Cluster zugreifen können. In einem ASA r2-System- ONTAP Cluster mit vier Knoten gibt es zwei Speicherverfügbarkeitszonen. Jedes HA-Paar im Cluster hat Zugriff auf eine der Speicherverfügbarkeitszonen.

Beim Erstellen einer Speichereinheit (basierend auf einem LUN- oder NVMe-Namespace) erstellt ONTAP automatisch ein Volume in der entsprechenden Storage Availability Zone, um die Speichereinheit unterzubringen. Das neu erstellte Volume wird automatisch in der Storage Availability Zone platziert, um optimale Leistung und eine ausgewogene Kapazitätsauslastung zu gewährleisten. Abhängig von Ihrer ONTAP-Version unterstützen ASA r2-Systeme auch die automatische Neuverteilung von Speichereinheiten in der Storage Availability Zone und die automatische Neuverteilung von Workloads zwischen den Knoten in einem HA-Paar.

- Automatische Neugewichtung der Speichereinheiten

  Ab ONTAP 9.16.1 verschiebt ONTAP Speichereinheiten automatisch nach Bedarf, um die Auslastung auszugleichen und die Leistung zu optimieren, wenn eine Speichereinheit so zunimmt oder abnimmt, dass ein Ungleichgewicht in der Speicherauslastung in der gesamten Speicherverfügbarkeitszone entsteht.

- Automatischer Workload-Ausgleich

  Ab ONTAP 9.17.1 gleicht ONTAP die Workloads automatisch zwischen den Knoten eines ASA r2-System-HA-Paares aus, um optimale Leistung zu erzielen. Steigt beispielsweise die Auslastung eines Knotens auf 70 %, während die Auslastung des HA-Partners nur 30 % beträgt, verschiebt ONTAP die Workloads automatisch, sodass die Auslastung der einzelnen Knoten besser ausgeglichen wird. Da die Knoten des HA-Paares dieselbe Storage Availability Zone nutzen, erfolgt die Workload-Neuverteilung kopierfrei und ohne Auswirkungen auf die Leistung. Die automatische Workload-Neuverteilung wird standardmäßig 14 Tage nach dem Upgrade auf ONTAP 9.17.1 oder der Initialisierung eines neuen ONTAP 9.17.1 ASA r2-Clusters aktiviert. Sie können "Ändern Sie die Standardeinstellung" um die automatische Neuverteilung der Arbeitslast zu aktivieren oder zu deaktivieren oder um sie in einen beratenden Zustand zu versetzen, um unausgeglichene Arbeitslasten zu kennzeichnen, ohne sie automatisch zu verschieben.

Zusammenfassung der ASA r2-Systemunterschiede

ASA r2-Systeme unterscheiden sich von FAS, AFF und ASA -Systemen in folgenden Punkten:

	ASA r2	ASA	AFF	FAS
ONTAP-Persönlichkeit	ASA r2	ASA	Virtualisierung	Virtualisierung

	ASA r2	ASA	AFF	FAS
Unterstützung für SAN-Protokolle	Ja.	Ja.	Ja.	Ja.
Unterstützung des NAS-Protokolls	Nein	Nein	Ja.	Ja.
Unterstützung der Speicherschicht	Zone der Storage-Verfügbarkeit	Aggregate	Aggregate	Aggregate

Aufgrund dieses automatisierten und vereinfachten Ansatzes zur Speicherverwaltung sind bestimmte System Manager-Optionen, ONTAP -Befehle und REST-API-Endpunkte auf einem ASA r2-System nicht verfügbar oder nur eingeschränkt nutzbar. Da beispielsweise die Volume-Erstellung und -Verwaltung für ASA r2-Systeme automatisiert ist, wird das Menü **Volumes** im System Manager nicht angezeigt und die `volume create` Befehl wird nicht unterstützt. "Erfahren Sie mehr über nicht unterstützte ASA R2-Befehle" .

Die Hauptunterschiede zwischen ASA r2 Systemen und FAS, AFF und ASA Systemen, die für die ONTAP Befehlszeilenschnittstelle (CLI) und REST API relevant sind, werden im Folgenden beschrieben.

Standardmäßige SVM-Erstellung mit Protokolldiensten

Neue Cluster enthalten automatisch eine Standard-Daten-SVM, bei der die SAN-Protokolle aktiviert sind. IP-Daten-LIFs unterstützen iSCSI- und NVMe/TCP-Protokolle und verwenden `default-data-blocks` standardmäßig die Servicerichtlinie.

Automatische Volume-Erstellung

Durch Erstellen einer Storage-Einheit (LUN oder Namespace) wird automatisch ein Volume aus der Storage-Verfügbarkeitszone erstellt. Dies führt zu einem vereinfachten und gemeinsamen Namespace. Durch Löschen einer Speichereinheit wird das zugeordnete Volume automatisch gelöscht.

Änderungen an Thin Provisioning und Thick Provisioning

Storage-Einheiten werden auf ASA r2-Storage-Systemen immer über Thin Provisioning bereitgestellt. Thick Provisioning wird nicht unterstützt.

Änderungen an der Datenkomprimierung

Temperaturempfindliche Storage-Effizienz wird auf ASA r2-Systemen nicht angewendet. Auf ASA r2-Systemen basiert die Komprimierung nicht auf *Hot*-Daten (auf die häufig zugegriffen wird) oder *Cold*-Daten (auf die selten zugegriffen wird). Die Komprimierung beginnt, ohne auf Daten zu warten, die kalt werden.

Finden Sie weitere Informationen

- Erfahren Sie mehr über "ONTAP Hardwaresysteme".
- Siehe vollständige Konfigurationsunterstützung und -Einschränkungen für ASA- und ASA r2-Systeme in "NetApp Hardware Universe".

- Erfahren Sie mehr über die "NetApp ASA".

Unterstützung und Einschränkungen der ONTAP Software für ASA r2 Storage-Systeme

ASA r2 Systeme bieten zwar eine breite Unterstützung für SAN-Lösungen, bestimmte ONTAP Softwarefunktionen werden jedoch nicht unterstützt.

ASA r2-Systeme unterstützen Folgendes nicht:

- Standardmäßiger automatischer iSCSI-LIF-Failover

  Bei ASA r2 Systemen wird die Standard-Netzwerk-LIF von NVMe- und SCSI-Hosts gemeinsam genutzt, unterstützt also kein automatisches Failover. Um den automatischen iSCSI LIF Failover zu aktivieren, müssen Sie "Erstellen Sie eine nur iSCSI logische Schnittstelle". Automatischer Failover ist standardmäßig auf nur iSCSI LIFS aktiviert.

  Wenn automatisches iSCSI-LIF-Failover aktiviert ist, wird die iSCSI-LIF im Falle eines Storage-Failovers automatisch von dem Home Node oder Port des Node bzw. Ports des Home Ports zu dem Node bzw. Port des HA-Partners migriert und nach Abschluss des Failover wieder aufgenommen. Wenn der Port für eine iSCSI-LIF nicht mehr funktionstüchtiges ist, wird die LIF automatisch zu einem ordnungsgemäßen Port im aktuellen Home Node und anschließend zurück zu seinem ursprünglichen Port migriert, sobald der Port wieder funktionsfähig ist.

- FabricPool
- Thick Provisioning für LUNs
- MetroCluster
- Objektprotokolle
- ONTAP S3 SnapMirror und S3-APIs
- SnapMirror (asynchron und synchron) zur Cloud
- SnapMirror (asynchron und synchron) auf Systeme mit nicht-ASA r2

ASA r2-Systeme unterstützen Folgendes:

- SnapLock

  "Erfahren Sie, wie Sie Snapshots sperren" Auf Ihrem ASA r2-System.

- Dual-Layer-Verschlüsselung

  "Erfahren Sie, wie Sie eine zweischichtige Verschlüsselung anwenden" Auf Daten auf Ihrem ASA r2-System.

Finden Sie weitere Informationen

- "NetApp Hardware Universe"Weitere Informationen zur Unterstützung und zu Einschränkungen der ASA r2-Hardware finden Sie im.

ONTAP CLI-Unterstützung für ASA r2 Storage-Systeme

Anstelle von Aggregaten verwendet die Speicherebene in ASA r2-Systemen Speicherverfügbarkeitszonen. Eine Speicherverfügbarkeitszone ist ein gemeinsamer

Speicherpool, der einem einzelnen HA-Paar zur Verfügung steht. Beide Knoten im HA-Paar haben Zugriff auf alle verfügbaren Festplatten in ihrer gemeinsamen Speicherverfügbarkeitszone. Beim Erstellen einer Speichereinheit (LUN oder NVMe-Namespace) erstellt ONTAP automatisch ein Volume in der entsprechenden Speicherverfügbarkeitszone, um die Speichereinheit aufzunehmen.

Aufgrund dieses vereinfachten Ansatzes zur Speicherverwaltung `storage aggregate` Befehle werden auf ASA r2-Systemen nicht unterstützt. Unterstützung für bestimmte `lun` , `storage` Und `volume` Befehle und Parameter sind ebenfalls begrenzt.

Die folgenden Befehle und Befehlssets werden auf ASA unter r2 nicht unterstützt:

Nicht unterstützte <code>-</code>-Befehle

- `lun copy`
- `lun geometry`
- `lun maxsize`
- `lun move`
- `lun move-in-volume`

  Der `lun move-in-volume` Befehl wird ersetzt durch den `lun rename` und die `vserver nvme namespace rename` Befehle.

- `lun transition`

Nicht unterstützte <code>-</code>-Befehle

- `storage failover show-takeover`
- `storage failover show-giveback`
- `storage aggregate relocation`
- `storage disk assign`
- `storage disk partition`
- `storage disk reassign`

Nicht unterstützte <code>-</code>-Befehlssätze

- `volume activity-tracking`
- `volume analytics`
- `volume conversion`
- `volume file`
- `volume flexcache`
- `volume flexgroup`
- `volume inode-upgrade`
- `volume object-store`
- `volume qtree`
- `volume quota`
- `volume reallocation`
- `volume rebalance`
- `volume recovery-queue`
- `volume schedule-style`

Nicht unterstützte <code>-</code>-Befehle und -Parameter

- `volume autosize`
- `volume create`
- `volume delete`
- `volume expand`
- `volume modify`

  Der `volume modify` Der Befehl ist nicht verfügbar, wenn er in Verbindung mit den folgenden Parametern verwendet wird:

  - `-anti-ransomware-state`
  - `-autosize`
  - `-autosize-mode`
  - `-autosize-shrik-threshold-percent`
  - `-autosize-reset`
  - `-group`
  - `-is-cloud-write-enabled`
  - `-is-space-enforcement-logical`
  - `-max-autosize`
  - `-min-autosize`
  - `-offline`
  - `-online`
  - `-percent-snapshot-space`
  - `-qos*`
  - `-size`
  - `-snapshot-policy`
  - `-space-guarantee`
  - `-space-mgmt-try-first`
  - `-state`
  - `-tiering-policy`
  - `-tiering-minimum-cooling-days`
  - `-user`
  - `-unix-permisions`
  - `-vserver-dr-protection`
- `volume make-vsroot`

- `volume mount`
- `volume move`
- `volume offline`
- `volume rehost`
- `volume rename`
- `volume restrict`
- `volume transition-prepare-to-downgrade`
- `volume unmount`

Nicht unterstützte <code>-Befehle für die Clitzebaus-</code>

- `volume clone create`
- `volume clone split`

Nicht unterstützte <code>-SnapLock </code>-Befehle

- `volume snaplock modify`

Nicht unterstützte <code>-Befehle für den </code>-Ausschnapper

- `volume snapshot`
- `volume snapshot autodelete modify`
- `volume snapshot policy modify`

Finden Sie weitere Informationen

"ONTAP-Befehlsreferenz"Eine vollständige Liste der unterstützten Befehle finden Sie im

Richten Sie einen ONTAP ASA r2-Cluster mithilfe der CLI ein

Es wird empfohlen, dass Sie "Richten Sie den ONTAP ASA r2-Cluster mit System Manager ein". System Manager bietet einen schnellen und einfachen geleiteten Workflow zur Inbetriebnahme des Clusters. Wenn Sie jedoch bisher mit ONTAP-Befehlen arbeiten, kann die ONTAP-Befehlszeilenschnittstelle (CLI) optional für das Cluster-Setup verwendet werden. Die Cluster-Einrichtung über die CLI bietet keine weiteren Optionen oder Vorteile als die Einrichtung von Clustern mit System Manager.

Während der Cluster-Einrichtung wird Ihre standardmäßige Storage Virtual Machine (VM) erstellt, eine erste Storage-Einheit erstellt und Ihre Daten-LIFs werden automatisch erkannt. Optional können Sie das Domain Name System (DNS) aktivieren, um Hostnamen aufzulösen, Ihr Cluster so einstellen, dass es das Network Time Protocol (NTS) für die Zeitsynchronisierung verwendet und die Verschlüsselung von Daten im Ruhezustand aktiviert.

Bevor Sie beginnen

Stellen Sie die folgenden Informationen zusammen:

- Cluster-Management-IP-Adresse

  Die Cluster-Management-IP-Adresse ist eine eindeutige IPv4-Adresse für die Cluster-Managementoberfläche, die vom Cluster-Administrator für den Zugriff auf die Admin-Storage-VM und das Management des Clusters verwendet wird. Sie können diese IP-Adresse vom Administrator beziehen, der für das Zuweisen von IP-Adressen in Ihrem Unternehmen verantwortlich ist.

- Netzwerk-Subnetzmaske

  Während der Cluster-Einrichtung empfiehlt ONTAP eine Reihe von Netzwerkschnittstellen, die für die jeweilige Konfiguration geeignet sind. Sie können die Empfehlung bei Bedarf anpassen.

- IP-Adresse des Netzwerk-Gateways
- Partner-Node-IP-Adresse
- DNS-Domain-Namen
- IP-Adressen des DNS-Namensservers
- IP-Adressen des NTP-Servers
- Daten-Subnetzmaske

Schritte

1. Schalten Sie beide Nodes des HA-Paars ein.
2. Zeigt die im lokalen Netzwerk erkannten Nodes an:

   ```
   system node show-discovered -is-in-cluster false
   ```

3. Starten Sie den Cluster-Einrichtungsassistenten:

   ```
   cluster setup
   ```

4. Bestätigen Sie die AutoSupport-Anweisung.
5. Geben Sie Werte für den Port der Node-Managementoberfläche, die IP-Adresse, die Netmask und das Standard-Gateway ein.
6. Drücken Sie **Enter**, um die Einrichtung über die Befehlszeilenschnittstelle fortzusetzen; geben Sie dann **create** ein, um einen neuen Cluster zu erstellen.
7. Übernehmen Sie die Systemstandards oder geben Sie Ihre eigenen Werte ein.
8. Nachdem das Setup auf dem ersten Node abgeschlossen ist, melden Sie sich beim Cluster an.
9. Vergewissern Sie sich, dass das Cluster aktiv ist und der erste Node ordnungsgemäß funktioniert:

   ```
   system node show-discovered
   ```

10. Fügen Sie dem Cluster den zweiten Node hinzu:

```
cluster add-node -cluster-ip <partner_node_ip_address>
```

11. Optional können Sie die Systemzeit über das Cluster hinweg synchronisieren

Synchronisierung ohne symmetrische Authentifizierung	`cluster time-service ntp server create -server <server_name>`
Synchronisierung mit symmetrischer Authentifizierung	`cluster time-service ntp server create -server <server_ip_address> -key-id <key_id>`

a. Vergewissern Sie sich, dass das Cluster einem NTP-Server zugeordnet ist:

```
Cluster time-service ntp show
```

12. Optional können "Active IQ Config Advisor"Sie die Konfiguration herunterladen und ausführen.

Was kommt als Nächstes?

Sie können "Richten Sie den Datenzugriff ein"Ihre SAN-Clients auf Ihr System übertragen.

REST-API-Unterstützung für ASA r2

Die REST-API von ASA r2 basiert auf der REST-API, die mit der einheitlichen ONTAP-Persönlichkeit ausgestattet ist. Eine Reihe von Änderungen wird an die einzigartigen Merkmale und Funktionen der ASA r2-Persönlichkeit angepasst.

Typen von API-Änderungen

Es gibt verschiedene Arten von Unterschieden zwischen der REST API für ASA r2 Systeme und der einheitlichen ONTAP REST API für FAS, AFF und ASA Systeme. Wenn Sie die Arten von Änderungen verstehen, können Sie die Online-API-Referenzdokumentation besser nutzen.

Neue ASA r2 Endpunkte werden in Unified ONTAP nicht unterstützt

Die REST-API von ASA r2 wurde um mehrere Endpunkte erweitert, die mit Unified ONTAP nicht verfügbar sind.

Beispielsweise wurde der REST-API für ASA r2 Systeme ein neuer Block-Volume-Endpunkt hinzugefügt. Der Block-Volume-Endpunkt ermöglicht den Zugriff auf LUN- und NVMe Namespace-Objekte und eine aggregierte Ansicht der Ressourcen. Diese Funktion ist nur über die REST-API verfügbar.

Ein weiteres Beispiel: Die Endpunkte **Storage-units** bieten eine aggregierte Ansicht der LUNs und NVMe-Namespaces. Es gibt mehrere Endpunkte, die alle auf Basis oder abgeleitet von basieren

`/api/storage/storage-units`. Sie sollten auch überprüfen `/api/storage/luns` und `/api/storage/namespaces`.

Einschränkungen der HTTP-Methoden, die für einige Endpunkte verwendet werden

Mehrere mit ASA r2 verfügbare Endpunkte haben im Vergleich zu Unified ONTAP Einschränkungen, welche HTTP-Methoden verwendet werden können. Beispielsweise sind POST und DELETE nicht zulässig, wenn der Endpunkt `/api/protocols/nvme/services` mit ASA r2-Systemen verwendet wird.

Eigenschaftsänderungen für einen Endpunkt und eine HTTP-Methode

Einige ASA r2-Systemendpunkt- und Methodenkombinationen unterstützen nicht alle definierten Eigenschaften, die in der einheitlichen ONTAP-Persönlichkeit verfügbar sind. Wenn Sie beispielsweise PATCH mit dem Endpunkt verwenden `/api/storage/volumes/{uuid}`, werden mehrere Eigenschaften von ASA r2 nicht unterstützt, darunter:

- `autosize.maximum`
- `autosize.minimum`
- `autosize.mode`

Änderungen an der internen Verarbeitung

Es gibt mehrere Änderungen, wie ASA r2 bestimmte REST-API-Anforderungen verarbeitet. So `/api/storage/luns/{uuid}` wird beispielsweise eine LÖSCHANFORDERUNG mit dem Endpunkt asynchron verarbeitet.

Erhöhte Sicherheit mit OAuth 2.0

OAuth 2.0 ist das Standard-Autorisierungsframework der Branche. Er wird verwendet, um den Zugriff auf geschützte Ressourcen basierend auf signierten Zugriffstoken zu beschränken und zu steuern. Sie können OAuth 2.0 mit System Manager konfigurieren, um ASA r2-Systemressourcen zu schützen.

Nachdem OAuth 2.0 mit System Manager eingerichtet wurde, kann der Zugriff durch die REST-API-Clients gesteuert werden. Sie müssen zuerst ein Zugriffstoken von einem Autorisierungsserver beziehen. Der REST-Client leitet das Token dann als Inhabertoken über den Header der HTTP-Autorisierungsanforderung an das ASA r2-Cluster weiter. Weitere Informationen finden Sie unter "Authentifizierung und Autorisierung mit OAuth 2.0" .

Greifen Sie über die Swagger-Benutzeroberfläche auf die Referenzdokumentation zur ASA r2-API zu

Sie können über die Swagger-Benutzeroberfläche Ihres ASA r2-Systems auf die REST-API-Referenzdokumentation zugreifen.

Über diese Aufgabe

Details zur REST-API finden Sie auf der Referenzdokumentationsseite von ASA r2. Als Teil davon können Sie nach dem String **Plattformspezifika** suchen, um Details über die ASA r2 Systemunterstützung für die API-Aufrufe und -Eigenschaften zu finden.

Bevor Sie beginnen

Sie müssen Folgendes haben:

- Die IP-Adresse oder der Hostname der Cluster-Management-LIF des ASA r2-Systems
- Benutzername und Passwort für ein Konto, das über eine Berechtigung für den Zugriff auf die REST-API verfügt

Schritte

1. Geben Sie die URL in Ihren Browser ein und drücken Sie **Enter**:
   `https://<ip_address>/docs/api`
2. Melden Sie sich mit Ihrem Administratorkonto an.

   Die Dokumentationsseite der ASA r2-API wird angezeigt, wobei die API-Aufrufe in den wichtigsten Ressourcenkategorien organisiert sind.

3. Um ein Beispiel eines API-Aufrufs zu sehen, der nur für ASA r2-Systeme gilt, scrollen Sie nach unten in die Kategorie **SAN** und klicken Sie auf **GET /Storage/Storage-units**.

Allgemeine ONTAP -Funktionen, die auf ASA R2-Systemen unterstützt werden

Da auf ASA r2-Systemen eine optimierte Version von ONTAP ausgeführt wird, werden viele allgemeine ONTAP Aufgaben und System Manager-Funktionen auf ASA r2-Systemen auf die gleiche Weise ausgeführt wie auf anderen ONTAP Systemen.

Weitere Informationen zu allgemeinen Features und Funktionen finden Sie in der folgenden ONTAP Dokumentation.

ONTAP -Verwaltung

- "Erfahren Sie, wie Sie Informationen im ONTAP System Manager suchen, filtern und sortieren" .
- "Kombinieren Sie physische Ports, um Schnittstellengruppen zu erstellen" .
- "Erfahren Sie mehr über die Bereitstellung von NVMe over Fabrics (NVMe-oF)." .

Datensicherheit

- "Erfahren Sie mehr über die OAuth 2.0-Authentifizierung" .
- "Erfahren Sie mehr über Clientauthentifizierung und -autorisierung" .
- "Erfahren Sie, wie Sie die SAML-Authentifizierung konfigurieren" .
- "Verwalten des ONTAP Administratorzugriffs" .

Datensicherung

- "Konfigurieren Sie geclusterte externe Schlüsselserver in ONTAP" .
- "Externe Schlüsselverwaltung aktivieren (HW-basiert)" .
- "Externe Schlüsselverwaltung (NVE) aktivieren" .

Holen Sie sich Hilfe

Managen Sie AutoSupport auf ASA r2 Storage-Systemen

AutoSupport ist ein Mechanismus, der proaktiv den Zustand Ihres Systems überwacht und automatisch Meldungen an den technischen Support von NetApp, Ihre interne Support-Abteilung und einen Support-Partner sendet.

AutoSupport Meldungen für den technischen Support sind standardmäßig aktiviert, wenn Sie das Cluster einrichten. Sie müssen die richtigen Optionen festlegen und einen gültigen Mail-Host haben, um Nachrichten an Ihre interne Support-Organisation senden zu lassen. ONTAP beginnt 24 Stunden nach der Aktivierung mit dem Senden von AutoSupport Nachrichten.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um AutoSupport zu verwalten.

Testen Sie die AutoSupport Verbindung

Nachdem Sie das Cluster eingerichtet haben, sollten Sie die AutoSupport-Konnektivität testen, um sicherzustellen, dass der technische Support von AutoSupport generierte Meldungen erhält.

Schritte

1. Wählen Sie im System Manager **Cluster >Settings** aus.
2. Wählen Sie neben **AutoSupport** ⋮; dann **Verbindung testen**.
3. Geben Sie einen Betreff für die AutoSupport-Nachricht ein, und wählen Sie dann **Test-AutoSupport-Nachricht senden**.

Was kommt als Nächstes?

Sie haben bestätigt, dass der technische Support AutoSupport-Nachrichten von Ihrem ASA r2-System erhalten kann, um sicherzustellen, dass diese über die erforderlichen Daten verfügen, um Ihnen bei Problemen behilflich zu sein.

AutoSupport-Empfänger hinzufügen

Fügen Sie Mitglieder Ihrer internen Supportorganisation der Liste der E-Mail-Adressen hinzu, die AutoSupport-Nachrichten empfangen.

Schritte

1. Wählen Sie im System Manager **Cluster >Settings** aus.
2. Wählen Sie neben **AutoSupport** ⋮; und wählen Sie dann **Weitere Optionen**.
3. Wählen Sie neben **Email** ✎; und dann + Add .
4. Geben Sie die E-Mail-Adresse des Empfängers ein, dann die Empfängerkategorie.

   Wählen Sie für Partner **Partner** für die Empfängerkategorie aus. Wählen Sie **Allgemein** für Mitglieder Ihrer internen Support-Organisation.

5. Wählen Sie Speichern.

Was kommt als Nächstes?

Die von Ihnen hinzugefügten E-Mail-Adressen erhalten neue AutoSupport Nachrichten für die jeweilige Empfängerkategorie.

AutoSupport-Daten senden

Sollte auf Ihrem ASA r2-System ein Problem auftreten, können AutoSupport-Daten die Zeit zur Erkennung und Behebung von Problemen erheblich verkürzen.

Schritte

1. Wählen Sie im System Manager **Cluster >Settings** aus.
2. Wählen Sie neben **AutoSupport** ⋮; dann **Generieren und senden**.
3. Geben Sie einen Betreff für die AutoSupport-Nachricht ein, und wählen Sie dann **Senden**.

Was kommt als Nächstes?

Ihre AutoSupport-Daten werden an den technischen Support gesendet.

Unterdrücken Sie die Generierung von Support-Cases

Wenn Sie ein Upgrade oder eine Wartung auf Ihrem ASA r2-System durchführen, sollten Sie die AutoSupport-Generierung von Support-Fällen bis zum Abschluss des Upgrades oder der Wartung unterdrücken.

Schritte

1. Wählen Sie im System Manager **Cluster >Settings** aus.
2. Wählen Sie neben **AutoSupport** ⋮; dann **Support Case Generierung unterdrücken**.
3. Geben Sie die Anzahl der Stunden an, die die Generierung von Support-Fällen unterdrücken sollen, und wählen Sie dann die Nodes aus, für die keine Cases generiert werden sollen.
4. Wählen Sie **Senden**.

Was kommt als Nächstes?

AutoSupport-Fälle werden nicht während der von Ihnen angegebenen Zeit generiert. Wenn Sie das Upgrade oder die Wartung vor Ablauf der angegebenen Zeit abgeschlossen haben, sollten Sie die Generierung des Support-Cases sofort fortsetzen.

Setzen Sie die Generierung von Support-Cases fort

Wenn Sie die Generierung von Support-Cases während eines Upgrade- oder Wartungsfensters unterdrückt haben, sollten Sie die Erstellung von Support-Cases sofort nach Abschluss des Upgrades oder der Wartung fortsetzen.

Schritte

1. Wählen Sie im System Manager **Cluster >Settings** aus.
2. Wählen Sie neben **AutoSupport** ⋮; dann **Support Case Generation fortsetzen**.
3. Wählen Sie die Knoten aus, für die Sie die erstellten AutoSupport-Fälle fortsetzen möchten.
4. Wählen Sie **Senden**.

Ergebnis

AutoSupport-Cases werden bei Bedarf automatisch für Ihr ASA r2-System generiert.

Support-Cases für ASA r2-Speichersysteme übermitteln und anzeigen

Wenn bei einem Problem Unterstützung erforderlich ist, können Sie den ONTAP System Manager verwenden, um einen Case an den technischen Support zu übermitteln. Sie können ONTAP System Manager auch verwenden, um abgeschlossene oder laufende Fälle anzuzeigen.

Sie müssen "Bei Active IQ registriert"Support-Fälle für Ihr ASA r2-System anzeigen.

Schritte

1. Um einen Support-Fall zu senden, wählen Sie im System-Manager **Cluster >Support** aus, und wählen Sie dann **Gehe zu NetApp-Unterstützung** aus.
2. Um einen zuvor gesendeten Fall anzuzeigen, wählen Sie im System Manager **Cluster >Support** aus, und wählen Sie dann **Meine Fälle anzeigen** aus.

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

ONTAP

"Hinweis für ONTAP 9.16.1"