



# ASA r2 Dokumentation

## ASA r2

NetApp  
September 26, 2024

# Inhalt

ASA r2 Dokumentation	1
Versionshinweise	2
Neuerungen in ONTAP 9.16.0 für ASA r2-Systeme	2
Los geht's	3
Erfahren Sie mehr über ASA r2 Storage-Systeme	3
Schnellstart für ASA r2-Speichersysteme	3
Installieren Sie Ihr ASA r2-System	4
Richten Sie Ihr ASA r2-System ein	27
Nutzen Sie ONTAP für das Datenmanagement	31
ASA r2 Storage-System – Video-Demos	31
Managen Sie Ihren Storage	31
Sichern Sie Ihre Daten	41
Datensicherung	57
Administration und Überwachung	61
Management des Client-Zugriffs auf Storage-VMs auf ASA r2 Storage-Systemen	61
Managen Sie Cluster-Netzwerke auf ASA r2 Storage-Systemen	63
Überwachung der Nutzung und Erhöhung der Kapazität	65
Aktualisieren der Firmware auf ASA r2-Speichersystemen	68
ASA r2 Storage-System bietet Einblick in Cluster-Sicherheit und -Performance	70
Anzeigen von Clusterereignissen und -Jobs auf ASA r2-Speichersystemen	71
Managen von Nodes	72
Managen von Benutzerkonten und Rollen auf ASA r2 Storage-Systemen	73
Managen von Sicherheitszertifikaten auf ASA r2-Speichersystemen	75
Überprüfen Sie die Hostkonnektivität auf Ihrem ASA r2-Speichersystem	77
Wartung Ihres ASA r2 Storage-Systems	79
Weitere Informationen	80
ASA r2 für ONTAP Power User	80
Holen Sie sich Hilfe	91
Managen Sie AutoSupport auf ASA r2 Storage-Systemen	91
Support-Cases für ASA r2-Speichersysteme übermitteln und anzeigen	93
Rechtliche Hinweise	94
Urheberrecht	94
Marken	94
Patente	94
Datenschutzrichtlinie	94
Open Source	94

# ASA r2 Dokumentation

# Versionshinweise

## 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
Neuen Plattformen entwickelt	<p>Die folgenden neuen 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.</p> <ul style="list-style-type: none"><li>• ASAA1K</li><li>• ASAA70</li><li>• ASAA90</li></ul>

### System Manager

Aktualisieren	Beschreibung
"Optimierter Support für reine SAN-Kunden"	<p>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.</p>

### Storage-Management

Aktualisieren	Beschreibung
"Vereinfachtes Storage-Management"	<p>ASA r2-Systeme führen Storage-Einheiten mit Konsistenzgruppen ein, was das Storage-Management vereinfacht.</p> <ul style="list-style-type: none"><li>• Eine <i>Storage unit</i> 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.</li><li>• <i>Eine Consistency Group</i> ist eine Sammlung von Speichereinheiten, die als eine Einheit verwaltet werden.</li></ul>

### Datensicherheit

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

# Los geht's

## Erfahren Sie mehr über ASA r2 Storage-Systeme

Die neuen NetApp ASA r2 Systeme (ASA A1K, ASA A70 und ASA A90) bieten eine einheitliche Hardware- und Softwarelösung, mit der die Benutzerfreundlichkeit speziell auf die Anforderungen reiner SAN-Kunden abgestimmt wird.

ASA r2 Systeme unterstützen alle SAN-Protokolle (iSCSI, FC, NVMe/FC, NVMe/TCP) in einer einzigen HA-Paar-Implementierung. SCSI-Protokolle (iSCSI und FC) verwenden für Multipathing eine symmetrische aktiv/aktiv-Architektur, sodass alle Pfade zwischen Hosts und Storage aktiv/optimiert sind. NVMe-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 Storage-Einheiten und Konsistenzgruppen, um das Storage-Management und die Datensicherung zu vereinfachen. Angenommen, Sie haben eine Datenbank, die aus 10 Speichereinheiten in einer Konsistenzgruppe besteht, und Sie müssen die gesamte Datenbank sichern. Anstatt jede Storage-Einheit einzeln zu sichern, können Sie die gesamte Datenbank schützen, indem Sie die Konsistenzgruppe sichern.

ASA r2 Systeme unterstützen einen integrierten Schlüsselmanager, eine zweischichtige Verschlüsselung, manipulationssichere Snapshots, Multi-Faktor-Authentifizierung und die Verifizierung durch mehrere Administratoren, um Daten vor schädlichen Angriffen wie Diebstahl oder Ransomware zu schützen.

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 ["Die neuen ASA r2 Systeme 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 weiter zu implementieren und es als HA-Paar in Ihrer ONTAP Umgebung zu implementieren.

**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 Shelves 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-Shelves.

**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-Shelves.

### 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 der NS224-Einschubnummern
- Kreuzschlitzschraubendreher #2

### Vorsichtsmaßnahmen beim Anheben

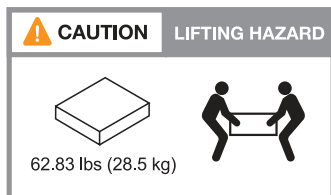
ASA r2 Storage-Systeme und NS224 Storage-Shelves sind schwer. Gehen Sie beim Anheben und Bewegen dieser Gegenstände vorsichtig vor.

### Gewichte des Storage-Systems

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

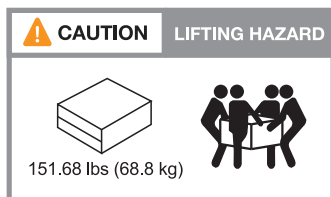
## ASA A1K

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



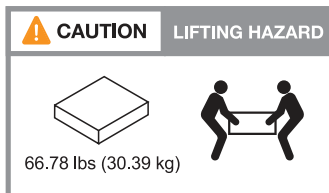
## ASA A70 und ASA A90

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



## Gewicht des Lagerregals

Ein NS224-Einlegeboden kann bis zu 30.29 kg (66.78 lbs) wiegen. Zum Anheben des Lagerregals zwei Personen oder einen Hydraulikhub verwenden. Halten Sie alle Komponenten im Lagerregal (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. Verwenden Sie ["NetApp Hardware Universe"](#), um zu überprüfen, ob Ihr Standort die Umgebungs- und Stromanforderungen für Ihr ASA r2 Storage-System erfüllt.
2. Stellen Sie sicher, dass ausreichend Platz im Rack vorhanden ist:
  - 4 HE in einer HA-Konfiguration für das Storage-System
  - 2 HE für jedes NS224 Storage-Shelf
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.



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.

Stellen Sie sicher, dass alle in den Kartons auf die Liste auf dem Packzettel passen. Wenn Abweichungen auftreten, notieren Sie sie für weitere Maßnahmen.

Hardware	* Kabel*	
<ul style="list-style-type: none"><li>• Blende</li><li>• Kabelverwaltungs-Gerät</li><li>• Storage-System</li><li>• Schienensätze mit Anweisungen (optional)</li><li>• Storage Shelf</li></ul>	<ul style="list-style-type: none"><li>• Management-Ethernet-Kabel (RJ-45-Kabel)</li><li>• Netzkabel</li><li>• Stromkabel</li><li>• Speicherkabel (wenn Sie zusätzlichen Speicher bestellt haben)</li><li>• Serielles USB-C-Anschlusskabel</li></ul>	

## 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 der Seriennummer Ihres Storage-Systems.

Sie finden die Nummer auf dem Packzettel, in Ihrer Bestätigungs-E-Mail oder nach dem Auspacken auf dem System Management-Modul des 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	<ol style="list-style-type: none"><li>Melden Sie sich mit Ihrem Benutzernamen und Passwort an.</li><li>Wählen Sie <b>Systeme &gt; Eigene Systeme</b>.</li><li>Bestätigen Sie, dass die neue Seriennummer aufgeführt ist.</li><li>Falls nicht, folgen Sie den Anweisungen für neue NetApp Kunden.</li></ol>
Neuer NetApp Kunde	<ol style="list-style-type: none"><li>Klicken Sie auf <b>Jetzt registrieren</b> und erstellen Sie ein Konto.</li><li>Wählen Sie <b>Systeme &gt; Systeme Registrieren</b>.</li><li>Geben Sie die Seriennummer des Storage-Systems und die angeforderten Details ein.</li></ol> <p>Nach der Registrierung können Sie die erforderliche Software herunterladen. Der Genehmigungsprozess kann bis zu 24 Stunden in Anspruch nehmen.</p>

### 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.

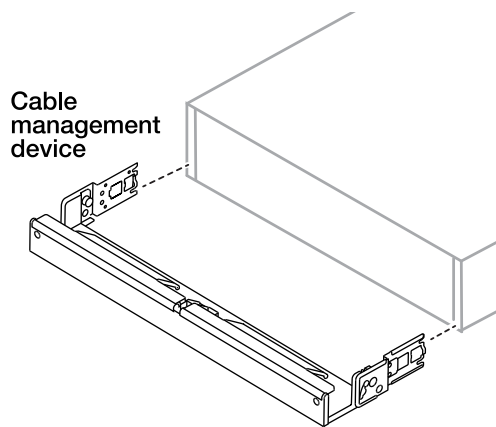
### Schritte

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 Schrankes oder des Telco-Racks, und stützen Sie das Speichersystem von unten ab, und schieben Sie es hinein.
  - b. Befestigen Sie das Speichersystem mit den mitgelieferten Befestigungsschrauben am Schrank oder Telco-Rack.
3. Montieren 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.
4. Schließen Sie die Kabelverwaltungsgeräte an der Rückseite des Speichersystems an.



5. Befestigen Sie die Blende an der Vorderseite des Speichersystems.

### Was kommt als Nächstes?

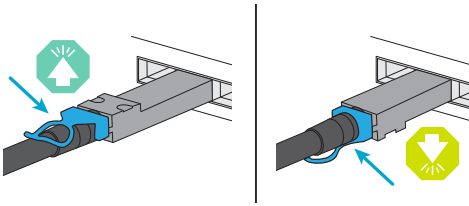
Nachdem Sie die Hardware für Ihr ASA r2-System installiert haben, können Sie ["Verkabeln Sie die Controller und Storage Shelves für Ihr ASA r2 System"](#).

## 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 Netzkabel für die Controller und verbinden Sie die Kabel zwischen den Controllern und Storage-Shelves.

### Bevor Sie beginnen

Prüfen Sie den Pfeil in der Abbildung in den Verkabelungsdiagrammen auf die richtige Ausrichtung der Zuglasche am Kabelanschluss.



- Wenn Sie den Anschluss einsetzen, sollten Sie spüren, dass er einrastet. Wenn Sie ihn nicht einrasten, entfernen Sie ihn, drehen Sie den Kabelkopf um und versuchen Sie es erneut.
- Wenn Sie eine Verbindung zu einem optischen Switch herstellen, stecken Sie den SFP-Transceiver (Small Form-Factor Pluggable) in den Controller-Port ein, bevor Sie den Port verkabeln.

### **Schritt 1: Verbinden Sie die Storage Controller mit Ihrem Netzwerk**

Verbinden Sie Ihre Controller direkt miteinander und mit Ihrem Host-Netzwerk.

#### **Bevor Sie beginnen**

Wenden Sie sich an Ihren Netzwerkadministrator, um Informationen zum Anschließen des Speichersystems an die Host-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](#)".

## ASA A1K

Verbinden Sie die Storage Controller miteinander, um die ONTAP-Cluster-Verbindungen zu erstellen, und verbinden Sie dann die Ethernet-Ports auf jedem Controller mit dem Host-Netzwerk.

### Schritte

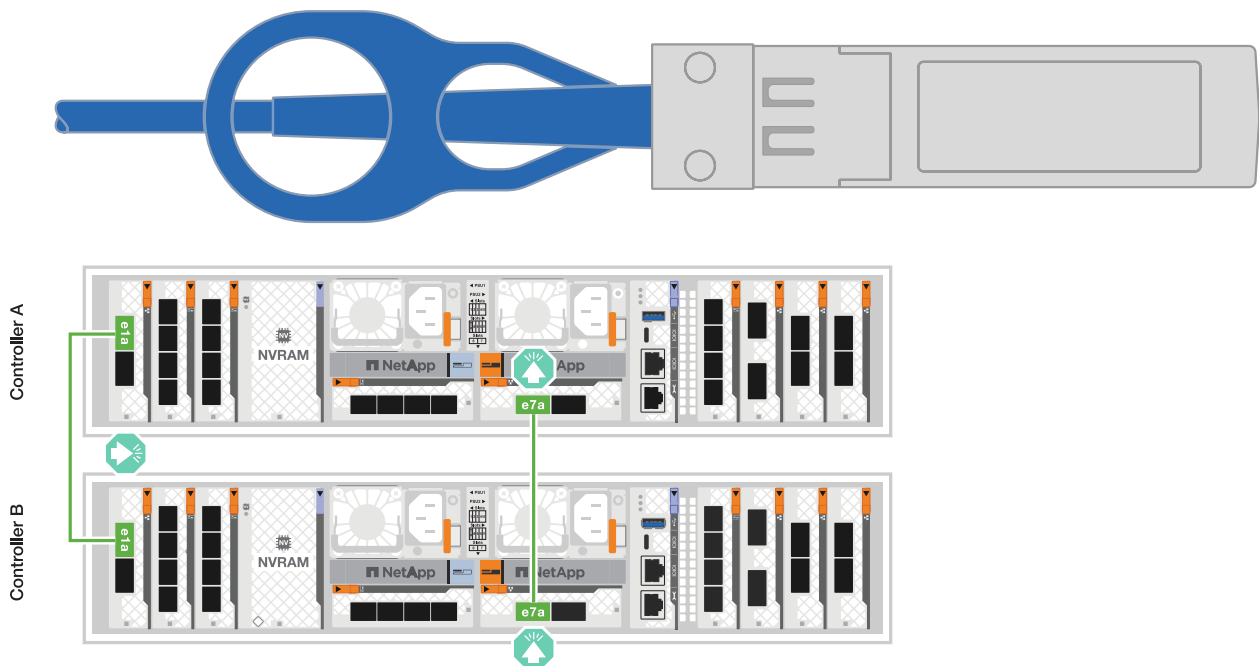
1. Verwenden Sie das Cluster/HA-Verbindungskabel, um die Ports e1a mit e1a und die Ports e7a mit e7a zu verbinden.



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

- a. Schließen Sie den Port e1a an Controller A an den Port E1A an Controller B. an
- b. Verbinden Sie Port e7a an Controller A mit Port E1A an Controller B.

### Cluster/HA Verbindungskabel



2. 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](#)".

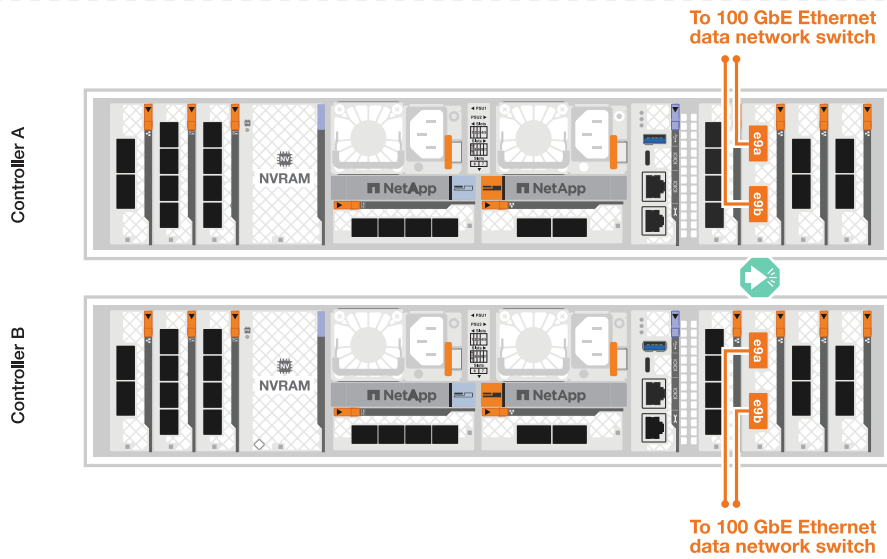
- a. Verbinden Sie die Ports e9a und e9b wie in der Abbildung dargestellt mit dem Ethernet-Datennetzwerk-Switch.



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.

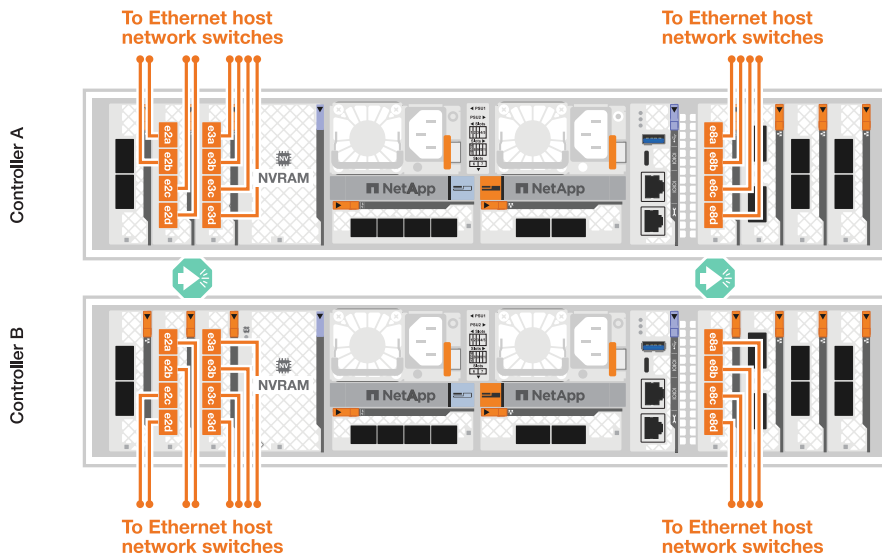
### 100-GbE-Kabel





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

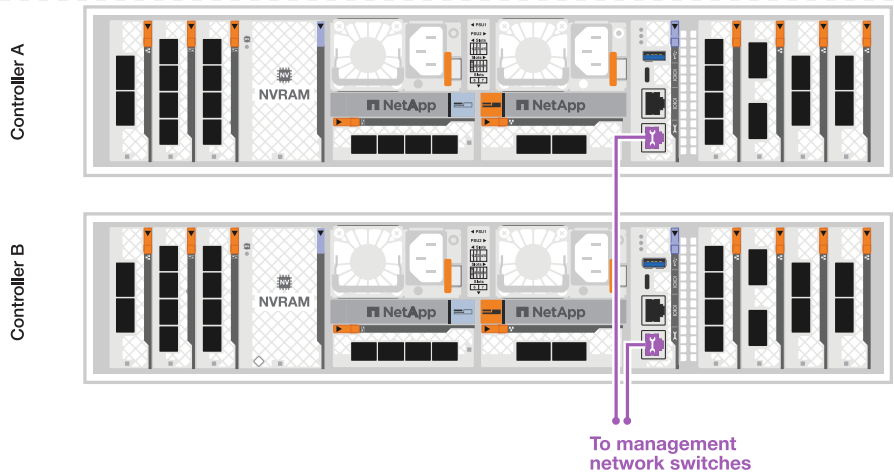
### 10/25 GbE Host



3. Verwenden Sie die 1000BASE-T RJ-45-Kabel, um die Controller-Management-Ports (Schraubenschlüssel) mit den Management-Netzwerk-Switches zu verbinden.



- 1000BASE-T RJ-45 KABEL \*



Stecken Sie die Netzkabel noch nicht ein.

### ASA A70 und ASA A90

Verbinden Sie die Storage Controller miteinander, um die ONTAP-Cluster-Verbindungen zu erstellen, und verbinden Sie dann die Ethernet-Ports auf jedem Controller mit dem Host-Netzwerk.

#### Schritte

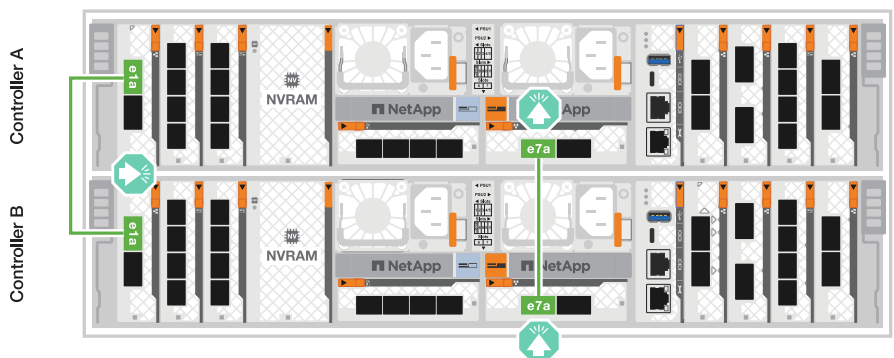
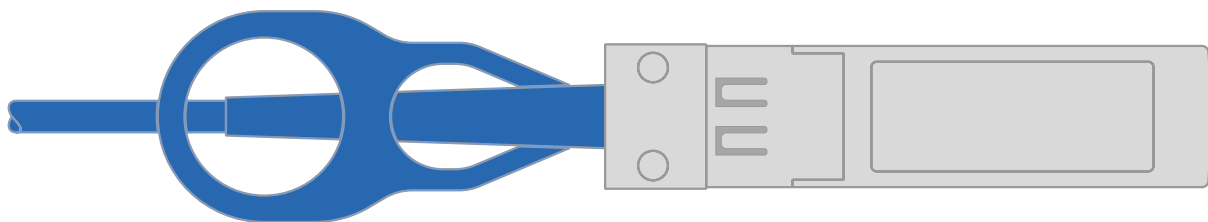
1. Verwenden Sie das Cluster/HA-Verbindungskabel, um die Ports e1a mit e1a und die Ports e7a mit e7a zu verbinden.



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

- a. Schließen Sie den Port e1a an Controller A an den Port E1A an Controller B. an
- b. Verbinden Sie Port e7a an Controller A mit Port E1A an Controller B.

#### Cluster/HA Verbindungskabel



## 2. Verbinden Sie die Ethernet-Modulports mit Ihrem Hostnetzwerk.

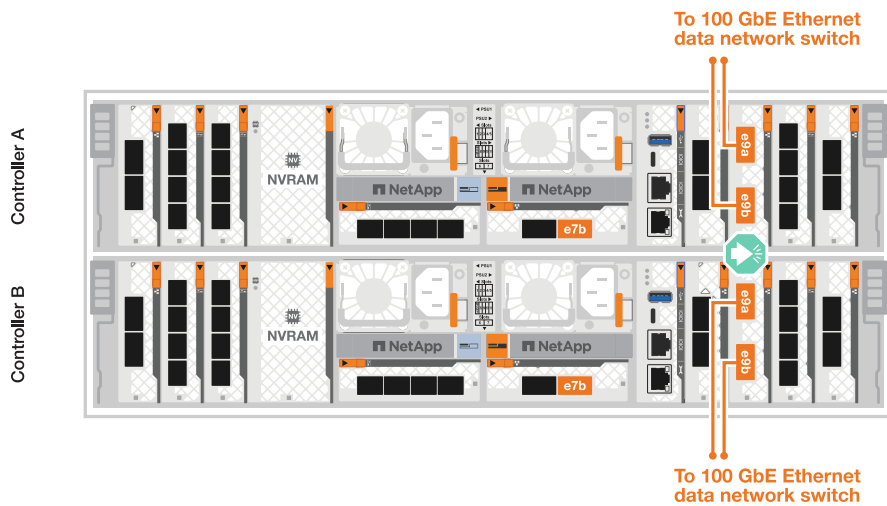
Im Folgenden finden Sie einige typische Beispiele für eine Verkabelung im Host-Netzwerk. Informationen zu Ihrer spezifischen Systemkonfiguration finden Sie unter "[NetApp Hardware Universe](#)".

- a. Verbinden Sie die Ports e9a und e9b wie in der Abbildung dargestellt mit dem Ethernet-Datennetzwerk-Switch.



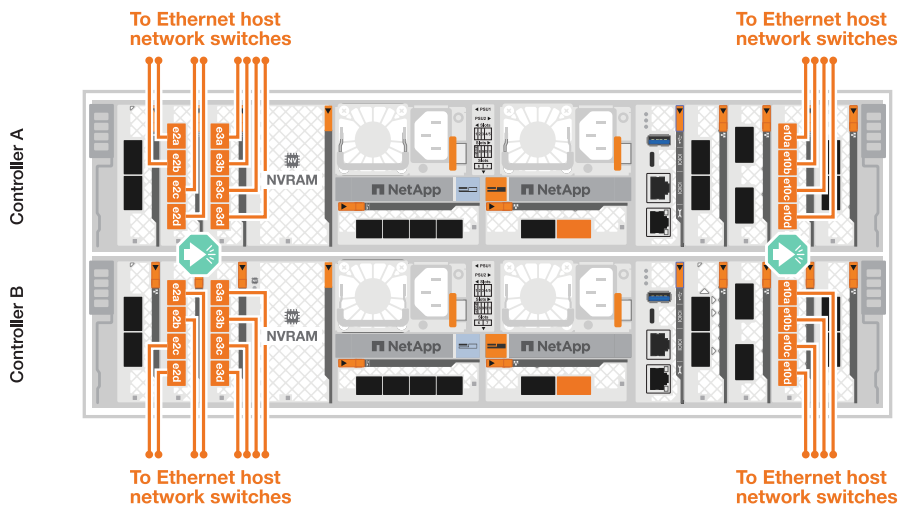
Verwenden Sie für maximale Systemperformance für Cluster- und HA-Datenverkehr die Ports e1b und e7b nicht für Host-Netzwerkverbindungen. Verwenden Sie eine separate Hostkarte, um die Leistung zu maximieren.

### 100-GbE-Kabel



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

### 4 Ports, 10/25 GbE Host

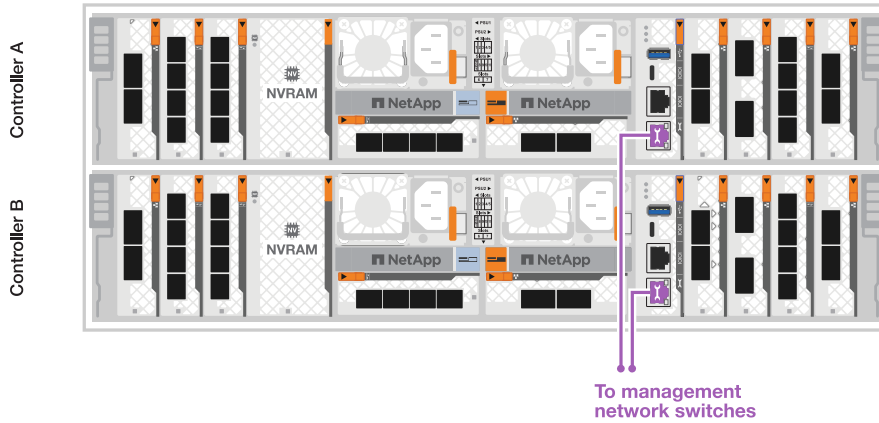




3. Verwenden Sie die 1000BASE-T RJ-45-Kabel, um die Controller-Management-Ports (Schraubenschlüssel) mit den Management-Netzwerk-Switches zu verbinden.



- 1000BASE-T RJ-45 KABEL \*



Stecken Sie die Netzkabel noch nicht ein.

## Schritt 2: Anschließen der Storage-Controller an die Storage-Shelfs

Die folgenden Verkabelungsverfahren zeigen, wie Sie Ihre Controller mit einem Shelf und zwei Shelfs verbinden. Sie können bis zu vier Shelfs direkt mit Ihren Controllern verbinden.

**ASA A1K**

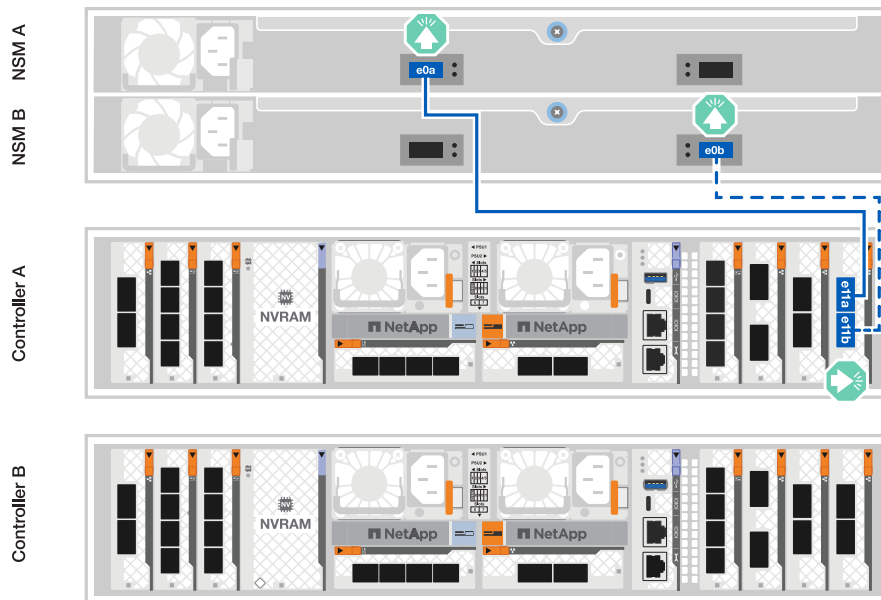
Wählen Sie eine der folgenden Verkabelungsoptionen, die Ihrem Setup entsprechen.

## Option 1: Verbinden der Controller mit einem NS224 Storage-Shelf

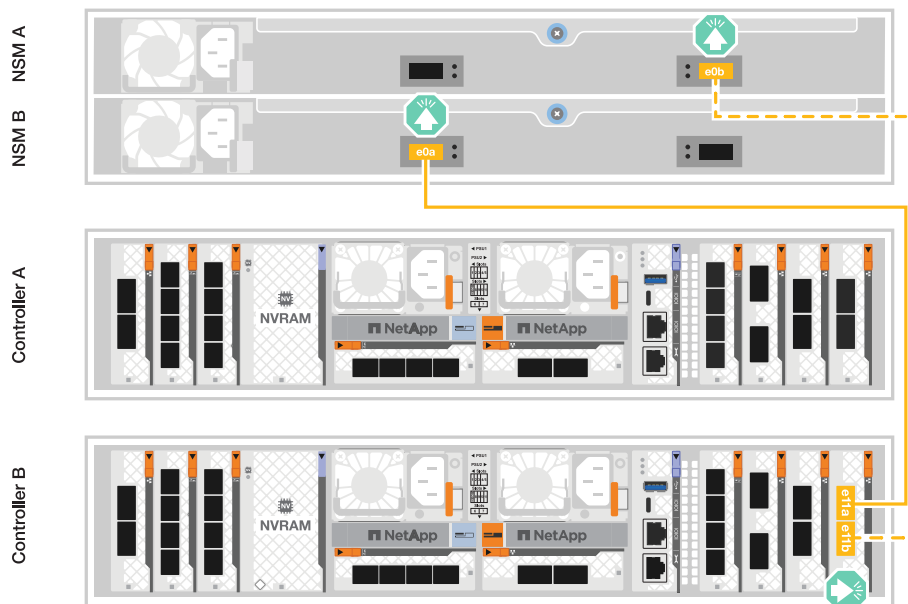
Verbinden Sie jeden Controller mit den NSM-Modulen im NS224-Shelf. Die Grafik zeigt die Verkabelung von den einzelnen Controllern: Die Verkabelung von Controller A wird blau und die Verkabelung von Controller B gelb dargestellt.

### 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.

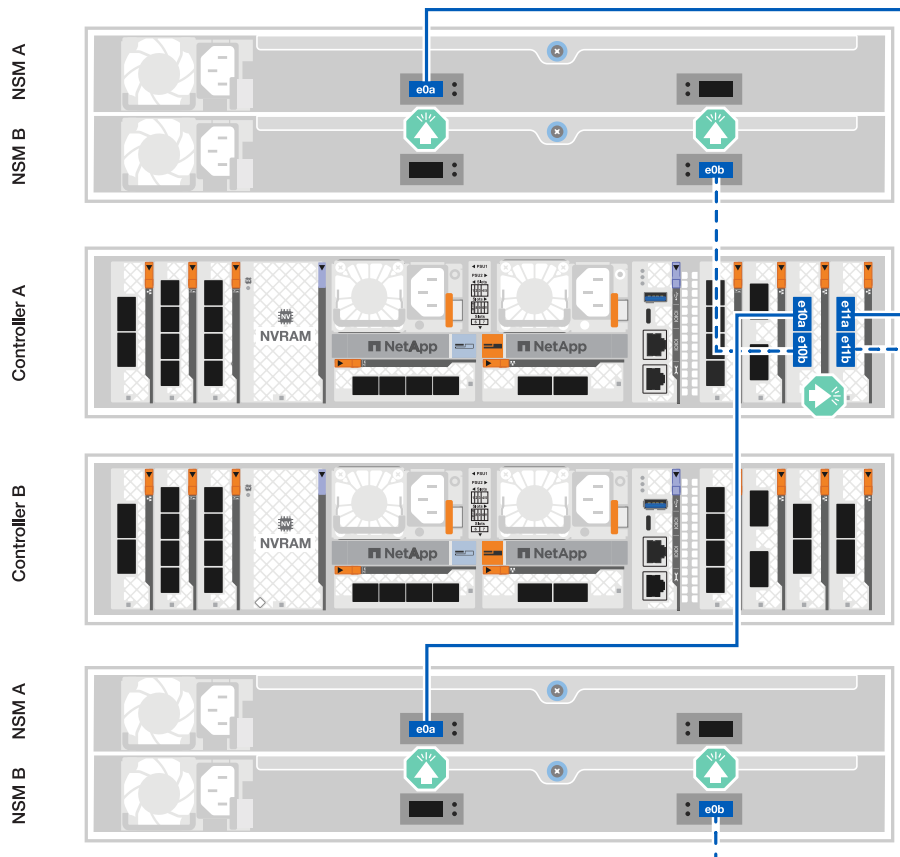


## Option 2: Verbinden der Controller mit zwei NS224 Storage-Shelfs

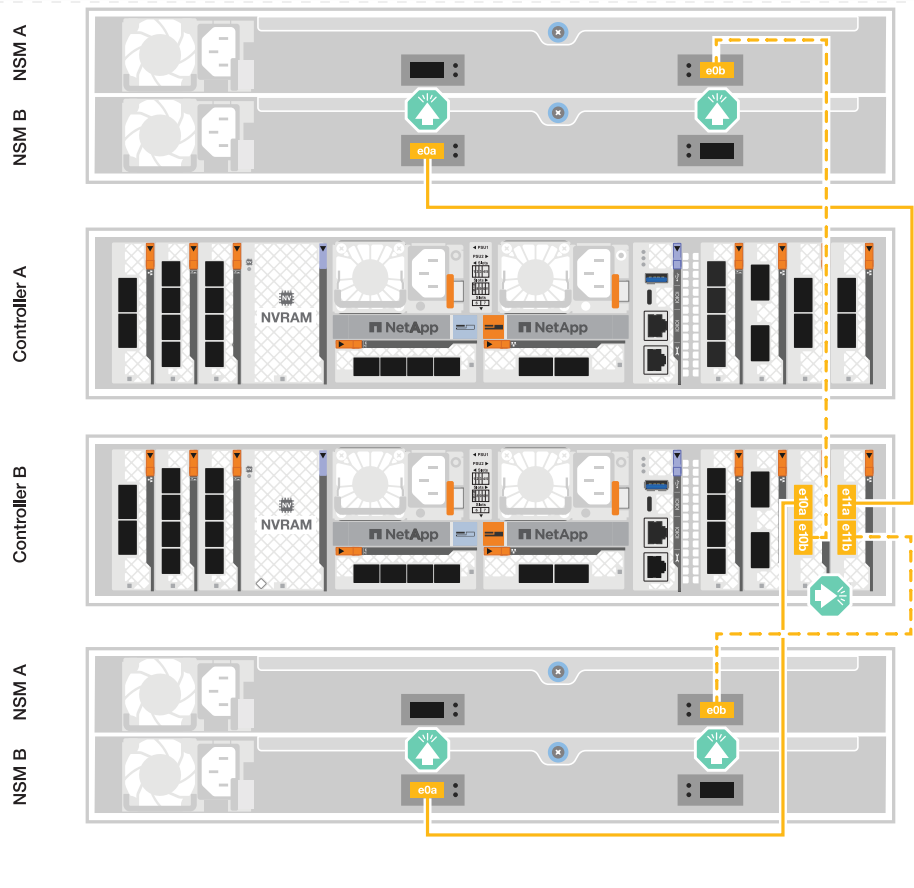
Verbinden Sie jeden Controller mit den NSM-Modulen beider NS224-Shelfs. Die Grafik zeigt die Verkabelung von den einzelnen Controllern: Die Verkabelung von Controller A wird blau und die Verkabelung von Controller B gelb dargestellt.

### 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.



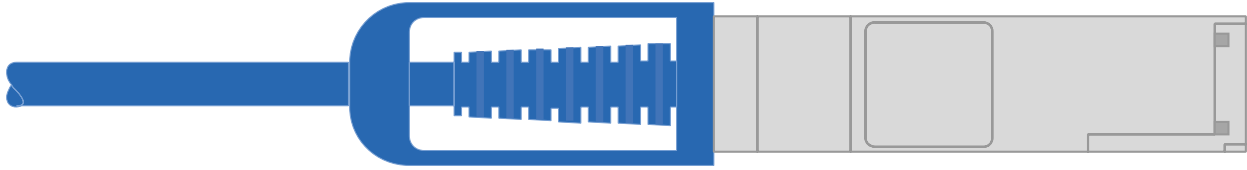
### ASA A70 und ASA A90

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

## Option 1: Verbinden der Controller mit einem NS224 Storage-Shelf

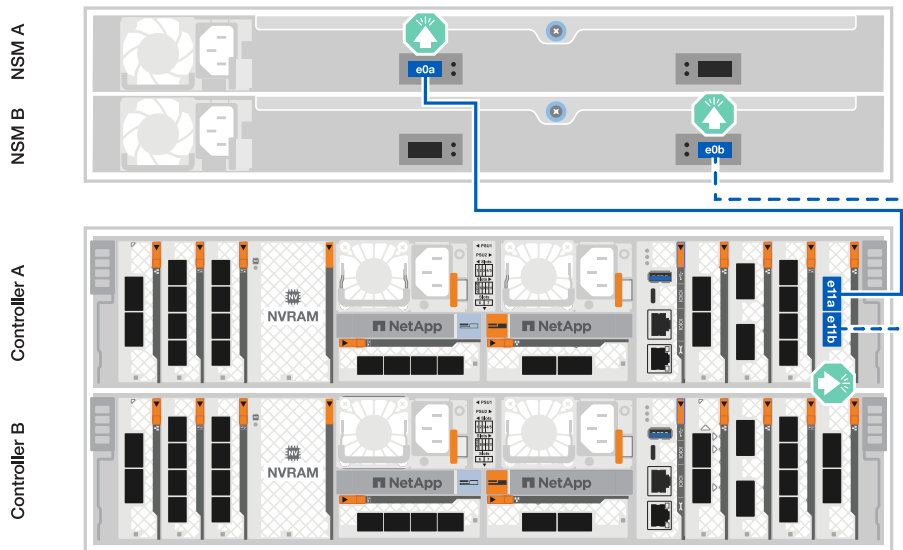
Verbinden Sie jeden Controller mit den NSM-Modulen im NS224-Shelf. Die Grafik zeigt die Verkabelung von den einzelnen Controllern: Die Verkabelung von Controller A wird blau und die Verkabelung von Controller B gelb dargestellt.

### 100 GbE QSFP28 Kupferkabel



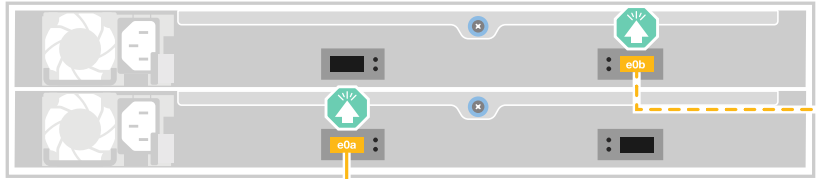
### Schritte

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.

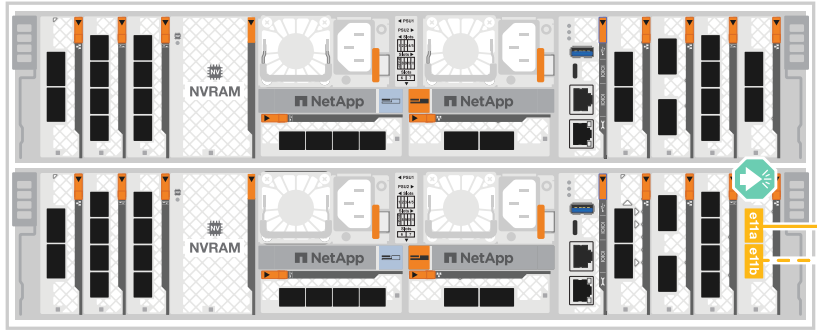


3. Verbinden Sie den Port e11a von Controller B mit dem Port e0a von NSM B.
4. Verbinden Sie den Port e11b des Controllers B mit dem Port e0b des NSM A.

NSM A  
NSM B



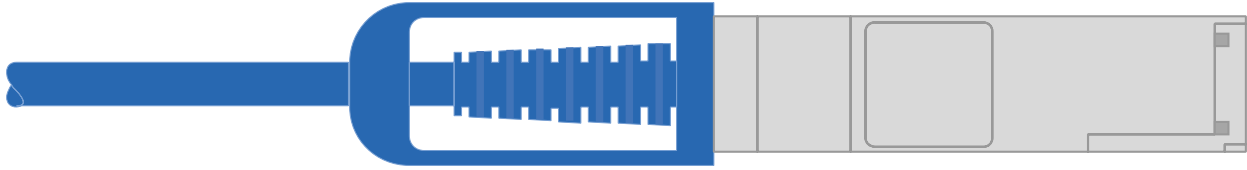
Controller A  
Controller B



## Option 2: Verbinden der Controller mit zwei NS224 Storage-Shelfs

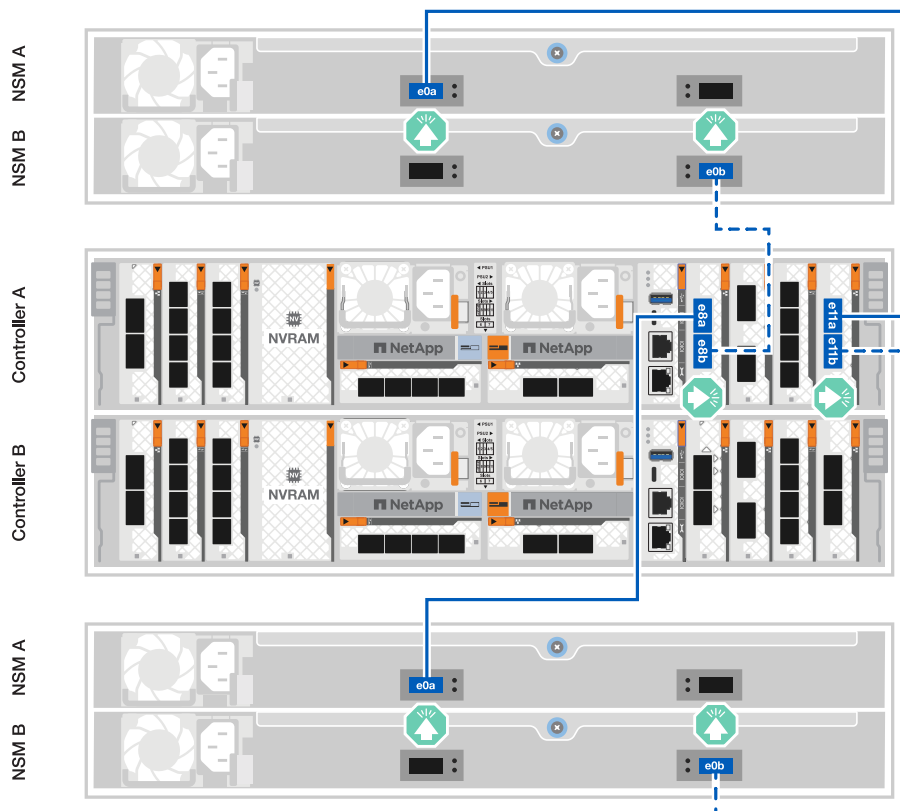
Verbinden Sie jeden Controller mit den NSM-Modulen beider NS224-Shelfs. Die Grafik zeigt die Verkabelung von den einzelnen Controllern: Die Verkabelung von Controller A wird blau und die Verkabelung von Controller B gelb dargestellt.

### 100 GbE QSFP28 Kupferkabel



### Schritte

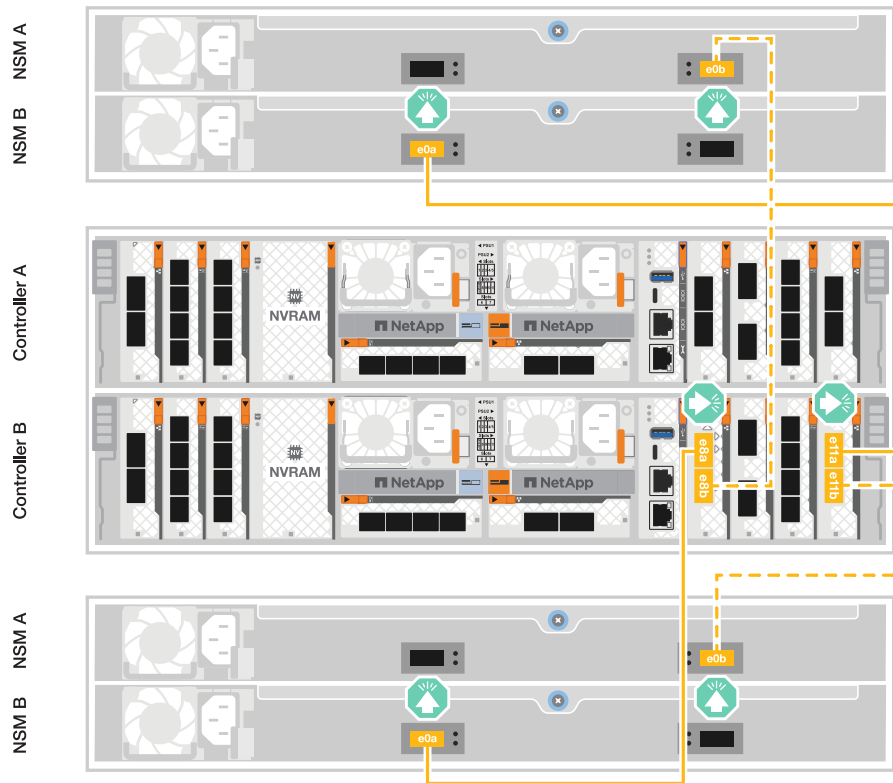
1. Verbinden Sie auf Controller A die folgenden Ports:
  - a. Verbinden Sie Port e11a mit Shelf 1, NSM A Port e0a.
  - b. Verbinden Sie den Port e11b mit Shelf 2, den NSM B Port e0b.
  - c. Verbinden Sie Port e8a mit Shelf 2, NSM A Port e0a.
  - d. Verbinden Sie Port e8b mit Shelf 1, NSM B Port e0b.



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.



### 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 Shelves installiert haben, sollten Sie die Storage-Shelves und Controller einschalten.

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

Jedes NS224-Shelf wird durch eine eindeutige Shelf-ID unterschieden. Diese ID stellt sicher, dass das Shelf innerhalb Ihrer Storage-System-Einrichtung unterscheidbar ist. Standardmäßig werden Shelf-IDs als '00' und '01' zugewiesen. Möglicherweise müssen Sie diese IDs jedoch anpassen, um die Eindeutigkeit in Ihrem Storage-System aufrechtzuerhalten.

#### Über diese Aufgabe

- Gültige Shelf-ID: 00 bis 99.
- 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.

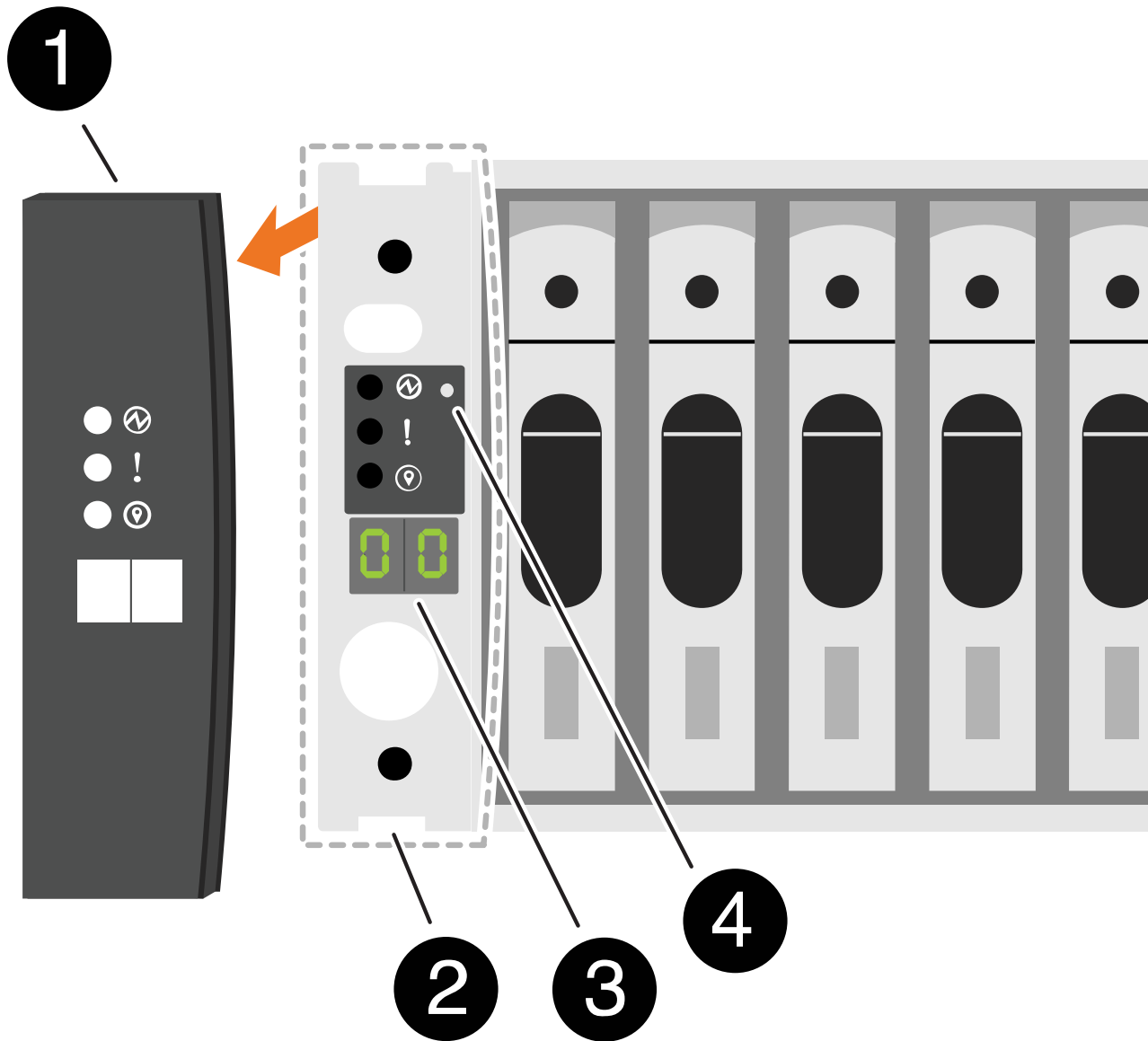
#### Schritte


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.



	Einlegeboden-Endkappe
---	-----------------------

	Ablagefaceplate
	Shelf-ID-Nummer
	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 Shelves eingeschaltet und ihnen eindeutige IDs zugewiesen haben, schalten Sie die Storage Controller ein.

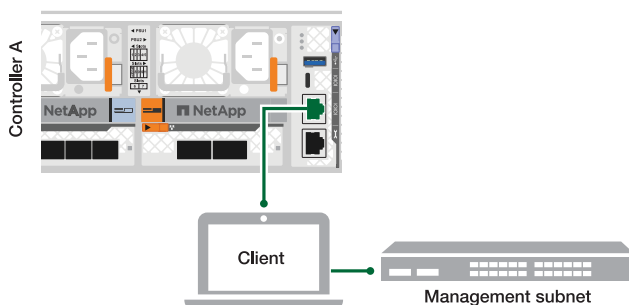
### Schritte

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

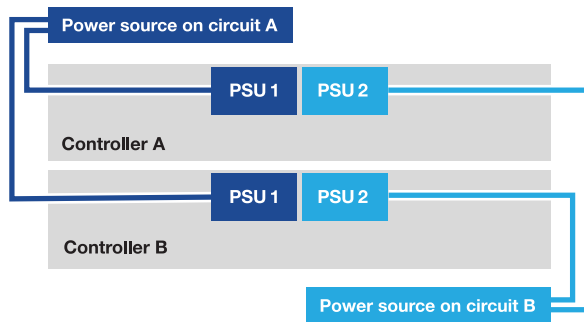


Anweisungen zum Konfigurieren des seriellen Konsolenports finden Sie in der Online-Hilfe Ihres Laptops.

- 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.



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



- Das Speichersystem beginnt zu booten. Das erste Booten kann bis zu acht Minuten dauern.
  - Die LEDs blinken auf, und die Lüfter starten, was darauf hinweist, dass die Controller eingeschaltet sind.
  - Die Lüfter sind beim ersten Starten möglicherweise sehr laut. Das Lüftergeräusch während des Startvorgangs ist normal.
3. Befestigen 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

- Verbinden Sie Ihren Laptop mit dem Management-Switch, und greifen Sie auf die Netzwerkcomputer und -Geräte zu.
- Öffnen Sie Den Datei-Explorer.
- Wählen Sie **Netzwerk** aus, klicken Sie mit der rechten Maustaste und wählen Sie **Aktualisieren** aus.
- 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**.

<b>Um IP zu konfigurieren (iSCSI und NVMe/TCP), gehen Sie folgendermaßen vor:</b>	<b>So konfigurieren Sie FC und NVMe/FC:</b>
<ul style="list-style-type: none"><li>a. Wählen Sie <b>IP</b>, und wählen Sie dann <b>IP-Schnittstellen konfigurieren</b>.</li><li>b. Wählen Sie <b>Subnetz hinzufügen</b>.</li><li>c. Geben Sie einen Namen für das Subnetz ein, und geben Sie dann die Subnetz-IP-Adressen ein.</li><li>d. Geben Sie die Subnetzmaske ein, und geben Sie optional ein Gateway ein; wählen Sie dann <b>Add</b> aus.</li><li>e. Wählen Sie das soeben erstellte Subnetz aus, und wählen Sie dann <b>Speichern</b>.</li><li>f. Wählen Sie <b>Speichern</b>.</li></ul>	<ul style="list-style-type: none"><li>a. Wählen Sie <b>FC</b>, und wählen Sie dann <b>Configure FC Interfaces</b> und/oder <b>Configure NVMe/FC Interfaces</b> aus.</li><li>b. Wählen Sie die FC- und/oder NVMe/FC-Ports aus, und wählen Sie dann <b>Save</b>.</li></ul>

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.

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

Um den Datenzugriff einzurichten, sollten Sie sicherstellen, dass bestimmte Parameter und Einstellungen auf Ihrem SAN-Client, die für den ordnungsgemäßen Betrieb mit ONTAP entscheidend sind, korrekt konfiguriert sind. Wenn Sie VMware verwenden, sollten Sie Ihre virtuellen Maschinen migrieren.

**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.

### **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  **Add** .
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, wird automatisch eine neue Host-Gruppe von ONTAP erstellt.

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

Option	Schritte
<p>Ändern Sie die standardmäßige QoS-Richtlinie (Quality of Service)</p> <p>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.</p>	<ol style="list-style-type: none"><li>a. Wählen Sie unter <b>Speicher und Optimierung</b> neben <b>Quality of Service (QoS)</b> die Option  .</li><li>b. Wählen Sie eine vorhandene QoS-Richtlinie aus.</li></ol>

Option	Schritte
Neue QoS-Richtlinie erstellen	<p>a. Wählen Sie unter <b>Speicher und Optimierung</b> neben <b>Quality of Service (QoS)</b> die Option  .</p> <p>b. Wählen Sie <b>neue Richtlinie definieren</b>.</p> <p>c. Geben Sie einen Namen für die neue QoS-Richtlinie ein.</p> <p>d. Legen Sie eine QoS-Grenze, eine QoS-Garantie oder beides fest.</p> <p style="padding-left: 20px;">i. Geben Sie unter <b>Limit</b> optional eine maximale Durchsatzgrenze, eine maximale IOPS-Grenze oder beides ein.</p> <p style="padding-left: 40px;">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.</p> <p style="padding-left: 20px;">ii. Geben Sie optional unter <b>Garantie</b> einen minimalen Durchsatz, ein Minimum an IOPS oder beides ein.</p> <p style="padding-left: 40px;">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.</p> <p>e. Wählen Sie <b>Hinzufügen</b>.</p>
Fügen Sie einen neuen SCSI-Host hinzu	<p>a. Wählen Sie unter <b>Host Information SCSI</b> für das Verbindungsprotokoll aus.</p> <p>b. Wählen Sie das Host-Betriebssystem aus.</p> <p>c. Wählen Sie unter <b>Host Mapping New Hosts</b> aus.</p> <p>d. Wählen Sie <b>FC</b> oder <b>iSCSI</b>.</p> <p>e. Wählen Sie vorhandene Host-Initiatoren aus, oder wählen Sie <b>Add Initiator</b>, um einen neuen Host-Initiator hinzuzufügen.</p> <p style="padding-left: 20px;">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“.</p>
Erstellen Sie eine neue SCSI-Host-Gruppe	<p>a. Wählen Sie unter <b>Host Information SCSI</b> für das Verbindungsprotokoll aus.</p> <p>b. Wählen Sie das Host-Betriebssystem aus.</p> <p>c. Wählen Sie unter <b>Host Mapping Neue Host-Gruppe</b> aus.</p> <p>d. Geben Sie einen Namen für die Host-Gruppe ein, und wählen Sie dann die Hosts aus, die der Gruppe hinzugefügt werden sollen.</p>

Option	Schritte
Hinzufügen eines neuen NVMe-Subsystems	<p>a. Wählen Sie unter <b>Host Information NVMe</b> für das Verbindungsprotokoll aus.</p> <p>b. Wählen Sie das Host-Betriebssystem aus.</p> <p>c. Wählen Sie unter <b>Host Mapping New NVMe Subsystem</b> aus.</p> <p>d. Geben Sie einen Namen für das Subsystem ein, oder übernehmen Sie den Standardnamen.</p> <p>e. Geben Sie einen Namen für den Initiator ein.</p> <p>f. Wenn Sie die bandinterne Authentifizierung oder Transport Layer Security (TLS) aktivieren möchten, wählen Sie ; und dann Ihre Optionen aus.</p> <p>Die in-Band-Authentifizierung ermöglicht eine sichere bidirektionale und unidirektionale Authentifizierung zwischen den NVMe Hosts und dem ASA r2 System.</p> <p>TLS verschlüsselt alle Daten, die zwischen Ihren NVMe/TCP-Hosts und Ihrem ASA r2-System über das Netzwerk gesendet werden.</p> <p>g. Wählen Sie <b>Add Initiator</b>, um weitere Initiatoren hinzuzufügen.</p> <p>Die Host-NQN sollte als &lt;nqn.yyyy-mm&gt; 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</p>

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.

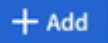
#### Bevor Sie beginnen

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  .
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
<ol style="list-style-type: none"><li>a. Wählen Sie <b>Neue Hosts</b>.</li><li>b. Wählen Sie <b>FC</b> oder <b>iSCSI</b> aus, und wählen Sie dann die Host-Initiatoren aus.</li><li>c. Wählen Sie optional <b>Configure Host Proximity</b>.  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.</li><li>d. Wenn Sie neue Initiatoren hinzufügen müssen, wählen Sie <b>Initiatoren hinzufügen</b> aus.</li></ol>	<ol style="list-style-type: none"><li>a. Wählen Sie <b>existing Hosts</b>.</li><li>b. Wählen Sie den Host aus, den Sie hinzufügen möchten.</li><li>c. Wählen Sie <b>Hinzufügen</b>.</li></ol>

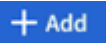
6. Wählen Sie **Hinzufügen**.

### 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  .
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.

## Erstellen von Host-Gruppen

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 sie nun einer Speichereinheit 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 zuordnenden 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	<ol style="list-style-type: none"> <li>Wählen Sie unter <b>Snapshot to Clone Use an existing snapshot</b> aus.</li> <li>Wählen Sie den Snapshot aus, den Sie für den Klon verwenden möchten.</li> </ol>
Erstellen Sie eine neue Hostgruppe	<ol style="list-style-type: none"> <li>Wählen Sie unter <b>Host Mapping New Host Group</b> aus.</li> <li>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.</li> </ol>
Fügen Sie einen neuen Host hinzu	<ol style="list-style-type: none"> <li>Wählen Sie unter <b>Host Mapping New Hosts</b> aus.</li> <li>Geben Sie den A-Namen für den neuen Host ein, und wählen Sie dann <b>FC</b> oder <b>iSCSI</b> aus.</li> <li>Wählen Sie die Host-Initiatoren aus der Liste der vorhandenen Initiatoren aus, oder wählen Sie <b>Add</b>, um neue Initiatoren für den Host hinzuzufügen.</li> </ol>

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	<ol style="list-style-type: none"><li>a. Wählen Sie unter <b>Snapshot to Clone</b> die Option <b>Use an existing Snapshot</b> aus.</li><li>b. Wählen Sie den Snapshot aus, den Sie für den Klon verwenden möchten.</li></ol>
Erstellen Sie eine neue Hostgruppe	<ol style="list-style-type: none"><li>a. Wählen Sie unter <b>Host Mapping New Host Group</b> aus.</li><li>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.</li></ol>
Fügen Sie einen neuen Host hinzu	<ol style="list-style-type: none"><li>a. Wählen Sie unter <b>Host Mapping New Hosts</b> aus.</li><li>b. Geben Sie den Namen des neuen Hostnamens ein, und wählen Sie dann <b>FC</b> oder <b>iSCSI</b>.</li><li>c. Wählen Sie die Host-Initiatoren aus der Liste der vorhandenen Initiatoren aus, oder wählen Sie <b>Add Initiator</b>, um neue Initiatoren für den Host hinzuzufügen.</li></ol>

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.

## **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.


## 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:

<b>Max. Nodes pro Cluster</b>	2
<b>Maximale Größe der Speichereinheit</b>	128 TB

#### 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.

## 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 mit derselben Kapazität und demselben Host-Betriebssystem erstellt. Um jeder Einheit eine andere Kapazität zuzuweisen, wählen Sie **Weitere Optionen** und wählen Sie dann **eine andere Kapazität hinzufügen**.

4. Wählen Sie das Host-Betriebssystem und die Host-Zuordnung aus.
5. 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 erstellten ["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	<ol style="list-style-type: none"><li>i. Wählen Sie  <b>Add</b> ; und geben Sie dann die Snapshot Policy-Parameter ein.</li><li>ii. Wählen Sie <b>Richtlinie hinzufügen</b>.</li></ol>

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	<ol style="list-style-type: none"><li>i. Wählen Sie  <b>Add</b> ; und geben Sie dann die Snapshot Policy-Parameter ein.</li><li>ii. Wählen Sie <b>Richtlinie hinzufügen</b>.</li></ol>

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.

## 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 von einem ASA r2 Storage-System wird nur auf einem anderen ASA r2 Storage-System unterstützt. Sie können Snapshots von einem ASA r2-System nicht auf ein aktuelles ASA-, AFF- oder FAS-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.

#### 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.	<ol style="list-style-type: none"> <li>a. Wählen Sie <b>Asynchron</b>.</li> <li>b. Akzeptieren Sie unter <b>Transfer Snapshots from source</b> den Standard-Übertragungszeitplan oder wählen Sie einen anderen aus.</li> <li>c. Wählen Sie diese Option aus, um alle Snapshots zu übertragen oder Regeln zu erstellen, um festzulegen, welche Snapshots übertragen werden sollen.</li> <li>d. Aktivieren Sie optional die Netzwerkkomprimierung.</li> </ol>
Schreiben Sie Daten gleichzeitig an die Quell- und Remote-Standorte.	<ol style="list-style-type: none"> <li>a. Wählen Sie * Synchron*.</li> </ol>

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	<ol style="list-style-type: none"><li>a. Wählen Sie <b>Lokale Ziele</b>, und wählen Sie dann .</li><li>b. Suchen Sie die Quell-Konsistenzgruppe, und wählen Sie sie aus.</li></ol> <p>Die Konsistenzgruppe „<i>Source</i>“ bezieht sich auf die Konsistenzgruppe in Ihrem lokalen Cluster, die Sie replizieren möchten.</p>

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

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"](#) nicht mehr lesen können, wenn eine Festplatte in Ihrem ASA r2 System neu zugewiesen, zurückgegeben, verlegt oder gestohlen wird.

## Sichern Sie Ihre Kubernetes-Applikationen auf ASA r2 Storage-Systemen

Schützen Sie Ihre Kubernetes-Applikationen mit Astra Control Center. Mit Astra Control Center können Sie Applikationen und Daten von einem Kubernetes-Cluster zu einem anderen migrieren, Applikationen mithilfe der NetApp SnapMirror Technologie auf ein Remote-System replizieren und Applikationen von Staging zu Produktion klonen.

### Finden Sie weitere Informationen

["Weitere Informationen zum Schutz von Kubernetes-Applikationen mit Astra Control"](#).

## 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.

### 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	<ol style="list-style-type: none"><li>Wählen Sie  <b>Add</b> ;, und geben Sie den neuen Richtliniennamen ein.</li><li>Wählen Sie den Richtlinienumfang aus.</li><li>Wählen Sie unter <b>Zeitpläne</b>  <b>Add</b> .</li><li>Wählen Sie den Namen aus, der unter <b>Terminplanname</b> angezeigt wird;  Wählen Sie anschließend .</li><li>Wählen Sie den Richtlinienzeitplan aus.</li><li>Geben Sie unter <b>Maximum Snapshots</b> die maximale Anzahl der Snapshots ein, die Sie von der Konsistenzgruppe behalten möchten.</li><li>Optional unter <b>SnapMirror Label</b> ein SnapMirror Label eingeben.</li><li>Wählen Sie <b>Speichern</b>.</li></ol>

6. Wählen Sie **Bearbeiten**.


### Wie es weiter geht

Da Ihre Daten nun mit Snapshots gesichert werden, sollten Sie "[Richten Sie die Snapshot-Replikation ein](#)" Ihre Konsistenzgruppen für 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.


### 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. Nachdem Sie eine zuvor vorhandene Replikationskonsistenzgruppe gelöscht haben, bleiben die Speichereinheiten, die sich in der Konsistenzgruppe befanden, auf dem 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.

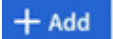
### Erstellen Sie einen neuen Zeitplan für Schutzrichtlinien

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  .
3. Geben Sie einen Namen für den Zeitplan ein, und wählen Sie dann die Zeitplanparameter aus.
4. Wählen Sie **Speichern**.

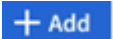
### Was kommt als Nächstes?

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  .
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.

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	<ol style="list-style-type: none"> <li>a. Wählen Sie <b>Onboard Key Manager</b>, um die Schlüsselservers hinzuzufügen.</li> <li>b. Geben Sie eine Passphrase ein.</li> </ol>
Konfigurieren Sie einen externen Schlüsselmanager	<ol style="list-style-type: none"> <li>a. Wählen Sie <b>External Key Manager</b>, um die Schlüsselservers hinzuzufügen.</li> <li>b. Wählen Sie <b>+ Add</b> diese Option aus, um die Schlüsselservers hinzuzufügen.</li> <li>c. Fügen Sie die CA-Zertifikate des KMIP-Servers hinzu.</li> <li>d. Fügen Sie die KMIP-Client-Zertifikate hinzu.</li> </ol>

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.

## Schutz vor Ransomware-Angriffen auf ASA r2 Storage-Systeme


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**.

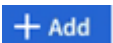

#### Was kommt als Nächstes?

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"](#).

### 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  .
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.

# Administration und Überwachung

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

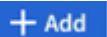
Storage-Einheiten eines ASA r2-Systems befinden sich in Storage Virtual Machines (VMs). Storage-VMs dienen der Bereitstellung von Daten für Ihre SAN-Clients. Erstellen Sie mit ONTAP System Manager eine LIF (Netzwerkschnittstelle) für Ihre SAN-Clients, um eine Storage-VM anzuschließen und auf Daten in 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 von IPspaces

Ein IPspace ist ein eindeutiger 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 Netzwerkdomeänen 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

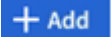
Ein Subnetz ermöglicht es Ihnen, bestimmte Blöcke von IPv4- oder IPv6-Adressen zuzuweisen, die beim Erstellen einer LIF (Netzwerkschnittstelle) verwendet werden sollen. Ein Subnetz vereinfacht die LIF-Erstellung, da Sie in der Lage sind, den Subnetznamen anstelle einer bestimmten IP-Adresse und Netzwerkmaske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

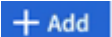
Eine LIF (Netzwerkschnittstelle) ist eine IP-Adresse, die einem physischen oder logischen Port zugeordnet ist. Erstellen Sie LIFs an den Ports, die Sie für den Datenzugriff verwenden möchten. Storage-VMs stellen Daten über ein oder mehrere LIFs für Clients bereit. Bei einem Komponentenausfall kann eine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

Wenn eine IP-Daten-LIF erstellt wird, kann sie standardmäßig sowohl iSCSI- als auch NVMe/TCP-Datenverkehr verarbeiten. Für den FC- und NVMe/FC-Datenverkehr müssen getrennte Daten-LIFs erstellt werden.

### 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  .
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.

## 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.

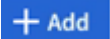
Sie können zusätzliche Broadcast-Domänen erstellen, nachdem das Cluster initialisiert wurde. Wenn Sie eine Broadcast-Domäne erstellen, wird automatisch eine Failover-Gruppe erstellt, die dieselben Ports enthält.

### 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  .
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 jeden Tag einen Performance-Abfall zur gleichen Zeit. 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.

Die Datenreduzierungsration gibt den durch Storage-Effizienz eingesparten Speicherplatz an.

### 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 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.


## 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 neben **Automatic Update** , und wählen Sie dann **enable**.
3. Lesen und akzeptieren Sie die EULA.
4. Akzeptieren Sie die Standardeinstellungen, um Ihre Firmware und Systemdateien automatisch zu aktualisieren. Wählen Sie optional aus, um Benachrichtigungen anzuzeigen oder empfohlene Updates automatisch zu verwerfen.
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 neben **Automatic Update** , und wählen Sie dann **Disable**.


### 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 **Automatisches Update** , 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 **Automatisches Update** , und wählen Sie dann **Automatische Updates bearbeiten**.
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 wählen Sie dann **Update**.
3. Wählen Sie **Firmware-Update**; die Option .

### Ergebnis

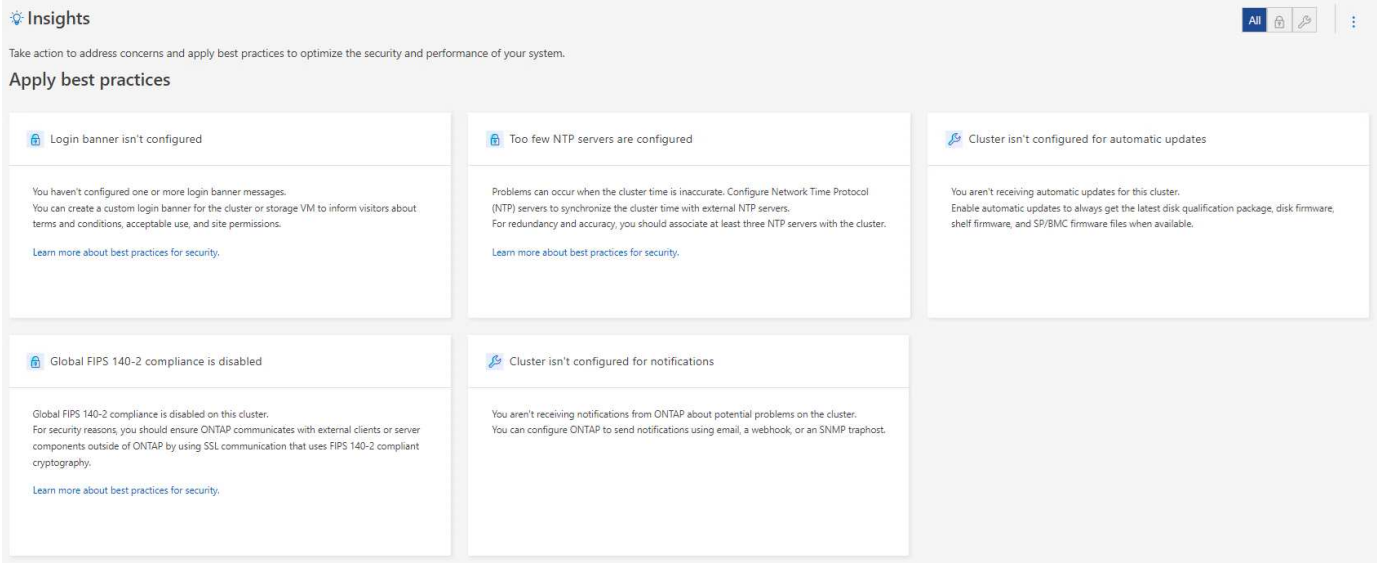
Ihre Firmware wird aktualisiert.

## 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


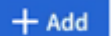
Um dies anzuzeigen...	Tun Sie das...
Cluster-Ereignisse	Wählen Sie <b>Events</b> , und wählen Sie dann <b>Event Log</b> .
Vorschläge von Active IQ	Wählen Sie <b>Ereignisse</b> und dann <b>Active IQ Suggestions</b> .
Systemmeldungen	<ol style="list-style-type: none"> <li>a. Wählen Sie <b>System Alerts</b>.</li> <li>b. Wählen Sie die Systemwarnung aus, für die Sie Maßnahmen ergreifen möchten.</li> <li>c. Bestätigen oder unterdrücken Sie die Warnmeldung.</li> </ol>

Um dies anzuzeigen...	Tun Sie das...
Cluster-Jobs	Wählen Sie <b>Jobs</b> .
Prüfprotokolle	Wählen Sie <b>Audit-Protokolle</b> .

## 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 .
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

### 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.

## 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 Benutzerkontrollen, 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.


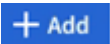
### Was kommt als Nächstes?

Sie können jetzt die SAML-Authentifizierung für Ihre Benutzerkonten verwenden.

## Erstellen von Benutzerkontrollen

Rollen für Cluster-Administratoren und Storage-VM-Administratoren werden automatisch erstellt, wenn das Cluster initialisiert wird. Erstellen Sie zusätzliche Benutzerkontrollen, 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 .

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 options** das Thema hinzu, wählen Sie ; und dann die gewünschten Aktualisierungen vornehmen.
5. Wählen Sie **Erzeugen**.


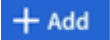
### Ergebnis

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  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:
<ol style="list-style-type: none"> <li>Wählen Sie ; und dann <b>erneuern</b>.</li> <li>Geben Sie die Zertifikatinformationen ein oder importieren Sie sie, und wählen Sie dann <b>Renew</b> aus.</li> </ol>	<ol style="list-style-type: none"> <li>Wählen Sie ; und dann <b>Löschen</b>.</li> <li>Bestätigen Sie, dass Sie löschen möchten, und wählen Sie dann <b>Löschen</b>.</li> </ol>

### 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:
<ol style="list-style-type: none"><li>a. Wählen Sie <b>⋮</b>; und dann <b>erneuern</b>.</li><li>b. Geben Sie die Zertifikatinformationen ein oder importieren Sie sie, und wählen Sie dann <b>Renew</b> aus.</li></ol>	<p>Wählen Sie <b>⋮</b>; und dann <b>Löschen</b>.</p>

### 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 – Dokumentation verwalten](#)" 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 einheitliche Hardware- und Softwarelösung für reine SAN-Umgebungen, die auf All-Flash-Plattformen basieren. ASA r2 Systeme unterscheiden sich bei der Implementierung ihrer Storage-Ebene, unterstützter Protokolle und ONTAP Persönlichkeit von anderen ONTAP Systemen (ASA, AFF und FAS).

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, die auf allen anderen ONTAP Systemen (ASA, AFF, FAS) ausgeführt werden, 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.

Die Storage-Ebene für ONTAP Systeme, auf denen die Unified ONTAP Personality ausgeführt wird, verwendet Aggregate als Storage-Basiseinheit. Ein Aggregat besitzt einen bestimmten Satz der in einem Storage-System verfügbaren Festplatten. Das Aggregat weist den Speicherplatz auf den Festplatten zu, denen es Volumes für LUNs und Namespaces besitzt. Ein einheitlicher ONTAP-Benutzer kann über die Befehlszeilenschnittstelle (CLI) Aggregate, Volumes, LUNs und Namespaces erstellen und ändern.

Die Storage-Ebene in ASA r2 Systemen verwendet anstelle von Aggregaten eine Storage-Verfügbarkeitszone. Eine Storage-Verfügbarkeitszone ist ein gemeinsamer Speicherpool, der Zugriff auf alle verfügbaren Festplatten im Speichersystem hat. Die Storage-Verfügbarkeitszone ist für beide Nodes in einem ASA r2 HA-Paar sichtbar. Bei der Erstellung einer Storage-Einheit (entweder auf Basis einer LUN oder eines NVMe Namespace) erstellt ONTAP automatisch ein Volume mit einer Storage Virtual Machine (VM) in der Storage-Verfügbarkeitszone, um die Storage-Einheit zu beherbergen. Aufgrund dieses automatisierten und vereinfachten Ansatzes für das Storage-Management sind bestimmte System Manager Optionen, ONTAP Befehle und REST-API-Endpunkte nicht verfügbar oder werden von einem ASA r2 System nur eingeschränkt genutzt. Da beispielsweise `volume create` die Erstellung und Verwaltung von Volumes für ASA r2-Systeme automatisiert ist, wird das Menü **Volumes** im System-Manager nicht angezeigt und der Befehl wird nicht unterstützt.

ASA r2 Storage wird wie folgt mit anderen ONTAP Storage-Systemen verglichen:

	ASA r2	ASA	AFF	FAS
<b>ONTAP-Persönlichkeit</b>	ASA r2	ASA	Virtualisierung	Virtualisierung
<b>Unterstützung für SAN-Protokolle</b>	Ja.	Ja.	Ja.	Ja.
<b>Unterstützung des NAS-Protokolls</b>	Nein	Nein	Ja.	Ja.
<b>Unterstützung der Speicherschicht</b>	Zone der Storage-Verfügbarkeit	Aggregate	Aggregate	Aggregate

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

- ASAA1K
- ASAA70
- ASAA90

#### 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"](#).

#### Zusammenfassung der ASA r2-Systemunterschiede

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 für werden auf ASA r2-Storage-Systemen immer über Thin Provisioning bereitgestellt. Thick Provisioning wird nicht unterstützt.

## 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:

- iSCSI LIF-Failover
- FabricPool
- Thick Provisioning für LUNs
- MetroCluster
- Objektprotokolle
- ONTAP S3 SnapMirror und S3-APIs
- Von SnapMirror zur Cloud
- SnapMirror auf Systeme mit nicht-ASA r2
- Selektive LUN-Zuordnung (SLM)

### ASA r2-Systeme unterstützen Folgendes:

- SnapLock
- Dual-Layer-Verschlüsselung

### Finden Sie weitere Informationen

- ["NetApp Hardware Universe"](#) Weitere Informationen zur Unterstützung und zu Einschränkungen der ASA r2-Hardware finden Sie im.
- ["Erfahren Sie, wie Sie Snapshots sperren"](#) Auf Ihrem ASA r2-System.
- ["Erfahren Sie, wie Sie eine zweischichtige Verschlüsselung anwenden"](#) Auf Daten auf Ihrem ASA r2-System.

## ONTAP CLI-Unterstützung für ASA r2 Storage-Systeme

Anstelle von herkömmlichen Aggregaten, die einen bestimmten Satz der in einem Storage-System verfügbaren Festplatten besitzen, verwenden ASA r2 Systeme eine Storage-Verfügbarkeitszone\_. Eine Storage-Verfügbarkeitszone ist ein gemeinsamer Speicherpool, der Zugriff auf alle verfügbaren Festplatten im Speichersystem hat. Die Storage-Verfügbarkeitszone ist für beide Nodes in einem ASA r2 HA-Paar sichtbar. Bei der Erstellung einer Storage-Einheit (LUN oder NVMe Namespace) erstellt ONTAP automatisch ein Volume mit einer Storage Virtual Machine (VM) in der Storage-Verfügbarkeitszone, um die Storage-Einheit zu beherbergen.

Aufgrund dieses vereinfachten Ansatzes `storage aggregate` für das Storage-Management werden Befehle auf ASA r2 Systemen nicht unterstützt. `lun `volume`` Auch die Unterstützung bestimmter Befehle und Parameter und ist begrenzt.

Die folgenden Befehle und Befehlssets werden auf ASA unter r2 nicht unterstützt:

#### **Nicht unterstützte `-`-Befehle**

- `lun copy`
- `lun geometry`
- `lun import`
- `lun mapping add-reportng-nodes`
- `lun mapping-remove-reporting-nodes`
- `lun maxsize`
- `lun move`
- `lun move-in-volume`

Dieser Befehl wurde durch `lun-Umbenennung/vserver nvme-Namespace-Umbenennung` ersetzt.

- `lun transition`

## Nicht unterstützte `-`-Befehle und -Parameter

- `volume autosize`
- `volume create`
- `volume delete`
- `volume expand`
- `volume modify`

Dieser 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-permissions`
- `-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 `-Befehle für die Clitzebaus-`**

- volume clone create
- volume clone split

#### **Nicht unterstützte `-SnapLock -Befehle`**

- volume snaplock modify

#### **Nicht unterstützte `-Befehle für den -Ausschnapper`**

- volume snapshot
- volume snapshot autodelete modify
- volume snapshot policy modify

## Nicht unterstützte `-`-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 `-`-Befehle

- `storage failover show-takeover`
- `storage failover show-giveback`
- `storage aggregate relocation`
- `storage disk assign`
- `storage disk partition`
- `storage disk reassign`

## 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

<b>Synchronisierung ohne symmetrische Authentifizierung</b>	<pre>cluster time-service ntp server create -server &lt;server_name&gt;</pre>
<b>Synchronisierung mit symmetrischer Authentifizierung</b>	<pre>cluster time-service ntp server create -server &lt;server_ip_address&gt; -key-id &lt;key_id&gt;</pre>

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](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**.

# 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 überprüft, ob der technische Support AutoSupport Meldungen von Ihrem ASA r2 System erhalten kann und über die erforderlichen Daten verfügt, um Ihnen bei einem Problem zu helfen.

### 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/"](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/"](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/"](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.



## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

## Markeninformationen

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