Storage-Management mit Element Software

Element Software

NetApp
January 15, 2024

Inhalt

Storage-Management mit Element Software

Mit Element Software können Sie SolidFire Storage einrichten, Cluster-Kapazität und -Performance überwachen und Storage-Aktivitäten in einer mandantenfähigen Infrastruktur managen.

Element ist das Storage-Betriebssystem, das Herzstück eines SolidFire Clusters ist. Element Software wird auf allen Nodes im Cluster unabhängig ausgeführt. Es ermöglicht den Nodes des Clusters, Ressourcen zu kombinieren und externen Clients als einzelnes Storage-System zur Verfügung zu stellen. Element Software ist für die gesamte Clusterkoordination, den Umfang und das Management des Systems verantwortlich.

Die Softwareschnittstelle basiert auf der Element API.

- "Greifen Sie auf die Benutzeroberfläche der Element Software zu"
- "Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen"
- "Aktualisieren von Komponenten des Storage-Systems"
- "Verwenden Sie grundlegende Optionen in der UI für Element Software"
- "Konten verwalten"
- "Management des Systems"
- "Management von Volumes und virtuellen Volumes"
- "Sichern Sie Ihre Daten"
- "Fehler im System beheben"

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Greifen Sie auf die Benutzeroberfläche der Element Software zu

Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.

Sie müssen sicherstellen, dass Popup-Blocker und NoScript-Einstellungen in Ihrem Browser deaktiviert sind.

Je nach Konfiguration während der Cluster-Erstellung können Sie über IPv4- und IPv6-Adressen auf die UI zugreifen.

1. Folgenden Optionen wählbar:
   - IPv6: Geben Sie https://[IPv6 MVIP-Adresse ein, z. B.:

     ```
     https://[fd20:8b1e:b256:45a::1234]/
     ```

- IPv4: Geben Sie https://[IPv4 MVIP-Adresse ein, z. B.:

```
https://10.123.456.789/
```

2. Geben Sie für DNS den Hostnamen ein.
3. Klicken Sie durch alle Authentifizierungszertifikatmeldungen.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen

Nach der Einrichtung des SolidFire Systems sollten Sie möglicherweise einige optionale Aufgaben ausführen.

Wenn Sie die Anmeldedaten im System ändern, sollten Sie die Auswirkungen auf andere Komponenten kennen.

Darüber hinaus können Einstellungen für Multi-Faktor-Authentifizierung, externes Verschlüsselungsmanagement und die Sicherheit von Federal Information Processing Standards (FIPS) konfiguriert werden. Sie sollten sich auch die Aktualisierung von Kennwörtern ansehen, wenn nötig.

Weitere Informationen

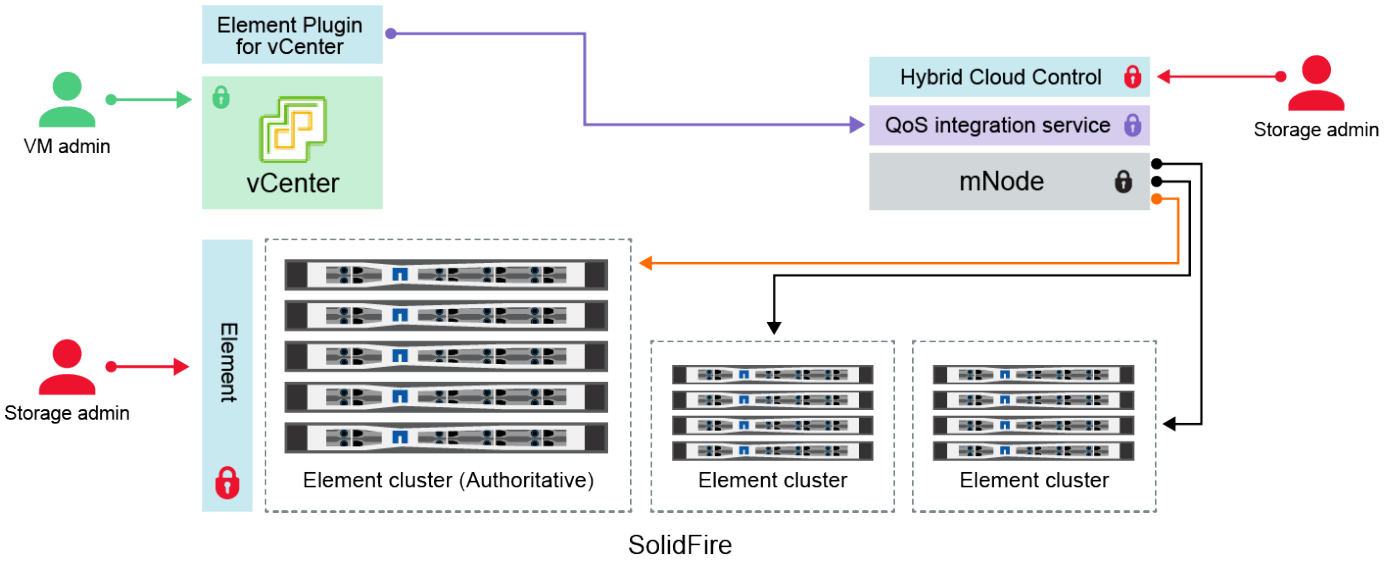
- "Anmeldedaten in NetApp HCI und NetApp SolidFire ändern"
- "Ändern Sie das Standard-SSL-Zertifikat der Element Software"
- "Ändern Sie das IPMI-Passwort für Knoten"
- "Multi-Faktor-Authentifizierung aktivieren"
- "Erste Schritte mit externem Verschlüsselungsmanagement"
- "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt"

Anmeldedaten in NetApp HCI und NetApp SolidFire ändern

Abhängig von den Sicherheitsrichtlinien im Unternehmen, die NetApp HCI oder NetApp SolidFire implementiert haben, gehört das Ändern von Anmeldedaten oder Passwörtern in der Regel zu den Sicherheitspraktiken. Bevor Sie Passwörter ändern, sollten Sie sich der Auswirkungen auf andere Softwarekomponenten in der Bereitstellung bewusst sein.

Wenn Sie die Anmeldedaten für eine Komponente einer NetApp HCI- oder NetApp SolidFire-Implementierung ändern, enthält die folgende Tabelle Anweisungen zu den Auswirkungen auf andere Komponenten.

Interaktionen von NetApp SolidFire-Komponenten:



Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
Anmeldedaten für Element 	**Gilt für**: NetApp HCI und SolidFire Administratoren verwenden diese Anmeldedaten zur Anmeldung bei: • Element Benutzeroberfläche auf dem Element Storage-Cluster • Hybrid Cloud Control auf dem Management-Node (mNode) Wenn Hybrid Cloud Control mehrere Storage-Cluster managt, akzeptiert es nur die Admin-Anmeldeinformationen für die Storage-Cluster, bekannt als das *autorisierende Cluster*, für das der mNode ursprünglich eingerichtet wurde. Bei Storage-Clustern, die später zu Hybrid Cloud Control hinzugefügt werden, speichert der mNode die Anmeldedaten des Administrators sicher. Wenn Anmeldeinformationen für nachträglich hinzugefügte Speicher-Cluster geändert werden, müssen die Anmeldeinformationen auch im mnode mit der mNode-API aktualisiert werden.	• "Aktualisieren der Passwörter für den Storage-Cluster-Administrator." • Aktualisieren Sie die Anmeldedaten des Storage-Cluster-Administrators im mNode mithilfe des "Modifizierter clusteradmin API".

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
VSphere Single Sign On – Zugangsdaten 	**Gilt nur für**: NetApp HCI Administratoren verwenden diese Zugangsdaten, um sich beim VMware vSphere Client anzumelden. Wenn vCenter Teil der Installation von NetApp HCI ist, werden in der NetApp Deployment Engine die folgenden Anmeldedaten konfiguriert: • username@vsphere.local mit dem angegebenen Passwort, und • administrator@vsphere.local mit dem angegebenen Passwort. Wenn ein vorhandenes vCenter für die Implementierung von NetApp HCI verwendet wird, werden die Anmeldeinformationen für vSphere Single Sign-On von DEN IT-VMware-Administratoren gemanagt.	"Aktualisieren der vCenter- und ESXi-Anmeldedaten".
Baseboard Management Controller (BMC) Zugangsdaten 	**Gilt nur für**: NetApp HCI Administratoren melden sich mithilfe dieser Anmeldedaten beim BMC der NetApp Computing-Nodes in einer NetApp HCI-Implementierung an. Das BMC bietet grundlegende Hardware-Überwachung und Funktionen der virtuellen Konsole. BMC-Anmeldeinformationen (auch als „*IPMI*“ bezeichnet) für jeden NetApp Computing-Node werden in NetApp HCI-Implementierungen sicher auf dem mNode gespeichert. NetApp Hybrid Cloud Control verwendet BMC-Anmeldeinformationen in einem Service-Konto, um während eines Upgrades der Computing-Node-Firmware mit dem BMC in den Computing-Nodes zu kommunizieren. Wenn die BMC-Anmeldedaten geändert werden, müssen auch die Anmeldeinformationen für die jeweiligen Computing-Nodes auf dem mnode aktualisiert werden, damit alle Hybrid Cloud Control-Funktionen erhalten bleiben.	• "Konfigurieren Sie IPMI für jeden Node in NetApp HCI". • Für H410C, H610C und H615C Nodes "Ändern Sie das Standard-IPMI-Passwort". • Für H410S und H610S Nodes "Ändern Sie das IPM-Standardpasswort". • "Ändern Sie BMC-Anmeldeinformationen auf dem Management-Node".

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
ESXi Anmeldedaten 	**Gilt nur für**: NetApp HCI Administratoren können sich über SSH oder die lokale DCUI mit einem lokalen Root-Konto bei ESXi Hosts anmelden. In NetApp HCI-Implementierungen ist der Benutzername „root“, und das Passwort wurde bei der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. ESXi Root-Anmeldedaten für jeden NetApp Computing-Node werden in NetApp HCI-Implementierungen sicher auf dem mnode gespeichert. NetApp Hybrid Cloud Control verwendet die Zugangsdaten in der Kapazität eines Service-Kontos, um direkt während Upgrades der Firmware des Computing-Nodes und Zustandsprüfungen mit ESXi Hosts zu kommunizieren. Wenn die ESXi-Root-Anmeldedaten von einem VMware-Administrator geändert werden, müssen die Anmeldeinformationen für die jeweiligen Computing-Nodes auf dem mnode aktualisiert werden, damit die Hybrid Cloud Control-Funktionalität erhalten bleibt.	"Anmeldedaten für vCenter- und ESXi-Hosts aktualisieren".
Passwort für die QoS-Integration 	**Gilt für**: NetApp HCI und optional in SolidFire Nicht für interaktive Anmeldungen durch Administratoren verwendet. Die QoS-Integration zwischen VMware vSphere und Element Software wird durch folgende aktiviert: • Element Plug-in für vCenter Server und • QoS-Service auf dem mNode. Für die Authentifizierung verwendet der QoS-Service ein Passwort, das ausschließlich in diesem Zusammenhang verwendet wird. Das QoS-Passwort wird bei der Erstinstallation des Element Plug-in für vCenter Server angegeben oder während der NetApp HCI-Implementierung automatisch generiert. Keine Auswirkung auf andere Komponenten.	"Aktualisieren Sie die QoSSIOC-Anmeldeinformationen im NetApp Element-Plug-in für vCenter Server". Das SIOC-Passwort des NetApp Element-Plug-ins für vCenter-Server wird auch als *QoSSIOC-Passwort* bezeichnet. Lesen Sie den Element Plug-in for vCenter Server KB Artikel.

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
Anmeldedaten für vCenter Service Appliance 	**Gilt für**: NetApp HCI nur bei Einrichtung über die NetApp Deployment Engine Administratoren können sich bei den virtuellen Maschinen der vCenter Server Appliance anmelden. In NetApp HCI-Implementierungen ist der Benutzername „root“, und das Passwort wurde bei der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. Je nach der bereitgestellten VMware vSphere Version können sich auch bestimmte Administratoren in der vSphere Single Sign-On-Domäne bei der Appliance anmelden. Keine Auswirkung auf andere Komponenten.	Es sind keine Änderungen erforderlich.
Anmeldedaten für NetApp Management-Node-Admin 	**Gilt für**: NetApp HCI und optional in SolidFire Zur erweiterten Konfiguration und Fehlerbehebung können sich Administratoren bei Virtual Machines des NetApp Management Node anmelden. Je nach implementierter Management-Node-Version ist die Anmeldung über SSH nicht standardmäßig aktiviert. In NetApp HCI-Implementierungen wurden Benutzername und Passwort vom Benutzer während der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. Keine Auswirkung auf andere Komponenten.	Es sind keine Änderungen erforderlich.

Weitere Informationen

- "Ändern Sie das Standard-SSL-Zertifikat der Element Software"
- "Ändern Sie das IPMI-Passwort für Knoten"
- "Multi-Faktor-Authentifizierung aktivieren"
- "Erste Schritte mit externem Verschlüsselungsmanagement"
- "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt"

Ändern Sie das Standard-SSL-Zertifikat der Element Software

Sie können mithilfe der NetApp Element API das Standard-SSL-Zertifikat und den privaten Schlüssel des Storage-Node im Cluster ändern.

Beim Erstellen eines NetApp Element-Software-Clusters erstellt das Cluster ein einzigartiges SSL-Zertifikat (Secure Sockets Layer) mit einem privaten Schlüssel, das für die gesamte HTTPS-Kommunikation über die Element-UI, die UI pro Node oder die APIs verwendet wird. Die Element Software unterstützt selbstsignierte Zertifikate sowie Zertifikate, die von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt und

verifiziert werden.

Sie können die folgenden API-Methoden verwenden, um mehr Informationen über das Standard-SSL-Zertifikat zu erhalten und Änderungen vorzunehmen.

- **GetSSLZertifikat**

  Sie können das verwenden "GetSSLCertificate-Methode" So rufen Sie Informationen zum derzeit installierten SSL-Zertifikat ab, einschließlich aller Zertifikatdetails.

- **SetSSLZertifikat**

  Sie können das verwenden "SetSSLCertificate-Methode" Zum Festlegen der Cluster- und Node-SSL-Zertifikate auf das von Ihnen zur Verfügung gestellt Zertifikat und den privaten Schlüssel. Das System überprüft das Zertifikat und den privaten Schlüssel, um zu verhindern, dass ein ungültiges Zertifikat angewendet wird.

- **RemoveSSLZertifikat**

  Der "RemoveSSLCertificate-Methode" Entfernt das derzeit installierte SSL-Zertifikat und den privaten Schlüssel. Das Cluster generiert dann ein neues selbstsigniertes Zertifikat und einen privaten Schlüssel.

> Das Cluster-SSL-Zertifikat wird automatisch auf alle neuen Nodes angewendet, die dem Cluster hinzugefügt wurden. Jeder Node, der aus dem Cluster entfernt wurde, wird auf ein selbstsigniertes Zertifikat zurückgesetzt und alle benutzerdefinierten Zertifikate und Schlüsselinformationen werden vom Node entfernt.

Weitere Informationen

- "Ändern Sie das Standard-SSL-Zertifikat für den Management-Node"
- "Welche Anforderungen gelten für das Festlegen benutzerdefinierter SSL-Zertifikate in der Element Software?"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Ändern Sie das Standard-IPMI-Passwort für Nodes

Sie können das Standard-Administratorpasswort für die Intelligent Platform Management Interface (IPMI) ändern, sobald Sie Remote-IPMI-Zugriff auf den Node haben. Sie möchten dies möglicherweise tun, wenn Installationsupdates vorhanden sind.

Weitere Informationen zur Konfiguration des IPM-Zugriffs für Knoten finden Sie unter "Konfigurieren Sie IPMI für jeden Node".

Sie können das IPM-Passwort für diese Knoten ändern:

- H410S Nodes
- H610S Nodes

Ändern Sie das Standard-IPMI-Passwort für H410S-Nodes

Sie sollten das Standardpasswort für das IPMI-Administratorkonto auf jedem Speicherknoten ändern, sobald Sie den IPMI-Netzwerkport konfigurieren.

Was Sie benötigen

Sie sollten die IPMI-IP-Adresse für jeden Storage-Node konfiguriert haben.

Schritte

1. Öffnen Sie einen Webbrowser auf einem Computer, der das IPMI-Netzwerk erreichen kann, und navigieren Sie zu der IPMI-IP-Adresse für den Knoten.
2. Geben Sie den Benutzernamen ein `ADMIN` Und Passwort `ADMIN` In der Eingabeaufforderung für die Anmeldung.
3. Klicken Sie beim Anmelden auf die Registerkarte **Konfiguration**.
4. Klicken Sie Auf **Benutzer**.
5. Wählen Sie die aus `ADMIN` Benutzer und klicken Sie auf **Benutzer ändern**.
6. Aktivieren Sie das Kontrollkästchen **Passwort ändern**.
7. Geben Sie ein neues Passwort in die Felder **Passwort** und **Passwort bestätigen** ein.
8. Klicken Sie auf **Ändern** und dann auf **OK**.
9. Wiederholen Sie dieses Verfahren für alle anderen H410S-Nodes mit Standard-IPMI-Kennwörtern.

Ändern Sie das Standard-IPMI-Passwort für H610S-Nodes

Sie sollten das Standardpasswort für das IPMI-Administratorkonto auf jedem Speicherknoten ändern, sobald Sie den IPMI-Netzwerkport konfigurieren.

Was Sie benötigen

Sie sollten die IPMI-IP-Adresse für jeden Storage-Node konfiguriert haben.

Schritte

1. Öffnen Sie einen Webbrowser auf einem Computer, der das IPMI-Netzwerk erreichen kann, und navigieren Sie zu der IPMI-IP-Adresse für den Knoten.
2. Geben Sie den Benutzernamen ein `root` Und Passwort `calvin` In der Eingabeaufforderung für die Anmeldung.
3. Wenn Sie sich anmelden, klicken Sie oben links auf der Seite auf das Symbol für die Menünavigation, um das Fach für die Seitenleiste zu öffnen.
4. Klicken Sie Auf **Einstellungen**.
5. Klicken Sie Auf **Benutzerverwaltung**.
6. Wählen Sie den **Administrator**-Benutzer aus der Liste aus.
7. Aktivieren Sie das Kontrollkästchen **Passwort ändern**.
8. Geben Sie ein neues, starkes Passwort in die Felder **Passwort** und **Passwort bestätigen** ein.
9. Klicken Sie unten auf der Seite auf **Speichern**.
10. Wiederholen Sie dieses Verfahren für alle anderen H610S-Nodes mit Standard-IPMI-Kennwörtern.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Verwenden Sie grundlegende Optionen in der UI für Element Software

Über die NetApp Element Software-Webbenutzeroberfläche (Element UI) können Sie allgemeine Aufgaben auf Ihrem SolidFire-System überwachen und ausführen.

Zu den grundlegenden Optionen gehören die Anzeige von API-Befehlen, die durch UI-Aktivitäten aktiviert sind, und die Angabe von Feedback.

- "Zeigt die API-Aktivität an"
- "Symbole in der Element-Schnittstelle"
- "Feedback mitteilen"

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Zeigt die API-Aktivität an

Das Element System nutzt die NetApp Element API als Grundlage für seine Funktionen. Mit der Element UI können Sie verschiedene Arten von API-Aktivitäten in Echtzeit auf dem System anzeigen, während Sie die Schnittstelle verwenden. Mit dem API-Protokoll können Sie vom Benutzer initiierte und Hintergrund-System-API-Aktivitäten sowie API-Aufrufe auf der Seite anzeigen, die Sie derzeit anzeigen.

Mithilfe des API-Protokolls können Sie ermitteln, welche API-Methoden für bestimmte Aufgaben verwendet werden. Außerdem erfahren Sie, wie Sie die API-Methoden und -Objekte zum Erstellen benutzerdefinierter Anwendungen verwenden.

Informationen zu den einzelnen Methoden finden Sie unter "Element Software-API-Referenz".

1. Klicken Sie in der Element UI-Navigationsleiste auf **API-Protokoll**.
2. So ändern Sie den Typ der API-Aktivität, die im Fenster API-Protokoll angezeigt wird:
   a. Wählen Sie **Requests**, um API-Request-Traffic anzuzeigen.
   b. Wählen Sie **Antworten**, um den API-Antwortdatenverkehr anzuzeigen.
   c. Filtern Sie die Typen von API-Traffic, indem Sie eine der folgenden Optionen auswählen:
      - **Benutzer initiiert**: API-Verkehr durch Ihre Aktivitäten während dieser Web-UI-Sitzung.
      - **Hintergrundabfrage**: API-Traffic, der durch Systemaktivität im Hintergrund erzeugt wird.
      - **Aktuelle Seite**: API Traffic generiert durch Aufgaben auf der Seite, die Sie gerade sehen.

Weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Aktualisierungsrate der Schnittstelle, die von einer Clusterlast beeinflusst wird

Abhängig von den API-Reaktionszeiten kann das Cluster möglicherweise das Datenaktualisierungsintervall für bestimmte Teile der NetApp Element Softwareseite automatisch anpassen, die Sie anzeigen.

Das Aktualisierungsintervall wird auf die Standardeinstellung zurückgesetzt, wenn Sie die Seite in Ihrem Browser neu laden. Sie können das aktuelle Aktualisierungsintervall anzeigen, indem Sie oben rechts auf der Seite auf den Cluster-Namen klicken. Beachten Sie, dass das Intervall steuert, wie oft API-Anforderungen erstellt werden, nicht wie schnell die Daten vom Server zurückkommen.

Wenn ein Cluster stark beansprucht ist, können API-Anforderungen von der Element UI in die Warteschlange gestellt werden. Wenn die Systemantwort erheblich verzögert wird, z. B. eine langsame Netzwerkverbindung in Verbindung mit einem überlasteten Cluster, werden Sie möglicherweise von der Element UI abgemeldet, wenn das System nicht schnell genug auf API-Anfragen in der Warteschlange reagiert. Wenn Sie zum Abmeldebildschirm umgeleitet werden, können Sie sich erneut anmelden, nachdem Sie eine erste Browser-Authentifizierungsaufforderung abgesagt haben. Wenn Sie zur Übersichtsseite zurückkehren, werden Sie möglicherweise nach Cluster-Anmeldedaten gefragt, wenn diese nicht vom Browser gespeichert werden.

Symbole in der Element-Schnittstelle

Die NetApp Element-Softwareoberfläche zeigt Symbole an, die Aktionen darstellen, die Sie für Systemressourcen ergreifen können.

Folgende Tabelle enthält eine Kurzübersicht:

Symbol	Beschreibung
	Aktionen
	Backup auf
	Klon oder Kopie
	Löschen oder löschen
	Bearbeiten

	Filtern
	Paar
	Aktualisierung
	Wiederherstellen
	Wiederherstellen von
	Rollback
	Snapshot

Feedback mitteilen

Sie können die Webbenutzeroberfläche der Element Software verbessern und alle UI-Probleme beheben, indem Sie das Feedback-Formular verwenden, das über die gesamte Benutzeroberfläche zugänglich ist.

1. Klicken Sie auf einer beliebigen Seite in der Element UI auf die Schaltfläche **Feedback**.
2. Geben Sie relevante Informationen in die Felder Zusammenfassung und Beschreibung ein.
3. Fügen Sie hilfreiche Screenshots an.
4. Geben Sie einen Namen und eine E-Mail-Adresse ein.
5. Aktivieren Sie das Kontrollkästchen, um Daten zu Ihrer aktuellen Umgebung einzuschließen.
6. Klicken Sie Auf **Absenden**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konten verwalten

In SolidFire Storage-Systemen können Mandanten Konten verwenden, um Clients eine Verbindung zu Volumes in einem Cluster zu ermöglichen. Wenn Sie ein Volume erstellen, wird es einem bestimmten Konto zugewiesen. Sie können auch Cluster-

Administratorkonten für ein SolidFire Storage-System verwalten.

- "Arbeiten Sie mit Konten, die CHAP verwenden"
- "Verwalten von Benutzerkonten für Cluster-Administratoren"

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Arbeiten Sie mit Konten, die CHAP verwenden

In SolidFire Storage-Systemen können Mandanten Konten verwenden, um Clients eine Verbindung zu Volumes in einem Cluster zu ermöglichen. Ein Konto enthält die CHAP-Authentifizierung (Challenge-Handshake Authentication Protocol), die für den Zugriff auf die ihm zugewiesenen Volumes erforderlich ist. Wenn Sie ein Volume erstellen, wird es einem bestimmten Konto zugewiesen.

Einem Konto können bis zu zweitausend Volumes zugewiesen sein, ein Volume kann jedoch nur zu einem Konto gehören.

Erstellen Sie ein Konto

Sie können ein Konto erstellen, um den Zugriff auf Volumes zu ermöglichen.

Jeder Kontoname im System muss eindeutig sein.

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie Auf **Konto Erstellen**.
3. Geben Sie einen **Benutzername** ein.
4. Geben Sie im Abschnitt **CHAP-Einstellungen** die folgenden Informationen ein:

   Lassen Sie die Felder für Anmeldeinformationen leer, um ein Kennwort automatisch zu generieren.

   - **Initiatorschlüssel** für CHAP-Knoten-Session-Authentifizierung.
   - **Target Secret** für CHAP-Knoten-Session-Authentifizierung.
5. Klicken Sie Auf **Konto Erstellen**.

Kontodetails anzeigen

Sie können Leistungsaktivitäten für einzelne Konten in einem grafischen Format anzeigen.

Die Diagramminformationen liefern I/O- und Durchsatzinformationen für das Konto. Die Aktivitätslevel der durchschnittlichen und Spitzenwerte werden in Schritten von 10 Sekunden angezeigt. Diese Statistiken enthalten Aktivitäten für alle Volumes, die dem Konto zugewiesen sind.

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie auf das Symbol Aktionen für ein Konto.

3. Klicken Sie Auf **Details Anzeigen**.

Hier sind einige Details:

- **Status**: Der Status des Kontos. Mögliche Werte:
  - Aktiv: Ein aktives Konto.
  - Gesperrt: Ein gesperrtes Konto.
  - Entfernt: Ein Konto, das gelöscht und gelöscht wurde.
- **Aktive Volumes**: Die Anzahl der aktiven Volumes, die dem Konto zugewiesen sind.
- **Komprimierung**: Die Komprimierungs-Effizienzbewertung für die dem Konto zugewiesenen Volumes.
- **Deduplizierung**: Die Deduplizierungs-Effizienzbewertung für die Volumes, die dem Account zugewiesen sind.
- **Thin Provisioning**: Die Thin Provisioning-Effizienzbewertung für die dem Konto zugewiesenen Volumes.
- **Gesamteffizienz**: Die Gesamteffizienz-Punktzahl für die dem Account zugewiesenen Volumes.

Bearbeiten Sie ein Konto

Sie können ein Konto bearbeiten, um den Status zu ändern, die CHAP-Schlüssel zu ändern oder den Kontonamen zu ändern.

Das Ändern von CHAP-Einstellungen in einem Konto oder das Entfernen von Initiatoren oder Volumes aus einer Zugriffsgruppe kann dazu führen, dass Initiatoren unerwartet den Zugriff auf Volumes verlieren. Um zu überprüfen, ob der Volume-Zugriff nicht unerwartet verloren geht, loggen Sie sich immer iSCSI-Sitzungen aus, die von einer Konto- oder Zugriffsgruppenänderung betroffen sind, und überprüfen Sie, ob die Initiatoren nach Abschluss der Änderungen an den Initiatoreinstellungen und den Cluster-Einstellungen eine Verbindung zu Volumes herstellen können.

> Persistente Volumes, die mit Managementservices verknüpft sind, werden einem neuen Konto zugewiesen, das während der Installation oder Aktualisierung erstellt wird. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie das zugehörige Konto nicht.

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie auf das Symbol Aktionen für ein Konto.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. **Optional:** Bearbeiten Sie den **Benutzername**.
5. **Optional:** Klicken Sie auf die Dropdown-Liste **Status** und wählen Sie einen anderen Status aus.

> Wenn Sie den Status auf **gesperrt** ändern, werden alle iSCSI-Verbindungen zum Konto beendet, und das Konto kann nicht mehr aufgerufen werden. Volumes, die mit dem Konto verbunden sind, werden gepflegt. Die Volumes können jedoch nicht über iSCSI erkannt werden.

6. **Optional:** Bearbeiten Sie unter **CHAP-Einstellungen** die Anmeldeinformationen **Initiator Secret** und **Target Secret** für die Knotensitzauthentifizierung.

Wenn Sie die **CHAP-Einstellungen**-Anmeldeinformationen nicht ändern, bleiben diese unverändert. Wenn Sie die Felder für die Anmeldeinformationen leer lassen, generiert das System neue Passwörter.

7. Klicken Sie Auf **Änderungen Speichern**.

Löschen Sie ein Konto

Sie können ein Konto löschen, wenn es nicht mehr benötigt wird.

Löschen und löschen Sie alle Volumes, die mit dem Konto verknüpft sind, bevor Sie das Konto löschen.

Persistente Volumes, die mit Managementservices verknüpft sind, werden einem neuen Konto zugewiesen, das während der Installation oder Aktualisierung erstellt wird. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie das zugehörige Konto nicht.

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie auf das Aktionen-Symbol für das Konto, das Sie löschen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.
4. Bestätigen Sie die Aktion.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Verwalten von Benutzerkonten für Cluster-Administratoren

Sie können Cluster-Administratorkonten für ein SolidFire-Speichersystem verwalten, indem Sie Cluster-Administratorkonten erstellen, löschen und bearbeiten, das Kennwort für den Cluster-Administrator ändern und LDAP-Einstellungen konfigurieren, um den Systemzugriff für Benutzer zu verwalten.

Kontotypen für Storage-Cluster-Administratoren

In einem Storage-Cluster mit NetApp Element Software können zwei Arten von Administratorkonten vorhanden sein: Das primäre Cluster-Administratorkonto und ein Cluster-Administratorkonto.

- **Primary Cluster Administrator Account**

  Dieses Administratorkonto wird erstellt, wenn das Cluster erstellt wird. Dieses Konto ist das primäre administrative Konto mit der höchsten Zugriffsebene auf das Cluster. Dieses Konto ist analog zu einem Root-Benutzer in einem Linux-System. Sie können das Kennwort für dieses Administratorkonto ändern.

- **Cluster-Administratorkonto**

  Sie können einem Cluster-Administratorkonto einen begrenzten administrativen Zugriff gewähren, um bestimmte Aufgaben in einem Cluster auszuführen. Die jedem Cluster-Administratorkonto zugewiesenen Zugangsdaten werden zur Authentifizierung von API- und Element-UI-Anforderungen innerhalb des Storage-Systems verwendet.

Ein lokales (nicht-LDAP)-Cluster-Administratorkonto ist erforderlich, um über die UI pro Node auf aktive Knoten in einem Cluster zuzugreifen. Kontoanmeldeinformationen sind für den Zugriff auf einen Node, der noch nicht Teil eines Clusters ist, nicht erforderlich.

Zeigen Sie Details zum Cluster-Administrator an

1. So erstellen Sie ein Cluster-weites (nicht-LDAP)-Cluster-Administratorkonto:
   a. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
2. Auf der Seite Cluster-Administratoren auf der Registerkarte Benutzer können Sie die folgenden Informationen anzeigen:
   - **ID**: Dem Cluster Administrator Konto zugewiesene sequentielle Nummer.
   - **Benutzername**: Der Name, der dem Cluster Administrator-Konto bei der Erstellung gegeben wurde.
   - **Zugriff**: Die dem Benutzerkonto zugewiesenen Benutzerberechtigungen. Mögliche Werte:
     - Lesen
     - Berichterstellung
     - Knoten
     - Laufwerke
     - Volumes
     - Konten
     - Clusteradministratoren
     - Verwalter

     Alle Berechtigungen sind für den Zugriffstyp des Administrators verfügbar.
   - **Typ**: Der Typ des Clusteradministrators. Mögliche Werte:
     - Cluster
     - Ldap
   - **Attributes**: Wenn das Cluster-Administratorkonto mit der Element API erstellt wurde, zeigt diese Spalte alle Name-Wert-Paare an, die mit dieser Methode festgelegt wurden.

     Siehe "NetApp Element Software-API-Referenz".

Erstellen eines Cluster-Administratorkontos

Sie können neue Cluster-Administratorkonten mit Berechtigungen erstellen, um den Zugriff auf bestimmte Bereiche des Storage-Systems zu ermöglichen oder einzuschränken. Wenn Sie Berechtigungen für ein Cluster-Administratorkonto festlegen, gewährt das System schreibgeschützte Rechte für alle Berechtigungen, die Sie dem Cluster-Administrator nicht zuweisen.

Wenn Sie ein LDAP-Cluster-Administratorkonto erstellen möchten, stellen Sie sicher, dass LDAP auf dem Cluster konfiguriert ist, bevor Sie beginnen.

"Aktivieren Sie die LDAP-Authentifizierung über die Benutzeroberfläche von Element"

Sie können später Berechtigungen für Cluster-Administratorkonten für Berichterstellung, Nodes, Laufwerke, Volumes, Konten, Und Cluster-Level-Zugriff. Wenn Sie eine Berechtigung aktivieren, weist das System

Schreibzugriff für diese Ebene zu. Das System gewährt dem Administrator-Benutzer schreibgeschützten Zugriff für die Ebenen, die Sie nicht auswählen.

Sie können auch ein vom Systemadministrator erstelltes Cluster-Administratorkonto später entfernen. Sie können das primäre Cluster-Administratorkonto, das beim Erstellen des Clusters erstellt wurde, nicht entfernen.

1. So erstellen Sie ein Cluster-weites (nicht-LDAP)-Cluster-Administratorkonto:
   a. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
   b. Klicken Sie Auf **Cluster-Admin Erstellen**.
   c. Wählen Sie den Benutzertyp **Cluster** aus.
   d. Geben Sie einen Benutzernamen und ein Kennwort für das Konto ein und bestätigen Sie das Passwort.
   e. Wählen Sie Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
   f. Aktivieren Sie das Kontrollkästchen, um der Endnutzer-Lizenzvereinbarung zuzustimmen.
   g. Klicken Sie Auf **Cluster-Admin Erstellen**.
2. So erstellen Sie ein Cluster-Administratorkonto im LDAP-Verzeichnis:
   a. Klicken Sie auf **Cluster** > **LDAP**.
   b. Stellen Sie sicher, dass die LDAP-Authentifizierung aktiviert ist.
   c. Klicken Sie auf **Benutzerauthentifizierung testen** und kopieren Sie den Distinguished Name, der für den Benutzer oder eine der Gruppen angezeigt wird, deren Mitglied der Benutzer ist, damit Sie ihn später einfügen können.
   d. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
   e. Klicken Sie Auf **Cluster-Admin Erstellen**.
   f. Wählen Sie den LDAP-Benutzertyp aus.
   g. Befolgen Sie im Feld Distinguished Name das Beispiel im Textfeld, um einen vollständigen Distinguished Name für den Benutzer oder die Gruppe einzugeben. Alternativ können Sie ihn aus dem Distinguished Name einfügen, den Sie früher kopiert haben.

      Wenn der Distinguished Name Teil einer Gruppe ist, hat jeder Benutzer, der Mitglied dieser Gruppe auf dem LDAP-Server ist, Berechtigungen für dieses Administratorkonto.

   Um LDAP Cluster Admin-Benutzer oder -Gruppen hinzuzufügen, lautet das allgemeine Format des Benutzernamens „`LDAP:<Full Distinguished Name>`“.

   a. Wählen Sie Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
   b. Aktivieren Sie das Kontrollkästchen, um der Endnutzer-Lizenzvereinbarung zuzustimmen.
   c. Klicken Sie Auf **Cluster-Admin Erstellen**.

Berechtigungen für Cluster-Administratoren bearbeiten

Sie können die Berechtigungen für Cluster-Administratorkonten für Berichterstellung, Nodes, Laufwerke, Volumes, Konten, Und Cluster-Level-Zugriff. Wenn Sie eine Berechtigung aktivieren, weist das System Schreibzugriff für diese Ebene zu. Das System gewährt dem Administrator-Benutzer schreibgeschützten Zugriff für die Ebenen, die Sie nicht auswählen.

1. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
2. Klicken Sie auf das Symbol Aktionen für den Cluster-Administrator, den Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Wählen Sie Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
5. Klicken Sie Auf **Änderungen Speichern**.

Ändern Sie Passwörter für Cluster-Administratorkonten

Mithilfe der Element-UI können Sie die Kennwörter für den Cluster-Administrator ändern.

1. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
2. Klicken Sie auf das Symbol Aktionen für den Cluster-Administrator, den Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Geben Sie im Feld Passwort ändern ein neues Passwort ein und bestätigen Sie es.
5. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

- "Aktivieren Sie die LDAP-Authentifizierung über die Benutzeroberfläche von Element"
- "Deaktivieren Sie LDAP"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

LDAP verwalten

Sie können das Lightweight Directory Access Protocol (LDAP) einrichten, um eine sichere, Verzeichnisbasierte Anmeldefunktion für den SolidFire-Speicher zu ermöglichen. Sie können LDAP auf Clusterebene konfigurieren und LDAP-Benutzer und -Gruppen autorisieren.

Zum Verwalten von LDAP wird die LDAP-Authentifizierung auf einem SolidFire-Cluster unter Verwendung einer vorhandenen Microsoft Active Directory-Umgebung eingerichtet und die Konfiguration getestet.

Sie können IPv4- und IPv6-Adressen verwenden.

Die Aktivierung von LDAP umfasst die folgenden grundlegenden Schritte, die im Detail beschrieben werden:

1. * Vorkonfigurationsschritte für LDAP-Unterstützung durchführen*. Stellen Sie sicher, dass Sie über alle erforderlichen Details zur Konfiguration der LDAP-Authentifizierung verfügen.
2. **LDAP-Authentifizierung aktivieren**. Verwenden Sie entweder die Element-UI oder die Element-API.
3. **Validierung der LDAP-Konfiguration**. Überprüfen Sie optional, ob der Cluster mit den richtigen Werten konfiguriert ist, indem Sie die GetLdapConfiguration API-Methode ausführen oder die LCAP-Konfiguration über die Element-UI prüfen.
4. **Testen Sie die LDAP-Authentifizierung** (mit dem `readonly` Benutzer). Überprüfen Sie, ob die LDAP-Konfiguration korrekt ist, indem Sie die TestLdapAuthentication API-Methode oder die Element-UI ausführen. Verwenden Sie für diesen ersten Test den Benutzernamen “sAMAccountName” des `readonly`

Benutzer: Dadurch wird überprüft, ob Ihr Cluster für die LDAP-Authentifizierung richtig konfiguriert ist, und es wird auch überprüft, dass die `readonly` Anmeldedaten und Zugriff sind korrekt. Wenn dieser Schritt fehlschlägt, wiederholen Sie die Schritte 1 bis 3.

5. **Testen Sie die LDAP-Authentifizierung** (mit einem Benutzerkonto, das Sie hinzufügen möchten). Wiederholen Sie setp 4 mit einem Benutzerkonto, das Sie als Element Cluster-Administrator hinzufügen möchten. Kopieren Sie die `distinguished` Name (DN) oder der Benutzer (oder die Gruppe). Dieser DN wird in Schritt 6 verwendet.
6. **Fügen Sie den LDAP-Cluster-Admin** hinzu (kopieren Sie den DN aus dem Test-LDAP-Authentifizierungsschritt und fügen Sie ihn ein). Erstellen Sie mit der Element UI oder der AddLdapClusterAdmin API-Methode einen neuen Cluster-Admin-Benutzer mit der entsprechenden Zugriffsebene. Fügen Sie für den Benutzernamen den vollständigen DN ein, den Sie in Schritt 5 kopiert haben. Dadurch wird sichergestellt, dass der DN korrekt formatiert ist.
7. **Testen Sie den Cluster-Administratorzugriff**. Loggen Sie sich mit dem neu erstellten LDAP-Cluster-Admin-Benutzer beim Cluster ein. Wenn Sie eine LDAP-Gruppe hinzugefügt haben, können Sie sich als jeder Benutzer dieser Gruppe anmelden.

Führen Sie die Schritte zur Vorkonfiguration für die LDAP-Unterstützung durch

Bevor Sie die LDAP-Unterstützung in Element aktivieren, sollten Sie einen Windows Active Directory-Server einrichten und weitere Vorkonfigurationsaufgaben durchführen.

Schritte

1. Richten Sie einen Windows Active Directory-Server ein.
2. **Optional:** LDAPS-Support aktivieren.
3. Erstellen von Benutzern und Gruppen
4. Erstellen Sie ein schreibgeschütztes Dienstkonto (z. B. „`sfReadonly`“), das für das Durchsuchen des LDAP-Verzeichnisses verwendet werden soll.

Aktivieren Sie die LDAP-Authentifizierung über die Benutzeroberfläche von Element

Sie können die Integration des Speichersystems mit einem vorhandenen LDAP-Server konfigurieren. Dies ermöglicht LDAP-Administratoren ein zentrales Management des Speichersystemzugriffs für Benutzer.

Sie können LDAP entweder mit der Element-Benutzeroberfläche oder der Element-API konfigurieren. In diesem Verfahren wird beschrieben, wie LDAP über die Element-UI konfiguriert wird.

Dieses Beispiel zeigt, wie die LDAP-Authentifizierung auf SolidFire konfiguriert und verwendet wird `SearchAndBind` Als Authentifizierungstyp. Das Beispiel verwendet einen einzelnen Windows Server 2012 R2 Active Directory Server.

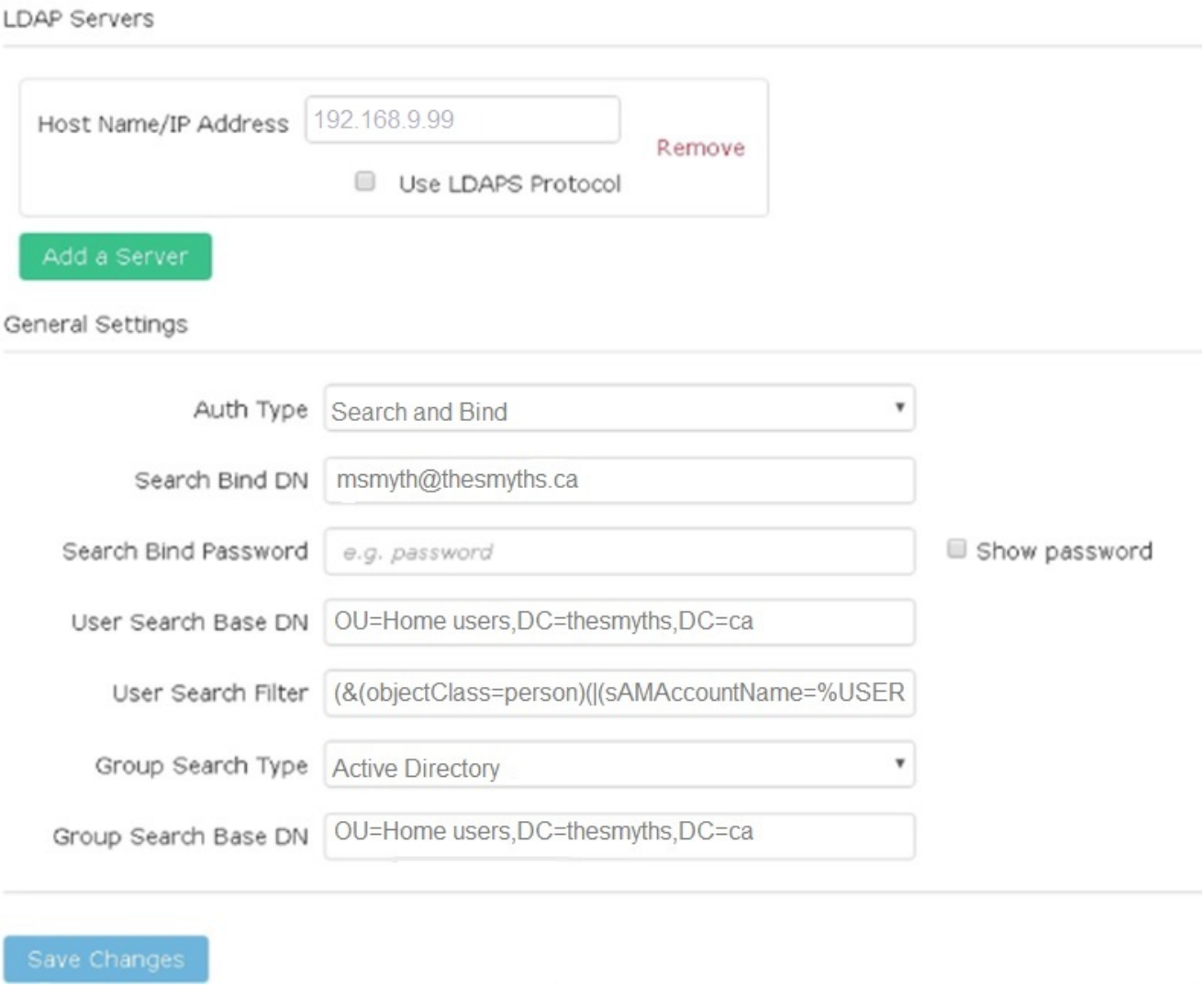
Schritte

1. Klicken Sie auf **Cluster** > **LDAP**.
2. Klicken Sie auf **Ja**, um die LDAP-Authentifizierung zu aktivieren.
3. Klicken Sie auf **Server hinzufügen**.
4. Geben Sie die * Hostname/IP-Adresse* ein.

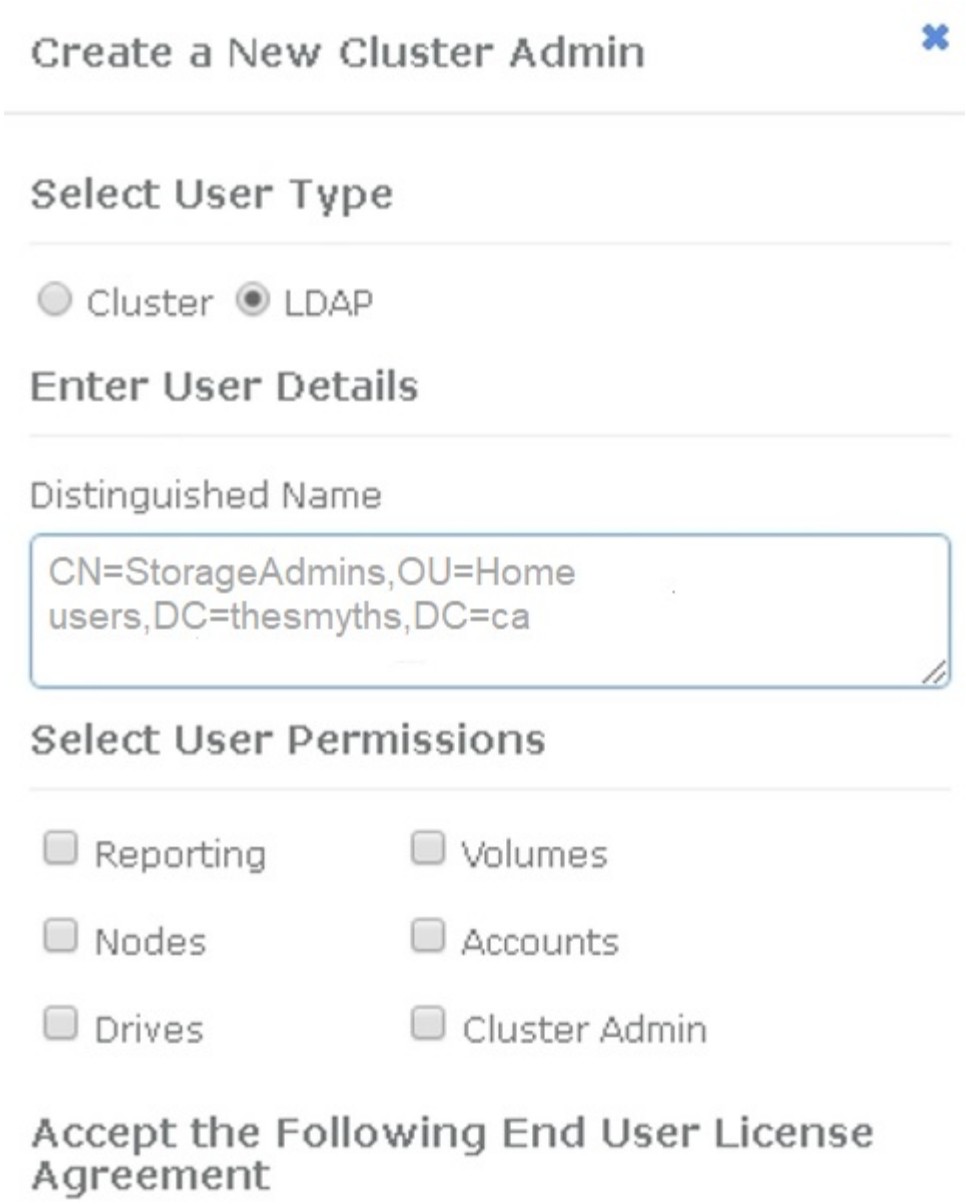
   Es kann auch eine optionale benutzerdefinierte Portnummer eingegeben werden.

   Wenn Sie beispielsweise eine benutzerdefinierte Portnummer hinzufügen möchten, geben Sie <Host Name oder ip-Adresse>:<Port number> ein

5. **Optional:** Wählen Sie **LDAPS-Protokoll verwenden**.
6. Geben Sie die erforderlichen Informationen unter **Allgemeine Einstellungen** ein.



7. Klicken Sie auf **LDAP aktivieren**.
8. Klicken Sie auf **Benutzerauthentifizierung testen**, wenn Sie den Serverzugriff für einen Benutzer testen möchten.
9. Kopieren Sie den Distinguished Name und Benutzergruppeninformationen, die später beim Erstellen von Cluster-Administratoren angezeigt werden.
10. Klicken Sie auf **Änderungen speichern**, um neue Einstellungen zu speichern.
11. Um einen Benutzer in dieser Gruppe zu erstellen, damit sich jeder anmelden kann, führen Sie Folgendes aus:
    a. Klicken Sie Auf **Benutzer** > **Ansicht**.



b. Klicken Sie für den neuen Benutzer auf **LDAP** für den Benutzertyp, und fügen Sie die Gruppe ein, die Sie in das Feld Distinguished Name kopiert haben.
c. Wählen Sie die Berechtigungen aus, normalerweise alle Berechtigungen.
d. Scrollen Sie nach unten zur Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Ich akzeptiere**.
e. Klicken Sie Auf **Cluster-Admin Erstellen**.

   Jetzt haben Sie einen Benutzer mit dem Wert einer Active Directory-Gruppe.

Um dies zu testen, melden Sie sich von der Element UI ab und melden Sie sich als Benutzer in dieser Gruppe an.

Aktivieren Sie die LDAP-Authentifizierung mit der Element API

Sie können die Integration des Speichersystems mit einem vorhandenen LDAP-Server konfigurieren. Dies ermöglicht LDAP-Administratoren ein zentrales Management des Speichersystemzugriffs für Benutzer.

Sie können LDAP entweder mit der Element-Benutzeroberfläche oder der Element-API konfigurieren. In

diesem Verfahren wird beschrieben, wie LDAP mithilfe der Element-API konfiguriert wird.

Um die LDAP-Authentifizierung auf einem SolidFire-Cluster zu nutzen, aktivieren Sie zuerst die LDAP-Authentifizierung auf dem Cluster mithilfe der `EnableLdapAuthentication` API-Methode.

Schritte

1. Aktivieren Sie die LDAP-Authentifizierung zuerst auf dem Cluster mithilfe des `EnableLdapAuthentication` API-Methode.
2. Geben Sie die erforderlichen Informationen ein.

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. Ändern Sie die Werte der folgenden Parameter:

Verwendete Parameter	Beschreibung
AuthType: SearchAndBind	Gibt an, dass der Cluster das Readonly-Dienstkonto verwendet, um zuerst nach dem authentifizierten Benutzer zu suchen und diesen Benutzer anschließend zu binden, wenn er gefunden und authentifiziert wurde.
GroupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Gibt den Speicherort in der LDAP-Struktur an, der mit der Suche nach Gruppen beginnt. In diesem Beispiel haben wir die Wurzel unseres Baumes verwendet. Wenn Ihr LDAP-Baum sehr groß ist, sollten Sie diesen auf eine granularere Unterstruktur setzen, um die Suchzeiten zu verkürzen.

Verwendete Parameter	Beschreibung
UserSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Gibt den Speicherort in der LDAP-Struktur an, der mit der Suche nach Benutzern beginnt. In diesem Beispiel haben wir die Wurzel unseres Baumes verwendet. Wenn Ihr LDAP-Baum sehr groß ist, sollten Sie diesen auf eine granularere Unterstruktur setzen, um die Suchzeiten zu verkürzen.
GroupSearchType: ActiveDirectory	Verwendet den Windows Active Directory-Server als LDAP-Server.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Um den userPrincipalName (E-Mail-Adresse für die Anmeldung) zu verwenden, können Sie den Suchfilter folgendermaßen ändern:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
Oder, um sowohl userPrincipalName als auch sAMAccountName zu suchen, können Sie den folgenden BenutzerSearchFilter verwenden:
 	
`"(&(objectClass=person)(`
	(SAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))“ ----

Nutzt den sAMAccountName als unseren Benutzernamen für die Anmeldung beim SolidFire-Cluster. Diese Einstellungen weisen LDAP darauf hin, nach dem bei der Anmeldung im sAMAccountName angegebenen Benutzernamen zu suchen und die Suche auch auf Einträge zu beschränken, die “Person” als Wert im objectClass-Attribut haben.	SuchhinBindDN
Dies ist der Distinguished Name of Readonly user, der für die Suche nach dem LDAP-Verzeichnis verwendet wird. Für Active Directory ist es in der Regel am einfachsten, den userPrincipalName (E-Mail-Adressformat) für den Benutzer zu verwenden.	SucheBindPasswort

Um dies zu testen, melden Sie sich von der Element UI ab und melden Sie sich als Benutzer in dieser Gruppe an.

LDAP-Details anzeigen

Zeigen Sie LDAP-Informationen auf der LDAP-Seite auf der Registerkarte Cluster an.

Sie müssen LDAP aktivieren, um diese LDAP-Konfigurationseinstellungen anzuzeigen.

1. Um LDAP-Details mit der Element UI anzuzeigen, klicken Sie auf **Cluster** > **LDAP**.
   - **Hostname/IP-Adresse**: Adresse eines LDAP- oder LDAPS-Verzeichnisservers.
   - **Auth Typ**: Die Benutzerauthentifizierungsmethode. Mögliche Werte:
     - Direct Bind
     - Suche Und Bindung
   - **Suche Bind DN**: Ein vollständig qualifizierter DN zur Anmeldung bei, um eine LDAP-Suche für den Benutzer durchzuführen (benötigt Bindeebene-Zugriff auf das LDAP-Verzeichnis).
   - **Suche Bind Password**: Passwort zur Authentifizierung des Zugriffs auf den LDAP-Server.
   - **Basis-DN der Benutzersuche**: Der Basis-DN des Baums, der zum Starten der Benutzersuche verwendet wird. Das System sucht die Unterstruktur vom angegebenen Speicherort aus.
   - **User Search Filter**: Geben Sie unter Verwendung Ihres Domainnamens Folgendes ein:

     ```
     (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
     ```

   - **Gruppenkuchsart**: Suchart, die den verwendeten Standardfilter für die Gruppensuche steuert. Mögliche Werte:
     - Active Directory: Verschachtelte Mitgliedschaft aller LDAP-Gruppen eines Benutzers.
     - Keine Gruppen: Keine Gruppenunterstützung.
     - Mitglied-DN: Gruppen im Mitgliedsstil (Einzelebene).
   - **Gruppensuche Basis-DN**: Der Basis-DN des Baumes, der zum Starten der Gruppensuche verwendet wird. Das System sucht die Unterstruktur vom angegebenen Speicherort aus.
   - **Benutzerauthentifizierung testen**: Nachdem LDAP konfiguriert ist, testen Sie den Benutzernamen und die Passwort-Authentifizierung für den LDAP-Server. Geben Sie ein Konto ein, das bereits vorhanden ist, um dies zu testen. Der Distinguished Name und Benutzergruppeninformationen werden angezeigt, die Sie beim Erstellen von Cluster-Administratoren kopieren können.

Testen Sie die LDAP-Konfiguration

Nach der Konfiguration von LDAP sollten Sie es entweder mit der Element-UI oder der Element-API testen `TestLdapAuthentication` Methode.

Schritte

1. So testen Sie die LDAP-Konfiguration mit der Element UI:
   a. Klicken Sie auf **Cluster** > **LDAP**.
   b. Klicken Sie auf **LDAP-Authentifizierung testen**.
   c. Lösen Sie Probleme, indem Sie die Informationen in der folgenden Tabelle verwenden:

Fehlermeldung	Beschreibung
`xLDAPUserNotFound`	• Der zu testenden Benutzer wurde im konfigurierten nicht gefunden `userSearchBaseDN` Unterbaum. • Der `userSearchFilter` Ist falsch konfiguriert.
`xLDAPBindFailed (Error: Invalid credentials)`	• Der getestete Benutzername ist ein gültiger LDAP-Benutzer, aber das angegebene Passwort ist falsch. • Der getestete Benutzername ist ein gültiger LDAP-Benutzer, das Konto ist jedoch derzeit deaktiviert.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	Der LDAP-Server-URI ist falsch.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Der schreibgeschützte Benutzername oder das Kennwort ist falsch konfiguriert.
`xLDAPSearchFailed (Error: No such object)`	Der `userSearchBaseDN` Ist kein gültiger Speicherort innerhalb der LDAP-Struktur.
`xLDAPSearchFailed (Error: Referral)`	• Der `userSearchBaseDN` Ist kein gültiger Speicherort innerhalb der LDAP-Struktur. • Der `userSearchBaseDN` Und `groupSearchBaseDN` Befinden sich in einer geschachtelten Organisationseinheit. Dies kann zu Berechtigungsproblemen führen. Die Problemumgehung besteht darin, die Organisationseinheit in die Benutzer- und Gruppenbasis-DN-Einträge einzubeziehen (z. B.: `ou=storage, cn=company, cn=com`)

2. So testen Sie die LDAP-Konfiguration mit der Element API:
   a. Rufen Sie die TestLdapAuthentication-Methode auf.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

b. Überprüfen Sie die Ergebnisse. Wenn der API-Aufruf erfolgreich ist, enthalten die Ergebnisse den Distinguished Name des angegebenen Benutzers sowie eine Liste der Gruppen, in denen der Benutzer Mitglied ist.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

Deaktivieren Sie LDAP

Sie können die LDAP-Integration über die Element-UI deaktivieren.

Bevor Sie beginnen, sollten Sie alle Konfigurationseinstellungen beachten, da die Deaktivierung von LDAP alle Einstellungen löscht.

Schritte

1. Klicken Sie auf **Cluster** > **LDAP**.
2. Klicken Sie Auf **Nein**.
3. Klicken Sie auf **LDAP deaktivieren**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Management des Systems

Sie können Ihr System in der Element UI verwalten. Dies ermöglicht die Multi-Faktor-

Authentifizierung, das Managen von Cluster-Einstellungen, unterstützt FIPS (Federal Information Processing Standards) und nutzt externes Verschlüsselungsmanagement.

- "Multi-Faktor-Authentifizierung aktivieren"
- "Konfigurieren Sie Cluster-Einstellungen"
- "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt"
- "Erste Schritte mit externem Verschlüsselungsmanagement"

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Multi-Faktor-Authentifizierung aktivieren

Multi-Faktor-Authentifizierung (MFA) verwendet zum Verwalten von Benutzersitzungen einen Drittanbieter-Identitätsanbieter (IdP) über die Security Assertion Markup Language (SAML). MFA ermöglicht Administratoren, zusätzliche Authentifizierungsfaktoren wie Passwort und Textnachricht, Kennwort und E-Mail-Nachricht nach Bedarf zu konfigurieren.

Richten Sie die Multi-Faktor-Authentifizierung ein

Sie können diese grundlegenden Schritte über die Element API verwenden, um Ihr Cluster zur Multi-Faktor-Authentifizierung einzurichten.

Details zu jeder API-Methode finden Sie im "Element-API-Referenz".

1. Erstellen Sie eine neue IdP-Konfiguration (Identity Provider) eines Drittanbieters für das Cluster, indem Sie die folgende API-Methode aufrufen und die IdP-Metadaten im JSON-Format übergeben: `CreateIdpConfiguration`

   IDP-Metadaten werden im Klartextformat aus dem Drittanbieter-IdP abgerufen. Diese Metadaten müssen validiert werden, um sicherzustellen, dass sie korrekt in JSON formatiert sind. Es stehen zahlreiche JSON-Formatierer-Anwendungen zur Verfügung, die Sie verwenden können, z. B.:https://freeformatter.com/json-escape.html.

2. Abrufen der Cluster-Metadaten über sMetadataUrl, um Daten in die IdP eines Drittanbieters zu kopieren, indem Sie die folgende API-Methode aufrufen: `ListIdpConfigurations`

   SpMetadataUrl ist eine URL, mit der die Metadaten des Dienstanbieters für das IdP aus dem Cluster abgerufen werden, um eine Vertrauensbeziehung aufzubauen.

3. Konfigurieren Sie die SAML-Behauptungen auf dem IdP eines Drittanbieters so, dass das Attribut „ `NameID`“ verwendet wird, dass ein Benutzer für die Prüfprotokollierung eindeutig identifiziert wird und dass Single Logout ordnungsgemäß funktioniert.
4. Erstellen Sie ein oder mehrere Cluster-Administrator-Benutzerkonten, die von einem Drittanbieter-IdP zur Autorisierung authentifiziert wurden, indem Sie die folgende API-Methode aufrufen:`AddIdpClusterAdmin`

Der Benutzername für den IdP-Clusteradministrator muss mit dem SAML-Attribut Name/Wert-Mapping für den gewünschten Effekt übereinstimmen, wie in den folgenden Beispielen dargestellt:

- Email=bob@company.com — wobei das IdP so konfiguriert ist, dass es eine E-Mail-Adresse in den SAML-Attributen gibt.
- Group=Cluster-Administrator - wobei das IdP so konfiguriert ist, dass es eine Gruppeneigenschaft freigibt, in der alle Benutzer Zugriff haben sollen. Beachten Sie, dass die Paarung des SAML-Attributs Name/Wert zwischen Groß- und Kleinschreibung und Sicherheit beachtet wird.

5. MFA für das Cluster aktivieren, indem Sie die folgende API-Methode aufrufen: `EnableIdpAuthentication`

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Zusätzliche Informationen für Multi-Faktor-Authentifizierung

Beachten Sie die folgenden Einschränkungen bei der Multi-Faktor-Authentifizierung.

- Um nicht mehr gültige IdP-Zertifikate zu aktualisieren, müssen Sie einen nicht-IdP-Admin-Benutzer verwenden, um die folgende API-Methode aufrufen zu können: `UpdateIdpConfiguration`
- MFA ist nicht kompatibel mit Zertifikaten, die weniger als 2048 Bit lang sind. Standardmäßig wird auf dem Cluster ein 2048-Bit-SSL-Zertifikat erstellt. Sie sollten beim Aufruf der API-Methode vermeiden, ein kleineres Zertifikat einzurichten: `SetSSLCertificate`

Wenn das Cluster ein Zertifikat verwendet, das vor dem Upgrade weniger als 2048-Bit enthält, muss das Cluster-Zertifikat nach dem Upgrade auf Element 12.0 oder höher mit einem Zertifikat von mindestens 2048 Bit aktualisiert werden.

- IDP Admin-Benutzer können nicht dazu verwendet werden, API-Aufrufe direkt (beispielsweise über SDKs oder Postman) zu tätigen oder andere Integrationen (z. B. OpenStack Cinder oder vCenter Plug-in) zu verwenden. Fügen Sie entweder LDAP-Cluster-Administratorbenutzer oder lokale Cluster-Admin-Benutzer hinzu, wenn Sie Benutzer mit diesen Fähigkeiten erstellen müssen.

Weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konfigurieren Sie Cluster-Einstellungen

Sie können die Einstellungen für das gesamte Cluster anzeigen und ändern und Cluster-spezifische Aufgaben über die Registerkarte Cluster der Element UI ausführen.

Sie können Einstellungen wie den Schwellenwert für die Clusterfülle konfigurieren, Zugriff, Verschlüsselung im Ruhezustand, virtuelle Volumes, SnapMirror, Und NTP-Broadcast-Client.

Optionen

- Arbeiten mit virtuellen Volumes
- SnapMirror Replizierung zwischen Element und ONTAP Clustern
- Legen Sie den Schwellenwert für den vollen Cluster fest
- Aktivieren und deaktivieren Sie den Zugriff auf den Support
- "Wie werden die BlockSpace Schwellenwerte für Element berechnet"
- Aktivieren und Deaktivieren der Verschlüsselung für ein Cluster
- Banner für Nutzungsbedingungen verwalten
- Konfigurieren Sie die Network Time Protocol-Server für das abzufragenden Cluster
- SNMP managen
- Verwalten Sie Laufwerke
- Managen von Nodes
- Managen Sie virtuelle Netzwerke
- Zeigen Sie Details zu Fibre Channel-Ports an

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Aktivieren und deaktivieren Sie die Verschlüsselung für ein Cluster im Ruhezustand

Mit SolidFire Clustern können Sie alle auf Cluster-Laufwerken gespeicherten Daten im Ruhezustand verschlüsseln. Sie können den Cluster-weiten Schutz von Self-Encrypting Drives (SED) mit beiden aktivieren "Hardware- oder softwarebasierte Verschlüsselung im Ruhezustand".

Die Hardware-Verschlüsselung im Ruhezustand wird über die Element UI oder API aktiviert. Die Aktivierung der Hardware-Verschlüsselung im Ruhezustand hat keine Auswirkungen auf die Performance und Effizienz des Clusters. Die Softwareverschlüsselung im Ruhezustand ist nur mit der Element API möglich.

Die hardwarebasierte Verschlüsselung für Daten im Ruhezustand ist bei der Cluster-Erstellung standardmäßig nicht aktiviert und kann von der Element UI aktiviert und deaktiviert werden.

> Bei SolidFire All-Flash-Storage-Clustern muss die Softwareverschlüsselung im Ruhezustand während der Cluster-Erstellung aktiviert sein und nach dem Erstellen des Clusters nicht deaktiviert werden können.

Was Sie benötigen

- Sie verfügen über Cluster-Administratorrechte zum Aktivieren oder Ändern von Verschlüsselungseinstellungen.
- Bei der hardwarebasierten Verschlüsselung im Ruhezustand haben Sie vor der Änderung von Verschlüsselungseinstellungen sichergestellt, dass sich das Cluster in einem ordnungsgemäßen Zustand befindet.
- Wenn Sie die Verschlüsselung deaktivieren, müssen zwei Knoten an einem Cluster teilnehmen, um auf den Schlüssel zuzugreifen, um die Verschlüsselung auf einem Laufwerk zu deaktivieren.

Überprüfen Sie den Status der Verschlüsselung im Ruhezustand

Mithilfe der können Sie den aktuellen Status der Verschlüsselung im Ruhezustand und/oder Softwareverschlüsselung im Ruhezustand auf dem Cluster anzeigen "GetClusterInfo" Methode. Sie können das verwenden "GetSoftwareVerschlüsselungAtRestInfo" Methode zum Abrufen von Informationen, die das Cluster verwendet, um Daten im Ruhezustand zu verschlüsseln.

Das UI-Dashboard der Element Software unter `https://<MVIP>/` Derzeit wird für hardwarebasierte Verschlüsselung nur die Verschlüsselung im Ruhezustand angezeigt.

Optionen

- Hardwarebasierte Verschlüsselung für Daten im Ruhezustand
- Softwarebasierte Verschlüsselung im Ruhezustand aktivieren
- Deaktivieren Sie die hardwarebasierte Verschlüsselung für Daten im Ruhezustand

Hardwarebasierte Verschlüsselung für Daten im Ruhezustand

Um die Verschlüsselung im Ruhezustand über eine externe Verschlüsselungsmanagementkonfiguration zu aktivieren, müssen Sie die Verschlüsselung im Ruhezustand über die aktivieren "API". Wenn Sie die Verwendung der Schaltfläche der vorhandenen Element-Benutzeroberfläche aktivieren, wird die Nutzung intern generierter Schlüssel wiederhergestellt.

1. Wählen Sie in der Element-UI die Option **Cluster** > **Einstellungen**.
2. Wählen Sie **Verschlüsselung im Ruhezustand aktivieren**.

Softwarebasierte Verschlüsselung im Ruhezustand aktivieren

Die Softwareverschlüsselung für Daten im Ruhezustand kann nicht deaktiviert werden, nachdem sie auf dem Cluster aktiviert ist.

1. Führen Sie während der Cluster-Erstellung den aus "Cluster-Methode erstellen" Mit `enableSoftwareEncryptionAtRest` Auf einstellen `true`.

Deaktivieren Sie die hardwarebasierte Verschlüsselung für Daten im Ruhezustand

1. Wählen Sie in der Element-UI die Option **Cluster** > **Einstellungen**.
2. Wählen Sie **Verschlüsselung im Ruhezustand deaktivieren**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Legen Sie den Schwellenwert für den vollen Cluster fest

Sie können die Ebene ändern, auf der das System eine Warnung zur Blockclusterfülle generiert, indem Sie die folgenden Schritte durchführen. Darüber hinaus können Sie die ModifyClusterFullThreshold API-Methode verwenden, um den Level zu ändern, auf dem das System eine Block- oder Metadaten-Warnung erzeugt.

Was Sie benötigen

Sie müssen über Administratorrechte für den Cluster verfügen.

Schritte

1. Klicken Sie Auf **Cluster** > **Einstellungen**.
2. Geben Sie im Abschnitt „Cluster Full Settings“ einen Prozentsatz in **Warnung anheben ein, wenn die Kapazität von _ % verbleibt, bevor Helix nach einem Node-Ausfall nicht wieder herstellen konnte**.
3. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

"Wie werden die BlockSpace Schwellenwerte für Element berechnet"

Aktivieren und deaktivieren Sie den Zugriff auf den Support

Sie können den Support-Zugriff für die Fehlerbehebung vorübergehend für den Zugriff von NetApp Support-Mitarbeitern auf Storage Nodes über SSH aktivieren.

Um den Support-Zugriff zu ändern, müssen Sie über Berechtigungen für Cluster-Administratoren verfügen.

1. Klicken Sie Auf **Cluster** > **Einstellungen**.
2. Geben Sie im Abschnitt Support-Zugriff aktivieren/deaktivieren die Dauer (in Stunden) ein, die Sie dem Support Zugriff gewähren möchten.
3. Klicken Sie Auf **Support-Zugriff Aktivieren**.
4. **Optional:** um den Support-Zugriff zu deaktivieren, klicken Sie auf **Support-Zugriff deaktivieren**.

Banner für Nutzungsbedingungen verwalten

Sie können ein Banner aktivieren, bearbeiten oder konfigurieren, das eine Nachricht für den Benutzer enthält.

Optionen

Aktivieren Sie das Banner für Nutzungsbedingungen Bearbeiten Sie den Banner für Nutzungsbedingungen Deaktivieren Sie den Banner für die Nutzungsbedingungen

Aktivieren Sie das Banner für Nutzungsbedingungen

Sie können ein Banner für Nutzungsbedingungen aktivieren, das angezeigt wird, wenn sich ein Benutzer bei der Element-Benutzeroberfläche anmeldet. Wenn der Benutzer auf das Banner klickt, wird ein Textfeld mit der für den Cluster konfigurierten Meldung angezeigt. Das Banner kann jederzeit abgewiesen werden.

Sie müssen über Berechtigungen für Cluster-Administratoren verfügen, um die Nutzungsbestimmungen aktivieren zu können.

1. Klicken Sie auf **Benutzer** > **Nutzungsbedingungen**.
2. Geben Sie im Formular **Nutzungsbedingungen** den Text ein, der für das Dialogfeld Nutzungsbedingungen angezeigt werden soll.

   Überschreiten Sie maximal 4096 Zeichen.

3. Klicken Sie Auf **Aktivieren**.

Bearbeiten Sie den Banner für Nutzungsbedingungen

Sie können den Text bearbeiten, den ein Benutzer sieht, wenn er das Anmeldebanner „Nutzungsbedingungen“ ausgewählt hat.

Was Sie benötigen

- Um die Nutzungsbedingungen zu konfigurieren, müssen Sie über Berechtigungen für Cluster-Administratoren verfügen.
- Stellen Sie sicher, dass die Funktion „Nutzungsbedingungen“ aktiviert ist.

Schritte

1. Klicken Sie auf **Benutzer** > **Nutzungsbedingungen**.
2. Bearbeiten Sie im Dialogfeld **Nutzungsbedingungen** den Text, der angezeigt werden soll.

   Überschreiten Sie maximal 4096 Zeichen.

3. Klicken Sie Auf **Änderungen Speichern**.

Deaktivieren Sie den Banner für die Nutzungsbedingungen

Sie können den Banner „Nutzungsbedingungen“ deaktivieren. Bei deaktiviertem Banner wird der Benutzer nicht mehr aufgefordert, die Nutzungsbedingungen bei Verwendung der Element-UI zu akzeptieren.

Was Sie benötigen

- Um die Nutzungsbedingungen zu konfigurieren, müssen Sie über Berechtigungen für Cluster-Administratoren verfügen.
- Stellen Sie sicher, dass die Nutzungsbedingungen aktiviert sind.

Schritte

1. Klicken Sie auf **Benutzer** > **Nutzungsbedingungen**.
2. Klicken Sie Auf **Deaktivieren**.

Legen Sie das Network Time Protocol fest

Das Einrichten des Network Time Protocol (NTP) lässt sich auf zwei Arten erreichen: Entweder weisen Sie jeden Knoten in einem Cluster an, nach Broadcasts zu hören, oder weisen Sie jeden Knoten an, einen NTP-Server nach Updates abzufragen.

Mit NTP werden Uhren über ein Netzwerk synchronisiert. Die Verbindung zu einem internen oder externen NTP-Server sollte Teil der ersten Cluster-Einrichtung sein.

Konfigurieren Sie die Network Time Protocol-Server für das abzufragenden Cluster

Sie können jeden Node in einem Cluster anweisen, einen NTP-Server (Network Time Protocol) nach Updates abzufragen. Das Cluster kontaktiert nur konfigurierte Server und fordert von ihnen NTP-Informationen an.

Konfigurieren Sie NTP auf dem Cluster, um auf einen lokalen NTP-Server zu verweisen. Sie können die IP-

Adresse oder den FQDN-Hostnamen verwenden. Der NTP-Standardserver zum Erstellungszeitpunkt des Clusters ist auf us.pool.ntp.org eingestellt. Es kann jedoch nicht immer eine Verbindung zu diesem Standort hergestellt werden, abhängig vom physischen Standort des SolidFire Clusters.

Die Verwendung des FQDN hängt davon ab, ob die DNS-Einstellungen des einzelnen Speicherknoten vorhanden und betriebsbereit sind. Konfigurieren Sie dazu die DNS-Server auf jedem Speicherknoten und stellen Sie sicher, dass die Ports geöffnet sind, indem Sie die Seite Netzwerkport-Anforderungen überprüfen.

Sie können bis zu fünf verschiedene NTP-Server eingeben.

Sie können IPv4- und IPv6-Adressen verwenden.

Was Sie benötigen

Um diese Einstellung zu konfigurieren, müssen Sie über Berechtigungen für Cluster-Administratoren verfügen.

Schritte

1. Konfigurieren Sie eine Liste der IPs und/oder FQDNs in den Servereinstellungen.
2. Stellen Sie sicher, dass DNS auf den Knoten ordnungsgemäß eingestellt ist.
3. Klicken Sie Auf **Cluster** > **Einstellungen**.
4. Wählen Sie unter Network Time Protocol Settings **No** die standardmäßige NTP-Konfiguration.
5. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Konfigurieren Sie das Cluster, um NTP-Broadcasts abzuhören

Mithilfe des Broadcast-Modus können Sie jeden Node in einem Cluster anweisen, um auf dem Netzwerk nach NTP (Network Time Protocol)-Broadcast-Meldungen von einem bestimmten Server abzuhören.

Was Sie benötigen

- Um diese Einstellung zu konfigurieren, müssen Sie über Berechtigungen für Cluster-Administratoren verfügen.
- Sie müssen einen NTP-Server im Netzwerk als Broadcast-Server konfigurieren.

Schritte

1. Klicken Sie Auf **Cluster** > **Einstellungen**.
2. Geben Sie den NTP-Server oder die Server, die den Broadcast-Modus in die Serverliste verwenden, ein.
3. Wählen Sie unter Network Time Protocol Settings **Ja** aus, um einen Broadcast-Client zu verwenden.
4. Um den Broadcast-Client einzustellen, geben Sie im Feld **Server** den NTP-Server ein, den Sie im Broadcast-Modus konfiguriert haben.
5. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

SNMP managen

Sie können Simple Network Management Protocol (SNMP) in Ihrem Cluster konfigurieren.

Sie können einen SNMP-Anforderer auswählen, die zu verwendende SNMP-Version auswählen, den Benutzer des SNMP-Benutzerbasierten Sicherheitsmodells (USM) identifizieren und Traps zur Überwachung des SolidFire-Clusters konfigurieren. Sie können auch die Basisdateien des Managements für Informationen anzeigen und auf sie zugreifen.

Sie können IPv4- und IPv6-Adressen verwenden.

SNMP-Details

Auf der SNMP-Seite der Registerkarte Cluster können Sie die folgenden Informationen anzeigen:

- **SNMP MIBs**

  Die MIB-Dateien, die für Sie zum Anzeigen oder Herunterladen zur Verfügung stehen.

- **Allgemeine SNMP-Einstellungen**

  Sie können SNMP aktivieren oder deaktivieren. Nachdem Sie SNMP aktiviert haben, können Sie wählen, welche Version verwendet werden soll. Wenn Sie Version 2 verwenden, können Sie Anfragesteller hinzufügen, und wenn Sie Version 3 verwenden, können Sie USM-Benutzer einrichten.

- **SNMP-Trap-Einstellungen**

  Sie können ermitteln, welche Traps erfasst werden sollen. Sie können den Host, Port und die Community-Zeichenfolge für jeden Trap-Empfänger festlegen.

Konfigurieren eines SNMP-Anforderers

Wenn die SNMP-Version 2 aktiviert ist, können Sie einen Anforderer aktivieren oder deaktivieren und die Anfragesteller so konfigurieren, dass autorisierte SNMP-Anforderungen empfangen werden.

1. Klicken Sie auf Menü:Cluster[SNMP].
2. Klicken Sie unter **Allgemeine SNMP-Einstellungen** auf **Ja**, um SNMP zu aktivieren.
3. Wählen Sie aus der Liste **Version Version 2**.
4. Geben Sie im Abschnitt * Requitors* die Informationen **Community String** und **Network** ein.

Standardmäßig ist die Community-Zeichenfolge öffentlich, und das Netzwerk ist localhost. Sie können diese Standardeinstellungen ändern.

5. **Optional:** um einen weiteren Anforderer hinzuzufügen, klicken Sie auf **Antragsteller hinzufügen** und geben die Informationen **Community String** und **Network** ein.
6. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

- Konfigurieren Sie SNMP-Traps
- Zeigen Sie verwaltete Objektdaten mithilfe von Management-Informationen-Basisdateien an

Konfigurieren eines SNMP-USM-Benutzers

Wenn Sie SNMP-Version 3 aktivieren, müssen Sie einen USM-Benutzer so konfigurieren, dass er autorisierte SNMP-Anforderungen erhält.

1. Klicken Sie auf **Cluster** > **SNMP**.
2. Klicken Sie unter **Allgemeine SNMP-Einstellungen** auf **Ja**, um SNMP zu aktivieren.
3. Wählen Sie aus der Liste **Version** die Option **Version 3** aus.
4. Geben Sie im Abschnitt **USM-Benutzer** den Namen, das Passwort und die Passphrase ein.
5. **Optional:** um einen anderen USM-Benutzer hinzuzufügen, klicken Sie auf **USM-Benutzer hinzufügen** und geben den Namen, das Passwort und die Passphrase ein.
6. Klicken Sie Auf **Änderungen Speichern**.

Konfigurieren Sie SNMP-Traps

Systemadministratoren können SNMP-Traps verwenden, die auch als Benachrichtigungen bezeichnet werden, um den Zustand des SolidFire Clusters zu überwachen.

Wenn SNMP-Traps aktiviert sind, generiert das SolidFire-Cluster Traps im Zusammenhang mit Ereignisprotokolleinträgen und Systemwarnungen. Um SNMP-Benachrichtigungen zu erhalten, müssen Sie die Traps auswählen, die erzeugt werden sollen, und die Empfänger der Trap-Informationen identifizieren. Standardmäßig werden keine Traps generiert.

1. Klicken Sie auf **Cluster** > **SNMP**.
2. Wählen Sie im Abschnitt **SNMP Trap Settings** einen oder mehrere Traps aus, die vom System generiert werden sollen:
   - Cluster-Fehler-Traps
   - Cluster-Gelöste Fehler-Traps
   - Cluster-Event-Köder
3. Geben Sie im Abschnitt **Trap-Empfänger** die Informationen zu Host, Port und Community-Zeichenfolge für einen Empfänger ein.
4. **Optional**: Um einen anderen Trap-Empfänger hinzuzufügen, klicken Sie auf **Trap-Empfänger hinzufügen** und geben Sie Host-, Port- und Community-String-Informationen ein.
5. Klicken Sie Auf **Änderungen Speichern**.

Zeigen Sie verwaltete Objektdaten mithilfe von Management-Informationen-Basisdateien an

Sie können die Management Information Base (MIB)-Dateien anzeigen und herunterladen, die zum Definieren der verwalteten Objekte verwendet werden. Die SNMP-Funktion unterstützt schreibgeschützten Zugriff auf die Objekte, die in der SolidFire-Storage-ecluster-MIB definiert sind.

Die statistischen Daten in der MIB zeigen die Systemaktivität für die folgenden:

- Cluster-Statistiken
- Volume-Statistiken
- Volumes nach Kontostatistiken
- Node-Statistiken
- Andere Daten wie Berichte, Fehler und Systemereignisse

Das System unterstützt auch den Zugriff auf die MIB-Datei, die die OIDS (OIDS) für SF-Series-Produkte enthält.

Schritte

1. Klicken Sie auf **Cluster** > **SNMP**.
2. Klicken Sie unter **SNMP MIBs** auf die MIB-Datei, die Sie herunterladen möchten.
3. Öffnen oder speichern Sie die MIB-Datei in dem sich daraus ergebenden Downloadfenster.

Verwalten Sie Laufwerke

Jeder Node enthält mindestens ein physisches Laufwerk, für das ein Teil der Daten für das Cluster gespeichert wird. Das Cluster verwendet die Kapazität und Performance des Laufwerks, nachdem das Laufwerk erfolgreich zu einem Cluster hinzugefügt wurde. Sie können die Element UI zum Managen von Laufwerken verwenden.

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Laufwerke für Details

Auf der Seite Laufwerke auf der Registerkarte Cluster finden Sie eine Liste der aktiven Laufwerke im Cluster. Sie können die Seite filtern, indem Sie auf den Registerkarten „aktiv“, „verfügbar“, „Entfernen“, „Löschen“ und „Fehlgeschlagen“ auswählen.

Beim ersten Initialisieren eines Clusters ist die Liste der aktiven Laufwerke leer. Sie können Laufwerke hinzufügen, die einem Cluster nicht zugewiesen sind und auf der Registerkarte verfügbar aufgeführt sind, nachdem ein neues SolidFire Cluster erstellt wurde.

Die folgenden Elemente werden in der Liste der aktiven Laufwerke angezeigt.

- **Fahrausweis**

Die dem Laufwerk zugewiesene sequenzielle Nummer.

- **Knoten-ID**

  Die Node-Nummer, die beim Hinzufügen des Node zum Cluster zugewiesen ist.

- **Knotenname**

  Der Name des Knotens, der das Laufwerk beherbergt.

- **Slot**

  Die Steckplatznummer, in der sich das Laufwerk befindet.

- * Kapazität*

  Die Größe des Laufwerks, in GB.

- **Seriell**

  Die Seriennummer des Laufwerks.

- **Tragen Sie Rest**

  Die Verschleißanzeige.

  Das Storage-System meldet den ungefähren Verschleiß der einzelnen Solid State Drives (SSDs) zum Schreiben und Löschen von Daten. Ein Laufwerk, das 5 Prozent seiner entworfenen Schreib- und Löschzyklen verbraucht hat, meldet 95 Prozent verbleibende Abnutzung. Die Informationen zum Laufwerksverschleiß werden vom System nicht automatisch aktualisiert. Sie können die Seite aktualisieren oder schließen und neu laden, um die Informationen zu aktualisieren.

- **Typ**

  Der Laufwerkstyp. Der Typ kann entweder Block- oder Metadaten sein.

Managen von Nodes

Sie können SolidFire Storage und Fibre Channel Nodes über die Seite Nodes auf der Registerkarte Cluster verwalten.

Wenn ein neu hinzugefügter Node mehr als 50 % der gesamten Cluster-Kapazität beträgt, wird einige der Kapazitäten dieses Node unbrauchbar („ungenutzt“) gemacht, sodass die Kapazitätsregel eingehalten wird. Dies bleibt der Fall, bis mehr Storage hinzugefügt wird. Wenn ein sehr großer Node hinzugefügt wird, der auch die Kapazitätsregel nicht befolgt, kann der zuvor isolierte Node nicht mehr ungenutzt bleiben, während der neu hinzugefügte Node ungenutzt ist. Um dies zu vermeiden, sollte immer paarweise Kapazität hinzugefügt werden. Wenn ein Node ungenutzt wird, ist ein geeigneter Cluster-Fehler zu werfen.

Weitere Informationen

Fügen Sie einem Cluster einen Node hinzu

Fügen Sie einem Cluster einen Node hinzu

Sie können einem Cluster Nodes hinzufügen, wenn mehr Storage benötigt wird oder nach der Cluster-Erstellung. Nodes müssen die Erstkonfiguration erfordern, wenn sie zum ersten Mal eingeschaltet sind. Nachdem der Node konfiguriert wurde, wird er in der Liste der ausstehenden Nodes angezeigt und Sie können ihn einem Cluster hinzufügen.

Die Softwareversion auf jedem Node in einem Cluster muss kompatibel sein. Wenn Sie einem Cluster einen Node hinzufügen, installiert das Cluster nach Bedarf die Cluster-Version der NetApp Element Software auf dem neuen Node.

Sie können einem vorhandenen Cluster Nodes mit kleineren oder größeren Kapazitäten hinzufügen. Sie können einem Cluster größere Node-Kapazitäten hinzufügen, um eine Kapazitätssteigerung zu ermöglichen. Größere Nodes, die zu einem Cluster mit kleineren Nodes hinzugefügt werden, müssen paarweise hinzugefügt werden. So kann Double Helix die Daten im Fall eines Ausfall eines der größeren Nodes ausreichend Speicherplatz verschieben. Einem größeren Node-Cluster können kleinere Node-Kapazitäten hinzugefügt werden, um die Performance zu verbessern.

> Wenn ein neu hinzugefügter Node mehr als 50 % der gesamten Cluster-Kapazität beträgt, wird einige der Kapazitäten dieses Node unbrauchbar („ungenutzt“) gemacht, sodass die Kapazitätsregel eingehalten wird. Dies bleibt der Fall, bis mehr Storage hinzugefügt wird. Wenn ein sehr großer Node hinzugefügt wird, der auch die Kapazitätsregel nicht befolgt, kann der zuvor isolierte Node nicht mehr ungenutzt bleiben, während der neu hinzugefügte Node ungenutzt ist. Um dies zu vermeiden, sollte immer paarweise Kapazität hinzugefügt werden. Wenn ein Node gestrandet wird, wird der stranddecacity-Cluster-Fehler geworfen.

"NetApp Video: Skalieren nach eigenen Regeln: Erweitern eines SolidFire-Clusters"

Sie können NetApp HCI Appliances Nodes hinzufügen.

Schritte

1. Wählen Sie **Cluster** > **Knoten**.
2. Klicken Sie auf **Ausstehend**, um die Liste der ausstehenden Knoten anzuzeigen.

   Wenn der Vorgang zum Hinzufügen von Nodes abgeschlossen ist, werden diese in der Liste der aktiven Nodes angezeigt. Bis dahin werden die ausstehenden Knoten in der Liste „Ausstehend aktiv“ angezeigt.

   SolidFire installiert die Element Softwareversion des Clusters auf den ausstehenden Nodes, wenn Sie sie einem Cluster hinzufügen. Dies kann einige Minuten dauern.

3. Führen Sie einen der folgenden Schritte aus:
   - Um einzelne Knoten hinzuzufügen, klicken Sie auf das Symbol **Aktionen** für den Knoten, den Sie hinzufügen möchten.
   - Um mehrere Knoten hinzuzufügen, aktivieren Sie das Kontrollkästchen der Knoten, die hinzugefügt werden sollen, und dann **Massenaktionen**. **Hinweis:** Wenn der Knoten, den Sie hinzufügen, eine andere Version der Element-Software hat als die Version, die auf dem Cluster ausgeführt wird, aktualisiert der Cluster den Knoten asynchron auf die Version der Element-Software, die auf dem Cluster-Master ausgeführt wird. Nach der Aktualisierung des Node wird er sich automatisch dem Cluster hinzugefügt. Während dieses asynchronen Prozesses befindet sich der Knoten im hängenden Zustand aktiv.
4. Klicken Sie Auf **Hinzufügen**.

Der Node wird in der Liste der aktiven Nodes angezeigt.

Weitere Informationen

Node-Versionierung und -Kompatibilität

Node-Versionierung und -Kompatibilität

Die Node-Kompatibilität basiert auf der auf einem Node installierten Version der Element Software. Bei Element Software-basierten Storage-Clustern wird automatisch ein Node zur Element Softwareversion im Cluster Image erstellt, wenn der Node und das Cluster nicht kompatible Versionen aufweisen.

In der folgenden Liste werden die Signifikanzstufen der Softwareversion, aus der die Versionsnummer der Element Software bestand, beschrieben:

- **Major**

  Die erste Zahl bezeichnet eine Software-Version. Ein Node mit einer Hauptkomponentennummer kann keinem Cluster mit Nodes einer anderen Major-Patch-Nummer hinzugefügt werden. Bei Nodes mit gemischten Hauptversionen kann kein Cluster erstellt werden.

- **Klein**

  Die zweite Zahl bezeichnet kleinere Software-Funktionen oder Verbesserungen an vorhandenen Softwarefunktionen, die zu einer größeren Version hinzugefügt wurden. Diese Komponente wird innerhalb einer Hauptversionskomponente erhöht, um anzugeben, dass diese inkrementelle Version nicht mit anderen inkrementellen Versionen von Element Software mit einer anderen kleineren Komponente kompatibel ist. Beispielsweise ist 11.0 nicht mit 11.1 kompatibel und 11.1 nicht mit 11.2 kompatibel.

- **Mikro**

  Die dritte Zahl bezeichnet einen kompatiblen Patch (inkrementelle Freigabe) für die Element-Softwareversion, die von den Hauptkomponenten dargestellt wird. Beispielsweise ist 11.0.1 kompatibel mit 11.0.2, und 11.0.2 ist kompatibel mit 11.0.3.

Major- und Minor-Versionsnummern müssen für Kompatibilität übereinstimmen. Micronummern müssen nicht übereinstimmen, um Kompatibilität zu gewährleisten.

Kapazität des Clusters in einer gemischten Node-Umgebung

Sie können verschiedene Node-Typen in einem Cluster kombinieren. SF-Series 2405, 3010, 4805, 6010, 9605 9010, 19210, 38410 und H-Series können gleichzeitig in einem Cluster eingesetzt werden.

Die H-Series besteht aus H610S-1, H610S-2, H610S-4 und H410S Nodes. Diese Nodes sind sowohl 10 GbE als auch 25 GbE fähig.

Am besten dürfen nicht verschlüsselte und verschlüsselte Nodes miteinander kombiniert werden. In einem Cluster mit gemischten Nodes kann kein Node mehr als 33 % der gesamten Cluster-Kapazität enthalten. Beispielsweise ist in einem Cluster mit vier SF-Series 4805 Nodes der größte Node, der allein hinzugefügt werden kann, eine SF-Series 9605. Der Cluster-Kapazitätsschwellenwert wird anhand des potenziellen Verlusts des größten Node in dieser Situation berechnet.

Ab Element 12.0 werden die folgenden Storage-Nodes der SF-Series nicht unterstützt:

- SF3010
- SF6010
- SF9010

Wenn Sie einen dieser Storage-Nodes auf Element 12.0 aktualisieren, wird ein Fehler angezeigt, der angibt, dass dieser Node nicht von Element 12.0 unterstützt wird.

Zeigen Sie Node-Details an

Sie können Details für einzelne Nodes wie Service-Tags, Laufwerkdetails und Grafiken für die Nutzung und Laufwerksstatistiken anzeigen. Die Seite Nodes der Registerkarte Cluster enthält die Spalte Version, in der Sie die Softwareversion jedes Node anzeigen können.

Schritte

1. Klicken Sie Auf **Cluster** > **Knoten**.
2. Um die Details für einen bestimmten Knoten anzuzeigen, klicken Sie auf das Symbol **Aktionen** für einen Knoten.
3. Klicken Sie Auf **Details Anzeigen**.
4. Überprüfen Sie die Node-Details:
   - **Knoten-ID**: Die vom System generierte ID für den Knoten.
   - **Knotenname**: Der Hostname des Knotens.
   - **Verfügbare 4.000 IOPS**: Die für den Knoten konfigurierten IOPS.
   - **Knotenrolle**: Die Rolle, die der Knoten im Cluster hat. Mögliche Werte:
     - Cluster Master: Der Knoten, der clusterweite administrative Aufgaben ausführt und MVIP und SVIP enthält.
     - Ensemble Node: Ein Knoten, der am Cluster teilnimmt. Je nach Clustergröße gibt es entweder 3 oder 5 Ensemble-Knoten.
     - Fibre Channel: Ein Node im Cluster.
   - **Node Typ**: Der Modelltyp des Knotens.
   - **Aktive Laufwerke**: Die Anzahl der aktiven Laufwerke im Knoten.
   - **Management IP**: Die Management-IP-Adresse (MIP), die dem Knoten für 1GbE- oder 10GbE-Netzwerkadministratoraufgaben zugewiesen wurde.
   - **Cluster IP**: Die Cluster IP (CIP) Adresse, die dem Knoten zugewiesen wurde, der für die Kommunikation zwischen Knoten im selben Cluster verwendet wurde.
   - **Speicher-IP**: Die Speicher-IP (SIP)-Adresse, die dem Knoten zugewiesen ist, der für die iSCSI-Netzwerkerkennung und den gesamten Datenverkehr im Datennetz verwendet wird.
   - **Management VLAN ID**: Die virtuelle ID für das Management Local Area Network.
   - **Storage VLAN ID**: Die virtuelle ID für das Storage Local Area Network.
   - **Version**: Die Version der Software, die auf jedem Knoten ausgeführt wird.
   - **Replication Port**: Der Port, der auf Knoten für die Remote-Replikation verwendet wird.

- **Service-Tag**: Die dem Knoten zugewiesene eindeutige Service-Tag-Nummer.

Zeigen Sie Details zu Fibre Channel-Ports an

Sie können Details zu Fibre Channel-Ports, z. B. deren Status, ihr Name und ihre Port-Adresse, auf der Seite FC-Ports anzeigen.

Zeigen Sie Informationen zu den Fibre Channel-Ports an, die mit dem Cluster verbunden sind.

Schritte

1. Klicken Sie auf **Cluster** > **FC-Ports**.
2. Um Informationen auf dieser Seite zu filtern, klicken Sie auf **Filter**.
3. Überprüfen Sie die Details:
   - **Knoten-ID**: Der Knoten, der die Sitzung für die Verbindung hostet.
   - **Knotenname**: Vom System generierter Knotenname.
   - **Steckplatz**: Steckplatznummer, wo sich der Fibre Channel-Port befindet.
   - **HBA-Port**: Physischer Port am Fibre Channel Host Bus Adapter (HBA).
   - **WWNN**: Der World Wide Node Name.
   - **WWPN**: Der weltweite Zielname des Ports.
   - **Switch WWN**: Der weltweite Name des Fibre Channel Switch.
   - **Port State**: Aktueller Zustand des Ports.
   - **NPort-ID**: Die Node-Port-ID auf der Fibre Channel Fabric.
   - **Geschwindigkeit**: Die ausgehandelte Fibre Channel-Geschwindigkeit. Folgende Werte sind möglich:
     - 4 Gbit/s
     - 8 Gbit/s
     - 16 Gbit/s

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Managen Sie virtuelle Netzwerke

Durch das virtuelle Netzwerk im SolidFire Storage kann der Datenverkehr zwischen mehreren Clients, die sich in separaten logischen Netzwerken befinden, mit einem Cluster verbunden werden. Die Verbindungen zum Cluster werden im Netzwerk-Stack durch VLAN-Tagging getrennt.

Weitere Informationen

- Fügen Sie ein virtuelles Netzwerk hinzu
- Aktivieren Sie virtuelles Routing und Forwarding
- Bearbeiten eines virtuellen Netzwerks

- VRF-VLANs bearbeiten
- Löschen Sie ein virtuelles Netzwerk

Fügen Sie ein virtuelles Netzwerk hinzu

Sie können einer Cluster-Konfiguration ein neues virtuelles Netzwerk hinzufügen, um eine mandantenfähige Umgebungsverbindung zu einem Cluster zu ermöglichen, auf dem Element Software ausgeführt wird.

Was Sie benötigen

- Identifizieren Sie den Block der IP-Adressen, der den virtuellen Netzwerken auf den Clusterknoten zugewiesen wird.
- Geben Sie eine SVIP-Adresse (Storage-Netzwerk-IP) an, die als Endpunkt für den gesamten NetApp Element-Datenverkehr verwendet werden soll.

Für diese Konfiguration müssen Sie die folgenden Kriterien berücksichtigen:

- Bei VLANs, die nicht VRF-aktiviert sind, müssen sich Initiatoren in demselben Subnetz wie das SVIP befinden.
- VLANs, die VRF-aktiviert sind, müssen sich keine Initiatoren in demselben Subnetz wie die SVIP befinden und Routing wird unterstützt.
- Der Standard-SVIP erfordert keine Initiatoren, die sich im selben Subnetz wie der SVIP befinden, und Routing wird unterstützt.

Wenn ein virtuelles Netzwerk hinzugefügt wird, wird für jeden Node eine Schnittstelle erstellt und jeder benötigt eine virtuelle Netzwerk-IP-Adresse. Die Anzahl der IP-Adressen, die Sie beim Erstellen eines neuen virtuellen Netzwerks angeben, muss der Anzahl der Nodes im Cluster entsprechen oder größer sein. Virtuelle Netzwerkadressen werden von einzelnen Nodes automatisch bereitgestellt und ihnen zugewiesen. Sie müssen den Nodes im Cluster keine virtuellen Netzwerkadressen manuell zuweisen.

Schritte

1. Klicken Sie Auf **Cluster** > **Netzwerk**.
2. Klicken Sie auf **VLAN erstellen**.
3. Geben Sie im Dialogfeld **Neues VLAN** Werte in die folgenden Felder ein:
   - **VLAN-Name**
   - **VLAN-Tag**
   - **SVIP**
   - **Netzmaske**
   - (Optional) **Beschreibung**
4. Geben Sie die **Starting IP**-Adresse für den IP-Adressbereich in **IP-Adressblöcken** ein.
5. Geben Sie die **Größe** des IP-Bereichs als Anzahl der IP-Adressen ein, die in den Block einbezogen werden sollen.
6. Klicken Sie auf **Einen Block hinzufügen**, um einen nicht kontinuierlichen Block von IP-Adressen für dieses VLAN hinzuzufügen.
7. Klicken Sie auf **VLAN erstellen**.

Details zum virtuellen Netzwerk anzeigen

Schritte

1. Klicken Sie Auf **Cluster** > **Netzwerk**.
2. Überprüfen Sie die Details.
   - **ID**: Eindeutige ID des VLAN-Netzwerks, das vom System zugewiesen wird.
   - **Name**: Eindeutiger vom Benutzer zugewiesener Name für das VLAN-Netzwerk.
   - **VLAN Tag**: VLAN-Tag, der beim Erstellen des virtuellen Netzwerks zugewiesen wurde.
   - **SVIP**: Speicher virtuelle IP-Adresse, die dem virtuellen Netzwerk zugewiesen ist.
   - **Netzmaske**: Netzmaske für dieses virtuelle Netzwerk.
   - **Gateway**: Eindeutige IP-Adresse eines virtuellen Netzwerk-Gateways. VRF muss aktiviert sein.
   - **VRF aktiviert**: Angabe, ob virtuelles Routing und Forwarding aktiviert ist oder nicht.
   - **Verwendete IPs**: Der Bereich der virtuellen Netzwerk-IP-Adressen, die für das virtuelle Netzwerk verwendet werden.

Aktivieren Sie virtuelles Routing und Forwarding

Sie können virtuelles Routing und Forwarding (VRF) aktivieren, wodurch mehrere Instanzen einer Routing-Tabelle in einem Router existieren und gleichzeitig arbeiten können. Diese Funktion ist nur für Speichernetzwerke verfügbar.

Sie können VRF nur zum Zeitpunkt der Erstellung eines VLANs aktivieren. Wenn Sie wieder zu nicht-VRF wechseln möchten, müssen Sie das VLAN löschen und neu erstellen.

1. Klicken Sie Auf **Cluster** > **Netzwerk**.
2. Um VRF auf einem neuen VLAN zu aktivieren, wählen Sie **VLAN erstellen**.
   a. Geben Sie relevante Informationen für das neue VRF/VLAN ein. Siehe Hinzufügen eines virtuellen Netzwerks.
   b. Aktivieren Sie das Kontrollkästchen **VRF aktivieren**.
   c. **Optional**: Geben Sie ein Gateway ein.
3. Klicken Sie auf **VLAN erstellen**.

Weitere Informationen

Fügen Sie ein virtuelles Netzwerk hinzu

Bearbeiten eines virtuellen Netzwerks

Sie können VLAN-Attribute wie VLAN-Name, Netzmaske und Größe der IP-Adressblöcke ändern. VLAN-Tag und SVIP können nicht für ein VLAN geändert werden. Das Gateway-Attribut ist kein gültiger Parameter für nicht-VRF-VLANs.

Wenn iSCSI-, Remote-Replikation- oder andere Netzwerksitzungen vorhanden sind, kann die Änderung fehlschlagen.

Beim Verwalten der Größe von VLAN-IP-Adressbereichen sollten Sie die folgenden Einschränkungen beachten:

- Sie können IP-Adressen nur aus dem ursprünglichen IP-Adressbereich entfernen, der zum Zeitpunkt der Erstellung des VLANs zugewiesen wurde.
- Sie können einen IP-Adressblock entfernen, der nach dem ursprünglichen IP-Adressbereich hinzugefügt wurde, aber Sie können einen IP-Adressenblock nicht durch Entfernen von IP-Adressen ändern.
- Wenn Sie versuchen, IP-Adressen entweder aus dem anfänglichen IP-Adressbereich oder in einem IP-Block zu entfernen, die von Nodes im Cluster verwendet werden, kann der Vorgang fehlschlagen.
- Sie können bestimmte nicht verwendete IP-Adressen nicht anderen Nodes im Cluster neu zuweisen.

Sie können einen IP-Adressblock hinzufügen, indem Sie wie folgt vorgehen:

1. Wählen Sie **Cluster** > **Netzwerk**.
2. Wählen Sie das Aktionen-Symbol für das zu bearbeitende VLAN aus.
3. Wählen Sie **Bearbeiten**.
4. Geben Sie im Dialogfeld **VLAN bearbeiten** die neuen Attribute für das VLAN ein.
5. Wählen Sie **Einen Block hinzufügen** aus, um einen nicht kontinuierlichen Block mit IP-Adressen für das virtuelle Netzwerk hinzuzufügen.
6. Wählen Sie **Änderungen Speichern**.

Link zur Fehlerbehebung in KB-Artikeln

Link zu den Knowledge Base-Artikeln, um Hilfe bei der Fehlerbehebung bei der Verwaltung Ihrer VLAN-IP-Adressbereiche zu erhalten.

- "Doppelte IP-Warnung nach Hinzufügen eines Speicherknoten in VLAN zu Element Cluster"
- "So legen Sie fest, welche VLAN-IP-Adressen verwendet werden und welchen Knoten diese IP-Adressen in Element zugewiesen sind"

VRF-VLANs bearbeiten

Sie können VRF-VLAN-Attribute wie VLAN-Name, Netmask, Gateway und IP-Adressblöcke ändern.

1. Klicken Sie Auf **Cluster** > **Netzwerk**.
2. Klicken Sie auf das Aktionen-Symbol für das zu bearbeitende VLAN.
3. Klicken Sie Auf **Bearbeiten**.
4. Geben Sie im Dialogfeld **VLAN bearbeiten** die neuen Attribute für das VRF-VLAN ein.
5. Klicken Sie Auf **Änderungen Speichern**.

Löschen Sie ein virtuelles Netzwerk

Sie können ein virtuelles Netzwerkobjekt entfernen. Sie müssen die Adressblöcke einem anderen virtuellen Netzwerk hinzufügen, bevor Sie ein virtuelles Netzwerk entfernen.

1. Klicken Sie Auf **Cluster** > **Netzwerk**.
2. Klicken Sie auf das Symbol Aktionen für das zu löschende VLAN.
3. Klicken Sie Auf **Löschen**.
4. Bestätigen Sie die Meldung.

Weitere Informationen

Bearbeiten eines virtuellen Netzwerks

Erstellen eines Clusters, das FIPS-Laufwerke unterstützt

Für die Implementierung von Lösungen in vielen Kundenumgebungen wird die Sicherheit immer wichtiger. Federal Information Processing Standards (FIPS) sind Standards für die Sicherheit und Interoperabilität von Computern. Die nach FIPS 140-2 zertifizierte Verschlüsselung für Daten im Ruhezustand ist Bestandteil der Gesamtlösung.

- "Vermeiden Sie das Kombinieren von Nodes für FIPS-Laufwerke"
- "Verschlüsselung für Daten im Ruhezustand aktivieren"
- "Ermitteln, ob Nodes für die FIPS-Laufwerksfunktion bereit sind"
- "Aktivierung der FIPS-Laufwerksfunktion"
- "Prüfen Sie den FIPS-Laufwerksstatus"
- "Fehlerbehebung für die FIPS-Laufwerksfunktion"

Vermeiden Sie das Kombinieren von Nodes für FIPS-Laufwerke

Damit die Funktion von FIPS-Laufwerken aktiviert werden kann, sollten Nodes, bei denen einige FIPS-Laufwerke unterstützen und andere nicht, nicht kombiniert werden.

Ein Cluster gilt als FIPS-Laufwerke, die den folgenden Bedingungen entsprechen:

- Alle Laufwerke sind als FIPS-Laufwerke zertifiziert.
- Alle Nodes sind FIPS-Laufwerke.
- Die Verschlüsselung für Daten im Ruhezustand (OHR) ist aktiviert.
- Die FIPS-Laufwerksfunktion ist aktiviert. Alle Laufwerke und Nodes müssen FIPS-fähig sein und die Verschlüsselung im Ruhezustand muss aktiviert sein, um die FIPS-Laufwerksfunktion zu aktivieren.

Verschlüsselung für Daten im Ruhezustand aktivieren

Die Cluster-weite Verschlüsselung im Ruhezustand wird aktiviert und deaktiviert. Diese Funktion ist standardmäßig nicht aktiviert. Zur Unterstützung von FIPS-Laufwerken müssen Sie die Verschlüsselung im Ruhezustand aktivieren.

1. Klicken Sie in der NetApp Element Software-Benutzeroberfläche auf **Cluster** > **Einstellungen**.
2. Klicken Sie auf **Verschlüsselung im Ruhezustand aktivieren**.

Weitere Informationen

- Aktivieren und Deaktivieren der Verschlüsselung für ein Cluster
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Ermitteln, ob Nodes für die FIPS-Laufwerksfunktion bereit sind

Sie sollten überprüfen, ob alle Nodes im Storage Cluster zur Unterstützung von FIPS-Laufwerken bereit sind. Hierzu verwenden Sie die NetApp Element Software GetFipsReport API-Methode.

Der resultierende Bericht zeigt einen der folgenden Status an:

- Keine: Node unterstützt nicht die FIPS-Laufwerksfunktion.
- Partiell: Node ist FIPS-fähig, nicht alle Laufwerke sind FIPS-Laufwerke.
- Bereit: Node ist FIPS-fähig. Alle Laufwerke sind FIPS-Laufwerke oder es sind keine Laufwerke vorhanden.

Schritte

1. Prüfen Sie mithilfe der Element API, ob die Nodes und Laufwerke im Storage-Cluster FIPS-Laufwerke unterstützen:

   ```
   GetFipsReport
   ```

2. Überprüfen Sie die Ergebnisse, und notieren Sie alle Knoten, die keinen Status von „bereit“ aufweisen.
3. Prüfen Sie bei Knoten, die keinen Status bereit hatten, ob das Laufwerk die FIPS-Laufwerksfunktion unterstützt:
   - Geben Sie mithilfe der Element API Folgendes ein: `GetHardwareList`
   - Notieren Sie sich den Wert des **DriveEncrypting CapabilityType**. Ist der FIPS-2, unterstützt die Hardware die FIPS-Laufwerksfunktion.

     Siehe Details zu `GetFipsReport` Oder `ListDriveHardware` Im "Element-API-Referenz".
4. Wenn das Laufwerk die FIPS-Laufwerksfunktion nicht unterstützt, ersetzen Sie die Hardware durch FIPS-Hardware (entweder Node oder Laufwerke).

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Aktivierung der FIPS-Laufwerksfunktion

Die Funktion für FIPS-Laufwerke kann über die NetApp Element Software aktiviert werden `EnableFeature` API-Methode.

Die Verschlüsselung im Ruhezustand muss auf dem Cluster aktiviert sein und alle Nodes und Laufwerke müssen FIPS-fähig sein, wie angegeben, wenn der GetFipsReport den Status bereit für alle Nodes anzeigt.

Schritt

1. Aktivieren Sie mithilfe der Element API FIPS auf allen Laufwerken, indem Sie Folgendes eingeben:

   ```
   EnableFeature params: FipsDrives
   ```

Weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Prüfen Sie den FIPS-Laufwerksstatus

Sie können mithilfe der NetApp Element Software prüfen, ob die FIPS-Laufwerksfunktion auf dem Cluster aktiviert ist `GetFeatureStatus` API-Methode, die angibt, ob der Status „FIPS Drives enabled“ wahr oder „false“ ist.

1. Überprüfen Sie mithilfe der Element API die FIPS-Laufwerksfunktion auf dem Cluster, indem Sie Folgendes eingeben:

   ```
   GetFeatureStatus
   ```

2. Überprüfen Sie die Ergebnisse der `GetFeatureStatus` API-Aufruf. Wenn der Wert für aktivierte FIPS-Laufwerke den Wert hat, ist die Funktion für FIPS-Laufwerke aktiviert.

   ```
   {"enabled": true,
   "feature": "FipsDrives"
   }
   ```

Weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Fehlerbehebung für die FIPS-Laufwerksfunktion

Über die NetApp Element Software-UI lassen sich Benachrichtigungen über Clusterfehler oder Fehler im System anzeigen, die sich auf die FIPS-Laufwerksfunktion beziehen.

1. Wählen Sie über die Element-UI die Option **Reporting** > **Alerts** aus.
2. Suchen Sie nach Clusterfehlern, einschließlich:
   - Übereinstimmende FIPS-Laufwerke
   - FIPS führt zu Compliance-Verstößen
3. Vorschläge zur Problembehebung finden Sie unter Informationen zu Cluster-Fehlercodes.

Weitere Informationen

- Cluster-Fehlercodes
- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"

- "NetApp Element Plug-in für vCenter Server"

Aktivieren Sie FIPS 140-2 für HTTPS auf dem Cluster

Sie können die API-Methode EnableFeature verwenden, um den FIPS 140-2-Betriebsmodus für HTTPS-Kommunikation zu aktivieren.

NetApp Element ermöglicht die Aktivierung des Betriebsmodus Federal Information Processing Standards (FIPS) 140-2 auf dem Cluster. Wenn Sie diesen Modus aktivieren, wird das NetApp Cryptographic Security Module (NCSM) aktiviert und für die gesamte Kommunikation über HTTPS mit der NetApp Element UI und API auf FIPS 140-2 Level 1 zertifizierte Verschlüsselung genutzt.

> Nach Aktivierung des FIPS 140-2-Modus kann dieser nicht deaktiviert werden. Wenn FIPS 140-2-Modus aktiviert ist, wird jeder Node im Cluster neu gebootet und läuft über einen Selbsttest, ob das NCSM korrekt aktiviert ist und im FIPS 140-2-zertifizierten Modus betrieben wird. Dies führt zu einer Unterbrechung der Management- und Storage-Verbindungen auf dem Cluster. Sie sollten diesen Modus sorgfältig planen und nur aktivieren, wenn Ihre Umgebung die von ihm angebotenen Verschlüsselungsmechanismen benötigt.

Weitere Informationen finden Sie unter Element API Informationen.

Dies ist ein Beispiel für die API-Anforderung zur Aktivierung von FIPS:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

Nach Aktivierung dieses Betriebsmodus werden alle HTTPS-Kommunikationen mit den nach FIPS 140-2 genehmigten Chiffren verwendet.

Weitere Informationen

- SSL-Chiffren
- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

SSL-Chiffren

SSL-Chiffren sind Verschlüsselungsalgorithmen, die von Hosts zur Einrichtung einer sicheren Kommunikation verwendet werden. Es gibt Standardchiffren, die Element Software unterstützt und nicht-Standardchiffren, wenn der FIPS 140-2-Modus aktiviert ist.

Die folgenden Listen enthalten die von der Element-Software unterstützten Standard-SSL-Chiffren (Secure

Socket Layer) und die SSL-Chiffren, die unterstützt werden, wenn der FIPS 140-2-Modus aktiviert ist:

- **FIPS 140-2 deaktiviert**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) – C

  TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) – A

  TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A

  TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) – A

  TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A

  TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A

  TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (RSA 2048) - A

  TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (RSA 2048) - A

  TLS_RSA_WITH_IDEA_CBC_SHA (RSA 2048) - A

  TLS_RSA_WITH_RC4_128_MD5 (RSA 2048) – C

  TLS_RSA_WITH_RC4_128_SHA (RSA 2048) – C

  TLS_RSA_WITH_SEED_CBC_SHA (RSA 2048) - A

- **FIPS 140-2 aktiviert**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECT571R1) - A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECT571R1) - A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECT571R1) - A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECT571R1) - A

TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) – C

TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) – A

TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) – A

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A

Weitere Informationen

Aktivieren Sie FIPS 140-2 für HTTPS auf dem Cluster

Erste Schritte mit externem Verschlüsselungsmanagement

EKM (External Key Management) bietet eine sichere Verwaltung des Authentifizierungsschlüssels (AK) in Verbindung mit einem externen EKS-Server (Off-Cluster). Die AKS werden verwendet, um Self-Encrypting Drives (SEDs) zu sperren und zu entsperren "Verschlüsselung für Daten im Ruhezustand" Ist auf dem Cluster aktiviert. Der EKS sorgt für die sichere Erzeugung und Lagerung der AKS. Der Cluster verwendet für die Kommunikation mit dem EKS das Key Management Interoperability Protocol (KMIP), ein OASIS-definiertes Standardprotokoll.

- "Externe Verwaltung einrichten"
- "Verschlüsselung der Software beim Rest-Master-Schlüssel"
- "Wiederherstellen von nicht zugänglichen oder ungültigen Authentifizierungsschlüsseln"
- "Befehle für externes Verschlüsselungsmanagement-API"

Weitere Informationen

- "CreateCluster API, die zur Aktivierung der Softwareverschlüsselung im Ruhezustand verwendet werden kann"

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Externes Verschlüsselungsmanagement einrichten

Sie können diese Schritte ausführen und die aufgeführten Element-API-Methoden verwenden, um Ihre externe Verschlüsselungsmanagementfunktion einzurichten.

Was Sie benötigen

- Wenn Sie externes Verschlüsselungsmanagement in Kombination mit Softwareverschlüsselung im Ruhezustand einrichten, ist die Softwareverschlüsselung im Ruhezustand aktiviert "CreateCluster erstellen" Methode auf einem neuen Cluster, das keine Volumes enthält.

Schritte

1. Bauen Sie eine Vertrauensbeziehung mit dem externen Key Server (EKS) auf.
   a. Erstellen Sie ein öffentliches/privates Schlüsselpaar für das Element Cluster, das zur Schaffung einer Vertrauensbeziehung mit dem Schlüsselserver verwendet wird, indem Sie die folgende API-Methode aufrufen: "CreatePublicPrivateKeyPair"
   b. Holen Sie sich die Zertifikatsign-Anforderung (CSR), die die Zertifizierungsstelle unterzeichnen muss. Der CSR ermöglicht dem Schlüsselserver zu überprüfen, ob das Element-Cluster, das auf die Schlüssel zugreift, als Element-Cluster authentifiziert ist. Rufen Sie die folgende API-Methode auf: "GetClientCertificateSignRequest"
   c. Verwenden Sie die EKS/Zertifizierungsstelle, um den abgerufenen CSR zu unterzeichnen. Weitere Informationen finden Sie in der Dokumentation von Drittanbietern.
2. Erstellen Sie auf dem Cluster einen Server und Provider, um mit dem EKS zu kommunizieren. Ein Schlüsselanbieter legt fest, wo ein Schlüssel abgerufen werden soll, und ein Server definiert die spezifischen Attribute der EKS, die mit kommuniziert werden.
   a. Erstellen Sie einen Schlüsselanbieter, bei dem die Schlüsselserverdetails gespeichert werden, indem Sie die folgende API-Methode aufrufen: "CreateKeyProviderKmip"
   b. Erstellen Sie einen Schlüsselserver mit dem signierten Zertifikat und dem öffentlichen Schlüsselzertifikat der Zertifizierungsstelle, indem Sie die folgenden API-Methoden aufrufen: "CreateKeyServerkmip" "TestKeyServerkmip"

      Wenn der Test fehlschlägt, überprüfen Sie die Serverkonnektivität und -Konfiguration. Wiederholen Sie dann den Test.

   c. Fügen Sie den Schlüsselserver in den Container des Schlüsselanbieters hinzu, indem Sie die folgenden API-Methoden aufrufen:"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

      Wenn der Test fehlschlägt, überprüfen Sie die Serverkonnektivität und -Konfiguration. Wiederholen Sie dann den Test.
3. Führen Sie als nächsten Schritt für die Verschlüsselung im Ruhezustand einen der folgenden Schritte aus:
   a. (Für Hardware-Verschlüsselung im Ruhezustand) aktivieren "Hardware-Verschlüsselung für Daten im Ruhezustand" Durch Angabe der ID des Schlüsselanbieters, der den Schlüsselserver enthält, der zum Speichern der Schlüssel verwendet wird, indem der angerufen wird "EnableVerschlüsselungAtZiel" API-Methode.

Sie müssen die Verschlüsselung im Ruhezustand über das aktivieren "API". Die Aktivierung der Verschlüsselung im Ruhezustand mithilfe der vorhandenen Element UI-Schaltfläche bewirkt, dass die Funktion mithilfe intern generierter Schlüssel zurückgesetzt wird.

b. (Für Softwareverschlüsselung im Ruhezustand) in der Reihenfolge "Softwareverschlüsselung für Daten im Ruhezustand" Um den neu erstellten Schlüsselanbieter nutzen zu können, geben Sie die Schlüssel-Provider-ID an den weiter "RekeySoftwareVerschlüsselungAtRestMasterKey" API-Methode.

Weitere Informationen

- "Aktivieren und Deaktivieren der Verschlüsselung für ein Cluster"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Verschlüsselung der Software beim Rest-Master-Schlüssel

Mit der Element-API können Sie einen vorhandenen Schlüssel neu Schlüssel rekeykey. Durch diesen Prozess wird ein neuer Master-Ersatzschlüssel für Ihren externen Verschlüsselungsmanagement-Server erstellt. Master-Schlüssel werden immer durch neue Master-Schlüssel ersetzt und nie dupliziert oder überschrieben.

Unter Umständen müssen Sie die Daten im Rahmen eines der folgenden Verfahren erneut keywichtigen:

- Erstellen Sie einen neuen Schlüssel im Rahmen einer Änderung vom internen Verschlüsselungsmanagement bis zum externen Verschlüsselungsmanagement.
- Erstellen Sie einen neuen Schlüssel als Reaktion auf oder als Schutz gegen sicherheitsrelevante Ereignisse.

Dieser Prozess ist asynchron und gibt eine Antwort zurück, bevor der Rekeyvorgang abgeschlossen ist. Sie können das verwenden "GetAsyncResult" Methode zum Abfragen des Systems, um zu sehen, wann der Prozess abgeschlossen ist.

Was Sie benötigen

- Mithilfe des haben Sie die Softwareverschlüsselung im Ruhezustand aktiviert "CreateCluster erstellen" Methode in einem neuen Cluster, das keine Volumes enthält und keinen I/O enthält Verwenden Sie den Link:./API/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] Um zu bestätigen, dass der Staat ist `enabled` Bevor Sie fortfahren.
- Das ist schon "Sie haben eine Vertrauensbeziehung aufgebaut" Zwischen dem SolidFire-Cluster und einem externen Schlüsselserver (EKS). Führen Sie die aus "TestKeyProviderKmip" Methode, um zu überprüfen, ob eine Verbindung zum Schlüsselanbieter hergestellt wurde.

Schritte

1. Führen Sie die aus "ListKeyProvidersKmip" Befehl und Kopie der Schlüssel-Provider-ID (`keyProviderID`).
2. Führen Sie die aus "RekeySoftwareVerschlüsselungAtRestMasterKey" Mit dem `keyManagementType` Parameter als `external` Und `keyProviderID` Als ID-Nummer des Schlüsselanbieters aus dem vorherigen Schritt:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. Kopieren Sie die `asyncHandle` Wert aus dem `RekeySoftwareEncryptionAtRestMasterKey` Befehlsantwort.
4. Führen Sie die aus "GetAsyncResult" Befehl mit dem `asyncHandle` Wert aus dem vorherigen Schritt, um die Änderung der Konfiguration zu bestätigen. In der Befehlsantwort sollten Sie sehen, dass die ältere Master Key-Konfiguration mit neuen Schlüsselinformationen aktualisiert wurde. Kopieren Sie die neue Schlüssel-Provider-ID zur Verwendung in einem späteren Schritt.

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. Führen Sie die aus `GetSoftwareEncryptionatRestInfo` Befehl, um zu bestätigen, dass neue wichtige Details, einschließlich `keyProviderID`, Wurden aktualisiert.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Weitere Informationen

- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Wiederherstellen von nicht zugänglichen oder ungültigen Authentifizierungsschlüsseln

Gelegentlich kann es zu einem Fehler kommen, der Benutzereingriff erfordert. Im Fehlerfall wird ein Cluster-Fehler (auch als Cluster-Fehlercode bezeichnet) generiert. Die beiden wahrscheinlichsten Fälle werden hier beschrieben.

Das Cluster kann die Laufwerke nicht entsperren, da ein KmipServerFault-Clusterfehler vorliegt.

Dies kann auftreten, wenn das Cluster zum ersten Mal gebootet wird und der Schlüsselserver nicht zugänglich ist oder der erforderliche Schlüssel nicht verfügbar ist.

1. Befolgen Sie ggf. die Wiederherstellungsschritte in den Cluster-Fehlercodes.

Es kann ein SliceServiceUnHealthy Fehler gesetzt werden, weil die Metadaten-Laufwerke als fehlgeschlagen markiert und in den Status „verfügbar“ gesetzt wurden.

Schritte zum Löschen:

1. Fügen Sie die Laufwerke erneut hinzu.
2. Prüfen Sie nach 3 bis 4 Minuten, dass der `sliceServiceUnhealthy` Fehler wurde behoben.

Siehe "Cluster-Fehlercodes" Finden Sie weitere Informationen.

Befehle für externes Verschlüsselungsmanagement-API

Liste aller zur Verwaltung und Konfiguration von EKM verfügbaren APIs.

Wird zum Aufbau einer Vertrauensbeziehung zwischen dem Cluster und externen Servern im Kundenbesitz verwendet:

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

Wird zur Definition der spezifischen Details externer kundeneigener Server verwendet:

- CreateKeyServerkmip
- ModifyKeyServerkmip
- DeleteKeyServerkmip
- GetKeyServerkmip
- ListKeyServersKmip
- TestKeyServerkmip

Wird zur Erstellung und Verwaltung von Schlüsselanbietern verwendet, die externe Schlüsselserver verwalten:

- CreateKeyProviderKmip
- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareVerschlüsselungAtRestMasterKey
- TestKeyProviderKmip

Informationen zu den API-Methoden finden Sie unter "API-Referenzinformationen".

Management von Volumes und virtuellen Volumes

Sie können die Daten in einem Cluster verwalten, auf dem die Element Software ausgeführt wird, auf der Registerkarte Management in der Element UI. Verfügbare Cluster-Managementfunktionen umfassen die Erstellung und das Management von Daten-Volumes, Volume-Zugriffsgruppen, Initiatoren und QoS-Richtlinien (Quality of Service).

- "Arbeiten mit Volumes"
- "Arbeiten mit virtuellen Volumes"
- "Arbeiten Sie mit Volume-Zugriffsgruppen und -Initiatoren"

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Arbeiten mit Volumes

Das SolidFire System stellt mithilfe von Volumes Storage bereit. Volumes sind Blockgeräte, auf die über das Netzwerk von iSCSI- oder Fibre Channel-Clients zugegriffen wird. Auf der Seite Volumes auf der Registerkarte Management können Sie Volumes auf einem Node erstellen, bearbeiten, klonen und löschen. Es lassen sich außerdem Statistiken zur Volume-Bandbreite und zur I/O-Auslastung anzeigen.

Weitere Informationen

- "Management von Quality-of-Service-Richtlinien"
- "Erstellen eines Volumes"
- "Anzeige individueller Performance-Details für Volumes"
- "Aktive Volumes bearbeiten"
- "Löschen Sie ein Volume"
- "Wiederherstellen eines gelöschten Volumes"
- "Löschen Sie ein Volumen"
- "Klonen Sie ein Volume"
- "Weisen Sie LUNs Fibre Channel Volumes zu"
- "Wenden Sie eine QoS-Richtlinie auf Volumes an"
- "Entfernen Sie die QoS-Richtlinienzuordnung eines Volumes"

Management von Quality-of-Service-Richtlinien

Eine QoS-Richtlinie (Quality of Service) ermöglicht das Erstellen und Speichern einer standardisierten Quality of Service-Einstellung, die auf viele Volumes angewendet werden kann. Sie können QoS-Richtlinien auf der Seite QoS-Richtlinien auf der Registerkarte Management erstellen, bearbeiten und löschen.

> Wenn Sie QoS-Richtlinien verwenden, verwenden Sie keine benutzerdefinierte QoS für ein Volume. Durch benutzerdefinierte QoS werden die QoS-Richtlinienwerte für Volume-QoS-Einstellungen überschrieben und angepasst.

"NetApp Video: SolidFire Quality of Service-Richtlinien"

Siehe "Leistung und Servicequalität".

- Erstellen einer QoS-Richtlinie
- Bearbeiten einer QoS-Richtlinie
- Löschen einer QoS-Richtlinie

Erstellen einer QoS-Richtlinie

Sie können QoS-Richtlinien erstellen und sie bei der Erstellung von Volumes anwenden.

1. Wählen Sie **Management** > **QoS-Richtlinien**.

2. Klicken Sie auf **QoS-Richtlinie erstellen**.
3. Geben Sie den **Policy Name** ein.
4. Geben Sie die**Min IOPS**-, **Max IOPS**- und **Burst IOPS**-Werte ein.
5. Klicken Sie auf **QoS-Richtlinie erstellen**.

Bearbeiten einer QoS-Richtlinie

Sie können den Namen einer vorhandenen QoS-Richtlinie ändern oder die mit der Richtlinie verknüpften Werte bearbeiten. Die Änderung einer QoS-Richtlinie wirkt sich auf alle Volumes aus, die mit der Richtlinie verknüpft sind.

1. Wählen Sie **Management** > **QoS-Richtlinien**.
2. Klicken Sie auf das Symbol Aktionen für die QoS-Richtlinie, die Sie bearbeiten möchten.
3. Wählen Sie im Menü Ergebnis die Option**Bearbeiten** aus.
4. Ändern Sie im Dialogfeld **QoS-Richtlinie bearbeiten** die folgenden Eigenschaften nach Bedarf:
   - Name Der Richtlinie
   - IOPS-Minimum
   - IOPS-Maximum
   - IOPS-Burst
5. Klicken Sie Auf **Änderungen Speichern**.

Löschen einer QoS-Richtlinie

Die QoS-Richtlinie kann gelöscht werden, wenn sie nicht mehr benötigt wird. Wenn Sie eine QoS-Richtlinie löschen, behalten alle mit der Richtlinie verknüpften Volumes die QoS-Einstellungen bei, werden aber einer Richtlinie nicht zugeordnet.

> Wenn Sie versuchen, die Zuordnung eines Volumes zu einer QoS-Richtlinie aufzuheben, können Sie die QoS-Einstellungen für dieses Volume individuell ändern.

1. Wählen Sie **Management** > **QoS-Richtlinien**.
2. Klicken Sie auf das Symbol Aktionen für die QoS-Richtlinie, die Sie löschen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.
4. Bestätigen Sie die Aktion.

Weitere Informationen

- "Entfernen Sie die QoS-Richtlinienzuordnung eines Volumes"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Volumes managen

Das SolidFire System stellt mithilfe von Volumes Storage bereit. Volumes sind Blockgeräte, auf die über das Netzwerk von iSCSI- oder Fibre Channel-Clients zugegriffen wird.

Auf der Seite Volumes auf der Registerkarte Management können Sie Volumes auf einem Node erstellen, bearbeiten, klonen und löschen.

Erstellen eines Volumes

Sie können ein Volume erstellen und das Volume einem bestimmten Konto zuordnen. Jedes Volume muss einem Konto zugeordnet sein. Mit dieser Zuordnung kann das Konto über die iSCSI-Initiatoren mit den CHAP-Anmeldeinformationen auf das Volume zugreifen.

Sie können die QoS-Einstellungen für ein Volume während der Erstellung festlegen.

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie Auf **Volume Erstellen**.
3. Geben Sie im Dialogfeld **Neues Volume erstellen** den **Volume-Namen** ein.
4. Geben Sie die Gesamtgröße des Volumes ein.

   Die standardmäßige Auswahl der Volume-Größe ist in GB. Sie können Volumes mithilfe der Größe in GB oder gib erstellen:

   - 1 GB = 1 000 000 000 Bytes
   - 1 gib = 1 073 741 824 Byte
5. Wählen Sie für das Volume eine **Blockgröße** aus.
6. Klicken Sie auf die Dropdown-Liste **Konto** und wählen Sie das Konto aus, das Zugriff auf das Volume haben soll.

   Wenn kein Konto vorhanden ist, klicken Sie auf den Link **Konto erstellen**, geben Sie einen neuen Kontonamen ein und klicken Sie auf **Erstellen**. Der Account wird erstellt und dem neuen Volume zugeordnet.

   Wenn mehr als 50 Konten vorhanden sind, wird die Liste nicht angezeigt. Beginnen Sie mit der Eingabe, und die automatische Vervollständigung zeigt mögliche Werte an, die Sie auswählen können.
7. Um die * Quality of Service* einzustellen, führen Sie einen der folgenden Schritte aus:
   a. Unter **Richtlinie** können Sie eine vorhandene QoS-Richtlinie auswählen, sofern verfügbar.
   b. Legen Sie unter **Benutzerdefinierte Einstellungen** benutzerdefinierte Mindest-, Maximum- und Burst-Werte für IOPS fest oder verwenden Sie die Standard-QoS-Werte.

      Volumes mit einem IOPS-Wert von max oder Burst über 20,000 IOPS erfordern möglicherweise eine hohe Warteschlangentiefe oder mehrere Sitzungen, um diesen IOPS-Level auf einem einzelnen Volume zu erreichen.
8. Klicken Sie Auf **Volume Erstellen**.

Zeigen Sie Volume-Details an

1. Wählen Sie **Management** > **Volumes**.
2. Überprüfen Sie die Details.
   - **ID**: Die vom System generierte ID für das Volume.

- **Name**: Der Name, der dem Volume bei seiner Erstellung gegeben wurde.
- **Konto**: Der Name des Kontos, der dem Volume zugewiesen ist.
- **Access Groups**: Der Name der Volume Access Group oder der Gruppen, zu denen das Volume gehört.
- **Zugriff**: Die Art des Zugriffs, die dem Volume bei der Erstellung zugewiesen wurde. Mögliche Werte:
  - Lese-/Schreibzugriff: Alle Lese- und Schreibvorgänge werden akzeptiert.
  - Schreibgeschützt: Alle Leseaktivitäten sind zulässig; Schreibvorgänge sind nicht zulässig.
  - Gesperrt: Nur Administratorzugriff zulässig.
  - ReplicationTarget: Als Ziel-Volume in einem replizierten Volume-Paar festgelegt.
- **Verwendet**: Der Prozentsatz des genutzten Speicherplatzes im Volumen.
- **Größe**: Die Gesamtgröße (in GB) des Volumens.
- **Snapshots**: Die Anzahl der Snapshots, die für den Datenträger erstellt wurden.
- **QoS-Richtlinie**: Name und Link zur benutzerdefinierten QoS-Richtlinie.
- **Minimum IOPS**: Die Mindestzahl an IOPS für das Volume garantiert.
- **Maximale IOPS**: Die maximale Anzahl von IOPS für das Volume zulässig.
- **Burst IOPS**: Die maximale Anzahl an IOPS über einen kurzen Zeitraum für das Volume zulässig. Standard = 15,000.
- **Attributes**: Attribute, die dem Volumen über eine API-Methode als Schlüssel/Wert-Paar zugewiesen wurden.
- **512e**: Gibt an, ob 512e auf einem Volumen aktiviert ist. Mögliche Werte:
  - Ja.
  - Nein
- **Erstellt am**: Das Datum und die Uhrzeit, zu der der Band erstellt wurde.

Details zu einzelnen Volumes anzeigen

Sie können Performance-Statistiken für einzelne Volumes anzeigen.

1. Wählen Sie **Reporting** > **Volume Performance**.
2. Klicken Sie in der Liste Volume auf das Aktionen-Symbol für ein Volume.
3. Klicken Sie Auf **Details Anzeigen**.

   Unten auf der Seite wird ein Fach mit allgemeinen Informationen zum Volume angezeigt.

4. Um weitere Informationen zum Volumen anzuzeigen, klicken Sie auf **Weitere Details**.

   Das System zeigt detaillierte Informationen sowie Performance-Diagramme für das Volume an.

Aktive Volumes bearbeiten

Volume-Attribute wie QoS-Werte, Volume-Größe und die Maßeinheit, in der Byte-Werte berechnet werden, können geändert werden. Außerdem haben Sie die Möglichkeit, den Kontozugriff für die Replizierungsnutzung zu ändern oder den Zugriff auf das Volume zu beschränken.

Sie können die Größe eines Volume ändern, wenn unter den folgenden Bedingungen genügend Speicherplatz

auf dem Cluster vorhanden ist:

- Normale Betriebsbedingungen.
- Volume-Fehler oder -Ausfälle werden gemeldet.
- Das Volume ist zu klonen.
- Das Volume wird neu synchronisiert.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie im Fenster **Active** auf das Aktionen-Symbol für das zu bearbeitende Volumen.
3. Klicken Sie Auf **Bearbeiten**.
4. **Optional:** Ändern Sie die Gesamtgröße des Volumens.
   - Sie können die Volume-Größe vergrößern, aber nicht verkleinern. Sie können die Größe eines Volumes nur in einem einzigen Größenänderungs-Vorgang anpassen. Speicherbereinigung und Software-Upgrades unterbrechen die Größenänderung nicht.
   - Wenn Sie die Volume-Größe für die Replikation anpassen, sollten Sie zuerst die Größe des Volumes erhöhen, das als Replikationsziel zugewiesen wurde. Anschließend können Sie die Größe des Quellvolumens anpassen. Das Zielvolume kann größer oder gleich groß sein wie das Quellvolume, kann aber nicht kleiner sein.

     Die standardmäßige Auswahl der Volume-Größe ist in GB. Sie können Volumes mithilfe der Größe in GB oder gib erstellen:

   - 1 GB = 1 000 000 000 Bytes
   - 1 gib = 1 073 741 824 Byte
5. **Optional:** Wählen Sie eine andere Zugriffsebene für ein Konto aus einer der folgenden Optionen:
   - Schreibgeschützt
   - Lese-/Schreibzugriff
   - Gesperrt
   - Replizierungsziel
6. **Optional:** Wählen Sie das Konto aus, das Zugriff auf das Volumen haben soll.

   Wenn das Konto nicht vorhanden ist, klicken Sie auf den Link **Konto erstellen**, geben Sie einen neuen Kontonamen ein und klicken Sie auf **Erstellen**. Der Account wird erstellt und dem Volume zugeordnet.

   > Wenn mehr als 50 Konten vorhanden sind, wird die Liste nicht angezeigt. Beginnen Sie mit der Eingabe, und die automatische Vervollständigung zeigt mögliche Werte an, die Sie auswählen können.

7. **Optional:** um die Auswahl in **Quality of Service** zu ändern, führen Sie einen der folgenden Schritte aus:
   a. Unter **Richtlinie** können Sie eine vorhandene QoS-Richtlinie auswählen, sofern verfügbar.
   b. Legen Sie unter **Benutzerdefinierte Einstellungen** benutzerdefinierte Mindest-, Maximum- und Burst-Werte für IOPS fest oder verwenden Sie die Standard-QoS-Werte.

Wenn Sie QoS-Richtlinien für ein Volume verwenden, können Sie durch benutzerdefinierte QoS festlegen, dass die QoS-Richtlinie, die mit dem Volume verbunden ist, entfernt wird. Durch benutzerdefinierte QoS werden die QoS-Richtlinienwerte für Volume-QoS-Einstellungen überschrieben und angepasst.

Wenn Sie IOPS-Werte ändern, sollten Sie sich Dutzende oder Hunderte erhöhen. Eingabewerte erfordern gültige ganze Zahlen.

Konfigurieren Sie Volumes mit einem extrem hohen Burst-Wert. So kann das System gelegentlich sequenzielle Workloads mit großen Blöcken schneller verarbeiten und zugleich die anhaltenden IOPS für ein Volume einschränken.

8. Klicken Sie Auf **Änderungen Speichern**.

Löschen Sie ein Volume

Ein oder mehrere Volumes können aus einem Element Storage-Cluster gelöscht werden.

Das System löscht kein gelöschtes Volume sofort; das Volume bleibt etwa acht Stunden lang verfügbar. Wenn Sie ein Volume wiederherstellen, bevor das System es bereinigt, wird das Volume wieder online geschaltet und die iSCSI-Verbindungen werden wiederhergestellt.

Wenn ein Volume, das zum Erstellen eines Snapshots verwendet wird, gelöscht wird, werden die zugehörigen Snapshots inaktiv. Wenn die gelöschten Quell-Volumes gelöscht werden, werden auch die zugehörigen inaktiven Snapshots aus dem System entfernt.

Persistente Volumes, die mit Managementservices verbunden sind, werden bei der Installation oder bei einem Upgrade einem neuen Konto erstellt und zugewiesen. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie die Volumes oder ihr zugehörigem Konto nicht.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. So löschen Sie ein einzelnes Volume:
   a. Klicken Sie auf das Symbol Aktionen für das zu löschende Volume.
   b. Klicken Sie im Menü Ergebnis auf **Löschen**.
   c. Bestätigen Sie die Aktion.

   Das System verschiebt das Volumen in den Bereich **gelöscht** auf der Seite **Bände**.
3. So löschen Sie mehrere Volumes:
   a. Aktivieren Sie in der Liste der Volumes das Kontrollkästchen neben den Volumes, die Sie löschen möchten.
   b. Klicken Sie Auf **Massenaktionen**.
   c. Klicken Sie im Menü Ergebnis auf **Löschen**.
   d. Bestätigen Sie die Aktion.

   Das System verschiebt die Volumes in den Bereich **gelöscht** auf der Seite **Volumes**.

Wiederherstellen eines gelöschten Volumes

Sie können ein Volume im System wiederherstellen, wenn es gelöscht, aber noch nicht gelöscht wurde. Etwa acht Stunden nach dem Löschen löscht das System ein Volume automatisch. Wenn das System das Volume gelöscht hat, können Sie es nicht wiederherstellen.

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie auf die Registerkarte **gelöscht**, um die Liste der gelöschten Volumes anzuzeigen.
3. Klicken Sie auf das Symbol Aktionen für das Volume, das Sie wiederherstellen möchten.
4. Klicken Sie im Menü Ergebnis auf **Wiederherstellen**.
5. Bestätigen Sie die Aktion.

   Das Volume wird in der Liste **Active** Volumes platziert und iSCSI-Verbindungen zum Volume werden wiederhergestellt.

Löschen Sie ein Volumen

Wenn ein Volume gelöscht wird, wird es dauerhaft aus dem System entfernt. Alle Daten auf dem Volume gehen verloren.

Das System löscht gelöschte Volumes automatisch acht Stunden nach dem Löschen. Wenn Sie jedoch ein Volumen vor der geplanten Zeit löschen möchten, können Sie dies tun.

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie auf die Schaltfläche **gelöscht**.
3. Führen Sie die Schritte zum Löschen eines einzelnen Volumes oder mehrerer Volumes durch.

Option	Schritte
Löschen Sie ein einzelnes Volumen	a. Klicken Sie auf das Aktionen-Symbol für das zu löschung gewünschte Volumen. b. Klicken Sie Auf **Löschen**. c. Bestätigen Sie die Aktion.
Löschen mehrerer Volumes	a. Wählen Sie die Volumes aus, die Sie löschen möchten. b. Klicken Sie Auf **Massenaktionen**. c. Wählen Sie im Menü Ergebnis die Option **Löschen** aus. d. Bestätigen Sie die Aktion.

Klonen Sie ein Volume

Sie können einen Klon eines einzelnen Volumes oder mehrerer Volumes erstellen, um eine zeitpunktgenaue Kopie der Daten zu erstellen. Wenn Sie ein Volume klonen, erstellt das System einen Snapshot des Volume und erstellt dann eine Kopie der Daten, auf die der Snapshot verweist. Dies ist ein asynchroner Prozess und die erforderliche Zeit hängt von der Größe des zum Klonen benötigten Volumes und der aktuellen Cluster-Last ab.

Das Cluster unterstützt bis zu zwei aktuell laufende Klonanforderungen pro Volume und bis zu acht aktive

Volume-Klonvorgänge gleichzeitig. Anforderungen, die über diese Grenzen hinausgehen, werden zur späteren Verarbeitung in die Warteschlange gestellt.

> Betriebssysteme unterscheiden sich in der Behandlung geklonter Volumes. VMware ESXi behandelt ein geklontes Volume als Volume-Kopie oder als Snapshot Volume. Das Volume ist ein verfügbares Gerät zur Erstellung eines neuen Datastores. Weitere Informationen zum Mounten von Klon-Volumes und zum Handling von Snapshot-LUNs finden Sie in der VMware-Dokumentation auf "Mounten einer VMFS-Datastore-Kopie" Und "Managen doppelter VMFS-Datenspeicher".

> Bevor Sie ein geklontes Volume auf eine geringere Größe klonen, müssen Sie die Partitionen so vorbereiten, dass sie sich in das kleinere Volume integrieren.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. Um ein einzelnes Volume zu klonen, führen Sie folgende Schritte aus:
   a. Klicken Sie in der Liste der Volumes auf der Seite **Active** auf das Aktionen-Symbol für das zu klonenden Volume.
   b. Klicken Sie im Menü Ergebnis auf **Klonen**.
   c. Geben Sie im Fenster **Clone Volume** einen Volume-Namen für das neu geklonte Volume ein.
   d. Wählen Sie eine Größe und Messung für das Volumen aus, indem Sie die Spinbox **Volume Size** und die Liste verwenden.

      > Die standardmäßige Auswahl der Volume-Größe ist in GB. Sie können Volumes mithilfe der Größe in GB oder gib erstellen:

      - 1 GB = 1 000 000 000 Bytes
      - 1 gib = 1 073 741 824 Byte

   e. Wählen Sie den Zugriffstyp für das neu geklonte Volume aus.
   f. Wählen Sie aus der Liste **Konto** ein Konto aus, das dem neu geklonten Volume zugeordnet werden soll.

      > Sie können in diesem Schritt ein Konto erstellen, wenn Sie auf den Link **Konto erstellen** klicken, einen Kontonamen eingeben und auf **Erstellen** klicken. Das System fügt das Konto nach dem Erstellen automatisch der **Konto**-Liste hinzu.

3. So klonen Sie mehrere Volumes:
   a. Aktivieren Sie in der Liste der Volumes auf der Seite **Active** das Kontrollkästchen neben beliebigen Volumes, die Sie klonen möchten.
   b. Klicken Sie Auf **Massenaktionen**.
   c. Wählen Sie im Menü Ergebnis die Option **Klonen** aus.
   d. Geben Sie im Dialogfeld **mehrere Volumes klonen** ein Präfix für die geklonten Volumes im Feld **New Volume Name Prefix** ein.
   e. Wählen Sie aus der Liste **Konto** ein Konto aus, das mit den geklonten Volumes verknüpft werden soll.
   f. Wählen Sie den Zugriffstyp für die geklonten Volumes aus.

4. Klicken Sie Auf **Klonen Starten**.

> Wenn Sie die Volume-Größe eines Klons erhöhen, führt dies zu einem neuen Volume mit zusätzlichem freien Speicherplatz am Ende des Volumes. Je nachdem, wie Sie das Volume nutzen, müssen Sie unter Umständen Partitionen erweitern oder neue Partitionen im freien Speicherplatz erstellen, um es nutzen zu können.

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Weisen Sie LUNs Fibre Channel Volumes zu

Sie können die LUN-Zuweisung für ein Fibre Channel-Volume in einer Volume-Zugriffsgruppe ändern. Sie können auch Fibre Channel-Volume-LUN-Zuweisungen erstellen, wenn Sie eine Volume-Zugriffsgruppe erstellen.

Das Zuweisen neuer Fibre Channel-LUNs ist eine erweiterte Funktion und kann unbekannte Auswirkungen auf den verbundenen Host haben. Beispielsweise wird die neue LUN-ID möglicherweise nicht automatisch auf dem Host erkannt, und der Host benötigt möglicherweise einen erneuten Scan, um die neue LUN-ID zu ermitteln.

1. Wählen Sie **Management** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol Aktionen für die Zugriffsgruppe, die Sie bearbeiten möchten.
3. Wählen Sie im Menü Ergebnis die Option**Bearbeiten** aus.
4. Klicken Sie unter **LUN-IDs zuweisen** im Dialogfeld **Volume-Zugriffsgruppe bearbeiten** auf den Pfeil in der Liste **LUN-Zuweisungen**.
5. Geben Sie für jedes Volume in der Liste, dem Sie eine LUN zuweisen möchten, einen neuen Wert in das entsprechende Feld **LUN** ein.
6. Klicken Sie Auf **Änderungen Speichern**.

Wenden Sie eine QoS-Richtlinie auf Volumes an

Sie können Massen eine vorhandene QoS-Richtlinie auf ein oder mehrere Volumes anwenden.

Die QoS-Richtlinie, die Sie als Massenware anwenden möchten, muss vorhanden sein.

1. Wählen Sie **Management** > **Volumes**.
2. Aktivieren Sie in der Liste der Volumes das Kontrollkästchen neben allen Volumes, auf die Sie die QoS-Richtlinie anwenden möchten.
3. Klicken Sie Auf **Massenaktionen**.
4. Klicken Sie im Menü Ergebnis auf **QoS Policy anwenden**.
5. Wählen Sie die QoS-Richtlinie aus der Dropdown-Liste aus.
6. Klicken Sie Auf **Anwenden**.

Weitere Informationen

Quality of Service-Richtlinien

Entfernen Sie die QoS-Richtlinienzuordnung eines Volumes

Sie können eine QoS-Richtlinienzuordnung aus einem Volume entfernen, indem Sie benutzerdefinierte QoS-Einstellungen auswählen.

Das Volume, das Sie ändern möchten, sollte einer QoS-Richtlinie zugewiesen werden.

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie auf das Symbol Aktionen für ein Volume, das eine QoS-Richtlinie enthält, die Sie ändern möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Klicken Sie im Ergebnismenü unter **Quality of Service** auf **Benutzerdefinierte Einstellungen**.
5. Ändern Sie **Min IOPS**, **Max IOPS** und **Burst IOPS** oder behalten Sie die Standardeinstellungen bei.
6. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

Löschen einer QoS-Richtlinie

Arbeiten mit virtuellen Volumes

Über die Element UI lassen sich Informationen anzeigen und Aufgaben für virtuelle Volumes und deren zugehörigen Storage-Container, Protokollendpunkte, Bindungen und Hosts ausführen.

Das Storage-System der NetApp Element Software ist mit deaktivierter Virtual Volumes (VVols)-Funktion ausgestattet. Sie müssen eine einmalige Aufgabe ausführen, vSphere VVol Funktionen manuell über die Element UI zu aktivieren.

Nachdem Sie die VVol Funktionen aktiviert haben, wird eine Registerkarte VVols in der Benutzeroberfläche angezeigt, die VVols-bezogene Monitoring-Optionen und begrenzte Managementoptionen bietet. Zudem fungiert eine Storage-seitige Softwarekomponente, bekannt als VASA Provider, als Storage Awareness-Service für vSphere. Die meisten VVols Befehle, beispielsweise die Erstellung von VVols, das Klonen und die Bearbeitung, werden von einem vCenter Server oder ESXi Host initiiert und vom VASA Provider zu Element APIs für das Element Software Storage-System übersetzt. Über die Element UI lassen sich Befehle zum Erstellen, Löschen und Managen von Storage-Containern und zum Löschen virtueller Volumes ausführen.

In vSphere sind die meisten für die Nutzung der Virtual Volumes-Funktion mit Element Software-Storage-Systemen erforderlichen Konfigurationen vorhanden. Informationen zum Registrieren von VASA Provider in vCenter finden Sie im Konfigurationsleitfaden zu VMware vSphere Virtual Volumes für SolidFire Storage_, zum Erstellen und Managen von VVol Datastores und zum Management von Storage auf Basis von Richtlinien.

Registrieren Sie nicht mehr als einen NetApp Element VASA Provider in einer einzelnen vCenter Instanz. Wenn ein zweiter NetApp Element VASA Provider hinzugefügt wird, macht das alle VVOL Datastores unzugänglich.

VASA-Unterstützung für mehrere vCenters steht als Upgrade-Patch zur Verfügung, wenn Sie bereits einen VASA Provider bei vCenter registriert haben. Laden Sie die VASA39 .tar.gz-Datei von der herunter, um sie zu installieren "NetApp Software-Downloads" Ort und folgen Sie den Anweisungen im Manifest. Der NetApp Element VASA Provider verwendet ein NetApp Zertifikat. Bei diesem Patch wird das Zertifikat von vCenter nicht verändert, um mehrere vCenters für die Verwendung von VASA und VVols zu unterstützen. Ändern Sie das Zertifikat nicht. Benutzerdefinierte SSL-Zertifikate werden von VASA nicht unterstützt.

Weitere Informationen

- Aktivierung virtueller Volumes
- Details zu virtuellen Volumes anzeigen
- Löschen Sie ein virtuelles Volume
- Erstellen eines Storage-Containers
- Bearbeiten eines Speichercontainers
- Löschen eines Speichercontainers
- Protokollendpunkte
- Bindungen
- Host-Details

Aktivierung virtueller Volumes

Sie müssen die Funktion von vSphere Virtual Volumes (VVols) manuell über die NetApp Element Software aktivieren. Im Element Software-System ist die VVols-Funktion standardmäßig deaktiviert und wird nicht automatisch im Rahmen einer neuen Installation oder eines neuen Upgrades aktiviert. Die Aktivierung der VVols-Funktion ist eine einmalige Konfigurationsaufgabe.

Was Sie benötigen

- Der Cluster muss Element 9.0 oder höher ausführen.
- Der Cluster muss mit einer ESXi 6.0 Umgebung oder höher verbunden sein, die mit VVols kompatibel ist.
- Wenn Sie Element 11.3 oder höher verwenden, muss der Cluster mit einer ESXi 6.0 Update 3 oder höher Umgebung verbunden sein.

Durch die Aktivierung der Funktion von vSphere Virtual Volumes wird die Konfiguration der Element Software dauerhaft geändert. Die VVols Funktionalität sollten nur aktiviert werden, wenn das Cluster mit einer mit VMware ESXi VVols kompatiblen Umgebung verbunden ist. Sie können die VVols-Funktion deaktivieren und nur die Standardeinstellungen wiederherstellen, indem Sie das Cluster wieder zum Werkseinstellungen zurücksetzen, d. h. alle Daten im System werden gelöscht.

Schritte

1. Wählen Sie **Cluster** > **Einstellungen**.
2. Ermitteln Sie Cluster-spezifische Einstellungen für Virtual Volumes.
3. Klicken Sie Auf **Virtuelle Volumes Aktivieren**.

4. Klicken Sie auf **Ja**, um die Änderung der Konfiguration der virtuellen Volumes zu bestätigen.

   Die Registerkarte **VVols** wird in der Element-UI angezeigt.

   Wenn die VVols Funktion aktiviert ist, startet das SolidFire Cluster den VASA Provider, öffnet Port 8444 für den VASA Traffic und erstellt Protokollendpunkte, die von vCenter und allen ESXi Hosts erkannt werden können.

5. Kopieren Sie die VASA Provider-URL aus den Virtual Volumes (VVols) Einstellungen unter **Cluster** > **Einstellungen**. Sie verwenden diese URL, um den VASA Provider in vCenter zu registrieren.
6. Erstellen Sie einen Speicher-Container in **VVols** > **Storage Container**.

   Sie müssen mindestens einen Storage-Container erstellen, damit VMs in einem VVol Datastore bereitgestellt werden können.

7. Wählen Sie **VVols** > **Protokollendpunkte** aus.
8. Vergewissern Sie sich, dass für jeden Node im Cluster ein Protokollendpunkt erstellt wurde.

   Weitere Konfigurationsaufgaben sind in vSphere erforderlich. Informationen zum Registrieren von VASA Provider in vCenter finden Sie im Konfigurationsleitfaden zu VMware vSphere Virtual Volumes für SolidFire Storage_, zum Erstellen und Managen von VVol Datastores und zum Management von Storage auf Basis von Richtlinien.

Weitere Informationen

"Konfigurationsleitfaden für VMware vSphere Virtual Volumes für SolidFire Storage"

Details zu virtuellen Volumes anzeigen

Sie können Informationen zu virtuellen Volumes für alle aktiven virtuellen Volumes auf dem Cluster in der Element UI prüfen. Sie können außerdem Performance-Aktivitäten für jedes virtuelle Volume anzeigen, einschließlich Eingaben, Ausgaben, Durchsatz, Latenz, Warteschlangentiefe und Volume-Informationen

Was Sie benötigen

- Die VVols Funktion sollte in der Element UI für den Cluster aktiviert sein.
- Sie sollten einen zugeordneten Speicher-Container erstellt haben.
- Sie sollten vSphere Cluster entsprechend der VVols Funktion der Element Software konfigurieren.
- Sie sollten mindestens eine VM in vSphere erstellt haben.

Schritte

1. Klicken Sie auf **VVols** > **Virtual Volumes**.

   Die Informationen für alle aktiven virtuellen Volumes werden angezeigt.

2. Klicken Sie auf das Symbol **Aktionen** für das virtuelle Volume, das Sie überprüfen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Details anzeigen**.

Details

Die Seite Virtual Volumes auf der Registerkarte VVols bietet Informationen zu jedem aktiven virtuellen Volume des Clusters, z. B. Volume-ID, Snapshot ID, ID des übergeordneten virtuellen Volumes und die ID des virtuellen Volumes.

- **Volumen-ID**: Die ID des zugrunde liegenden Volumens.
- **Snapshot ID**: Die ID des zugrunde liegenden Volumen-Snapshots. Der Wert ist 0, wenn das virtuelle Volume keinen SolidFire-Snapshot darstellt.
- **Parent Virtual Volume ID**: Die virtuelle Volume-ID des übergeordneten virtuellen Volume. Wenn die ID null ist, ist das virtuelle Volume unabhängig und es besteht keine Verknüpfung zu einem übergeordneten Volume.
- **Virtual Volume ID**: Die UUID des virtuellen Volumes.
- **Name**: Der Name, der dem virtuellen Volume zugewiesen ist.
- **Storage Container**: Der Speicher-Container, der das virtuelle Volume besitzt.
- **Gast-OS-Typ**: Betriebssystem, das mit dem virtuellen Volume verknüpft ist.
- **Virtual Volume Typ**: Der virtuelle Volume-Typ: Konfiguration, Daten, Speicher, Swap, oder andere.
- **Zugriff**: Die Lese-Schreib-Berechtigungen, die dem virtuellen Volume zugewiesen sind.
- **Größe**: Die Größe des virtuellen Volumes in GB oder gib.
- **Snapshots**: Die Anzahl der damit verbundenen Snapshots. Klicken Sie auf die Nummer, um die Snapshot-Details zu verknüpfen.
- **Minimum IOPS**: Die minimale IOPS QoS Einstellung des virtuellen Volumes.
- **Maximale IOPS**: Die maximale IOPS-QoS-Einstellung des virtuellen Volumes.
- **Burst IOPS**: Die maximale Burst-QoS-Einstellung des virtuellen Volumes.
- **VMW_VmID**: Informationen in Feldern, die mit "VMW_" vorstehen, werden von VMware definiert.
- **Erstellungszeit**: Die Zeit, die die Erstellung des virtuellen Volumes abgeschlossen wurde.

Details für einzelne virtuelle Volumes

Die Seite Virtual Volumes auf der Registerkarte VVols bietet folgende Informationen zu virtuellen Volumes, wenn Sie ein einzelnes virtuelles Volume auswählen und dessen Details anzeigen.

- **VMW_XXX**: Informationen in Feldern, die mit "VMW_" konfrontiert sind, werden von VMware definiert.
- **Parent Virtual Volume ID**: Die virtuelle Volume-ID des übergeordneten virtuellen Volume. Wenn die ID null ist, ist das virtuelle Volume unabhängig und es besteht keine Verknüpfung zu einem übergeordneten Volume.
- **Virtual Volume ID**: Die UUID des virtuellen Volumes.
- **Virtual Volume Typ**: Der virtuelle Volume-Typ: Konfiguration, Daten, Speicher, Swap, oder andere.
- **Volumen-ID**: Die ID des zugrunde liegenden Volumens.
- **Zugriff**: Die Lese-Schreib-Berechtigungen, die dem virtuellen Volume zugewiesen sind.
- **Kontoname**: Name des Kontos, das den Datenträger enthält.
- **Zugriffsgruppen**: Zugeordnete Volume-Zugriffsgruppen.
- **Gesamtvolumen Größe**: Insgesamt bereitgestellte Kapazität in Bytes.
- **Non-Zero Blocks**: Gesamtzahl von 4KiB Blöcken mit Daten nach Abschluss des letzten Garbage

Collection Vorgangs.

- **Zero Blocks**: Gesamtzahl der 4KiB-Blöcke ohne Daten nach Abschluss der letzten Runde der Müllentnahme.
- **Snapshots**: Die Anzahl der damit verbundenen Snapshots. Klicken Sie auf die Nummer, um die Snapshot-Details zu verknüpfen.
- **Minimum IOPS**: Die minimale IOPS QoS Einstellung des virtuellen Volumes.
- **Maximale IOPS**: Die maximale IOPS-QoS-Einstellung des virtuellen Volumes.
- **Burst IOPS**: Die maximale Burst-QoS-Einstellung des virtuellen Volumes.
- **Enable 512**: Da virtuelle Volumes immer 512-Byte-Blockgrößen-Emulation verwenden, ist der Wert immer ja.
- **Volumen gekoppelt**: Gibt an, ob ein Volumen gekoppelt ist.
- **Erstellungszeit**: Die Zeit, die die Erstellung des virtuellen Volumes abgeschlossen wurde.
- **Blocks Größe**: Größe der Blöcke auf dem Volumen.
- **Nicht ausgerichtete Schreibvorgänge**: Für 512e Volumen, die Anzahl der Schreibvorgänge, die sich nicht an einer grenze des 4k-Sektors befanden. Eine hohe Anzahl von nicht ausgerichteten Schreibvorgängen kann auf eine falsche Ausrichtung der Partition hindeuten.
- **Nicht ausgerichtete Lesevorgänge**: Für 512e Volumen, die Anzahl der Leseoperationen, die sich nicht an der grenze des 4k-Sektors befanden. Eine hohe Anzahl von nicht ausgerichteten Lesevorgängen kann auf eine falsche Ausrichtung der Partition hindeuten.
- **ScsiEUIDeviceID**: Weltweit eindeutige SCSI-Geräte-ID für das Volumen im 16-Byte-Format EUI-64.
- **ScsiNAADeviceID**: Weltweit eindeutige SCSI-Geräte-ID für das Volume im NAA IEEE-Registered Extended-Format.
- **Attribute**: Liste von Name-Wert-Paaren im JSON-Objektformat.

Löschen Sie ein virtuelles Volume

Obwohl virtuelle Volumes immer aus der VMware Management-Ebene gelöscht werden sollten, ist die Funktion zum Löschen virtueller Volumes in der Element-UI aktiviert. Sie sollten ein virtuelles Volume nur bei Bedarf aus der Element UI löschen, beispielsweise wenn vSphere virtuelle Volumes auf dem SolidFire Storage nicht bereinigt.

1. Wählen Sie **VVols** > **Virtual Volumes** aus.
2. Klicken Sie auf das Aktionen-Symbol für das virtuelle Volume, das Sie löschen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.

> Sie sollten ein virtuelles Volume von der VMware Management-Ebene löschen, um vor dem Löschen sicherzustellen, dass das virtuelle Volume ordnungsgemäß getrennt wird. Sie sollten ein virtuelles Volume nur bei Bedarf aus der Element UI löschen, beispielsweise wenn vSphere virtuelle Volumes auf dem SolidFire Storage nicht bereinigt. Wenn Sie ein virtuelles Volume aus der Element UI löschen, wird das Volume sofort gelöscht.

4. Bestätigen Sie die Aktion.
5. Aktualisieren Sie die Liste der virtuellen Volumes, um zu bestätigen, dass das virtuelle Volume entfernt wurde.
6. **Optional**: Wählen Sie **Reporting** > **Ereignisprotokoll**, um zu bestätigen, dass die Löschung erfolgreich

war.

Management von Storage-Containern

Ein Storage-Container ist eine Darstellung von vSphere Datastores, die auf einem Cluster mit Element Software erstellt wurde.

Storage-Container werden erstellt und an NetApp Element Accounts gebunden. Ein auf Element Storage erstellter Storage-Container wird als vSphere Datastore in vCenter und ESXi angezeigt. Storage Container weisen keinem Speicherplatz auf Element Storage zu. Sie werden einfach dazu verwendet, virtuelle Volumes logisch zu verknüpfen.

Pro Cluster werden maximal vier Storage-Container unterstützt. Zur Aktivierung der VVols Funktion ist mindestens ein Storage-Container erforderlich.

Erstellen eines Storage-Containers

Es können Storage Container in der Element UI erstellt und in vCenter ermittelt werden. Sie müssen mindestens einen Storage-Container erstellen, um mit der Bereitstellung der auf VVol basierenden Virtual Machines zu beginnen.

Aktivieren Sie vor Beginn die VVols Funktion in der Element UI für das Cluster.

Schritte

1. Wählen Sie **VVols** > **Storage Container** aus.
2. Klicken Sie auf die Schaltfläche **Storage Container erstellen**.
3. Geben Sie im Dialogfeld **Erstellen eines neuen Speicherbehälters** Informationen zum Speichercontainer ein:
   a. Geben Sie einen Namen für den Speichercontainer ein.
   b. Konfigurieren Sie Initiator- und Zielschlüssel für CHAP.

      Lassen Sie die Felder für CHAP-Einstellungen leer, um automatisch Schlüssel zu generieren.

   c. Klicken Sie auf die Schaltfläche **Storage Container erstellen**.
4. Überprüfen Sie, ob der neue Speichercontainer in der Liste auf der Unterregisterkarte **Storage Container** angezeigt wird.

   Da eine NetApp Element-Konto-ID automatisch erstellt und dem Storage-Container zugewiesen wird, muss kein Konto manuell erstellt werden.

Zeigen Sie Details zum Storage-Container an

Auf der Seite Storage Container auf der Registerkarte VVols können Sie Informationen für alle aktiven Storage-Container auf dem Cluster anzeigen.

- **Konto-ID**: Die ID des NetApp Element-Kontos, das mit dem Speichercontainer verknüpft ist.
- **Name**: Der Name des Speicherbehälters.
- **Status**: Der Status des Lagerbehälters. Mögliche Werte:

- Aktiv: Der Speicherbehälter wird verwendet.
- Gesperrt: Der Speicherbehälter ist gesperrt.

- **PE Typ**: Der Protokollendpunkttyp (SCSI ist das einzige verfügbare Protokoll für Element Software).
- **Speicher-Container-ID**: Die UUID des virtuellen Volume-Speichercontainers.
- **Active Virtual Volumes**: Die Anzahl der aktiven virtuellen Volumes, die mit dem Speicher-Container verbunden sind.

Zeigen Sie die Details zu einzelnen Storage-Containern an

Sie können die Storage-Container-Informationen für einen einzelnen Storage-Container anzeigen. Wählen Sie dazu auf der Seite Storage-Container auf der Registerkarte VVols die entsprechende Option aus.

- **Konto-ID**: Die ID des NetApp Element-Kontos, das mit dem Speichercontainer verknüpft ist.
- **Name**: Der Name des Speicherbehälters.
- **Status**: Der Status des Lagerbehälters. Mögliche Werte:
  - Aktiv: Der Speicherbehälter wird verwendet.
  - Gesperrt: Der Speicherbehälter ist gesperrt.
- **CHAP-Initiatorschlüssel**: Der eindeutige CHAP-Schlüssel für den Initiator.
- **CHAP Target Secret**: Der eindeutige CHAP-Schlüssel für das Ziel.
- **Speicher-Container-ID**: Die UUID des virtuellen Volume-Speichercontainers.
- **Protocol Endpoint Type**: Gibt den Protokollendpunkttyp an (SCSI ist das einzige verfügbare Protokoll).

Bearbeiten eines Speichercontainers

Sie können die CHAP-Authentifizierung für Speichercontainer in der Element-UI ändern.

1. Wählen Sie **VVols** > **Storage Container** aus.
2. Klicken Sie auf das Symbol **Aktionen** für den Speichercontainer, den Sie bearbeiten möchten.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. Bearbeiten Sie unter CHAP-Einstellungen die Anmeldeinformationen für Initiatorschlüssel und Zielschlüssel, die für die Authentifizierung verwendet werden.

   Wenn Sie die Anmeldeinformationen für CHAP-Einstellungen nicht ändern, bleiben diese unverändert. Wenn Sie die Felder mit den Anmeldeinformationen leer lassen, generiert das System automatisch neue Geheimnisse.

5. Klicken Sie Auf **Änderungen Speichern**.

Löschen eines Speichercontainers

Sie können Storage Container von der Element UI löschen.

Was Sie benötigen

Stellen Sie sicher, dass alle Virtual Machines aus dem VVol Datastore entfernt wurden.

Schritte

1. Wählen Sie **VVols** > **Storage Container** aus.

2. Klicken Sie auf das Symbol **Aktionen** für den zu löschenden Speichercontainer.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.
4. Bestätigen Sie die Aktion.
5. Aktualisieren Sie die Liste der Speichercontainer auf der Unterregisterkarte **Speichercontainer**, um zu bestätigen, dass der Speichercontainer entfernt wurde.

Protokollendpunkte

Protokollendpunkte sind Zugriffspunkte, die von einem Host zur Storage-Adresse in einem Cluster verwendet werden, auf dem die NetApp Element Software ausgeführt wird. Protokollendpunkte können nicht von einem Benutzer gelöscht oder geändert werden, sind keinem Konto zugeordnet und können nicht einer Volume-Zugriffsgruppe hinzugefügt werden.

Ein Cluster, auf dem Element Software ausgeführt wird, erstellt automatisch einen Protokollendpunkt pro Storage-Node im Cluster. Ein Storage-Cluster mit sechs Nodes verfügt beispielsweise über sechs Protokollendpunkte, die jedem ESXi Host zugeordnet sind. Protokollendpunkte werden dynamisch von Element Software gemanagt und ohne Eingriffe erstellt, verschoben oder entfernt. Protokollendpunkte sind das Ziel für Multi-Pathing und fungieren als I/O-Proxy für subsidiäre LUNs. Jeder Protokollendpunkt nutzt eine verfügbare SCSI-Adresse, genau wie ein Standard-iSCSI-Ziel. Protokollendpunkte werden im vSphere Client als ein einzelnes Block-Storage-Gerät (512 Byte) angezeigt, dieses Storage-Gerät kann jedoch nicht formatiert oder als Storage verwendet werden.

ISCSI ist das einzige unterstützte Protokoll. Das Fibre Channel-Protokoll wird nicht unterstützt.

Details zu Protokollendpunkten

Die Seite Protokollendpunkte auf der Registerkarte VVols bieten Informationen zu Protokollendpunkten.

- * Primary Provider ID*

  Die ID des primären Protokollendpunktanbieters.

- **Sekundäre Provider-ID**

  Die ID des Endpunktanbieters für das sekundäre Protokoll.

- * Protokollendpunkt-ID*

  Die UUID des Protokollendpunkts.

- * Protokoll Endpunktzustand*

  Der Status des Protokollendpunkts. Folgende Werte sind möglich:

  - Aktiv: Der Protokollendpunkt wird verwendet.
  - Start: Der Protokollendpunkt wird gestartet.
  - Failover: Der Protokollendpunkt ist ein Failover aufgetreten.
  - Reserviert: Der Protokollendpunkt ist reserviert.

- * Anbieter Typ*

  Der Typ des Provider des Protokollendpunkts. Folgende Werte sind möglich:

  - Primär
  - Sekundär
- **SCSI NAA GERÄTE-ID**

  Die weltweit eindeutige SCSI-Gerätekennung für den Protokollendpunkt im NAA IEEE Registered Extended Format.

Bindungen

Um I/O-Vorgänge für ein virtuelles Volume durchzuführen, muss ein ESXi Host zuerst das virtuelle Volume binden.

Der SolidFire Cluster wählt einen optimalen Protokollendpunkt, erstellt eine Bindung, die den ESXi Host und das virtuelle Volume dem Protokollendpunkt zugeordnet und die Bindung an den ESXi Host zurückgibt. Nach der Bindung kann der ESXi Host I/O-Vorgänge mit dem gebundenen virtuellen Volume ausführen.

Details zu Bindungen

Die Seite Bindungen auf der Registerkarte VVols bietet verbindliche Informationen zu jedem virtuellen Volume.

Folgende Informationen werden angezeigt:

- **Host-ID**

  Die UUID für den ESXi-Host, der virtuelle Volumes hostet und dem Cluster bekannt ist.
- * Protokollendpunkt-ID*

  Protokollendpunkt-IDs, die jedem Node im SolidFire Cluster entsprechen.
- * Protokollendpunkt in Band-ID*

  Die SCSI-NAA-Geräte-ID des Protokollendpunkts.
- * Protokollendpunkt Typ*

  Der Endpunkt-Typ des Protokolls.
- **VVol Binding ID**

  Die bindende UUID des virtuellen Volumes.
- * VVol ID*

  Die Universally Unique Identifier (UUID) des virtuellen Volumes.
- **VVol Secondary ID**

Die sekundäre ID des virtuellen Volumes als LUN-ID der zweiten SCSI-Ebene.

Host-Details

Die Seite Hosts auf der Registerkarte VVols bietet Informationen zu VMware ESXi Hosts, die virtuelle Volumes hosten.

Folgende Informationen werden angezeigt:

- **Host-ID**

  Die UUID für den ESXi-Host, der virtuelle Volumes hostet und dem Cluster bekannt ist.

- **Host-Adresse**

  Die IP-Adresse oder der DNS-Name für den ESXi-Host.

- **Bindungen**

  Binding-IDs für alle virtuellen Volumes, die vom ESXi-Host gebunden sind.

- **ESX Cluster-ID**

  Die vSphere-Host-Cluster-ID oder vCenter-GUID.

- **Initiator-IQNs**

  Initiator-IQNs für den Host des virtuellen Volumes.

- **SolidFire-Protokoll Endpunkt-IDs**

  Die Protokollendpunkte, die derzeit für den ESXi Host sichtbar sind.

Arbeiten Sie mit Volume-Zugriffsgruppen und -Initiatoren

ISCSI-Initiatoren oder Fibre Channel-Initiatoren können auf die in den Volume-Zugriffsgruppen definierten Volumes zugreifen.

Sie können Zugriffsgruppen erstellen, indem Sie iSCSI-Initiator-IQNs oder Fibre Channel-WWPNs in einer Sammlung von Volumes zuordnen. Jeder IQN, den Sie einer Zugriffsgruppe hinzufügen, kann auf jedes Volume in der Gruppe zugreifen, ohne dass eine CHAP-Authentifizierung erforderlich ist.

Es gibt zwei Arten von CHAP-Authentifizierungsmethoden:

- CHAP-Authentifizierung auf Kontoebene: Sie können CHAP-Authentifizierung für das Konto zuweisen.
- CHAP-Authentifizierung auf Initiatorebene: Sie können bestimmten Initiatoren eindeutige CHAP-Ziele und Schlüssel zuweisen, ohne an ein einziges CHAP-Konto gebunden zu sein. Diese CHAP-Authentifizierung auf Initiatorebene ersetzt Anmeldeinformationen auf Kontoebene.

Optional können Sie mit CHAP pro Initiator die Initiatorautorisierung und die CHAP-Authentifizierung per Initiator erzwingen. Diese Optionen können pro Initiator definiert werden, und eine Zugriffsgruppe kann eine Kombination von Initiatoren mit verschiedenen Optionen enthalten.

Jeder WWPN, den Sie einer Zugriffsgruppe hinzufügen, ermöglicht den Fibre-Channel-Netzwerkzugriff auf die Volumes in der Zugriffsgruppe.

Volume-Zugriffsgruppen verfügen über die folgenden Grenzen:

- In einer Zugriffsgruppe sind maximal 64 IQNs oder WWPNs zulässig.
- Eine Zugriffsgruppe kann aus maximal 2000 Volumes bestehen.
- Ein IQN oder WWPN kann nur zu einer Zugriffsgruppe gehören.
- Ein einzelnes Volume kann zu maximal vier Zugriffsgruppen gehören.

Weitere Informationen

- Erstellen einer Volume-Zugriffsgruppe
- Fügen Sie einer Zugriffsgruppe Volumes hinzu
- Volumes aus einer Zugriffsgruppe entfernen
- Erstellen eines Initiators
- Bearbeiten Sie einen Initiator
- Fügen Sie einen einzelnen Initiator einer Volume-Zugriffsgruppe hinzu
- Fügen Sie einer Volume-Zugriffsgruppe mehrere Initiatoren hinzu
- Entfernen Sie Initiatoren aus einer Zugriffsgruppe
- Löschen Sie eine Zugriffsgruppe
- Löschen eines Initiators

Erstellen einer Volume-Zugriffsgruppe

Sie können Volume-Zugriffsgruppen erstellen, indem Sie Initiatoren einer Sammlung von Volumes für den gesicherten Zugriff zuordnen. Sie können dann den Zugriff auf die Volumes in der Gruppe mit einem Schlüssel-CHAP-Initiator und Zielschlüssel gewähren.

Wenn Sie Initiator-basiertes CHAP verwenden, können Sie CHAP-Anmeldeinformationen für einen einzelnen Initiator in einer Volume-Zugriffsgruppe hinzufügen, wodurch mehr Sicherheit gewährleistet wird. Damit können Sie diese Option für bereits vorhandene Volume Access Groups anwenden.

Schritte

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie Auf **Zugriffsgruppe Erstellen**.
3. Geben Sie im Feld **Name** einen Namen für die Zugriffsgruppe des Volumes ein.
4. Sie haben folgende Möglichkeiten, um der Volume-Zugriffsgruppe einen Initiator hinzuzufügen:

Option	Beschreibung
Hinzufügen eines Fibre Channel-Initiators	a. Wählen Sie unter Initiatoren hinzufügen einen vorhandenen Fibre Channel-Initiator aus der Liste Unbound Fibre Channel Initiatoren aus. b. Klicken Sie auf **FC-Initiator hinzufügen**. Sie können während dieses Schritts einen Initiator erstellen, wenn Sie auf den Link **Initiator erstellen** klicken, einen Initiatornamen eingeben und auf **Erstellen** klicken. Das System fügt den Initiator automatisch der Liste Initiatoren hinzu, nachdem Sie ihn erstellt haben. Ein Beispiel für das Format: `5f:47:ac:c0:5c:74:d4:02`
Hinzufügen eines iSCSI-Initiators	Wählen Sie unter Initiatoren hinzufügen einen vorhandenen Initiator aus der Liste Initiatoren aus. **Hinweis:** Wenn Sie in diesem Schritt auf den Link **Initiator erstellen** klicken, einen Initiatornamen eingeben und auf **Erstellen** klicken, können Sie einen Initiator erstellen. Das System fügt den Initiator automatisch der Liste Initiatoren hinzu, nachdem Sie ihn erstellt haben. Ein Beispiel für das Format: `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` Den Initiator-IQN für jedes Volume finden Sie, indem Sie im Menü Aktionen für das Volume auf der Liste **Verwaltung** > **Volumes** > **Active** die Option **Details anzeigen** wählen. Wenn Sie einen Initiator ändern, können Sie das requiredCHAP-Attribut auf „true“ umschalten, sodass Sie den Zielinitiatorschlüssel festlegen können. Weitere Informationen finden Sie unter API-Informationen zur ModifyInitiator API-Methode. "Storage-Management mit der Element API"

5. **Optional:** Fügen Sie weitere Initiatoren nach Bedarf hinzu.
6. Wählen Sie unter Volumes hinzufügen ein Volume aus der Liste **Volumes** aus.

   Der Datenträger wird in der Liste **angehängte Volumes** angezeigt.
7. **Optional:** Hinzufügen Sie weitere Volumen nach Bedarf.
8. Klicken Sie Auf **Zugriffsgruppe Erstellen**.

Weitere Informationen

Fügen Sie einer Zugriffsgruppe Volumes hinzu

Zeigen Sie die Details einzelner Zugriffsgruppen an

Sie können Details für eine einzelne Zugriffsgruppe, z. B. verbundene Volumes und Initiatoren, in einem grafischen Format anzeigen.

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol Aktionen für eine Zugriffsgruppe.
3. Klicken Sie Auf **Details Anzeigen**.

Details zu Volume-Zugriffsgruppen

Die Seite Zugriffsgruppen auf der Registerkarte Verwaltung enthält Informationen zu Volume Access Groups.

Folgende Informationen werden angezeigt:

- **ID**: Die vom System generierte ID für die Zugriffsgruppe.
- **Name**: Der Name, der der Zugriffsgruppe bei der Erstellung gegeben wurde.
- **Aktive Volumes**: Die Anzahl der aktiven Volumes in der Zugriffsgruppe.
- **Komprimierung**: Die Kompressionseffizienz für die Zugriffsgruppe.
- **Deduplizierung**: Die Deduplizierungs-Effizienzbewertung für die Zugriffsgruppe.
- **Thin Provisioning**: Die Thin Provisioning-Effizienzbewertung für die Zugriffsgruppe.
- **Gesamteffizienz**: Die Gesamteffizienz für die Access Group.
- **Initiatoren**: Die Anzahl der Initiatoren, die mit der Zugriffsgruppe verbunden sind.

Fügen Sie einer Zugriffsgruppe Volumes hinzu

Sie können Volumes zu einer Volume-Zugriffsgruppe hinzufügen. Jedes Volume kann mehr als einer Volume-Zugriffsgruppe angehören. Sie können die Gruppen sehen, zu denen jedes Volume gehört, auf der Seite **Active** Volumes.

Mit diesem Verfahren können Sie auch Volumes zu einer Zugriffsgruppe für Fibre Channel-Volumes hinzufügen.

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol Aktionen für die Zugriffsgruppe, der Sie Volumes hinzufügen möchten.
3. Klicken Sie auf die Schaltfläche **Bearbeiten**.
4. Wählen Sie unter Volumes hinzufügen ein Volume aus der Liste **Volumes** aus.

   Sie können weitere Volumes hinzufügen, indem Sie diesen Schritt wiederholen.

5. Klicken Sie Auf **Änderungen Speichern**.

Volumes aus einer Zugriffsgruppe entfernen

Wenn Sie ein Volume aus einer Zugriffsgruppe entfernen, hat die Gruppe keinen Zugriff mehr auf dieses Volume.

Das Ändern von CHAP-Einstellungen in einem Konto oder das Entfernen von Initiatoren oder Volumes aus einer Zugriffsgruppe kann dazu führen, dass Initiatoren unerwartet den Zugriff auf Volumes verlieren. Um zu überprüfen, ob der Volume-Zugriff nicht unerwartet verloren geht, melden Sie sich iSCSI-Sitzungen ab, die von einem Konto oder einer Zugriffsgruppenänderung betroffen sind, und überprüfen Sie, ob die Initiatoren nach Abschluss der Änderungen an den Initiatoreinstellungen und den Cluster-Einstellungen eine Verbindung zu Volumes herstellen können.

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol Aktionen für die Zugriffsgruppe, aus der Sie Volumes entfernen möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Klicken Sie unter Volumes hinzufügen im Dialogfeld **Volume Access Group** bearbeiten auf den Pfeil in der Liste **angehängte Volumes**.
5. Wählen Sie den gewünschten Datenträger aus der Liste aus und klicken Sie auf das Symbol **x**, um das Volume aus der Liste zu entfernen.

   Sie können weitere Volumes entfernen, indem Sie diesen Schritt wiederholen.

6. Klicken Sie Auf **Änderungen Speichern**.

Erstellen eines Initiators

Sie können iSCSI- oder Fibre Channel-Initiatoren erstellen und diese optional Aliase zuweisen.

Sie können auch initator-basierte CHAP-Attribute zuweisen, indem Sie einen API-Aufruf verwenden. Um einen CHAP-Kontonamen und Anmeldeinformationen pro Initiator hinzuzufügen, müssen Sie den verwenden `CreateInitiator` API-Aufruf zum Entfernen und Hinzufügen von CHAP-Zugriff und -Attributen. Der Initiatorzugriff kann auf ein oder mehrere VLANs beschränkt werden, indem ein oder mehrere virtuelle Netzwerk-IDs über das angegeben werden `CreateInitiators` Und `ModifyInitiators` API-Aufrufe. Wenn keine virtuellen Netzwerke angegeben werden, kann der Initiator auf alle Netzwerke zugreifen.

Details finden Sie in den API-Referenzinformationen."Storage-Management mit der Element API"

Schritte

1. Klicken Sie Auf **Management** > **Initiatoren**.
2. Klicken Sie Auf **Initiator Erstellen**.
3. Führen Sie die Schritte aus, um einen einzelnen Initiator oder mehrere Initiatoren zu erstellen:

Option	Schritte
Erstellen eines einzelnen Initiators	a. Klicken Sie auf **Einen einzelnen Initiator erstellen**. b. Geben Sie im Feld **IQN/WWPN** den IQN oder WWPN für den Initiator ein. c. Geben Sie im Feld **Alias** einen Anzeigenamen für den Initiator ein. d. Klicken Sie Auf **Initiator Erstellen**.

Option	Schritte
Erstellen Sie mehrere Initiatoren	a. Klicken Sie Auf **Bulk Create Initiatoren**. b. Geben Sie eine Liste von IQNs oder WWPNs in das Textfeld ein. c. Klicken Sie Auf **Initiatoren Hinzufügen**. d. Wählen Sie einen Initiator aus der Ergebnisliste aus, und klicken Sie in der Spalte **Alias** auf das entsprechende Add-Symbol, um einen Alias für den Initiator hinzuzufügen. e. Klicken Sie auf das Häkchen, um den neuen Alias zu bestätigen. f. Klicken Sie Auf **Initiatoren Erstellen**.

Bearbeiten Sie einen Initiator

Sie können den Alias eines bestehenden Initiators ändern oder einen Alias hinzufügen, wenn einer noch nicht vorhanden ist.

Um einen CHAP-Kontonamen und Anmeldeinformationen pro Initiator hinzuzufügen, müssen Sie den verwenden `ModifyInitiator` API-Aufruf zum Entfernen und Hinzufügen von CHAP-Zugriff und -Attributen.

Siehe "Storage-Management mit der Element API".

Schritte

1. Klicken Sie Auf **Management** > **Initiatoren**.
2. Klicken Sie auf das Symbol Aktionen für den Initiator, den Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Geben Sie im Feld **Alias** einen neuen Alias für den Initiator ein.
5. Klicken Sie Auf **Änderungen Speichern**.

Fügen Sie einen einzelnen Initiator einer Volume-Zugriffsgruppe hinzu

Sie können einem bestehenden Volume-Zugriffsgruppen einen Initiator hinzufügen.

Wenn Sie einer Volume-Zugriffsgruppe einen Initiator hinzufügen, hat der Initiator Zugriff auf alle Volumes in dieser Volume-Zugriffsgruppe.

Sie können den Initiator für jedes Volume finden, indem Sie auf das Aktionen-Symbol klicken und dann **Details anzeigen** für das Volume in der Liste der aktiven Volumes auswählen.

Wenn Sie Initiator-basiertes CHAP verwenden, können Sie CHAP-Anmeldeinformationen für einen einzelnen Initiator in einer Volume-Zugriffsgruppe hinzufügen, wodurch mehr Sicherheit gewährleistet wird. Damit können Sie diese Option für bereits vorhandene Volume Access Groups anwenden.

Schritte

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol **Aktionen** für die Zugriffsgruppe, die Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.

4. So fügen Sie der Zugriffsgruppe für Volumes einen Fibre Channel-Initiator hinzu:

   a. Wählen Sie unter Initiatoren hinzufügen einen vorhandenen Fibre Channel-Initiator aus der Liste **Unbound Fibre Channel Initiatoren** aus.

   b. Klicken Sie auf **FC-Initiator hinzufügen**.

   Sie können während dieses Schritts einen Initiator erstellen, wenn Sie auf den Link **Initiator erstellen** klicken, einen Initiatornamen eingeben und auf **Erstellen** klicken. Das System fügt den Initiator nach dem Erstellen automatisch der Liste **Initiatoren** hinzu.

   Ein Beispiel für das Format:

```
5f:47:ac:c0:5c:74:d4:02
```

5. Um der Volume Access Group einen iSCSI-Initiator hinzuzufügen, wählen Sie unter Add-Initiatoren einen bestehenden Initiator aus der Liste **Initiatoren** aus.

   Sie können während dieses Schritts einen Initiator erstellen, wenn Sie auf den Link **Initiator erstellen** klicken, einen Initiatornamen eingeben und auf **Erstellen** klicken. Das System fügt den Initiator nach dem Erstellen automatisch der Liste **Initiatoren** hinzu.

   Das akzeptierte Format eines Initiator-IQN lautet wie folgt: iqn.yyy-mm, wobei y und m Ziffern sind, gefolgt von Text, der nur Ziffern, alphabetische Kleinbuchstaben, einen Punkt (.), einen Doppelpunkt (:) oder Strich (-) enthalten darf.

   Ein Beispiel für das Format:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

   Den Initiator IQN für jedes Volume finden Sie auf der Seite **Verwaltung** > **Volumes** Aktive Volumes. Klicken Sie dazu auf das Aktionen-Symbol und wählen Sie dann **Details anzeigen** für das Volume aus.

6. Klicken Sie Auf **Änderungen Speichern**.

Fügen Sie einer Volume-Zugriffsgruppe mehrere Initiatoren hinzu

Sie können einer vorhandenen Volume-Zugriffsgruppe mehrere Initiatoren hinzufügen, um den Zugriff auf Volumes in der Volume-Zugriffsgruppe mit oder ohne CHAP-Authentifizierung zu ermöglichen.

Wenn Sie einer Volume-Zugriffsgruppe Initiatoren hinzufügen, haben die Initiatoren Zugriff auf alle Volumes in dieser Volume-Zugriffsgruppe.

Sie können den Initiator für jedes Volume finden, indem Sie auf das Aktionen-Symbol und dann **Details anzeigen** für das Volume in der Liste der aktiven Volumes klicken.

Sie können einer vorhandenen Volume-Zugriffsgruppe mehrere Initiatoren hinzufügen, um den Zugriff auf

Volumes zu ermöglichen und jedem Initiator innerhalb dieser Volume-Zugriffsgruppe eindeutige CHAP-Anmeldeinformationen zuzuweisen. Damit können Sie diese Option für bereits vorhandene Volume Access Groups anwenden.

Sie können initator-basierte CHAP-Attribute mit einem API-Aufruf zuweisen. Um einen CHAP-Kontonamen und Anmeldeinformationen pro Initiator hinzuzufügen, müssen Sie den API-Aufruf zum ModifyInitiator verwenden, um CHAP-Zugriff und -Attribute zu entfernen und hinzuzufügen.

Weitere Informationen finden Sie unter "Storage-Management mit der Element API".

Schritte

1. Klicken Sie Auf **Management** > **Initiatoren**.
2. Wählen Sie die Initiatoren aus, die einer Zugriffsgruppe hinzugefügt werden sollen.
3. Klicken Sie auf die Schaltfläche **Massenaktionen**.
4. Klicken Sie auf **zu Volume Access Group hinzufügen**.
5. Wählen Sie im Dialogfeld zu Volume Access Group hinzufügen eine Zugriffsgruppe aus der Liste **Volume Access Group** aus.
6. Klicken Sie Auf **Hinzufügen**.

Entfernen Sie Initiatoren aus einer Zugriffsgruppe

Wenn Sie einen Initiator aus einer Zugriffsgruppe entfernen, kann er nicht mehr auf die Volumes in dieser Volume-Zugriffsgruppe zugreifen. Der normale Account-Zugriff auf das Volume wird nicht unterbrochen.

Das Ändern von CHAP-Einstellungen in einem Konto oder das Entfernen von Initiatoren oder Volumes aus einer Zugriffsgruppe kann dazu führen, dass Initiatoren unerwartet den Zugriff auf Volumes verlieren. Um zu überprüfen, ob der Volume-Zugriff nicht unerwartet verloren geht, melden Sie sich iSCSI-Sitzungen ab, die von einem Konto oder einer Zugriffsgruppenänderung betroffen sind, und überprüfen Sie, ob die Initiatoren nach Abschluss der Änderungen an den Initiatoreinstellungen und den Cluster-Einstellungen eine Verbindung zu Volumes herstellen können.

Schritte

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol **Aktionen** für die Zugriffsgruppe, die Sie entfernen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. Klicken Sie unter Add Initiatoren im Dialogfeld **Edit Volume Access Group** auf den Pfeil in der Liste **Initiatoren**.
5. Wählen Sie für jeden Initiator das x-Symbol aus, das Sie aus der Zugriffsgruppe entfernen möchten.
6. Klicken Sie Auf **Änderungen Speichern**.

Löschen Sie eine Zugriffsgruppe

Sie können eine Zugriffsgruppe löschen, wenn sie nicht mehr benötigt wird. Sie müssen Initiator-IDs und Volume-IDs nicht aus der Volume-Zugriffsgruppe löschen, bevor Sie die Gruppe löschen. Nachdem Sie die Zugriffsgruppe gelöscht haben, wird der Gruppenzugriff auf die Volumes abgebrochen.

1. Klicken Sie Auf **Verwaltung** > **Zugriffsgruppen**.
2. Klicken Sie auf das Symbol **Aktionen** für die Zugriffsgruppe, die Sie löschen möchten.
3. Klicken Sie im Menü Ergebnis auf **Löschen**.
4. Um auch die Initiatoren zu löschen, die dieser Zugriffsgruppe zugeordnet sind, aktivieren Sie das Kontrollkästchen **Initiatoren löschen in dieser Zugriffsgruppe**.
5. Bestätigen Sie die Aktion.

Löschen eines Initiators

Sie können einen Initiator löschen, nachdem er nicht mehr benötigt wird. Wenn Sie einen Initiator löschen, wird dieser vom System aus einer zugehörigen Volume-Zugriffsgruppe entfernt. Verbindungen, die den Initiator verwenden, bleiben gültig, bis die Verbindung zurückgesetzt wird.

Schritte

1. Klicken Sie Auf **Management** > **Initiatoren**.
2. Führen Sie die Schritte zum Löschen eines einzelnen Initiators oder mehrerer Initiatoren durch:

Option	Schritte
Löschen Sie den einzelnen Initiator	a. Klicken Sie auf das Symbol **Aktionen** für den Initiator, den Sie löschen möchten. b. Klicken Sie Auf **Löschen**. c. Bestätigen Sie die Aktion.
Löschen Sie mehrere Initiatoren	a. Aktivieren Sie die Kontrollkästchen neben den Initiatoren, die Sie löschen möchten. b. Klicken Sie auf die Schaltfläche **Massenaktionen**. c. Wählen Sie im Menü Ergebnis die Option **Löschen** aus. d. Bestätigen Sie die Aktion.

Sichern Sie Ihre Daten

Die NetApp Element Software ermöglicht die Datensicherung auf unterschiedliche Weise mit Funktionen wie Snapshots für einzelne Volumes oder Volume-Gruppen, mit Replizierung zwischen Clustern und Volumes auf Element sowie mit Replizierung auf ONTAP Systemen.

- **Snapshots**

  Bei der Datensicherung nur mit Snapshots werden geänderte Daten zu einem bestimmten Zeitpunkt in ein Remote-Cluster repliziert. Es werden nur die Snapshots repliziert, die auf dem Quellcluster erstellt wurden. Aktive Schreibvorgänge vom Quell-Volume sind nicht.

  Nutzen Sie Volume Snapshots zur Datensicherung

- **Remote-Replikation zwischen Clustern und Volumes, die auf Element** ausgeführt werden

  Sie können Volume-Daten synchron oder asynchron aus einem der beiden Cluster in einem Cluster-Paar replizieren, die beide im Element für Failover- und Failback-Szenarien ausgeführt werden.

  Remote-Replizierung zwischen Clustern mit NetApp Element Software

- **Replizierung zwischen Element und ONTAP Clustern mit SnapMirror Technologie**

  Mit der NetApp SnapMirror Technologie können Snapshots repliziert werden, die für Disaster Recovery mithilfe von Element in ONTAP erstellt wurden. In einer SnapMirror Beziehung stellt Element einen Endpunkt dar, und ONTAP ist der andere.

  SnapMirror Replizierung zwischen Element und ONTAP Clustern

- **Sichern und Wiederherstellen von Volumes aus SolidFire-, S3- oder Swift-Objektspeichern**

  Backups und Restores von Volumes auf anderen SolidFire Storage sowie sekundäre Objektspeicher, die mit Amazon S3 oder OpenStack Swift kompatibel sind.

  Backup und Restore von Volumes in SolidFire-, S3- oder Swift-Objektspeichern

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Nutzen Sie Volume Snapshots zur Datensicherung

Ein Volume Snapshot ist eine zeitpunktgenaue Kopie eines Volumes. Sie können einen Snapshot eines Volumes erstellen und den Snapshot später verwenden, wenn Sie ein Volume zurück in den Zustand verschieben müssen, in dem es zum Zeitpunkt der Snapshot-Erstellung war.

Snapshots ähneln denen von Volume-Klonen. Allerdings sind Snapshots lediglich Replikate von Volume-Metadaten. Sie können also nicht mounten oder darauf schreiben. Das Erstellen eines Volume-Snapshots nimmt ebenfalls nur eine geringe Menge an Systemressourcen und Platz in Anspruch, sodass die Snapshot-Erstellung schneller als das Klonen erfolgt.

Sie können einen Snapshot eines einzelnen Volumes oder einer Gruppe von Volumes erstellen.

Optional können Sie Snapshots in einem Remote-Cluster replizieren und als Backup-Kopie des Volume verwenden. Dies ermöglicht Ihnen, ein Rollback eines Volumes zu einem bestimmten Zeitpunkt mithilfe des replizierten Snapshots durchzuführen. Alternativ können Sie aus einem replizierten Snapshot einen Klon eines Volumes erstellen.

Weitere Informationen

- Individuelle Volume Snapshots zur Datensicherung
- Gruppen-Snapshots für Datenschutzaufgabe wird verwendet
- Planen eines Snapshots

Individuelle Volume Snapshots zur Datensicherung

Ein Volume Snapshot ist eine zeitpunktgenaue Kopie eines Volumes. Sie können ein einzelnes Volume anstelle einer Gruppe von Volumes für den Snapshot verwenden.

Weitere Informationen

- Erstellen eines Volume-Snapshots
- Bearbeiten der Snapshot-Aufbewahrung
- Löschen eines Snapshots
- Klonen eines Volumes aus einem Snapshot
- Rollback eines Volumes zu einem Snapshot
- Sichern eines Volume-Snapshots in einem Amazon S3-Objektspeicher
- Ein Volume Snapshot wird in einem OpenStack Swift Objektspeicher gesichert
- Sichern eines Volume Snapshots auf einem SolidFire Cluster

Erstellen eines Volume-Snapshots

Sie können einen Snapshot eines aktiven Volumes erstellen, um das Volume Image zu einem beliebigen Zeitpunkt beizubehalten. Sie können bis zu 32 Snapshots für ein einzelnes Volume erstellen.

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volumen, das Sie für den Snapshot verwenden möchten.
3. Wählen Sie im Menü Ergebnis die Option **Snapshot** aus.
4. Geben Sie im Dialogfeld **Snapshot des Volumes erstellen** den neuen Snapshot-Namen ein.
5. **Optional:** Aktivieren Sie das Kontrollkästchen **Snapshot in Replikation einschließen, wenn gepaart** aktiviert ist, um sicherzustellen, dass der Snapshot bei der Replikation erfasst wird, wenn das übergeordnete Volume gekoppelt ist.
6. Um die Aufbewahrung für den Snapshot festzulegen, wählen Sie eine der folgenden Optionen aus:
   - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
   - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnboxen, um eine Zeitdauer für das System auszuwählen, um den Snapshot zu behalten.
7. So erstellen Sie einen einzigen, sofortigen Snapshot:
   a. Klicken Sie Auf **Momentaufnahme Jetzt Aufnehmen**.
   b. Klicken Sie Auf**Snapshot Erstellen**.
8. So planen Sie die Ausführung des Snapshots für einen späteren Zeitpunkt:
   a. Klicken Sie Auf **Snapshot Zeitplan Erstellen**.
   b. Geben Sie einen **neuen Terminplannamen** ein.
   c. Wählen Sie aus der Liste einen **Terminplantyp** aus.
   d. **Optional:** Aktivieren Sie das Kontrollkästchen **wiederkehrender Zeitplan**, um den geplanten Snapshot regelmäßig zu wiederholen.
   e. Klicken Sie Auf **Zeitplan Erstellen**.

Weitere Informationen

Planen Sie einen Snapshot

Bearbeiten der Snapshot-Aufbewahrung

Sie können den Aufbewahrungszeitraum für einen Snapshot ändern, um zu steuern, wann oder ob das System Snapshots löscht. Die von Ihnen angegebene Aufbewahrungsdauer beginnt, wenn Sie das neue Intervall eingeben. Wenn Sie einen Aufbewahrungszeitraum festlegen, können Sie einen Zeitraum auswählen, der zum aktuellen Zeitpunkt beginnt (die Aufbewahrung wird nicht aus der Snapshot-Erstellungszeit berechnet). Sie können Intervalle in Minuten, Stunden und Tagen festlegen.

Schritte

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den zu bearbeitenden Snapshot.
3. Klicken Sie im Menü Ergebnis auf **Bearbeiten**.
4. **Optional:** Aktivieren Sie das Kontrollkästchen**Snapshot in Replikation einschließen, wenn gekoppelt**, um sicherzustellen, dass der Snapshot bei der Replikation erfasst wird, wenn das übergeordnete Volume gekoppelt ist.
5. **Optional:** Wählen Sie eine Aufbewahrungsoption für den Snapshot:
   - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
   - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnkästen, um eine Zeitdauer für das System auszuwählen, um den Snapshot beizubehalten.
6. Klicken Sie Auf **Änderungen Speichern**.

Löschen Sie einen Snapshot

Sie können einen Volume-Snapshot aus einem Storage-Cluster löschen, auf dem Element Software ausgeführt wird. Wenn Sie einen Snapshot löschen, entfernt das System ihn sofort.

Sie können Snapshots löschen, die aus dem Quellcluster repliziert werden. Wenn ein Snapshot beim Löschen mit dem Zielcluster synchronisiert wird, wird die synchrone Replikation abgeschlossen und der Snapshot wird aus dem Quellcluster gelöscht. Der Snapshot wird nicht aus dem Ziel-Cluster gelöscht.

Sie können auch Snapshots löschen, die vom Zielcluster zum Ziel repliziert wurden. Der gelöschte Snapshot wird in einer Liste von gelöschten Snapshots auf dem Ziel aufbewahrt, bis das System erkennt, dass Sie den Snapshot auf dem Quell-Cluster gelöscht haben. Wenn das Ziel erkennt, dass Sie den Quell-Snapshot gelöscht haben, wird die Replikation des Snapshots durch das Ziel gestoppt.

Wenn Sie einen Snapshot aus dem Quellcluster löschen, ist der Ziel-Cluster-Snapshot nicht betroffen (die umgekehrte ist auch wahr).

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den zu löschenden Snapshot.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.

4. Bestätigen Sie die Aktion.

Klonen eines Volumes aus einem Snapshot

Sie können ein neues Volume aus einem Snapshot eines Volumes erstellen. Das wird verwendet, um ein neues Volume mithilfe der Snapshot-Informationen zu klonen. Dabei werden die Daten auf dem Volume zum Zeitpunkt der Erstellung des Snapshots verwendet. Dieser Prozess speichert Informationen über andere Snapshots des Volumes im neu erstellten Volume.

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den Snapshot, den Sie für den Volume-Klon verwenden möchten.
3. Klicken Sie im Menü Ergebnis auf **Clone Volume from Snapshot**.
4. Geben Sie im Dialogfeld **Clone Volume from Snapshot** einen **Volume Name** ein.
5. Wählen Sie eine **Gesamtgröße** und Einheiten der Größe für das neue Volumen aus.
6. Wählen Sie für das Volume einen **Access**-Typ aus.
7. Wählen Sie in der Liste ein **Konto** aus, das mit dem neuen Volume verknüpft werden soll.
8. Klicken Sie Auf **Klonen Starten**.

Führen Sie ein Rollback eines Volumes zu einem Snapshot durch

Sie können ein Volume jederzeit auf einen vorherigen Snapshot zurück verschieben. Hierdurch werden alle Änderungen an dem Volume zurückgesetzt, die seit der Erstellung des Snapshots vorgenommen wurden.

Schritte

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den Snapshot, den Sie für das Rollback des Volumes verwenden möchten.
3. Wählen Sie im Menü Ergebnis **Rollback Volume to Snapshot** aus.
4. **Optional:** zum Speichern des aktuellen Status des Volumens vor dem Rollback zum Snapshot:
   a. Wählen Sie im Dialogfeld **Rollback to Snapshot** den aktuellen Status des Volumes als Snapshot speichern* aus.
   b. Geben Sie einen Namen für den neuen Snapshot ein.
5. Klicken Sie Auf **Rollback Snapshot**.

Sichern Sie einen Volume-Snapshot

Sie können die integrierte Backup-Funktion verwenden, um einen Volume-Snapshot zu sichern. Sie können ein Backup von Snapshots aus einem SolidFire Cluster auf einem externen Objektspeicher oder auf einem anderen SolidFire Cluster erstellen. Wenn Sie einen Snapshot in einem externen Objektspeicher sichern, müssen Sie über eine Verbindung zum Objektspeicher verfügen, der Lese-/Schreibvorgänge ermöglicht.

- "Sichern Sie einen Volume Snapshot in einem Amazon S3-Objektspeicher"

- "Sichern Sie einen Volume Snapshot in einem OpenStack Swift Objektspeicher"
- "Sichern Sie einen Volume Snapshot auf einem SolidFire Cluster"

Sichern Sie einen Volume Snapshot in einem Amazon S3-Objektspeicher

Sie können ein Backup von SolidFire Snapshots auf externen Objektspeichern erstellen, die mit Amazon S3 kompatibel sind.

1. Klicken Sie Auf**Data Protection** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den Snapshot, den Sie sichern möchten.
3. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
4. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Backup in** die Option **S3** aus.
5. Wählen Sie eine Option unter **Datenformat** aus:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Geben Sie einen Hostnamen ein, der für den Zugriff auf den Objektspeicher im Feld **Hostname** verwendet werden soll.
7. Geben Sie im Feld **Zugriffsschlüssel-ID** eine Zugriffsschlüssel-ID für das Konto ein.
8. Geben Sie den geheimen Zugriffsschlüssel für das Konto im Feld * Secret Access Key* ein.
9. Geben Sie den S3-Bucket ein, in dem die Sicherung im Feld **S3 Bucket** gespeichert werden soll.
10. **Optional**: Geben Sie im Feld **Nametag** einen Namensschild ein, der dem Präfix angefügt werden soll.
11. Klicken Sie Auf **Lesen Starten**.

Sichern Sie einen Volume Snapshot in einem OpenStack Swift Objektspeicher

Sie können ein Backup von SolidFire Snapshots auf sekundären Objektspeichern erstellen, die mit OpenStack Swift kompatibel sind.

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf das Symbol **Aktionen** für den Snapshot, den Sie sichern möchten.
3. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
4. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Backup in** die Option **Swift** aus.
5. Wählen Sie eine Option unter **Datenformat** aus:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Geben Sie eine **URL** ein, um auf den Objektspeicher zuzugreifen.
7. Geben Sie einen **Benutzername** für das Konto ein.
8. Geben Sie den **Authentifizierungsschlüssel** für das Konto ein.
9. Geben Sie den **Container** ein, in dem die Sicherung gespeichert werden soll.
10. **Optional**: Geben Sie einen **Nametag** ein.
11. Klicken Sie Auf **Lesen Starten**.

Sichern Sie einen Volume Snapshot auf einem SolidFire Cluster

Sie können ein Backup von Volume Snapshots in einem SolidFire Cluster auf einem Remote SolidFire Cluster erstellen.

Stellen Sie sicher, dass die Quell- und Ziel-Cluster gekoppelt sind.

Beim Backup oder Restore von einem Cluster auf ein anderes generiert das System einen Schlüssel, der als Authentifizierung zwischen den Clustern verwendet wird. Dieser Schreibschlüssel für das Massenvolumen ermöglicht es dem Quellcluster, sich beim Schreiben auf das Ziel-Volume mit dem Ziel-Cluster zu authentifizieren. Im Rahmen des Backup- oder Wiederherstellungsprozesses müssen Sie vor dem Start des Vorgangs einen Schreibschlüssel für das Massenvolumen vom Zielvolume generieren.

1. Klicken Sie auf dem Ziel-Cluster auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Zielvolume.
3. Klicken Sie im Menü Ergebnis auf **aus** wiederherstellen.
4. Wählen Sie im Dialogfeld * Integrierter Restore* unter **Wiederherstellen von** die Option **SolidFire** aus.
5. Wählen Sie unter **Datenformat** ein Datenformat aus:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Klicken Sie Auf **Schlüssel Generieren**.
7. Kopieren Sie den Schlüssel aus der Box **Bulk Volume Write Key** in die Zwischenablage.
8. Klicken Sie im Quellcluster auf **Data Protection** > **Snapshots**.
9. Klicken Sie auf das Aktionen-Symbol für den Snapshot, den Sie für das Backup verwenden möchten.
10. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
11. Wählen Sie im Dialogfeld**Integriertes Backup** unter **Backup in** die Option **SolidFire** aus.
12. Wählen Sie im Feld **Datenformat** das gleiche Datenformat aus, das Sie zuvor ausgewählt haben.
13. Geben Sie die virtuelle Management-IP-Adresse des Clusters des Ziel-Volumes im Feld **Remote Cluster MVIP** ein.
14. Geben Sie den Benutzernamen für den Remote-Cluster in das Feld **Remote-Cluster-Benutzername** ein.
15. Geben Sie das Kennwort für den Remote-Cluster im Feld * Remote-Cluster-Kennwort* ein.
16. Fügen Sie im Feld **Bulk Volume Write Key** den Schlüssel ein, den Sie zuvor auf dem Ziel-Cluster generiert haben.
17. Klicken Sie Auf **Lesen Starten**.

Gruppen-Snapshots für Datenschutzaufgabe wird verwendet

Sie können einen Gruppen-Snapshot einer verwandten Gruppe von Volumes erstellen, um eine zeitpunktgenaue Kopie der Metadaten für jedes Volume aufzubewahren. Sie können den Gruppen-Snapshot zukünftig als Backup oder Rollback verwenden, um den Zustand der Volume-Gruppe in einen vorherigen Zustand wiederherzustellen.

Weitere Informationen

- Erstellen Sie einen Gruppen-Snapshot

- Gruppenschnappschüsse bearbeiten
- Mitglieder des Gruppenschnappschusses bearbeiten
- Löschen eines Gruppen-Snapshots
- Rollback von Volumes zu einem Gruppen-Snapshot
- Klonen mehrerer Volumes
- Mehrere Volumes aus einem Gruppen-Snapshot klonen

Snapshot-Details gruppieren

Die Seite Snapshots gruppieren auf der Registerkarte Datenschutz enthält Informationen über die Gruppen-Snapshots.

- **ID**

  Die vom System generierte ID für den Gruppen-Snapshot.

- **UUID**

  Die eindeutige ID des Gruppen-Snapshot.

- **Name**

  Benutzerdefinierter Name für den Gruppen-Snapshot.

- **Zeit Erstellen**

  Die Zeit, zu der der Gruppenschnappschuß erstellt wurde.

- **Status**

  Der aktuelle Status des Snapshots. Mögliche Werte:

  - Vorbereiten: Der Snapshot wird gerade für die Verwendung vorbereitet und ist noch nicht beschreibbar.
  - Fertig: Diese Momentaufnahme hat die Vorbereitung abgeschlossen und ist nun nutzbar.
  - Aktiv: Der Snapshot ist der aktive Verzweig.

- **# Volumen**

  Die Anzahl der Volumes in der Gruppe.

- **Bis** Aufbewahren

  Tag und Uhrzeit des Snapshots werden gelöscht.

- **Remote-Replikation**

  Gibt an, ob der Snapshot für die Replikation auf ein Remote-SolidFire-Cluster aktiviert ist oder nicht. Mögliche Werte:

  - Aktiviert: Der Snapshot ist für die Remote-Replikation aktiviert.
  - Deaktiviert: Der Snapshot ist für die Remote-Replikation nicht aktiviert.

Erstellen eines Gruppen-Snapshots

Sie können einen Snapshot einer Gruppe von Volumes erstellen und auch einen Gruppen-Snapshot-Zeitplan zur Automatisierung von Gruppen-Snapshots erstellen. Ein Snapshot einer einzelnen Gruppe kann konsistent bis zu 32 Volumen gleichzeitig erstellen.

Schritte

1. Klicken Sie Auf **Management** > **Volumes**.
2. Wählen Sie mithilfe der Kontrollkästchen mehrere Volumes für eine Volume-Gruppe aus.
3. Klicken Sie Auf **Massenaktionen**.
4. Klicken Sie Auf **Snapshot Gruppieren**.
5. Geben Sie im Dialogfeld „Snapshot von Volumes erstellen“ einen neuen Gruppennamen für den Snapshot ein.
6. **Optional:** Aktivieren Sie das Kontrollkästchen **jedes GruppenSnapshot-Mitglied in Replikation einschließen, wenn Sie die Replikation gekoppelt haben**, um sicherzustellen, dass jeder Snapshot bei der Replikation erfasst wird, wenn das übergeordnete Volume gekoppelt ist.
7. Wählen Sie eine Aufbewahrungsoption für den Gruppen-Snapshot:
   - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
   - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnboxen, um eine Zeitdauer für das System auszuwählen, um den Snapshot zu behalten.
8. So erstellen Sie einen einzigen, sofortigen Snapshot:
   a. Klicken Sie Auf **Gruppenmomentaufnahme Jetzt Aufnehmen**.
   b. Klicken Sie Auf **Gruppenmomentaufnahme Erstellen**.
9. So planen Sie die Ausführung des Snapshots für einen späteren Zeitpunkt:
   a. Klicken Sie Auf **Snapshot-Zeitplan Der Gruppe Erstellen**.
   b. Geben Sie einen **neuen Terminplannamen** ein.
   c. Wählen Sie einen **Terminplantyp** aus der Liste aus.
   d. **Optional:** Aktivieren Sie das Kontrollkästchen **wiederkehrender Zeitplan**, um den geplanten Snapshot regelmäßig zu wiederholen.
   e. Klicken Sie Auf **Zeitplan Erstellen**.

Gruppenschnappschüsse werden bearbeitet

Sie können die Replizierungs- und Aufbewahrungseinstellungen für vorhandene Gruppen-Snapshots bearbeiten.

1. Klicken Sie Auf **Datenschutz** > **Snapshots Gruppieren**.
2. Klicken Sie auf das Aktionen-Symbol für den Gruppen-Snapshot, den Sie bearbeiten möchten.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. **Optional:** zum Ändern der Replikationseinstellung für den Gruppenschnappschuß:
   a. Klicken Sie neben **Aktuelle Replikation** auf **Bearbeiten**.
   b. Aktivieren Sie das Kontrollkästchen **jedes Gruppenmitglied in Replikation einschließen bei**

Paarung, um sicherzustellen, dass jeder Snapshot bei der Replikation erfasst wird, wenn das übergeordnete Volume gekoppelt ist.

5. **Optional:** um die Aufbewahrungseinstellung für den Gruppenschnappschuß zu ändern, wählen Sie aus den folgenden Optionen:
   a. Klicken Sie neben **Aktuelle Aufbewahrung** auf **Bearbeiten**.
   b. Wählen Sie eine Aufbewahrungsoption für den Gruppen-Snapshot:
      - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
      - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnboxen, um eine Zeitdauer für das System auszuwählen, um den Snapshot zu behalten.
6. Klicken Sie Auf **Änderungen Speichern**.

Löschen eines Gruppen-Snapshots

Sie können einen Gruppen-Snapshot aus dem System löschen. Wenn Sie den Gruppen-Snapshot löschen, können Sie auswählen, ob alle mit der Gruppe verknüpften Snapshots als einzelne Snapshots gelöscht oder beibehalten werden.

Wenn Sie ein Volume oder einen Snapshot löschen, das Mitglied eines Gruppen-Snapshots ist, können Sie nicht mehr zum Gruppen-Snapshot zurückkehren. Sie können jedoch jedes Volume einzeln zurück verschieben.

1. Klicken Sie Auf **Datenschutz** > **Snapshots Gruppieren**.
2. Klicken Sie auf das Symbol Aktionen für den zu löschenden Snapshot.
3. Klicken Sie im Menü Ergebnis auf **Löschen**.
4. Wählen Sie im Bestätigungsdialogfeld eine der folgenden Optionen aus:
   - Klicken Sie auf **GruppenSnapshot und alle Mitglieder der Gruppe löschen**, um den Gruppen-Snapshot und alle Mitglieder-Snapshots zu löschen.
   - Klicken Sie auf **GruppenSnapshot-Mitglieder als einzelne Snapshots**, um den Gruppen-Snapshot zu löschen, aber alle Mitglieder-Snapshots zu behalten.
5. Bestätigen Sie die Aktion.

Rollback von Volumes zu einem Gruppen-Snapshot

Sie können jederzeit ein Rollback einer Gruppe von Volumes zu einem Gruppen-Snapshot durchführen.

Beim Rollback einer Gruppe von Volumes werden alle Volumes in der Gruppe in den Zustand wiederhergestellt, in dem sie sich zum Zeitpunkt der Erstellung des Gruppen-Snapshots befanden. Bei einem Rollback werden auch Volume-Größen an die Größe des ursprünglichen Snapshots wiederhergestellt. Wenn das System ein Volume bereinigt hat, wurden auch alle Snapshots des entsprechenden Volumes zum Zeitpunkt der Löschung gelöscht. Das System stellt keine gelöschten Volume-Snapshots wieder her.

1. Klicken Sie Auf **Datenschutz** > **Snapshots Gruppieren**.
2. Klicken Sie auf das Symbol Aktionen für den Gruppen-Snapshot, den Sie für das Rollback des Volumes verwenden möchten.
3. Wählen Sie im Ergebnismenü **Rollback-Volumes in Gruppenaufnahme** aus.

4. **Optional**: Zum Speichern des aktuellen Status der Volumes vor dem Rollback zum Snapshot:
   a. Wählen Sie im Dialogfeld **Rollback to Snapshot** den aktuellen Status von **Volumes speichern als GruppenSnapshot** aus.
   b. Geben Sie einen Namen für den neuen Snapshot ein.
5. Klicken Sie Auf **Rollback Group Snapshot**.

Bearbeiten von Mitgliedern des Gruppenschnappschusses

Sie können die Aufbewahrungseinstellungen für Mitglieder eines bestehenden Gruppen-Snapshots bearbeiten.

1. Klicken Sie Auf **Datenschutz** > **Snapshots**.
2. Klicken Sie auf die Registerkarte **Mitglieder**.
3. Klicken Sie auf das Aktionen-Symbol für das Gruppenmitglied, das Sie bearbeiten möchten.
4. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
5. Um die Replikationseinstellung für den Snapshot zu ändern, wählen Sie eine der folgenden Optionen aus:
   - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
   - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnboxen, um eine Zeitdauer für das System auszuwählen, um den Snapshot zu behalten.
6. Klicken Sie Auf **Änderungen Speichern**.

Klonen mehrerer Volumes

Sie können mehrere Volume-Klone in einem einzigen Vorgang erstellen, um eine zeitpunktgenaue Kopie der Daten in einer Gruppe von Volumes zu erstellen.

Wenn Sie ein Volume klonen, erstellt das System einen Snapshot des Volume und erstellt dann aus den Daten im Snapshot ein neues Volume. Sie können den neuen Volume-Klon mounten und schreiben. Das Klonen mehrerer Volumes ist ein asynchroner Prozess und erfordert eine variable Zeit, abhängig von der Größe und Anzahl der zu klonenden Volumes.

Die Volume-Größe und die aktuelle Cluster-Last beeinflussen die Zeit, die zum Abschließen eines Klonvorgangs erforderlich ist.

Schritte

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf die Registerkarte **Active**.
3. Aktivieren Sie die Kontrollkästchen, um mehrere Volumes auszuwählen und eine Gruppe von Volumes zu erstellen.
4. Klicken Sie Auf **Massenaktionen**.
5. Klicken Sie im resultierenden Menü auf **Clone**.
6. Geben Sie im Dialogfeld **mehrere Volumes klonen** einen **New Volume Name Prefix** ein.

   Das Präfix wird auf alle Volumes in der Gruppe angewendet.

7. **Optional:** Wählen Sie ein anderes Konto aus, zu dem der Klon gehören wird.

Wenn Sie kein Konto auswählen, weist das System dem aktuellen Volume-Konto die neuen Volumes zu.

8. **Optional:** Wählen Sie eine andere Zugriffsmethode für die Volumes im Klon aus.

   Wenn Sie keine Zugriffsmethode auswählen, verwendet das System den aktuellen Volumenzugriff.

9. Klicken Sie Auf **Klonen Starten**.

Klonen mehrerer Volumes aus einem Gruppen-Snapshot

Sie können eine Gruppe von Volumes aus einem zeitpunktgenauen Snapshot in Gruppen klonen. Für diesen Vorgang muss bereits ein Gruppen-Snapshot der Volumes vorhanden sein, da der Gruppen-Snapshot als Basis für die Erstellung der Volumes verwendet wird. Nachdem Sie die Volumes erstellt haben, können Sie sie wie jedes andere Volume im System verwenden.

Die Volume-Größe und die aktuelle Cluster-Last beeinflussen die Zeit, die zum Abschließen eines Klonvorgangs erforderlich ist.

1. Klicken Sie Auf **Datenschutz** > **Snapshots Gruppieren**.
2. Klicken Sie auf das Aktionen-Symbol für den Gruppen-Snapshot, den Sie für die Volume-Klone verwenden möchten.
3. Wählen Sie im Menü Ergebnis die Option **Volumes aus GruppenSnapshot** klonen.
4. Geben Sie im Dialogfeld **Clone Volumes from Group Snapshot** einen **New Volume Name Prefix** ein.

   Das Präfix wird auf alle Volumes angewendet, die aus dem Gruppen-Snapshot erstellt wurden.

5. **Optional:** Wählen Sie ein anderes Konto aus, zu dem der Klon gehören wird.

   Wenn Sie kein Konto auswählen, weist das System dem aktuellen Volume-Konto die neuen Volumes zu.

6. **Optional:** Wählen Sie eine andere Zugriffsmethode für die Volumes im Klon aus.

   Wenn Sie keine Zugriffsmethode auswählen, verwendet das System den aktuellen Volumenzugriff.

7. Klicken Sie Auf **Klonen Starten**.

Planen Sie einen Snapshot

Sie können Daten auf einem Volume oder einer Gruppe von Volumes schützen, indem Sie die Volume Snapshots in bestimmten Intervallen planen. Sie können entweder einzelne Volume-Snapshots planen oder Snapshots gruppieren, um automatisch auszuführen.

Wenn Sie einen Snapshot-Zeitplan konfigurieren, können Sie zwischen verschiedenen Zeitabständen wählen, die auf Wochentagen oder Tagen des Monats basieren. Sie können auch Tage, Stunden und Minuten festlegen, bevor der nächste Snapshot erstellt wird. Sie können die resultierenden Snapshots auf einem Remote-Storage-System speichern, wenn das Volume repliziert wird.

Weitere Informationen

- Erstellen eines Snapshot-Zeitplans

- Bearbeiten eines Snapshot-Zeitplans
- Löschen Sie einen Snapshot-Zeitplan
- Snapshot-Zeitplan kopieren

Einzelheiten zum Snapshot Zeitplan

Auf der Seite Data Protection > Schedules können Sie die folgenden Informationen in der Liste der Snapshot-Zeitpläne anzeigen.

- **ID**

  Die vom System generierte ID für den Snapshot.

- **Typ**

  Die Art des Zeitplans. Snapshot ist derzeit der einzige Typ, der unterstützt wird.

- **Name**

  Der Name, der dem Zeitplan beim Erstellen angegeben wurde. Snapshot-Planungsnamen können bis zu 223 Zeichen lang sein und a–z, 0–9 und Bindestrich (-) Zeichen enthalten.

- **Frequenz**

  Die Häufigkeit, mit der der Zeitplan ausgeführt wird. Die Häufigkeit kann in Stunden und Minuten, Wochen oder Monaten eingestellt werden.

- **Wiederkehrend**

  Angabe, ob der Zeitplan nur einmal oder in regelmäßigen Abständen ausgeführt werden soll.

- **Manuell Angehalten**

  Gibt an, ob der Zeitplan manuell angehalten wurde oder nicht.

- **Volume-IDs**

  Die ID des Volumens, das der Zeitplan bei der Ausführung des Zeitplans verwendet.

- **Letzter Lauf**

  Das letzte Mal, als der Zeitplan ausgeführt wurde.

- **Status Der Letzten Ausführung**

  Das Ergebnis der letzten Planausführung. Mögliche Werte:

  - Erfolg
  - Ausfall

Erstellen eines Snapshot-Zeitplans

Sie können einen Snapshot eines Volumes oder Volumes so planen, dass er automatisch in bestimmten Intervallen erfolgt.

Wenn Sie einen Snapshot-Zeitplan konfigurieren, können Sie zwischen verschiedenen Zeitabständen wählen, die auf Wochentagen oder Tagen des Monats basieren. Sie können auch einen wiederkehrenden Zeitplan erstellen und die Tage, Stunden und Minuten vor dem nächsten Snapshot festlegen.

Wenn Sie einen Snapshot für einen Zeitraum planen, der nicht durch 5 Minuten teilbar ist, wird der Snapshot zum nächsten Zeitraum ausgeführt, der durch 5 Minuten teilbar ist. Wenn Sie beispielsweise einen Snapshot für die Ausführung um 12:42:00 UTC planen, wird dieser um 12:45:00 UTC ausgeführt. Ein Snapshot kann nicht in Intervallen von weniger als 5 Minuten ausgeführt werden.

Schritte

1. Klicken Sie Auf **Datenschutz** > **Termine**.
2. Klicken Sie Auf **Zeitplan Erstellen**.
3. Geben Sie im Feld **Volume IDs CSV** eine einzelne Volume-ID oder eine kommagetrennte Liste von Volume-IDs ein, die in den Snapshot-Vorgang aufgenommen werden sollen.
4. Geben Sie einen neuen Planungsnamen ein.
5. Wählen Sie einen Zeitplantyp aus, und legen Sie den Zeitplan aus den verfügbaren Optionen fest.
6. **Optional:** Wählen Sie **wiederkehrender Zeitplan**, um den Snapshot-Zeitplan auf unbestimmte Zeit zu wiederholen.
7. **Optional:** Geben Sie im Feld **New Snapshot Name** einen Namen für den neuen Snapshot ein.

   Wenn Sie das Feld leer lassen, verwendet das System die Uhrzeit und das Datum der Erstellung des Snapshots als Namen.

8. **Optional:** Aktivieren Sie das Kontrollkästchen **Snapshots in Replikation einschließen bei gepaarten**, um sicherzustellen, dass die Snapshots bei der Replikation erfasst werden, wenn das übergeordnete Volume gekoppelt ist.
9. Um die Aufbewahrung für den Snapshot festzulegen, wählen Sie eine der folgenden Optionen aus:
   - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
   - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnboxen, um eine Zeitdauer für das System auszuwählen, um den Snapshot zu behalten.
10. Klicken Sie Auf **Zeitplan Erstellen**.

Bearbeiten eines Snapshot-Zeitplans

Sie können vorhandene Snapshot-Zeitpläne ändern. Nach der Änderung verwendet der Zeitplan bei der nächsten Ausführung die aktualisierten Attribute. Alle durch den ursprünglichen Zeitplan erstellten Snapshots verbleiben im Storage-System.

Schritte

1. Klicken Sie Auf **Datenschutz** > **Termine**.
2. Klicken Sie auf das Symbol **Aktionen** für den zu ändernden Zeitplan.
3. Klicken Sie im Menü Ergebnis auf **Bearbeiten**.
4. Ändern Sie im Feld **Volume IDs CSV** die Einzel-Volume-ID oder die kommagetrennte Liste der Volume-IDs, die derzeit im Snapshot-Vorgang enthalten sind.
5. Um den Zeitplan anzuhalten oder fortzusetzen, wählen Sie eine der folgenden Optionen aus:
   - Um einen aktiven Zeitplan anzuhalten, wählen Sie in der Liste **Zeitplan manuell anhalten** die Option **Ja** aus.

- Um einen angehaltenen Zeitplan fortzusetzen, wählen Sie in der Liste **Zeitplan manuell anhalten** die Option **Nein** aus.

6. Geben Sie bei Bedarf einen anderen Namen für den Zeitplan im Feld **Neuer Terminplanname** ein.
7. Um den Zeitplan an verschiedenen Wochentagen oder Monaten zu ändern, wählen Sie **Terminplantyp** aus und ändern Sie den Zeitplan aus den verfügbaren Optionen.
8. **Optional:** Wählen Sie **wiederkehrender Zeitplan**, um den Snapshot-Zeitplan auf unbestimmte Zeit zu wiederholen.
9. **Optional:** Geben Sie im Feld **New Snapshot Name** den Namen für den neuen Snapshot ein oder ändern Sie diesen.

   Wenn Sie das Feld leer lassen, verwendet das System die Uhrzeit und das Datum der Erstellung des Snapshots als Namen.

10. **Optional:** Aktivieren Sie das Kontrollkästchen **Snapshots in Replikation einschließen bei gepaarten**, um sicherzustellen, dass die Snapshots bei der Replikation erfasst werden, wenn das übergeordnete Volume gekoppelt ist.
11. Um die Aufbewahrungseinstellung zu ändern, wählen Sie eine der folgenden Optionen aus:
    - Klicken Sie auf **Keep Forever**, um den Snapshot auf dem System auf unbestimmte Zeit zu behalten.
    - Klicken Sie auf **Aufbewahrungszeitraum festlegen** und verwenden Sie die Datumspinnkästen, um eine Zeitdauer für das System auszuwählen, um den Snapshot beizubehalten.
12. Klicken Sie Auf **Änderungen Speichern**.

Snapshot-Zeitplan kopieren

Sie können einen Zeitplan kopieren und dessen aktuelle Attribute beibehalten.

1. Klicken Sie Auf **Datenschutz** > **Termine**.
2. Klicken Sie auf das Symbol Aktionen für den zu kopierenden Zeitplan.
3. Klicken Sie im Menü Ergebnis auf **Kopie erstellen**.

   Das Dialogfeld **Zeitplan erstellen** wird mit den aktuellen Attributen des Zeitplans ausgefüllt.

4. **Optional:** Geben Sie einen Namen und aktualisierte Attribute für den neuen Zeitplan ein.
5. Klicken Sie Auf **Zeitplan Erstellen**.

Löschen Sie einen Snapshot-Zeitplan

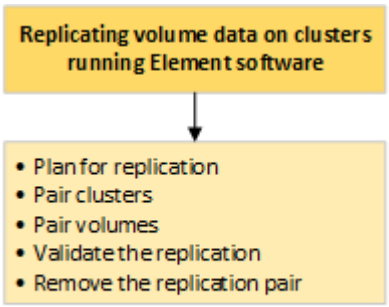
Sie können einen Snapshot-Zeitplan löschen. Nach dem Löschen des Zeitplans werden keine zukünftigen geplanten Snapshots ausgeführt. Alle Snapshots, die nach diesem Zeitplan erstellt wurden, verbleiben im Storage-System.

1. Klicken Sie Auf **Datenschutz** > **Termine**.
2. Klicken Sie für den zu löschenden Zeitplan auf das Symbol **Aktionen**.
3. Klicken Sie im Menü Ergebnis auf **Löschen**.
4. Bestätigen Sie die Aktion.

Remote-Replizierung zwischen Clustern mit NetApp Element Software

Bei Clustern mit Element Software ermöglicht Echtzeitreplizierung die schnelle Erstellung von Remote-Kopien von Volume-Daten. Ein Storage-Cluster kann mit bis zu vier anderen Storage-Clustern gekoppelt werden. Sie können Volume-Daten für Failover- und Failback-Szenarien synchron oder asynchron von einem Cluster in einem Cluster-Paar replizieren.

Der Replikationsprozess umfasst die folgenden Schritte:



- "Planen der Paarung von Clustern und Volumes für die Replizierung in Echtzeit"
- "Paarung von Clustern zur Replizierung"
- "Paar Volumes"
- "Volume-Replizierung validieren"
- "Löschen einer Volume-Beziehung nach der Replikation"
- "Managen Sie Volume-Beziehungen"

Planen der Paarung von Clustern und Volumes für die Replizierung in Echtzeit

Für die Echtzeitreplizierung müssen zwei Storage Cluster, auf denen Element Software ausgeführt wird, Volumes auf jedem Cluster gepaart werden und die Replizierung validiert werden. Nach Abschluss der Replikation sollten Sie die Volume-Beziehung löschen.

Was Sie benötigen

- Für ein oder beide Cluster, die gekoppelt werden, müssen Sie über Administratorrechte verfügen.
- Alle Node-IP-Adressen in Management- und Storage-Netzwerken für gepaarte Cluster werden miteinander verbunden.
- Die MTU aller verbundenen Nodes muss identisch sein und von einem End-to-End-System zwischen den Clustern unterstützt werden.
- Beide Speichercluster sollten eindeutige Cluster-Namen, MVIPs, SVIPs und alle Node-IP-Adressen haben.
- Der Unterschied zwischen den Element Software-Versionen auf den Clustern ist nicht größer als eine Hauptversion. Wenn der Unterschied größer ist, muss ein Cluster aktualisiert werden, um die Datenreplizierung durchzuführen.

WAN Accelerator Appliances wurden von NetApp bei der Datenreplizierung nicht für den Einsatz qualifiziert. Diese Appliances beeinträchtigen die Komprimierung und Deduplizierung, wenn sie zwischen zwei Clustern, bei denen Daten repliziert werden, bereitgestellt werden. Stellen Sie sicher, dass Sie die Auswirkungen jeder WAN Accelerator Appliance vollständig qualifizieren, bevor Sie sie in einer Produktionsumgebung bereitstellen.

Weitere Informationen

- Paarung von Clustern zur Replizierung
- Paar Volumes
- Weisen Sie gepaarten Volumes eine Replikationsquelle und ein Replikationsziel zu

Paarung von Clustern zur Replizierung

Sie müssen zwei Cluster als ersten Schritt mit der Echtzeitreplizierungsfunktion koppeln. Nachdem Sie zwei Cluster miteinander verbunden haben, können Sie aktive Volumes auf einem Cluster konfigurieren, sodass sie kontinuierlich zu einem zweiten Cluster repliziert werden. Dadurch profitieren Sie von kontinuierlicher Datensicherung (CDP).

Was Sie benötigen

- Für ein oder beide Cluster, die gekoppelt werden, müssen Sie über Administratorrechte verfügen.
- Alle Knoten-MIPs und Sips werden miteinander geroutet.
- Weniger als 2000 ms Paketumlauflatenz zwischen Clustern.
- Beide Speichercluster sollten eindeutige Cluster-Namen, MVIPs, SVIPs und alle Node-IP-Adressen haben.
- Der Unterschied zwischen den Element Software-Versionen auf den Clustern ist nicht größer als eine Hauptversion. Wenn der Unterschied größer ist, muss ein Cluster aktualisiert werden, um die Datenreplizierung durchzuführen.

Die Cluster-Paarung erfordert eine vollständige Konnektivität zwischen den Nodes im Managementnetzwerk. Zur Replizierung ist die Verbindung zwischen den einzelnen Nodes im Storage-Cluster-Netzwerk erforderlich.

Ein Cluster kann zu bis zu vier anderen Clustern zur Replizierung von Volumes zusammengefasst werden. Sie können Cluster auch innerhalb der Cluster-Gruppe miteinander kombinieren.

Weitere Informationen

Anforderungen an Netzwerk-Ports

Koppeln Sie Cluster mithilfe von MVIP oder einem Kopplschlüssel

Sie können ein Quell- und Zielcluster mithilfe des MVIP des Zielclusters koppeln, wenn auf beide Cluster-Administratoren Zugriff hat. Wenn der Zugriff des Cluster-Administrators nur auf einem Cluster in einem Cluster-Paar verfügbar ist, kann der Kopplungsschlüssel auf dem Ziel-Cluster verwendet werden, um die Cluster-Paarung abzuschließen.

1. Wählen Sie eine der folgenden Methoden, um Cluster zu koppeln:
   - Paircluster mit MVIP: Verwenden Sie diese Methode, wenn der Clusteradministrator auf beide Cluster

zugreifen kann. Diese Methode verwendet das MVIP des Remote-Clusters, um zwei Cluster zu koppeln.

- Koppeln Sie Cluster mithilfe eines Kopplungsschlüssels: Verwenden Sie diese Methode, wenn der Cluster-Administrator nur auf einen der Cluster zugreifen kann. Diese Methode generiert einen Kopplungsschlüssel, der auf dem Ziel-Cluster zum Abschließen der Cluster-Kopplung verwendet werden kann.

Weitere Informationen

- Koppeln Sie Cluster mit MVIP
- Koppeln Sie Cluster mithilfe eines Kopplschlüssels

Koppeln Sie Cluster mit MVIP

Sie können zwei Cluster für die Echtzeitreplikation koppeln, indem Sie das MVIP eines Clusters verwenden, um eine Verbindung mit dem anderen Cluster herzustellen. Der Zugriff auf beide Cluster-Administratoren ist zur Verwendung dieser Methode erforderlich. Der Clusteradministrator-Benutzername und das Passwort werden zur Authentifizierung des Clusterzugriffs verwendet, bevor die Cluster gekoppelt werden können.

1. Wählen Sie auf dem lokalen Cluster die Option **Data Protection** > **Cluster Pairs** aus.
2. Klicken Sie Auf **Cluster-Paare**.
3. Klicken Sie auf **Pairing starten** und klicken Sie auf **Ja**, um anzuzeigen, dass Sie Zugriff auf den Remote-Cluster haben.
4. Geben Sie die MVIP-Adresse des Remote-Clusters ein.
5. Klicken Sie auf **Pairing auf Remote Cluster abschließen**.

   Geben Sie im Fenster **Authentifizierung erforderlich** den Cluster Administrator Benutzernamen und das Kennwort des Remote-Clusters ein.

6. Wählen Sie auf dem Remote-Cluster die Option **Data Protection** > **Cluster Pairs** aus.
7. Klicken Sie Auf **Cluster-Paare**.
8. Klicken Sie Auf **Pairing Abschließen**.
9. Klicken Sie auf die Schaltfläche * Pairing abschließen*.

Weitere Informationen

- Koppeln Sie Cluster mithilfe eines Kopplschlüssels
- "Koppeln von Clustern mithilfe von MVIP (Video)"

Koppeln Sie Cluster mithilfe eines Kopplschlüssels

Wenn Sie Zugriff auf einen Cluster-Administrator auf ein lokales Cluster, jedoch nicht auf das Remote-Cluster haben, können Sie die Cluster mithilfe eines Kopplungsschlüssels koppeln. Ein Kopplungsschlüssel wird auf einem lokalen Cluster generiert und dann sicher an einen Cluster-Administrator an einem Remote-Standort gesendet, um eine Verbindung herzustellen und die Cluster-Paarung zur Echtzeitreplizierung abzuschließen.

1. Wählen Sie auf dem lokalen Cluster die Option **Data Protection** > **Cluster Pairs** aus.
2. Klicken Sie Auf **Cluster-Paare**.
3. Klicken Sie auf **Pairing starten** und klicken Sie auf **Nein**, um anzuzeigen, dass Sie keinen Zugriff auf das Remote-Cluster haben.
4. Klicken Sie Auf **Schlüssel Generieren**.

   Diese Aktion generiert einen Textschlüssel für das Pairing und erstellt ein nicht konfiguriertes Clusterpaar auf dem lokalen Cluster. Wenn Sie den Vorgang nicht abschließen, müssen Sie das Cluster-Paar manuell löschen.

5. Kopieren Sie den Cluster-Kopplungsschlüssel in die Zwischenablage.
6. Der Kopplungsschlüssel kann dem Clusteradministrator am Remote-Cluster-Standort zugänglich gemacht werden.

   Der Cluster-Kopplungsschlüssel enthält eine Version des MVIP, Benutzernamen, Kennwort und Datenbankinformationen, um Volume-Verbindungen für die Remote-Replikation zu ermöglichen. Dieser Schlüssel sollte sicher behandelt werden und nicht so gespeichert werden, dass ein versehentlicher oder ungesicherter Zugriff auf den Benutzernamen oder das Kennwort möglich wäre.

   Ändern Sie keine Zeichen im Kopplungsschlüssel. Der Schlüssel wird ungültig, wenn er geändert wird.

7. Wählen Sie auf dem Remote-Cluster die Option **Data Protection** > **Cluster Pairs** aus.
8. Klicken Sie Auf **Cluster-Paare**.
9. Klicken Sie auf **Pairing abschließen** und geben Sie den Kopplungschlüssel in das Feld * Pairing Key* ein (Paste ist die empfohlene Methode).
10. Klicken Sie Auf **Pairing Abschließen**.

Weitere Informationen

- Koppeln Sie Cluster mit MVIP
- "Koppeln von Clustern mithilfe eines Cluster-Kopplungsschlüssels (Video)"

Überprüfen Sie die Verbindung des Cluster-Paars

Nach Abschluss der Cluster-Paarung möchten Sie möglicherweise die Verbindung zum Cluster-Paar überprüfen, um den Erfolg der Replizierung zu gewährleisten.

1. Wählen Sie auf dem lokalen Cluster die Option **Data Protection** > **Cluster Pairs** aus.
2. Überprüfen Sie im Fenster **Cluster-Paare**, ob das Cluster-Paar verbunden ist.
3. **Optional:** Navigieren Sie zurück zum lokalen Cluster und dem Fenster **Cluster Pairs** und überprüfen Sie, ob das Cluster-Paar verbunden ist.

Paar Volumes

Nachdem Sie eine Verbindung zwischen den Clustern in einem Cluster-Paar hergestellt

haben, können Sie ein Volume auf einem Cluster mit einem Volume auf dem anderen Cluster des Paars koppeln. Wenn eine Volume-Pairing-Beziehung aufgebaut ist, müssen Sie angeben, welches Volume das Replikationsziel ist.

Sie können zwei Volumes für Echtzeitreplizierung kombinieren, die auf verschiedenen Storage-Clustern in einem verbundenen Cluster-Paar gespeichert sind. Nachdem Sie zwei Cluster miteinander verbunden haben, können Sie aktive Volumes auf einem Cluster konfigurieren, um kontinuierlich auf ein zweites Cluster zu replizieren. Dadurch erhalten Sie kontinuierliche Datensicherung (CDP). Sie können auch ein Volume als Quelle oder Ziel der Replikation zuweisen.

Volume-Paarungen sind immer eins zu eins. Nachdem ein Volume Teil einer Verbindung mit einem Volume auf einem anderen Cluster ist, können Sie es nicht mehr mit einem anderen Volume koppeln.

Was Sie benötigen

- Sie haben eine Verbindung zwischen Clustern in einem Cluster-Paar hergestellt.
- Sie haben Cluster-Administratorrechte für ein oder beide Cluster, die gekoppelt werden.

Schritte

1. Erstellung eines Ziel-Volumes mit Lese- oder Schreibzugriff
2. Koppeln von Volumes mithilfe einer Volume-ID oder eines Kopplungsschlüssels
3. Weisen Sie gepaarten Volumes eine Replikationsquelle und ein Replikationsziel zu

Erstellung eines Ziel-Volumes mit Lese- oder Schreibzugriff

Der Replikationsprozess umfasst zwei Endpunkte: Das Quell- und das Ziel-Volume. Wenn Sie das Ziel-Volume erstellen, wird das Volume automatisch auf den Lese-/Schreibmodus gesetzt, um die Daten während der Replikation zu akzeptieren.

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie Auf **Volume Erstellen**.
3. Geben Sie im Dialogfeld Neues Volume erstellen den Volume-Namen ein.
4. Geben Sie die Gesamtgröße des Volumes ein, wählen Sie eine Blockgröße für das Volume und wählen Sie das Konto aus, das Zugriff auf das Volume haben soll.
5. Klicken Sie Auf **Volume Erstellen**.
6. Klicken Sie im Fenster „aktiv“ auf das Aktionen-Symbol für das Volume.
7. Klicken Sie Auf **Bearbeiten**.
8. Ändern Sie die Kontozugriffsebene auf Replikationsziel.
9. Klicken Sie Auf **Änderungen Speichern**.

Koppeln von Volumes mithilfe einer Volume-ID oder eines Kopplungsschlüssels

Beim Pairing-Prozess werden zwei Volumes entweder über eine Volume-ID oder einen Kopplungsschlüssel gepaart.

1. Koppeln Sie Volumes, indem Sie eine der folgenden Methoden auswählen:
   - Verwendung einer Volume-ID: Verwenden Sie diese Methode, wenn der Cluster-Administrator auf beide Cluster zugreifen kann, auf denen Volumes gekoppelt werden sollen. Diese Methode verwendet

die Volume-ID des Volume des Remote-Clusters, um eine Verbindung zu initiieren.

- Verwenden eines Kopplungsschlüssels: Verwenden Sie diese Methode, wenn der Cluster-Administrator nur auf das Quell-Cluster Zugriff hat. Diese Methode generiert einen Kopplungsschlüssel, der auf dem Remote-Cluster zum Abschließen des Volume-Paars verwendet werden kann.

> Der Kopplungsschlüssel für das Volume enthält eine verschlüsselte Version der Volume-Informationen und kann vertrauliche Informationen enthalten. Diesen Schlüssel nur auf sichere Weise freigeben.

Weitere Informationen

- Kombinieren Sie Volumes mit einer Volume-ID
- Koppeln von Volumes mithilfe eines Kopplschlüssels

Kombinieren Sie Volumes mit einer Volume-ID

Sie können ein Volume mit einem anderen Volume in einem Remote-Cluster koppeln, wenn Sie über Cluster-Administratorberechtigungen für das Remote-Cluster verfügen.

Was Sie benötigen

- Stellen Sie sicher, dass die Cluster, die die Volumes enthalten, gekoppelt sind.
- Erstellen Sie ein neues Volume auf dem Remote-Cluster.

> Sie können eine Replikationsquelle und ein Replikationsziel nach dem Pairing-Prozess zuweisen. Eine Replikationsquelle oder ein Replikationsziel kann ein Volume in einem Volume-Paar sein. Sie sollten ein Ziel-Volume erstellen, das keine Daten enthält und exakt die Merkmale des Quell-Volume hat, z. B. Größe, Einstellung der Blockgröße für die Volumes (512 oder 4 kb) und QoS-Konfiguration. Wenn Sie ein vorhandenes Volume als Replikationsziel zuweisen, werden die Daten auf diesem Volume überschrieben. Das Zielvolume kann größer oder gleich groß sein wie das Quellvolume, kann aber nicht kleiner sein.

- Die Ziel-Volume-ID kennen.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volume, das Sie koppeln möchten.
3. Klicken Sie Auf **Paar**.
4. Wählen Sie im Dialogfeld **Pair Volume** die Option **Pairing starten** aus.
5. Wählen Sie **i do** aus, um anzugeben, dass Sie Zugriff auf den Remote-Cluster haben.
6. Wählen Sie aus der Liste einen **Replikationsmodus** aus:
   - **Echtzeit (Asynchron)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie auf dem Quellcluster erstellt wurden.
   - **Real-Time (Synchronous)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie sowohl auf den Quell- als auch auf den Ziel-Clustern festgelegt sind.
   - **Nur Snapshots**: Nur Snapshots, die auf dem Quellcluster erstellt wurden, werden repliziert. Aktive Schreibvorgänge vom Quell-Volume werden nicht repliziert.

7. Wählen Sie aus der Liste einen Remote-Cluster aus.
8. Wählen Sie eine Remote-Volume-ID aus.
9. Klicken Sie Auf **Pairing Starten**.

   Das System öffnet eine Webbrowser-Registerkarte, die eine Verbindung mit der Element-UI des Remote-Clusters herstellt. Unter Umständen müssen Sie sich mit den Anmeldedaten des Cluster-Administrators im Remote-Cluster anmelden.

10. Wählen Sie in der Element-UI des Remote-Clusters die Option **Complete Pairing**.
11. Bestätigen Sie die Details unter **Volume Pairing bestätigen**.
12. Klicken Sie Auf **Pairing Abschließen**.

    Nachdem Sie die Paarung bestätigt haben, beginnen die beiden Cluster den Prozess, die Volumes zum Koppeln zu verbinden. Während des Pairings können Sie Meldungen in der Spalte **Volume Status** des Fensters **Volume Pairs** sehen. Das Volume-Paar wird angezeigt `PausedMisconfigured` Bis die Quelle und das Ziel des Volume-Paars zugewiesen sind.

    Nach erfolgreichem Abschluss der Paarung sollten Sie die Volume-Tabelle aktualisieren, um die **Pair** -Option aus der **Aktionen**-Liste für das gepaarte Volumen zu entfernen. Wenn Sie die Tabelle nicht aktualisieren, bleibt die Option **Paar** zur Auswahl verfügbar. Wenn Sie die Option **Pair** erneut auswählen, wird eine neue Registerkarte geöffnet, und da das Volume bereits gekoppelt ist, meldet das System einen `StartVolumePairing Failed: xVolumeAlreadyPaired` Fehlermeldung im Fenster **Pair Volume** der Element UI Seite.

Weitere Informationen

- Meldungen zur Volume-Kopplung
- Warnungen zum Volume-Pairing
- Weisen Sie gepaarten Volumes eine Replikationsquelle und ein Replikationsziel zu

Koppeln von Volumes mithilfe eines Kopplschlüssels

Wenn für ein Remote-Cluster keine Cluster-Anmeldedaten vorhanden sind, können Sie ein Volume mithilfe eines Kopplungsschlüssels mit einem anderen Volume auf einem Remote-Cluster koppeln.

Was Sie benötigen

- Stellen Sie sicher, dass die Cluster, die die Volumes enthalten, gekoppelt sind.
- Stellen Sie sicher, dass auf dem Remote-Cluster ein Volume zum Koppeln vorhanden ist.

> Sie können eine Replikationsquelle und ein Replikationsziel nach dem Pairing-Prozess zuweisen. Eine Replikationsquelle oder ein Replikationsziel kann ein Volume in einem Volume-Paar sein. Sie sollten ein Ziel-Volume erstellen, das keine Daten enthält und exakt die Merkmale des Quell-Volume hat, z. B. Größe, Einstellung der Blockgröße für die Volumes (512 oder 4 kb) und QoS-Konfiguration. Wenn Sie ein vorhandenes Volume als Replikationsziel zuweisen, werden die Daten auf diesem Volume überschrieben. Das Zielvolume kann größer oder gleich groß sein wie das Quellvolume, kann aber nicht kleiner sein.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volume, das Sie koppeln möchten.
3. Klicken Sie Auf **Paar**.
4. Wählen Sie im Dialogfeld **Pair Volume** die Option **Pairing starten** aus.
5. Wählen Sie * Ich nicht* aus, um anzugeben, dass Sie keinen Zugriff auf den Remote-Cluster haben.
6. Wählen Sie aus der Liste einen **Replikationsmodus** aus:
   - **Echtzeit (Asynchron)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie auf dem Quellcluster erstellt wurden.
   - **Real-Time (Synchronous)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie sowohl auf den Quell- als auch auf den Ziel-Clustern festgelegt sind.
   - **Nur Snapshots**: Nur Snapshots, die auf dem Quellcluster erstellt wurden, werden repliziert. Aktive Schreibvorgänge vom Quell-Volume werden nicht repliziert.
7. Klicken Sie Auf **Schlüssel Generieren**.

   Diese Aktion generiert einen Textschlüssel für das Koppeln und erstellt ein nicht konfiguriertes Volume-Paar auf dem lokalen Cluster. Wenn Sie den Vorgang nicht abschließen, müssen Sie das Volume-Paar manuell löschen.

8. Kopieren Sie den Kopplungsschlüssel in die Zwischenablage Ihres Computers.
9. Der Kopplungsschlüssel kann dem Cluster-Administrator am Remote-Cluster-Standort zugänglich gemacht werden.

   Der Volume-Kopplungsschlüssel sollte sicher behandelt werden und nicht so verwendet werden, dass ein versehentlicher oder ungesicherter Zugriff möglich wäre.

   Ändern Sie keine Zeichen im Kopplungsschlüssel. Der Schlüssel wird ungültig, wenn er geändert wird.

10. Wählen Sie in der Remote Cluster Element UI die Option **Management** > **Volumes** aus.
11. Klicken Sie auf das Aktionen-Symbol für das Volume, das Sie koppeln möchten.
12. Klicken Sie Auf **Paar**.
13. Wählen Sie im Dialogfeld **Pair Volume** die Option **Complete Pairing** aus.
14. Fügen Sie den Kopplschlüssel aus dem anderen Cluster in die Box **Pairing Key** ein.
15. Klicken Sie Auf **Pairing Abschließen**.

    Nachdem Sie die Paarung bestätigt haben, beginnen die beiden Cluster den Prozess, die Volumes zum Koppeln zu verbinden. Während des Pairings können Sie Meldungen in der Spalte **Volume Status** des Fensters **Volume Pairs** sehen. Das Volume-Paar wird angezeigt `PausedMisconfigured` Bis die Quelle und das Ziel des Volume-Paars zugewiesen sind.

    Nach erfolgreichem Abschluss der Paarung sollten Sie die Volume-Tabelle aktualisieren, um die **Pair** -Option aus der **Aktionen**-Liste für das gepaarte Volumen zu entfernen. Wenn Sie die Tabelle nicht aktualisieren, bleibt die Option **Paar** zur Auswahl verfügbar. Wenn Sie die Option **Pair** erneut auswählen, wird eine neue Registerkarte geöffnet, und da das Volume bereits gekoppelt ist, meldet das System einen `StartVolumePairing Failed: xVolumeAlreadyPaired` Fehlermeldung im Fenster **Pair Volume**

der Element UI Seite.

Weitere Informationen

- Meldungen zur Volume-Kopplung
- Warnungen zum Volume-Pairing
- Weisen Sie gepaarten Volumes eine Replikationsquelle und ein Replikationsziel zu

Weisen Sie gepaarten Volumes eine Replikationsquelle und ein Replikationsziel zu

Nachdem Volumes gekoppelt wurden, müssen Sie ein Quell-Volume und sein Replikationsziel-Volume zuweisen. Eine Replikationsquelle oder ein Replikationsziel kann ein Volume in einem Volume-Paar sein. Sie können dieses Verfahren auch verwenden, um Daten, die an ein Quell-Volume gesendet werden, zu einem Remote-Ziel-Volume umzuleiten, falls das Quell-Volume nicht mehr verfügbar ist.

Was Sie benötigen

Sie haben Zugriff auf die Cluster, die die Quell- und Ziel-Volumes enthalten.

Schritte

1. Vorbereiten des Quellvolumens:

   a. Wählen Sie aus dem Cluster, der das Volume enthält, das Sie als Quelle zuweisen möchten, **Management** > **Volumes** aus.

   b. Klicken Sie auf das Symbol **Aktionen** für das Volume, das Sie als Quelle zuweisen möchten, und klicken Sie auf **Bearbeiten**.

   c. Wählen Sie in der Dropdown-Liste **Zugriff** die Option **Lesen/Schreiben** aus.

   > Wenn Sie die Quell- und Zielzuweisung umkehren, führt diese Aktion dazu, dass das Volume-Paar die folgende Meldung anzeigt, bis ein neues Replikationsziel zugewiesen ist: `PausedMisconfigured`

   Durch das Ändern des Zugriffs wird die Volume-Replizierung angehalten, und die Datenübertragung wird beendet. Vergewissern Sie sich, dass Sie diese Änderungen an beiden Standorten koordiniert haben.

   a. Klicken Sie Auf **Änderungen Speichern**.

2. Bereiten Sie das Zielvolumen vor:

   a. Wählen Sie aus dem Cluster, der das Volume enthält, das Sie als Ziel zuweisen möchten, **Management** > **Volumes** aus.

   b. Klicken Sie auf das Aktionen-Symbol für das Volume, das Sie als Ziel zuweisen möchten, und klicken Sie auf **Bearbeiten**.

   c. Wählen Sie in der Dropdown-Liste **Zugriff** die Option **Replikationsziel** aus.

   > Wenn Sie ein vorhandenes Volume als Replikationsziel zuweisen, werden die Daten auf diesem Volume überschrieben. Es sollte ein neues Ziel-Volume verwendet werden, das keine Daten enthält und exakt die Merkmale des Quell-Volume hat, z. B. Größe, 512-e-Einstellung und QoS-Konfiguration. Das Zielvolume kann größer oder gleich groß sein wie das Quellvolume, kann aber nicht kleiner sein.

d. Klicken Sie Auf **Änderungen Speichern**.

Weitere Informationen

- Kombinieren Sie Volumes mit einer Volume-ID
- Koppeln von Volumes mithilfe eines Kopplschlüssels

Volume-Replizierung validieren

Nach der Replizierung eines Volumes sollten Sie sicherstellen, dass die Quell- und Ziel-Volumes aktiv sind. Im aktiven Zustand werden Volumes gekoppelt. Die Daten werden vom Quell- an das Ziel-Volume gesendet, und die Daten werden im synchronen Modus gespeichert.

1. Wählen Sie in beiden Clustern die Option **Datenschutz** > **Volume Pairs** aus.
2. Vergewissern Sie sich, dass der Volume-Status aktiv ist.

Weitere Informationen

Warnungen zum Volume-Pairing

Löschen einer Volume-Beziehung nach der Replikation

Nachdem die Replikation abgeschlossen ist und Sie die Volume-Paar-Beziehung nicht mehr benötigen, können Sie die Volume-Beziehung löschen.

1. Wählen Sie **Data Protection** > **Volume Pairs**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volume-Paar, das Sie löschen möchten.
3. Klicken Sie Auf **Löschen**.
4. Bestätigen Sie die Meldung.

Managen Sie Volume-Beziehungen

Sie können Volume-Beziehungen auf unterschiedliche Weise verwalten, z. B. die Unterbrechung der Replikation, das Umkehren der Volume-Paarung, das Ändern des Replikationsmodus, das Löschen eines Volume-Paares oder das Löschen eines Cluster-Paars.

Weitere Informationen

- Unterbrechen Sie die Replikation
- Ändern Sie den Modus der Replikation
- Volume-Paare löschen

Unterbrechen Sie die Replikation

Sie können die Replizierung manuell unterbrechen, wenn Sie die I/O-Verarbeitung für kurze Zeit anhalten müssen. Möglicherweise möchten Sie die Replizierung unterbrechen,

wenn die I/O-Verarbeitung stark zulasten und die Verarbeitungslast reduzieren soll.

1. Wählen Sie **Data Protection** > **Volume Pairs**.
2. Klicken Sie auf das Aktionen-Symbol für das Volume-Paar.
3. Klicken Sie Auf **Bearbeiten**.
4. Im Fensterbereich **Volume Pair bearbeiten** wird der Replikationsprozess manuell angehalten.

> Wenn Sie die Volume-Replikation manuell unterbrechen oder fortsetzen, wird die Übertragung der Daten beendet oder fortgesetzt. Vergewissern Sie sich, dass Sie diese Änderungen an beiden Standorten koordiniert haben.

5. Klicken Sie Auf **Änderungen Speichern**.

Ändern Sie den Modus der Replikation

Sie können die Volume-Paar-Eigenschaften bearbeiten, um den Replikationsmodus der Volume-Paar-Beziehung zu ändern.

1. Wählen Sie **Data Protection** > **Volume Pairs**.
2. Klicken Sie auf das Aktionen-Symbol für das Volume-Paar.
3. Klicken Sie Auf **Bearbeiten**.
4. Wählen Sie im Fensterbereich **Volume Pair bearbeiten** einen neuen Replikationsmodus aus:
   - **Echtzeit (Asynchron)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie auf dem Quellcluster erstellt wurden.
   - **Real-Time (Synchronous)**: Schreibvorgänge werden dem Client bestätigt, nachdem sie sowohl auf den Quell- als auch auf den Ziel-Clustern festgelegt sind.
   - **Nur Snapshots**: Nur Snapshots, die auf dem Quellcluster erstellt wurden, werden repliziert. Aktive Schreibvorgänge vom Quell-Volume werden nicht repliziert. **Achtung:** die Änderung der Replikationsmodus ändert den Modus sofort. Vergewissern Sie sich, dass Sie diese Änderungen an beiden Standorten koordiniert haben.
5. Klicken Sie Auf **Änderungen Speichern**.

Volume-Paare löschen

Sie können ein Volume-Paar löschen, wenn Sie eine Paarverbindung zwischen zwei Volumes entfernen möchten.

1. Wählen Sie **Data Protection** > **Volume Pairs**.
2. Klicken Sie auf das Aktionen-Symbol für das Volume-Paar, das Sie löschen möchten.
3. Klicken Sie Auf **Löschen**.
4. Bestätigen Sie die Meldung.

Löschen eines Cluster-Paares

Sie können ein Cluster-Paar aus der Element-UI eines der Cluster im Paar löschen.

1. Klicken Sie Auf **Data Protection** > **Cluster Pairs**.

2. Auf das Aktionen-Symbol für ein Cluster-Paar klicken.
3. Klicken Sie im Menü Ergebnis auf **Löschen**.
4. Bestätigen Sie die Aktion.
5. Führen Sie die Schritte im zweiten Cluster in der Cluster-Paarung erneut aus.

Details zu dem Cluster-Paar

Die Seite Cluster-Paare auf der Registerkarte Datenschutz enthält Informationen zu Clustern, die gekoppelt wurden oder gerade gekoppelt werden. Das System zeigt Pairing- und Fortschrittsmeldungen in der Spalte Status an.

- **ID**

  Eine systemgenerierte ID für die einzelnen Cluster-Paare:

- **Remote Cluster Name**

  Der Name des anderen Clusters im Paar.

- * Remote MVIP*

  Die virtuelle Management-IP-Adresse des anderen Clusters im Paar.

- **Status**

  Replikationsstatus des Remote-Clusters

- **Replikation Von Volumes**

  Die Anzahl der Volumes des Clusters, die zur Replizierung gepaart werden.

- **UUID**

  Eine eindeutige ID, die jedem Cluster im Paar gegeben wurde.

Details zu Volume-Paaren

Die Seite Volume Pairs auf der Registerkarte Data Protection enthält Informationen zu Volumes, die gekoppelt wurden oder gerade gekoppelt werden. Das System zeigt Pairing- und Fortschrittsmeldungen in der Spalte Volume-Status an.

- **ID**

  Vom System generierte ID für das Volume:

- **Name**

  Der Name, der dem Volume bei seiner Erstellung gegeben wurde. Volume-Namen können bis zu 223 Zeichen lang sein und A-z, 0-9 und Bindestrich (-) enthalten.

- **Konto**

  Name des Kontos, der dem Volume zugewiesen wurde.

- **Volume-Status**

  Replikationsstatus des Volumes

- **Snapshot-Status**

  Status des Snapshot-Volumes.

- **Modus**

  Die Client-Schreibreplikationsmethode. Folgende Werte sind möglich:

  - Asynchron
  - Nur Snapshot
  - Synchron

- **Richtung**

  Richtung der Volume-Daten:

  - Quell-Volume-Symbol ( ) Gibt an, dass Daten auf ein Ziel außerhalb des Clusters geschrieben werden.
  - Zielvolume-Symbol ( ) Gibt an, dass Daten von einer externen Quelle auf das lokale Volume geschrieben werden.

- **Async Verzögerung**

  Dauer, seit das Volume zuletzt mit dem Remote-Cluster synchronisiert wurde. Wenn das Volume nicht gekoppelt ist, ist der Wert Null.

- * Remote Cluster*

  Name des Remote-Clusters, auf dem sich das Volume befindet.

- **Remote Volume ID**

  Volume-ID des Volumes im Remote-Cluster.

- **Remote Volume Name**

  Name, der dem Remotecomputer bei seiner Erstellung gegeben wurde.

Meldungen zur Volume-Kopplung

Sie können die Meldungen zur Volume-Kopplung während des ersten Pairing-Prozesses auf der Seite Volume Pairs auf der Registerkarte Data Protection anzeigen. Diese Meldungen können sowohl am Quell- als auch am Zielende des Paares in der Listenansicht „replizierte Volumes“ angezeigt werden.

- **PausedDisconnected**

  Zeitüberschreitung bei der Quellreplizierung oder Synchronisierung von RPCs. Die Verbindung zum Remote-Cluster wurde unterbrochen. Überprüfen Sie die Netzwerkverbindungen mit dem Cluster.

- **ResumingConnected**

  Die Synchronisierung der Remote-Replizierung ist jetzt aktiv. Mit dem Synchronisierungsprozess beginnen und auf Daten warten.

- **ResumingRRSync**

  Dem gekoppelten Cluster wird eine einzige Helix Kopie der Volume-Metadaten erstellt.

- **ResumingLocalSync**

  Dem gekoppelten Cluster wird eine doppelte Helix Kopie der Volume-Metadaten erstellt.

- **ResumingDataTransfer**

  Die Datenübertragung wurde fortgesetzt.

- * Aktiv*

  Volumes werden gekoppelt und Daten werden vom Quell-Volume an das Ziel-Volume gesendet, und die Daten werden synchron.

- **Frei**

  Es findet keine Replikationsaktivität statt.

Warnungen zum Volume-Pairing

Die Seite Thevolme Pairs auf der Registerkarte Datenschutz enthält diese Meldungen, nachdem Sie Volumes gepaart haben. Diese Meldungen können an den Quell- und Zielenden des Paares (sofern nicht anders angegeben) in der Listenansicht „replizierte Volumes“ angezeigt werden.

- * PausedClusterFull*

  Da das Ziel-Cluster voll ist, können die Quell-Replizierung und der Transfer von Massendaten nicht fortgesetzt werden. Die Meldung wird nur am Quellende des Paares angezeigt.

- **PausedExceedMaxSnapshotCount**

  Das Ziel-Volume verfügt bereits über die maximale Anzahl an Snapshots und kann keine zusätzlichen Snapshots replizieren.

- **PausedManual**

  Lokales Volume wurde manuell angehalten. Sie muss aufgehoben werden, bevor die Replikation fortgesetzt wird.

- **PausedManualRemote**

  Fernlautstärke befindet sich im manuellen Paused-Modus. Um das Remote-Volume vor dem Fortschreiten der Replikation zu unterbrechen, ist ein manueller Eingriff erforderlich.

- **PausedUnkonfiguriert**

Warten auf eine aktive Quelle und ein aktives Ziel. Manuelle Eingriffe sind erforderlich, um die Replikation fortzusetzen.

- **PausedQoS**

  Ziel-QoS konnte eingehende I/O nicht aufrechterhalten. Automatische Wiederaufnahme der Replikation. Die Meldung wird nur am Quellende des Paares angezeigt.

- **PausedSlowLink**

  Langsame Verbindung wurde erkannt und die Replikation wurde angehalten. Automatische Wiederaufnahme der Replikation. Die Meldung wird nur am Quellende des Paares angezeigt.

- **PausedVolumeSizeMischmatch**

  Das Ziel-Volume ist nicht dieselbe Größe wie das Quell-Volume.

- **PausedXCopy**

  Ein SCSI XCOPY-Befehl wird an ein Quell-Volume übergeben. Der Befehl muss abgeschlossen sein, bevor die Replikation fortgesetzt werden kann. Die Meldung wird nur am Quellende des Paares angezeigt.

- **StoppedMiskonfiguriert**

  Es wurde ein permanenter Konfigurationsfehler erkannt. Das entfernte Volume wurde gelöscht oder entpaart. Es ist keine Korrekturmaßnahme möglich; es muss eine neue Paarung eingerichtet werden.

SnapMirror Replizierung zwischen Element und ONTAP Clustern

Sie können SnapMirror Beziehungen auf der Registerkarte Datensicherheit in der NetApp Element Benutzeroberfläche erstellen. Um dies in der Benutzeroberfläche zu sehen, muss die SnapMirror Funktionalität aktiviert sein.

IPv6 wird für die SnapMirror Replizierung zwischen NetApp Element Software und ONTAP Clustern nicht unterstützt.

"NetApp Video: SnapMirror für NetApp HCI und Element Software"

Systeme mit NetApp Element Software unterstützen SnapMirror Funktionen zum Kopieren und Wiederherstellen von Snapshot Kopien mit NetApp ONTAP Systemen. Der Hauptgrund für den Einsatz dieser Technologie ist die Disaster Recovery von NetApp HCI auf ONTAP. Endpunkte sind ONTAP, ONTAP Select und Cloud Volumes ONTAP. Siehe TR-4641 NetApp HCI Datensicherung.

"Technischer Bericht 4641 zu NetApp HCI Datensicherung"

Weitere Informationen

- "Ihr Weg zur eigenen Data Fabric – mit NetApp HCI, ONTAP und konvergenter Infrastruktur"
- "Replizierung zwischen NetApp Element Software und ONTAP"

Übersicht über SnapMirror

Systeme mit NetApp Element Software unterstützen SnapMirror Funktionen zum

Kopieren und Wiederherstellen von Snapshots mit NetApp ONTAP Systemen.

Systeme mit Element können direkt mit SnapMirror auf ONTAP Systemen ab 9.3 kommunizieren. Die NetApp Element API bietet Methoden zur Aktivierung der SnapMirror Funktion in Clustern, Volumes und Snapshots. Außerdem verfügt die Element UI über alle erforderlichen Funktionen zum Management von SnapMirror Beziehungen zwischen Element Software und ONTAP Systemen.

Von ONTAP stammende Volumes können in bestimmten Anwendungsfällen mit eingeschränkter Funktionalität zu Element Volumes repliziert werden. Weitere Informationen finden Sie in der ONTAP-Dokumentation.

Weitere Informationen

"Replizierung zwischen Element Software und ONTAP"

Aktivieren Sie SnapMirror auf dem Cluster

Sie müssen die SnapMirror Funktion auf Cluster-Ebene manuell über die NetApp Element UI aktivieren. Im System ist die SnapMirror Funktion standardmäßig deaktiviert und wird im Rahmen einer neuen Installation oder eines Upgrades nicht automatisch aktiviert. Die Aktivierung der SnapMirror Funktion ist eine einmalige Konfigurationsaufgabe.

SnapMirror kann nur für Cluster aktiviert werden, auf denen Element Software in Verbindung mit Volumes auf einem NetApp ONTAP System verwendet wird. Sie sollten die SnapMirror Funktion nur aktivieren, wenn Ihr Cluster zur Verwendung mit NetApp ONTAP Volumes verbunden ist.

Was Sie benötigen

Der Storage Cluster muss die NetApp Element Software ausführen.

Schritte

1. Klicken Sie Auf **Cluster** > **Einstellungen**.
2. Suchen Sie die Cluster-spezifischen Einstellungen für SnapMirror.
3. Klicken Sie auf **SnapMirror aktivieren**.

> Durch die Aktivierung der SnapMirror Funktion wird die Konfiguration der Element Software endgültig geändert. Sie können die SnapMirror Funktion deaktivieren und nur die Standardeinstellungen wiederherstellen, indem Sie das Cluster wieder zum Werkseinstellungen zurücksetzen.

4. Klicken Sie auf **Ja**, um die SnapMirror-Konfigurationsänderung zu bestätigen.

Aktivieren Sie SnapMirror auf dem Volume

Sie müssen SnapMirror auf dem Volume in der Element UI aktivieren. Dies ermöglicht die Replikation von Daten auf festgelegte ONTAP-Volumes. Dies ist die Erlaubnis des Administrators des Clusters, auf dem die NetApp Element Software für SnapMirror ausgeführt wird, um ein Volume zu steuern.

Was Sie benötigen

- Sie haben SnapMirror in der Element UI für das Cluster aktiviert.

- Ein SnapMirror Endpunkt ist verfügbar.
- Das Volume muss mit einer Blockgröße von 512 E liegen.
- Das Volume ist nicht an der Remote-Replikation beteiligt.
- Der Volume-Zugriffstyp ist kein Replikationsziel.

Sie können diese Eigenschaft auch beim Erstellen oder Klonen eines Volumes festlegen.

Schritte

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volume, für das Sie SnapMirror aktivieren möchten.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. Aktivieren Sie im Dialogfeld **Volume bearbeiten** das Kontrollkästchen **SnapMirror aktivieren**.
5. Klicken Sie Auf **Änderungen Speichern**.

Erstellen eines SnapMirror Endpunkts

Sie müssen einen SnapMirror Endpunkt in der NetApp Element-Benutzeroberfläche erstellen, bevor Sie eine Beziehung erstellen können.

Ein SnapMirror Endpunkt ist ein ONTAP Cluster, das als Replizierungsziel für ein Cluster dient, auf dem die Element Software ausgeführt wird. Bevor Sie eine SnapMirror Beziehung erstellen, erstellen Sie zuerst einen SnapMirror Endpunkt.

Es können bis zu vier SnapMirror Endpunkte in einem Storage-Cluster, auf dem die Element Software ausgeführt wird, erstellt und gemanagt werden.

Wenn ein vorhandener Endpunkt ursprünglich mit der API erstellt wurde und keine Anmeldedaten gespeichert wurden, können Sie den Endpunkt in der Element-UI sehen und dessen Existenz überprüfen. Er kann jedoch nicht über die Element-UI gemanagt werden. Dieser Endpunkt kann dann nur mit der Element-API gemanagt werden.

Weitere Informationen zu API-Methoden finden Sie unter "Storage-Management mit der Element API".

Was Sie benötigen

- Sie sollten SnapMirror in der Element UI für den Storage-Cluster aktiviert haben.
- Ihnen kennen die ONTAP-Anmeldedaten für den Endpunkt.

Schritte

1. Klicken Sie auf **Datensicherung** > **SnapMirror Endpunkte**.
2. Klicken Sie Auf **Endpunkt Erstellen**.
3. Geben Sie im Dialogfeld **Neuen Endpunkt erstellen** die Cluster-Management-IP-Adresse des ONTAP-Systems ein.
4. Geben Sie die mit dem Endpunkt verknüpften Anmeldedaten für den ONTAP-Administrator ein.
5. Lesen Sie weitere Details durch:
    - LIFs: Listet die ONTAP clusterübergreifende logische Schnittstellen auf, die zur Kommunikation mit Element verwendet werden.

- Status: Zeigt den aktuellen Status des SnapMirror-Endpunkts an. Mögliche Werte sind: Verbunden, getrennt und nicht verwaltet.

6. Klicken Sie Auf **Endpunkt Erstellen**.

SnapMirror Beziehung erstellen

Sie müssen eine SnapMirror Beziehung in der NetApp Element UI erstellen.

> Wenn ein Volume für SnapMirror noch nicht aktiviert ist und Sie eine Beziehung aus der Element UI erstellen möchten, wird SnapMirror auf diesem Volume automatisch aktiviert.

Was Sie benötigen

SnapMirror ist auf dem Volume aktiviert.

Schritte

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol **Aktionen** für das Volume, das Teil der Beziehung sein soll.
3. Klicken Sie auf **Erstellen Sie eine SnapMirror Beziehung**.
4. Wählen Sie im Dialogfeld **eine SnapMirror-Beziehung erstellen** einen Endpunkt aus der Liste **Endpunkt** aus.
5. Wählen Sie aus, ob die Beziehung mit einem neuen ONTAP Volume oder einem vorhandenen ONTAP Volume erstellt werden soll.
6. Um ein neues ONTAP Volume in der Element UI zu erstellen, klicken Sie auf **Neues Volume erstellen**.
   a. Wählen Sie für diese Beziehung die **Storage Virtual Machine** aus.
   b. Wählen Sie aus der Dropdown-Liste das **Aggregat** aus.
   c. Geben Sie im Feld **Volume Name Suffix** ein Suffix ein.

      > Das System erkennt den Namen des Quell-Volumes und kopiert ihn in das Feld **Volume Name**. Das Suffix, das Sie eingeben, fügt den Namen an.

   d. Klicken Sie Auf **Zielvolumen Erstellen**.
7. Um ein vorhandenes ONTAP-Volume zu verwenden, klicken Sie auf **vorhandenes Volume verwenden**.
   a. Wählen Sie für diese Beziehung die **Storage Virtual Machine** aus.
   b. Wählen Sie das Volume aus, das das Ziel für diese neue Beziehung ist.
8. Wählen Sie im Abschnitt **Beziehungsdetails** eine Richtlinie aus. Wenn in der ausgewählten Richtlinie Regeln beibehalten sind, werden in der Tabelle Regeln die Regeln und die zugehörigen Beschriftungen angezeigt.
9. **Optional**: Wählen Sie einen Zeitplan aus.

   Dadurch wird festgelegt, wie oft die Beziehung Kopien erstellt.

10. **Optional**: Geben Sie im Feld **Limit Bandwidth to** die maximale Bandbreite ein, die von Datenübertragungen in Verbindung mit dieser Beziehung verbraucht werden kann.
11. Lesen Sie weitere Details durch:
    - **Zustand**: Aktueller Beziehungsstatus des Zielvolumens. Mögliche Werte sind:

        - Nicht initialisiert: Das Ziel-Volume wurde nicht initialisiert.
        - Snapmirrored: Das Ziel-Volume wurde initialisiert und ist bereit, SnapMirror Updates zu erhalten.
        - Broken-off: Der Zieldatenträger ist Lesen/Schreiben und Schnappschüsse sind vorhanden.
    - **Status**: Aktueller Status der Beziehung. Mögliche Werte sind inaktiv, übertragen, prüfen, stilllegen, stilllegen, Warteschlange, Vorbereitung, Fertigstellung, Abbruch und Abbrechen.
    - **Lag-Zeit**: Die Zeit in Sekunden, die das Zielsystem hinter das Quellsystem hinkt. Die Verzögerungszeit darf nicht länger als das Transferzeitintervall sein.
    - **Bandbreitenbegrenzung**: Die maximale Bandbreite, die von Datenübertragungen in Verbindung mit dieser Beziehung verbraucht werden kann.
    - **Letzter übertragen**: Zeitstempel des zuletzt übertragenen Snapshots. Klicken Sie auf, um weitere Informationen zu erhalten.
    - **Policy Name**: Der Name der ONTAP SnapMirror Politik für die Beziehung.
    - **Richtlinientyp**: Art der ONTAP-SnapMirror-Politik für die Beziehung ausgewählt. Mögliche Werte sind:
        - Async_Mirror
        - Mirror_Vault
    - **Terminplanname**: Name des bereits vorhandenen Zeitplans auf dem für diese Beziehung ausgewählten ONTAP-System.
12. Um die Initialisierung zu diesem Zeitpunkt nicht zu starten, stellen Sie sicher, dass das Kontrollkästchen **Initialisieren** nicht aktiviert ist.

    Initialisierung kann sehr zeitaufwendig sein. Möglicherweise möchten Sie dies in Zeiten geringerer Auslastung durchführen. Bei der Initialisierung wird ein Basistransfer durchgeführt. Es erstellt eine Snapshot Kopie des Quell-Volume und überträgt dann die Kopie sowie alle Datenblöcke, auf die er auf das Ziel-Volume verweist. Sie können den Initialisierungsprozess (und nachfolgende Updates) manuell initialisieren oder einen Zeitplan verwenden, um den Zeitplan zu starten.

13. Klicken Sie Auf **Beziehung Erstellen**.
14. Klicken Sie auf **Datensicherung** > **SnapMirror Beziehungen**, um diese neue SnapMirror Beziehung anzuzeigen.

Aktionen für SnapMirror Beziehungen

Auf der Seite SnapMirror Beziehungen auf der Registerkarte Datensicherung können Sie eine Beziehung konfigurieren. Die Optionen aus dem Aktionen-Symbol werden hier beschrieben.

- **Bearbeiten**: Bearbeitet die verwendete Richtlinie oder den Zeitplan für die Beziehung.
- **Löschen**: Löscht die SnapMirror-Beziehung. Diese Funktion löscht nicht das Zielvolume.
- **Initialize**: Führt den ersten Basistransfer der Daten durch, um eine neue Beziehung aufzubauen.
- **Update**: Führt eine On-Demand-Aktualisierung der Beziehung durch, repliziert neue Daten und Snapshot-Kopien, die seit der letzten Aktualisierung zum Ziel enthalten sind.
- **Quiesce**: Verhindert weitere Updates für eine Beziehung.
- **Fortsetzen**: Nimmt eine Beziehung auf, die stillgelegt wird.

- **Break**: Macht das Zielvolumen Lesen-Schreiben und stoppt alle aktuellen und zukünftigen Transfers. Legen Sie fest, dass Clients das ursprüngliche Quell-Volume nicht verwenden, da durch den umgekehrten Resync-Vorgang das ursprüngliche Quellvolumen schreibgeschützt ist.
- **Resync**: Stellt eine zerbrochene Beziehung in die gleiche Richtung wieder her, bevor die Pause stattfand.
- **Reverse Resync**: Automatisiert die notwendigen Schritte, um eine neue Beziehung in die entgegengesetzte Richtung zu erstellen und zu initialisieren. Dies kann nur geschehen, wenn die bestehende Beziehung in einem gebrochenen Zustand ist. Durch diesen Vorgang wird die aktuelle Beziehung nicht gelöscht. Das ursprüngliche Quell-Volume wird auf die zuletzt verwendete Snapshot Kopie zurückgesetzt und mit dem Ziel neu synchronisiert. Alle Änderungen, die seit der letzten erfolgreichen SnapMirror Aktualisierung auf dem ursprünglichen Quell-Volume vorgenommen werden, gehen verloren. Alle vorgenommenen Änderungen oder neu auf das aktuelle Ziel-Volume geschriebenen Daten werden zurück an das ursprüngliche Quell-Volume gesendet.
- **Abbrechen**: Bricht eine laufende Übertragung ab. Wenn ein SnapMirror Update für eine abgebrochene Beziehung ausgegeben wird, wird die Beziehung mit dem letzten Transfer vom letzten vor dem Abbrechen erstellten Neustart Checkpoint fortgesetzt.

SnapMirror-Labels

Ein SnapMirror-Label dient als Marker für die Übertragung eines angegebenen Snapshots nach den Aufbewahrungsregeln der Beziehung.

Durch das Anwenden eines Labels auf einen Snapshot wird es als Ziel für die SnapMirror Replikation markiert. Aufgabe der Beziehung ist es, die Regeln beim Datentransfer durchzusetzen, indem der passende Snapshot ausgewählt, auf das Ziel-Volume kopiert und die korrekte Anzahl von Kopien aufbewahrt wird. Er bezieht sich auf die Richtlinie zur Bestimmung der Anzahl der Aufbewahrung und des Aufbewahrungszeitraums. Die Richtlinie kann eine beliebige Anzahl von Regeln haben, und jede Regel hat eine eindeutige Kennzeichnung. Dieses Etikett dient als Verbindung zwischen dem Snapshot und der Aufbewahrungsregel.

Es ist das SnapMirror-Label, das angibt, welche Regel für den ausgewählten Snapshot, den Gruppen-Snapshot oder den ausgewählten Zeitplan angewendet wird.

Fügen Sie SnapMirror-Beschriftungen zu Snapshots hinzu

Die SnapMirror-Beschriftungen geben die Snapshot-Aufbewahrungsrichtlinie auf dem SnapMirror-Endpunkt an. Sie können Snapshots mit Beschriftungen hinzufügen und sie gruppieren.

Sie können verfügbare Beschriftungen in einem Dialogfeld für eine vorhandene SnapMirror Beziehung oder in dem NetApp ONTAP System Manager anzeigen.

> Wenn Sie einem Gruppen-Snapshot ein Etikett hinzufügen, werden alle vorhandenen Beschriftungen zu einzelnen Snapshots überschrieben.

Was Sie benötigen

- SnapMirror ist auf dem Cluster aktiviert.
- Die Beschriftung, die Sie hinzufügen möchten, ist bereits in ONTAP vorhanden.

Schritte

1. Klicken Sie auf **Data Protection** > **Snapshots** oder **Gruppen-Snapshots** Seite.
2. Klicken Sie auf das Symbol **Aktionen** für den Snapshot oder Gruppen-Snapshot, dem Sie ein SnapMirror-

Etikett hinzufügen möchten.

3. Geben Sie im Dialogfeld **Snapshot bearbeiten** Text in das Feld **SnapMirror-Bezeichnung** ein. Das Etikett muss mit einem Regellabel in der Richtlinie für die SnapMirror Beziehung übereinstimmen.
4. Klicken Sie Auf **Änderungen Speichern**.

Fügen Sie SnapMirror-Beschriftungen zu Snapshot-Zeitplänen hinzu

Sie können SnapMirror Beschriftungen zu Snapshot-Zeitplänen hinzufügen, um sicherzustellen, dass eine SnapMirror-Richtlinie angewendet wird. Sie können verfügbare Labels aus einem vorhandenen SnapMirror-Beziehungsdialogfeld oder NetAppONTAP System Manager anzeigen.

Was Sie benötigen

- SnapMirror muss auf Cluster-Ebene aktiviert sein.
- Die Beschriftung, die Sie hinzufügen möchten, ist bereits in ONTAP vorhanden.

Schritte

1. Klicken Sie Auf **Datenschutz** > **Termine**.
2. Sie können einem Zeitplan auf eine der folgenden Arten ein SnapMirror-Label hinzufügen:

Option	Schritte
Erstellen eines neuen Zeitplans	a. Wählen Sie **Zeitplan Erstellen**. b. Geben Sie alle anderen relevanten Details ein. c. Wählen Sie **Zeitplan Erstellen**.
Ändern des vorhandenen Zeitplans	a. Klicken Sie auf das Symbol **Aktionen** für den Zeitplan, dem Sie eine Bezeichnung hinzufügen möchten, und wählen Sie **Bearbeiten**. b. Geben Sie im daraufhin angezeigten Dialogfeld Text in das Feld **SnapMirror Label** ein. c. Wählen Sie **Änderungen Speichern**.

Weitere Informationen

Erstellen eines Snapshot-Zeitplans

Disaster Recovery mit SnapMirror

Bei einem Problem mit einem Volume oder Cluster, auf dem die NetApp Element Software ausgeführt wird, brechen Sie mithilfe der SnapMirror Funktion die Beziehung und ein Failover auf das Ziel-Volume ab.

Falls das ursprüngliche Cluster vollständig ausgefallen ist oder nicht vorhanden ist, wenden Sie sich an den NetApp Support, um weitere Unterstützung zu erhalten.

Führen Sie ein Failover von einem Element Cluster aus

Sie können ein Failover vom Element Cluster durchführen, um für Hosts auf der Zielseite das Lese-/Schreibvolume zu erhalten und auf diese zugreifen zu können. Bevor Sie ein Failover vom Element-Cluster durchführen, müssen Sie die SnapMirror Beziehung unterbrechen.

Verwenden Sie die Benutzeroberfläche von NetApp Element, um den Failover auszuführen. Wenn die Element-UI nicht verfügbar ist, können Sie auch den Befehl „Beziehungen unterbrechen“ mit ONTAP System Manager oder ONTAP CLI eingeben.

Was Sie benötigen

- Eine SnapMirror-Beziehung ist vorhanden und hat mindestens einen gültigen Snapshot auf dem Ziel-Volume.
- Aufgrund ungeplanter Ausfälle oder eines geplanten Ereignisses am primären Standort ist ein Failover auf das Ziel-Volume erforderlich.

Schritte

1. Klicken Sie in der Element UI auf **Data Protection** > **SnapMirror Relationships**.
2. Finden Sie die Beziehung zum Quellvolume, das Sie Failover ausführen möchten.
3. Klicken Sie auf das Symbol **Aktionen**.
4. Klicken Sie Auf **Pause**.
5. Bestätigen Sie die Aktion.

   Das Volume auf dem Ziel-Cluster verfügt jetzt über Lese- und Schreibzugriff, kann auf die Applikations-Hosts eingebunden werden, um die Produktions-Workloads wieder aufzunehmen. Durch diese Aktion wird die gesamte SnapMirror-Replikation angehalten. Die Beziehung zeigt einen Abbruch.

Führen Sie ein Failback zum Element durch

Wenn das Problem auf der primären Seite gemindert wurde, müssen Sie das ursprüngliche Quell-Volume neu synchronisieren und zur NetApp Element Software zurückkehren. Die entsprechenden Schritte hängen davon ab, ob das ursprüngliche Quell-Volume noch vorhanden ist oder Sie ein Failback auf ein neu erstelltes Volume durchführen müssen.

Weitere Informationen

- Führen Sie ein Failback durch, wenn das Quell-Volume noch vorhanden ist
- Führen Sie ein Failback durch, wenn das Quell-Volume nicht mehr vorhanden ist
- SnapMirror Failback-Szenarien

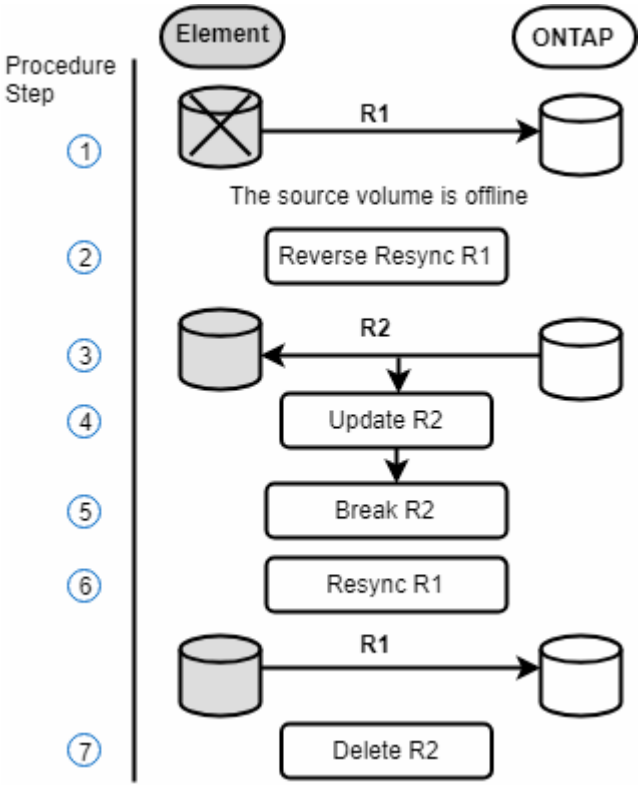
SnapMirror Failback-Szenarien

Die Disaster Recovery-Funktion von SnapMirror wird in zwei Failback-Szenarien dargestellt. Diese gehen davon aus, dass die ursprüngliche Beziehung (unterbrochen) fehlgeschlagen ist.

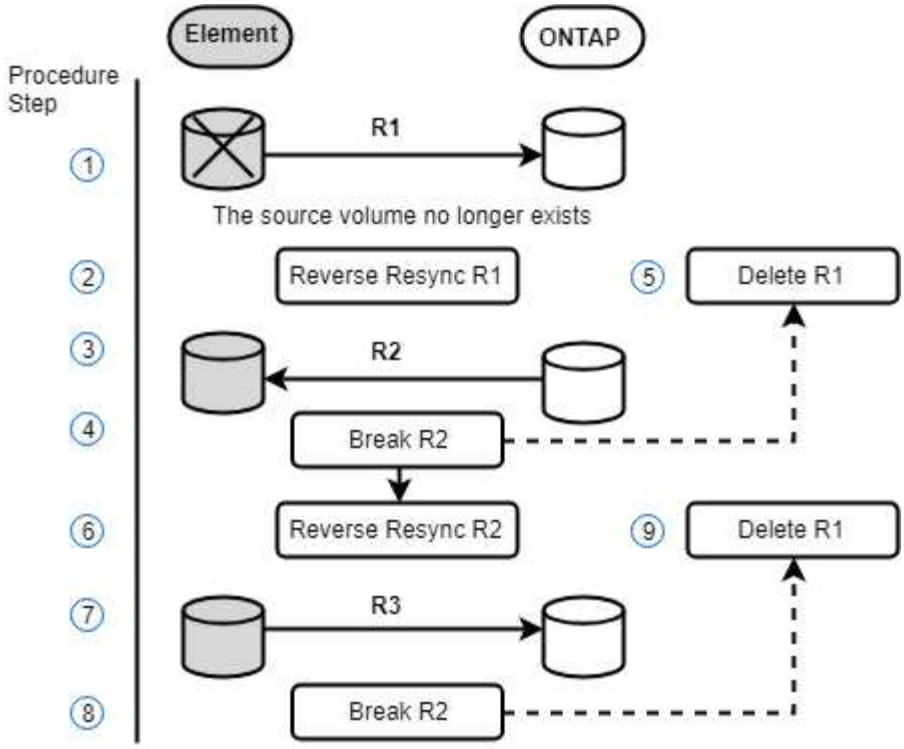
Die Schritte aus den entsprechenden Verfahren werden zur Referenz hinzugefügt.

In den hier gezeigten Beispielen lautet R1 = die ursprüngliche Beziehung, in der der Cluster, auf dem die NetApp Element Software ausgeführt wird, das ursprüngliche Quell-Volume (Element) ist und ONTAP das ursprüngliche Ziel-Volume (ONTAP). R2 und R3 stellen die inversen Beziehungen dar, die durch den umgekehrten Resync-Vorgang erstellt wurden.

Das folgende Bild zeigt das Failback-Szenario, wenn das Quell-Volume noch vorhanden ist:



Das folgende Bild zeigt das Failback-Szenario, wenn das Quell-Volume nicht mehr existiert:



Weitere Informationen

- Führen Sie ein Failback durch, wenn das Quell-Volume noch vorhanden ist
- Führen Sie ein Failback durch, wenn das Quell-Volume nicht mehr vorhanden ist

Führen Sie ein Failback durch, wenn das Quell-Volume noch vorhanden ist

Sie können das ursprüngliche Quell-Volume neu synchronisieren und mit der NetApp Element Benutzeroberfläche zurück sichern. Dieses Verfahren gilt für Szenarien, in denen das ursprüngliche Quell-Volume noch vorhanden ist.

1. Suchen Sie in der Element UI die Beziehung, die Sie unterbrochen haben, um das Failover auszuführen.
2. Klicken Sie auf das Symbol Aktionen und klicken Sie auf **Resync rückwärts**.
3. Bestätigen Sie die Aktion.

> Die Operation Reverse Resync erzeugt eine neue Beziehung, in der die Rollen der ursprünglichen Quell- und Zielvolumen umgekehrt werden (dies führt zu zwei Beziehungen, wenn die ursprüngliche Beziehung besteht). Alle neuen Daten vom ursprünglichen Ziel-Volume werden im Rahmen der umgekehrten Resynchronisierung auf das ursprüngliche Quell-Volume übertragen. Sie können weiterhin auf das aktive Volume auf der Zielseite zugreifen und dort Daten schreiben, müssen aber alle Hosts auf das Quell-Volume trennen und ein SnapMirror Update durchführen, bevor Sie zur ursprünglichen primären Ressource zurückkehren.

4. Klicken Sie auf das Aktionen-Symbol der umgekehrten Beziehung, die Sie gerade erstellt haben, und klicken Sie auf **Aktualisieren**.

   Jetzt, da Sie die umgekehrte Resynchronisierung abgeschlossen haben und sichergestellt haben, dass

keine aktiven Sitzungen mit dem Volume auf der Zielseite verbunden sind und die letzten Daten sich auf dem ursprünglichen primären Volume befinden, Sie können die folgenden Schritte durchführen, um das Failback abzuschließen und das ursprüngliche primäre Volume erneut zu aktivieren:

5. Klicken Sie auf das Aktionen-Symbol der umgekehrten Beziehung und klicken Sie auf **break**.
6. Klicken Sie auf das Aktionen-Symbol der ursprünglichen Beziehung und klicken Sie auf **Resync**.

> Das ursprüngliche primäre Volume kann nun gemountet werden, um die Produktions-Workloads auf dem ursprünglichen primären Volume wiederaufzunehmen. Die ursprüngliche SnapMirror Replizierung wird anhand der Richtlinie und des für die Beziehung konfigurierten Zeitplans fortgesetzt.

7. Nachdem Sie bestätigt haben, dass der ursprüngliche Beziehungsstatus “snapmirrored” lautet, klicken Sie auf das Aktionen-Symbol der inversen Beziehung und klicken Sie auf **Löschen**.

Weitere Informationen

SnapMirror Failback-Szenarien

Führen Sie ein Failback durch, wenn das Quell-Volume nicht mehr vorhanden ist

Sie können das ursprüngliche Quell-Volume neu synchronisieren und mit der NetApp Element Benutzeroberfläche zurück sichern. Dieser Abschnitt gilt für Szenarien, in denen das ursprüngliche Quell-Volume verloren wurde, das ursprüngliche Cluster jedoch weiterhin intakt ist. Anweisungen zur Wiederherstellung eines neuen Clusters finden Sie in der Dokumentation auf der NetApp Support Site.

Was Sie benötigen

- Sie verfügen über eine abgegebrochene Replizierungsbeziehung zwischen Element und ONTAP Volumes.
- Das Elementvolumen ist unwiederbringlich verloren.
- Der ursprüngliche Volume-Name wird als NICHT GEFUNDEN angezeigt.

Schritte

1. Suchen Sie in der Element UI die Beziehung, die Sie unterbrochen haben, um das Failover auszuführen.

   Best Practice: notieren Sie sich die SnapMirror Politik und planen Sie Einzelheiten zur ursprünglichen Abgebrochenen Beziehung. Diese Informationen sind erforderlich, wenn die Beziehung neu erstellt wird.

2. Klicken Sie auf das Symbol **Aktionen** und klicken Sie auf **Resync rückwärts**.
3. Bestätigen Sie die Aktion.

> Die Operation Reverse Resync erzeugt eine neue Beziehung, in der die Rollen des ursprünglichen Quellvolumens und des Zielvolumens umgekehrt werden (dies führt zu zwei Beziehungen, wenn die ursprüngliche Beziehung besteht). Da das ursprüngliche Volume nicht mehr vorhanden ist, erstellt das System ein neues Element Volume mit demselben Volume-Namen und derselben Volume-Größe wie das ursprüngliche Quell-Volume. Dem neuen Volume wird eine QoS-Standardrichtlinie namens SM-Recovery zugewiesen, die mit einem Standardkonto namens SM-Recovery verknüpft ist. Sie möchten das Konto und die QoS-Richtlinie für alle Volumes manuell bearbeiten, die von SnapMirror erstellt wurden, um die gelöschten ursprünglichen Quell-Volumes zu ersetzen.

Daten vom letzten Snapshot werden im Rahmen der umgekehrten Resynchronisierung auf das neue Volume übertragen. Sie können weiterhin auf die Daten zugreifen und diese auf die aktive Partition schreiben, aber Sie müssen alle Hosts auf den aktiven Volume trennen und ein SnapMirror-Update durchführen, bevor Sie die ursprüngliche primäre Beziehung in einem späteren Schritt wieder herstellen. Nach Abschluss der Resynchronisierung und Sicherstellung, dass keine aktiven Sitzungen mit dem Volume auf der Zielseite verbunden sind und dass sich die letzten Daten auf dem ursprünglichen primären Volume befinden, fahren Sie mit den folgenden Schritten fort, um das Failback abzuschließen und das ursprüngliche primäre Volume erneut zu aktivieren:

4. Klicken Sie auf das Symbol **Aktionen** der inversen Beziehung, die während der Operation Reverse Resync erstellt wurde, und klicken Sie auf **break**.
5. Klicken Sie auf das Symbol **Aktionen** der ursprünglichen Beziehung, in der das Quellvolume nicht vorhanden ist, und klicken Sie auf **Löschen**.
6. Klicken Sie auf das Symbol **Aktionen** der umgekehrten Beziehung, die Sie in Schritt 4 gebrochen haben, und klicken Sie auf **Resync rückwärts**.
7. Dies kehrt die Quelle und das Ziel um und führt zu einer Beziehung mit der gleichen Volumenquelle und dem gleichen Volume-Ziel wie die ursprüngliche Beziehung.
8. Klicken Sie auf das Symbol **Aktionen** und **Bearbeiten**, um diese Beziehung mit der ursprünglichen QoS-Richtlinie und den Zeitplaneinstellungen zu aktualisieren, die Sie zur Kenntnis genommen haben.
9. Jetzt ist es sicher, die umgekehrte Beziehung zu löschen, die Sie in Schritt 6 umkehren.

Weitere Informationen

SnapMirror Failback-Szenarien

Transfer oder einmalige Migration von ONTAP zu Element durchführen

Wenn Sie SnapMirror für Disaster Recovery von einem SolidFire Storage-Cluster mit NetApp Element Software auf die ONTAP Software verwenden, ist Element normalerweise die Quelle und ONTAP das Ziel. In einigen Fällen kann das ONTAP Storage-System jedoch als Quelle und Element als Ziel fungieren.

- Es gibt zwei Szenarien:
  - Es besteht keine frühere Disaster Recovery-Beziehung. Befolgen Sie alle Schritte in diesem Verfahren.
  - Eine frühere Disaster-Recovery-Beziehung existiert, nicht jedoch zwischen den Volumes, die für diese Risikominderung verwendet werden. Befolgen Sie in diesem Fall nur die Schritte 3 und 4 unten.

Was Sie benötigen

- Der Ziel-Node für Element muss ONTAP zugänglich gemacht worden sein.
- Das Element Volume muss für die SnapMirror Replizierung aktiviert worden sein.

Sie müssen den Zielpfad des Elements in Form hospip:/lun/<id_number> angeben, wobei lun die tatsächliche Zeichenfolge „`lun`“ ist und id_number die ID des Element-Volumes ist.

Schritte

1. Erstellen Sie mithilfe von ONTAP die Beziehung zum Element Cluster:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name -type XDP -schedule schedule -policy
    policy
```

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

2. Überprüfen Sie, ob die SnapMirror Beziehung mit dem ONTAP snapmirror show-Befehl erstellt wurde.

   Informationen zum Erstellen einer Replizierungsbeziehung in der ONTAP-Dokumentation und für eine vollständige Befehlssyntax finden Sie auf der ONTAP-man-Seite.

3. Verwenden der `ElementCreateVolume` API, Erstellung des Ziel-Volume und Einstellen des Ziel-Volume-Zugriffsmodus auf SnapMirror:

   Element Volume erstellen mithilfe der Element API

```
{
   "method": "CreateVolume",
   "params": {
        "name": "SMTargetVolumeTest2",
        "accountID": 1,
        "totalSize": 100000000000,
        "enable512e": true,
        "attributes": {},
        "qosPolicyID": 1,
        "enableSnapMirrorReplication": true,
        "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. Initialisieren Sie die Replikationsbeziehung mit dem ONTAP `snapmirror initialize` Befehl:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Backup und Restore von Volumes

Backups und Restores von Volumes auf anderen SolidFire Storage sowie sekundäre Objektspeicher, die mit Amazon S3 oder OpenStack Swift kompatibel sind.

Wenn Sie Volumes aus OpenStack Swift oder Amazon S3 wiederherstellen, benötigen Sie Manifest-Informationen aus dem ursprünglichen Backup-Prozess. Wenn Sie ein Volume wiederherstellen, das auf einem SolidFire Storage-System gesichert wurde, sind keine Manifest-Informationen erforderlich.

Weitere Informationen

- Volumes werden in einem Amazon S3-Objektspeicher gesichert
- Volumes werden in einem OpenStack Swift Objektspeicher gesichert
- Sicherung eines Volumes auf einem SolidFire Storage-Cluster
- Wiederherstellung eines Volumes aus einem Backup auf einem Amazon S3-Objektspeicher
- Wiederherstellung eines Volumes aus dem Backup in einem OpenStack Swift Objektspeicher
- Wiederherstellung eines Volumes aus einem Backup auf einem SolidFire Storage-Cluster

Volumes werden in einem Amazon S3-Objektspeicher gesichert

Sie können Backups von Volumes auf externen Objektspeichern erstellen, die mit Amazon S3 kompatibel sind.

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol Aktionen für das zu Sicherungsvolumen.
3. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
4. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Backup in** die Option **S3** aus.
5. Wählen Sie eine Option unter **Datenformat** aus:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Geben Sie einen Hostnamen ein, der für den Zugriff auf den Objektspeicher im Feld **Hostname** verwendet werden soll.
7. Geben Sie im Feld **Zugriffsschlüssel-ID** eine Zugriffsschlüssel-ID für das Konto ein.
8. Geben Sie den geheimen Zugriffsschlüssel für das Konto im Feld * Secret Access Key* ein.
9. Geben Sie den S3-Bucket ein, in dem die Sicherung im Feld **S3 Bucket** gespeichert werden soll.
10. Geben Sie im Feld **Nametag** einen Namensschild ein, der an das Präfix angefügt werden soll.
11. Klicken Sie Auf **Lesen Starten**.

Volumes werden in einem OpenStack Swift Objektspeicher gesichert

Sie können ein Backup von Volumes auf externen Objektspeichern erstellen, die mit OpenStack Swift kompatibel sind.

1. Klicken Sie Auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol Aktionen, über das das Volume gesichert werden soll.
3. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
4. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Backup in** die Option **Swift** aus.
5. Wählen Sie unter **Datenformat** ein Datenformat aus:

- **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
- **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.

6. Geben Sie eine URL für den Zugriff auf den Objektspeicher im Feld **URL** ein.
7. Geben Sie im Feld **Benutzername** einen Benutzernamen für das Konto ein.
8. Geben Sie den Authentifizierungsschlüssel für das Konto im Feld **Authentifizierungsschlüssel** ein.
9. Geben Sie den Container ein, in dem das Backup im Feld **Container** gespeichert werden soll.
10. **Optional**: Geben Sie im Feld **Nametag** ein Namensschild ein, das an das Präfix angefügt werden soll.
11. Klicken Sie Auf **Lesen Starten**.

Sicherung eines Volumes auf einem SolidFire Storage-Cluster

Sie können ein Backup von Volumes in einem Cluster auf einem Remote-Cluster für Storage-Cluster mit Element Software erstellen.

Stellen Sie sicher, dass die Quell- und Ziel-Cluster gekoppelt sind.

Siehe "Paarung von Clustern zur Replizierung".

Beim Backup oder Restore von einem Cluster auf ein anderes generiert das System einen Schlüssel, der als Authentifizierung zwischen den Clustern verwendet wird. Dieser Schreibschlüssel für das Massenvolumen ermöglicht es dem Quellcluster, sich beim Schreiben auf das Ziel-Volume mit dem Ziel-Cluster zu authentifizieren. Im Rahmen des Backup- oder Wiederherstellungsprozesses müssen Sie vor dem Start des Vorgangs einen Schreibschlüssel für das Massenvolumen vom Zielvolume generieren.

1. Auf dem Ziel-Cluster * Management* > **Volumes**.
2. Klicken Sie auf das Aktionen-Symbol für das Ziel-Volume.
3. Klicken Sie im Menü Ergebnis auf **aus** wiederherstellen.
4. Wählen Sie im Dialogfeld * Integrierter Restore* unter **Wiederherstellen von** die Option **SolidFire** aus.
5. Wählen Sie eine Option unter **Datenformat** aus:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Klicken Sie Auf **Schlüssel Generieren**.
7. Kopieren Sie den Schlüssel aus der Box **Bulk Volume Write Key** in die Zwischenablage.
8. Gehen Sie auf dem Quellcluster zu **Management** > **Volumes**.
9. Klicken Sie auf das Symbol Aktionen, über das das Volume gesichert werden soll.
10. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
11. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Backup in** die Option **SolidFire** aus.
12. Wählen Sie dieselbe Option aus, die Sie zuvor im Feld **Datenformat** ausgewählt haben.
13. Geben Sie die virtuelle Management-IP-Adresse des Clusters des Ziel-Volumes im Feld **Remote Cluster MVIP** ein.
14. Geben Sie den Benutzernamen für den Remote-Cluster in das Feld **Remote-Cluster-Benutzername** ein.
15. Geben Sie das Kennwort für den Remote-Cluster im Feld * Remote-Cluster-Kennwort* ein.
16. Fügen Sie im Feld **Bulk Volume Write Key** den Schlüssel ein, den Sie zuvor auf dem Ziel-Cluster

generiert haben.

17. Klicken Sie Auf **Lesen Starten**.

Wiederherstellung eines Volumes aus einem Backup auf einem Amazon S3-Objektspeicher

Sie können ein Volume anhand einer Backup auf einem Amazon S3-Objektspeicher wiederherstellen.

1. Klicken Sie Auf **Berichterstellung** > **Ereignisprotokoll**.
2. Suchen Sie das Backup-Ereignis, das das Backup erstellt hat, das Sie wiederherstellen müssen.
3. Klicken Sie in der Spalte **Details** für die Veranstaltung auf **Details anzeigen**.
4. Kopieren Sie die Manifestinformationen in die Zwischenablage.
5. Klicken Sie Auf **Management** > **Volumes**.
6. Klicken Sie auf das Symbol Aktionen für das Volume, das Sie wiederherstellen möchten.
7. Klicken Sie im Menü Ergebnis auf **aus** wiederherstellen.
8. Wählen Sie im Dialogfeld * Integrierter Restore* unter **Wiederherstellen von** die Option **S3** aus.
9. Wählen Sie unter **Datenformat** die Option aus, die der Datensicherung entspricht:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
10. Geben Sie einen Hostnamen ein, der für den Zugriff auf den Objektspeicher im Feld **Hostname** verwendet werden soll.
11. Geben Sie im Feld **Zugriffsschlüssel-ID** eine Zugriffsschlüssel-ID für das Konto ein.
12. Geben Sie den geheimen Zugriffsschlüssel für das Konto im Feld * Secret Access Key* ein.
13. Geben Sie den S3-Bucket ein, in dem die Sicherung im Feld **S3 Bucket** gespeichert werden soll.
14. Fügen Sie die Manifest-Informationen in das Feld * Manifestieren* ein.
15. Klicken Sie Auf **Schreiben Starten**.

Wiederherstellung eines Volumes aus dem Backup in einem OpenStack Swift Objektspeicher

Sie können ein Volume aus einem Backup auf einem OpenStack Swift Objektspeicher wiederherstellen.

1. Klicken Sie Auf **Berichterstellung** > **Ereignisprotokoll**.
2. Suchen Sie das Backup-Ereignis, das das Backup erstellt hat, das Sie wiederherstellen müssen.
3. Klicken Sie in der Spalte **Details** für die Veranstaltung auf **Details anzeigen**.
4. Kopieren Sie die Manifestinformationen in die Zwischenablage.
5. Klicken Sie Auf **Management** > **Volumes**.
6. Klicken Sie auf das Symbol Aktionen für das Volume, das Sie wiederherstellen möchten.
7. Klicken Sie im Menü Ergebnis auf **aus** wiederherstellen.
8. Wählen Sie im Dialogfeld * Integrierter Restore* unter **Wiederherstellen von** die Option **Swift** aus.
9. Wählen Sie unter **Datenformat** die Option aus, die der Datensicherung entspricht:

- **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
- **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.

10. Geben Sie eine URL für den Zugriff auf den Objektspeicher im Feld **URL** ein.
11. Geben Sie im Feld **Benutzername** einen Benutzernamen für das Konto ein.
12. Geben Sie den Authentifizierungsschlüssel für das Konto im Feld **Authentifizierungsschlüssel** ein.
13. Geben Sie den Namen des Containers ein, in dem das Backup im Feld **Container** gespeichert ist.
14. Fügen Sie die Manifest-Informationen in das Feld * Manifestieren* ein.
15. Klicken Sie Auf **Schreiben Starten**.

Wiederherstellung eines Volumes aus einem Backup auf einem SolidFire Storage-Cluster

Sie können ein Volume aus einem Backup auf einem SolidFire Storage Cluster wiederherstellen.

Beim Backup oder Restore von einem Cluster auf ein anderes generiert das System einen Schlüssel, der als Authentifizierung zwischen den Clustern verwendet wird. Dieser Schreibschlüssel für das Massenvolumen ermöglicht es dem Quellcluster, sich beim Schreiben auf das Ziel-Volume mit dem Ziel-Cluster zu authentifizieren. Im Rahmen des Backup- oder Wiederherstellungsprozesses müssen Sie vor dem Start des Vorgangs einen Schreibschlüssel für das Massenvolumen vom Zielvolume generieren.

1. Klicken Sie auf dem Ziel-Cluster auf **Management** > **Volumes**.
2. Klicken Sie auf das Symbol Aktionen für das Volume, das Sie wiederherstellen möchten.
3. Klicken Sie im Menü Ergebnis auf **aus** wiederherstellen.
4. Wählen Sie im Dialogfeld * Integrierter Restore* unter **Wiederherstellen von** die Option **SolidFire** aus.
5. Wählen Sie unter **Datenformat** die Option aus, die der Datensicherung entspricht:
   - **Native**: Ein komprimiertes Format, das nur von SolidFire-Speichersystemen lesbar ist.
   - **Unkomprimiert**: Ein unkomprimiertes Format, das mit anderen Systemen kompatibel ist.
6. Klicken Sie Auf **Schlüssel Generieren**.
7. Kopieren Sie die **Massenvolume-Schreibschlüssel**-Informationen in die Zwischenablage.
8. Klicken Sie im Quellcluster auf **Verwaltung** > **Volumes**.
9. Klicken Sie auf das Aktionen-Symbol für das Volume, das Sie für die Wiederherstellung verwenden möchten.
10. Klicken Sie im Menü Ergebnis auf **Sichern nach**.
11. Wählen Sie im Dialogfeld * Integriertes Backup* unter **Sichern nach** die Option **SolidFire** aus.
12. Wählen Sie unter **Datenformat** die Option aus, die der Sicherung entspricht.
13. Geben Sie die virtuelle Management-IP-Adresse des Clusters des Ziel-Volumes im Feld **Remote Cluster MVIP** ein.
14. Geben Sie den Benutzernamen für den Remote-Cluster in das Feld **Remote-Cluster-Benutzername** ein.
15. Geben Sie das Kennwort für den Remote-Cluster im Feld * Remote-Cluster-Kennwort* ein.
16. Fügen Sie den Schlüssel aus Ihrer Zwischenablage in das Feld **Massenvolumenschreibschlüssel** ein.
17. Klicken Sie Auf **Lesen Starten**.

Fehler im System beheben

Sie müssen das System zu Diagnosezwecken überwachen und Informationen zu Performance-Trends und Status verschiedener Systemvorgänge erhalten. Möglicherweise müssen Sie Nodes oder SSDs zu Wartungszwecken ersetzen.

- "Zeigt Informationen zu Systemereignissen an"
- "Status der ausgeführten Aufgaben anzeigen"
- "Anzeigen von Systemmeldungen"
- "Zeigen Sie die Node-Performance-Aktivitäten an"
- "Anzeigen der Volume-Performance"
- "Anzeigen von iSCSI-Sitzungen"
- "Zeigen Sie Fibre-Channel-Sitzungen an"
- "Fehlerbehebung bei Laufwerken"
- "Fehlerbehebung für Nodes"
- "Storage-Nodes: Dienstprogramme pro Node unterstützen"
- "Arbeiten Sie mit dem Management-Node"
- "Erläuterung der Cluster-Auslastungsebenen"

Finden Sie weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Zeigt Informationen zu Systemereignissen an

Sie können Informationen zu verschiedenen im System erkannten Ereignissen anzeigen. Das System aktualisiert die Ereignismeldungen alle 30 Sekunden. Im Ereignisprotokoll werden wichtige Ereignisse für das Cluster angezeigt.

1. Wählen Sie in der Element-UI die Option **Berichterstellung** > **Ereignisprotokoll**.

   Für jedes Ereignis werden die folgenden Informationen angezeigt:

Element	Beschreibung
ID	Eindeutige ID, die jedem Ereignis zugeordnet ist.
Art Des Events	Der Typ des protokollierten Ereignisses, z. B. API-Ereignisse oder Klonereignisse.
Nachricht	Dem Ereignis zugeordnete Nachricht.
Details	Informationen, mit denen der Grund des Ereignisses ermittelt werden kann.

Service-ID	Der Dienst, der das Ereignis gemeldet hat (falls zutreffend).
Knoten	Der Node, der das Ereignis gemeldet hat (falls zutreffend).
Laufwerks-ID	Das Laufwerk, das das Ereignis gemeldet hat (falls zutreffend).
Ereigniszeit	Die Zeit, zu der das Ereignis aufgetreten ist.

Weitere Informationen

Ereignistypen

Ereignistypen

Das System meldet mehrere Ereignistypen. Jedes Ereignis ist ein Vorgang, den das System abgeschlossen hat. Ereignisse können Routine-, normale Ereignisse oder Ereignisse sein, die vom Administrator beachtet werden müssen. Die Spalte Ereignistypen auf der Seite Ereignisprotokoll gibt an, in welchem Teil des Systems das Ereignis aufgetreten ist.

Das System protokolliert keine schreibgeschützten API-Befehle im Ereignisprotokoll.

In der folgenden Liste werden die Arten von Ereignissen beschrieben, die im Ereignisprotokoll angezeigt werden:

- **ApiEvent**

  Ereignisse, die von einem Benutzer über eine API oder eine Web-Benutzeroberfläche initiiert werden, die Einstellungen ändern.

- **BinAssignmentsEvent**

  Ereignisse im Zusammenhang mit der Zuordnung von Datenfächern. Fächer sind im Wesentlichen Container, in denen Daten gespeichert und über das gesamte Cluster hinweg zugeordnet sind.

- **BinSyncEvent**

  Systemereignisse zur Neuzuweisung von Daten zwischen Block-Services.

- **BsCheckEvent**

  Systemereignisse im Zusammenhang mit Blockserviceüberprüfungen.

- **BsKilEvent**

  Systemereignisse im Zusammenhang mit Blockdienstterminen.

- **BulkOpEvent**

  Ereignisse im Zusammenhang mit Vorgängen, die auf einem gesamten Volume ausgeführt werden, z. B. Backups, Wiederherstellungen, Snapshots oder Klone

- **KlonEvent**

  Ereignisse im Zusammenhang mit dem Klonen von Volumes.

- **ClusterMasterEvent**

  Ereignisse, die bei der Initialisierung des Clusters oder bei Änderungen der Konfiguration im Cluster angezeigt werden, z. B. Hinzufügen oder Entfernen von Nodes

- **CsumEvent**

  Ereignisse im Zusammenhang mit ungültigen Daten-Prüfsummen auf der Festplatte.

- **Datenereignis**

  Ereignisse im Zusammenhang mit dem Lesen und Schreiben von Daten.

- **DbEvent**

  Veranstaltungen im Zusammenhang mit der globalen Datenbank, die von Ensemble-Knoten im Cluster gepflegt wird.

- **Auffahrt**

  Ereignisse in Verbindung mit Laufwerksoperationen

- **VerschlüsselungAtRestEvent**

  Ereignisse im Zusammenhang mit dem Verschlüsselungsvorgang auf einem Cluster.

- **EnsembleEvent**

  Ereignisse, die sich auf die Erhöhung oder Verringerung der Anzahl der Knoten in einem Ensemble beziehen.

- **Fiber ChannelEvent**

  Ereignisse in Verbindung mit der Konfiguration von und Verbindungen zu den Nodes.

- **GcEvent**

  Ereignisse, die auf Prozessen zurückzuführen sind, werden alle 60 Minuten ausgeführt, um Speicher auf Blocklaufwerken zurückzugewinnen. Dieser Prozess wird auch als Garbage Collection bezeichnet.

- **IeEvent**

  Interner Systemfehler.

- **Installationsereignis**

  Automatische Softwareinstallationsereignisse. Die Software wird automatisch auf einem ausstehenden

Node installiert.

- **ISCSIEvent**

  Ereignisse im Zusammenhang mit iSCSI-Problemen im System.

- **EndEvent**

  Ereignisse im Zusammenhang mit der Anzahl von Volumes oder virtuellen Volumes in einem Konto oder im Cluster, die sich dem maximal zulässigen Wert nähern.

- **WartungModeEvent**

  Ereignisse im Zusammenhang mit dem Wartungsmodus des Node, z. B. Deaktivieren des Node.

- **NetworkEvent**

  Ereignisse im Zusammenhang mit dem Status virtueller Netzwerke.

- **HardwareEvent**

  Ereignisse im Zusammenhang mit Problemen, die auf Hardware-Geräten erkannt wurden.

- * Remote ClusterEvent*

  Ereignisse im Zusammenhang mit der Paarung von Remote-Clustern.

- **Termin**

  Ereignisse im Zusammenhang mit geplanten Snapshots.

- **ServiceEvent**

  Ereignisse im Zusammenhang mit dem Systemstatus.

- **SliceEvent**

  Ereignisse im Zusammenhang mit dem Slice Server, z. B. Entfernen eines Metadatenlaufwerks oder eines Volumes.

  Es gibt drei Arten von Ereignissen zur Umverteilung in Schichten, die Informationen über den Service enthalten, dem ein Volume zugewiesen wird:

  - Umdrehen: Ändern des primären Dienstes zu einem neuen primären Service

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - Verschieben: Ändern des sekundären Service zu einem neuen sekundären Service

    ```
    sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
    ```

  - Beschneidung: Entfernen eines Volumes aus einer Gruppe von Diensten

```
sliceID {oldSecondaryServiceID(s)}
```

- **SnmpTrapEvent**

  Ereignisse im Zusammenhang mit SNMP-Traps.

- **StatEvent**

  Ereignisse in Verbindung mit Systemstatistiken.

- **TsEvent**

  Ereignisse im Zusammenhang mit dem Systemtransportdienst.

- **UnexpectedException**

  Ereignisse im Zusammenhang mit unerwarteten Systemausnahmen.

- **UreEvent**

  Ereignisse im Zusammenhang mit nicht behebbaren Lesefehlern, die beim Lesen vom Speichergerät auftreten.

- **VasaProviderEvent**

  Ereignisse in Verbindung mit einem VASA Provider (vSphere APIs for Storage Awareness)

Status der ausgeführten Aufgaben anzeigen

Sie können den Fortschritt und den Abschlussstatus der ausgeführten Aufgaben in der Web-Benutzeroberfläche anzeigen, die von den API-Methoden ListSyncJobs und ListBulkVolumeJobs gemeldet werden. Über die Registerkarte „Reporting“ der Element-Benutzeroberfläche können Sie auf die Seite „ausgeführte Aufgaben“ zugreifen.

Wenn eine große Anzahl von Aufgaben vorhanden ist, kann das System sie in Warteschlange stellen und in Batches ausführen. Auf der Seite laufende Aufgaben werden die aktuell synchronisierten Dienste angezeigt. Wenn eine Aufgabe abgeschlossen ist, wird sie durch die nächste Synchronisierungsaufgabe in der Warteschlange ersetzt. Die Synchronisierung von Aufgaben wird möglicherweise weiterhin auf der Seite laufende Aufgaben angezeigt, bis keine Aufgaben mehr abgeschlossen sind.

Auf der Seite laufende Aufgaben des Clusters, der das Ziel-Volume enthält, werden die Replikationsdaten für Volumes angezeigt, die die Replikation durchlaufen.

Anzeigen von Systemmeldungen

Sie können Benachrichtigungen zu Cluster-Fehlern oder -Fehlern im System anzeigen. Warnmeldungen können Informationen, Warnungen oder Fehler sein und ein guter Indikator für die inwieweit das Cluster läuft. Die meisten Fehler lösen sich automatisch.

Sie können die API-Methode ListClusterStandards verwenden, um die Alarmüberwachung zu automatisieren.

So können Sie über alle auftretenden Warnmeldungen benachrichtigt werden.

1. Wählen Sie in der Element-UI die Option **Berichterstellung** > **Alarme** aus.

   Das System aktualisiert die Alarme auf der Seite alle 30 Sekunden.

   Für jedes Ereignis werden die folgenden Informationen angezeigt:

Element	Beschreibung
ID	Eine eindeutige ID, die einer Cluster-Warnmeldung zugeordnet ist.
Schweregrad	Der Grad der Wichtigkeit des Alarms. Mögliche Werte: • Warnung: Ein kleines Problem, das bald Aufmerksamkeit erfordert. Upgrades des Systems sind weiterhin zulässig. • Fehler: Ein Ausfall, der zu einer Performance-Verschlechterung oder einem Verlust von Hochverfügbarkeit führen kann. Fehler sollten in der Regel den Dienst nicht anderweitig beeinträchtigen. • Kritisch: Ein schwerwiegender Fehler, der den Dienst beeinträchtigt. Das System kann keine API- oder Client-I/O-Anfragen bereitstellen. Ein Betrieb in diesem Zustand kann zu einem potenziellen Datenverlust führen. • BestPractice: Eine empfohlene Best Practice für die Systemkonfiguration wird nicht verwendet.
Typ	Die Komponente, die sich auf den Fehler auswirkt. Nodes, Laufwerk, Cluster, Service oder Volume können verwendet werden.
Knoten	Node-ID für den Node, auf den sich dieser Fehler bezieht. Bei Knoten- und Laufwerkfehlern enthalten, andernfalls auf - (Dash) gesetzt.
Laufwerks-ID	Laufwerk-ID für das Laufwerk, auf das sich dieser Fehler bezieht. Bei Fahrfehlern enthalten, ansonsten auf - (Dash) eingestellt.
Fehlercode	Ein beschreibenden Code, der angibt, was den Fehler verursacht hat.
Details	Eine Beschreibung des Fehlers mit zusätzlichen Details.

Datum	Datum und Uhrzeit der Fehlerprotokollierung.

2. Klicken Sie auf **Details anzeigen**, um eine individuelle Warnung anzuzeigen, um Informationen über den Alarm anzuzeigen.
3. Um die Details aller Warnmeldungen auf der Seite anzuzeigen, klicken Sie auf die Spalte Details.

   Nachdem das System eine Meldung beseitigt hat, werden alle Informationen über die Warnmeldung einschließlich des Datums, an dem sie behoben wurde, in den aufgelösten Bereich verschoben.

Weitere Informationen

- Cluster-Fehlercodes
- "Storage-Management mit der Element API"

Cluster-Fehlercodes

Das System meldet einen Fehler oder einen Status, der durch das Generieren eines Fehlercodes, der auf der Seite „Meldungen“ aufgeführt ist, von Interesse sein könnte. Anhand dieser Codes können Sie ermitteln, welche Komponente des Systems die Warnmeldung erfahren hat und warum die Warnmeldung generiert wurde.

In der folgenden Liste werden die verschiedenen Arten von Codes beschrieben:

- **AuthentifizierungServiceFault**

  Der Authentifizierungsdienst auf einem oder mehreren Clusterknoten funktioniert nicht wie erwartet.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **VerfügbarVirtualNetworkIPAdresseLow**

  Die Anzahl der virtuellen Netzwerkadressen im Block der IP-Adressen ist gering.

  Um diesen Fehler zu beheben, fügen Sie dem Block der virtuellen Netzwerkadressen weitere IP-Adressen hinzu.

- * BlockClusterFull*

  Es ist nicht ausreichend freier Block-Speicherplatz zur Unterstützung eines Single-Node-Verlusts vorhanden. Weitere Informationen zu Cluster-Auslastungsstufen finden Sie in der GetClusterFullThreshold API-Methode. Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Stage3Low (Warnung): Benutzerdefinierter Schwellenwert wurde überschritten. Passen Sie Cluster-Volleinstellungen an oder fügen Sie weitere Nodes hinzu.
  - Stage4Critical (Fehler): Es gibt nicht genügend Speicherplatz zur Wiederherstellung nach einem Ausfall eines 1 Node. Das Erstellen von Volumes, Snapshots und Klonen ist nicht zulässig.
  - Stage5CompletelyConsumed (kritisch)1; es sind keine Schreibzugriffe oder neue iSCSI-Verbindungen zulässig. Aktuelle iSCSI-Verbindungen werden beibehalten. Schreibzugriffe scheitern, bis mehr Kapazität dem Cluster hinzugefügt wird. Löschen oder löschen Sie Volumes, um diesen Fehler zu beheben, oder fügen Sie dem Storage-Cluster einen weiteren Storage-Node hinzu.

- **BlocksDegradiert**

  Blockdaten werden aufgrund eines Ausfalls nicht mehr vollständig repliziert.

Schweregrad	Beschreibung
Warnung	Auf nur zwei vollständige Kopien der Blockdaten kann zugegriffen werden.
Fehler	Auf nur eine vollständige Kopie der Blockdaten kann zugegriffen werden.
Kritisch	Auf vollständige Kopien der Blockdaten kann nicht zugegriffen werden.

  Hinweis: der Warnstatus kann nur auf einem Triple Helix System auftreten.

  Um diesen Fehler zu beheben, stellen Sie alle Offline Nodes oder Block-Services wieder her oder wenden Sie sich an den NetApp Support, um Unterstützung zu erhalten.

- **BlockServiceTooFull**

  Ein Block-Service benötigt zu viel Speicherplatz.

  Um diesen Fehler zu beheben, fügen Sie mehr bereitgestellte Kapazität hinzu.

- **BlockServiceUnHealthy**

  Ein Blockdienst wurde als fehlerhaft erkannt:

  - Schweregrad = Warnung: Es werden keine Maßnahmen ergriffen. Dieser Warnzeitraum läuft in cTimeUntilBSIsKilledMSec=330000 Millisekunden ab.
  - Schweregrad = Fehler: Das System setzt Daten automatisch zurück und repliziert seine Daten auf andere gesunde Laufwerke.
  - Schweregrad = kritisch: Es gibt fehlerhafte Blockdienste auf mehreren Knoten, die größer oder gleich der Replikationszahl sind (2 für Doppelhelix). Die Daten sind nicht verfügbar, und die bin-Synchronisierung wird nicht beendet. Prüfen Sie auf Probleme mit der Netzwerkverbindung und Hardwarefehler. Es gibt weitere Fehler, wenn bestimmte Hardwarekomponenten ausgefallen sind. Der Fehler wird gelöscht, wenn der Blockservice aufgerufen wird oder wenn der Dienst deaktiviert wurde.

- **ClockSkewExceedsFaultThreshold**

  Zeitverzerrung zwischen dem Cluster-Master und dem Node, der ein Token enthält, übersteigt den empfohlenen Schwellenwert. Storage Cluster kann die Zeitverzerrung zwischen den Nodes nicht automatisch korrigieren.

  Um diesen Fehler zu beheben, verwenden Sie NTP-Server, die intern zu Ihrem Netzwerk sind, anstatt die Installationsstandards. Wenn Sie einen internen NTP-Server verwenden, wenden Sie sich an den NetApp Support.

- * ClusterCannotSync*

  Es ist ein nicht genügend Speicherplatz vorhanden, und Daten auf den Offline-Blockspeicherlaufwerken

können nicht mit Laufwerken synchronisiert werden, die noch aktiv sind.

Um diesen Fehler zu beheben, fügen Sie mehr Speicher hinzu.

- * ClusterFull*

  Es ist kein freier Speicherplatz im Storage-Cluster mehr verfügbar.

  Um diesen Fehler zu beheben, fügen Sie mehr Speicher hinzu.

- **ClusterIOPSAreüberProvistiert**

  Cluster-IOPS werden überprovisioniert. Die Summe aller minimalen QoS-IOPS ist größer als die erwarteten IOPS des Clusters. Eine minimale QoS kann nicht für alle Volumes gleichzeitig aufrechterhalten werden.

  Senken Sie zur Behebung dieses Problems die Mindesteinstellungen für QoS-IOPS für Volumes.

- **AbleDriveSecurityFailed**

  Das Cluster ist nicht für das Aktivieren der Laufwerksicherheit konfiguriert (Verschlüsselung im Ruhezustand), aber mindestens ein Laufwerk ist die Laufwerksicherheit aktiviert, was bedeutet, dass die Laufwerksicherheit auf diesen Laufwerken deaktiviert ist. Dieser Fehler wird mit dem Schweregrad „`Warnung`“ protokolliert.

  Um diesen Fehler zu beheben, überprüfen Sie die Fehlerdetails aus dem Grund, warum die Laufwerksicherheit nicht deaktiviert werden konnte. Mögliche Gründe sind:

  - Der Verschlüsselungsschlüssel konnte nicht erworben werden. Untersuchen Sie das Problem mit dem Zugriff auf den Schlüssel oder den externen Schlüsselserver.
  - Der Vorgang zum Deaktivieren des Laufwerks ist fehlgeschlagen. Stellen Sie fest, ob der falsche Schlüssel möglicherweise erfasst wurde. Wenn keiner dieser Gründe den Fehler Gründe hat, muss das Laufwerk möglicherweise ausgetauscht werden.

  Sie können versuchen, ein Laufwerk wiederherzustellen, das die Sicherheit nicht erfolgreich deaktiviert, selbst wenn der richtige Authentifizierungsschlüssel angegeben ist. Entfernen Sie die Laufwerke aus dem System, indem Sie sie auf verfügbar verschieben, löschen Sie sie sicher auf dem Laufwerk, und verschieben Sie sie wieder in aktiv.

- **DisconnectedClusterpaar**

  Ein Cluster-Paar ist getrennt oder falsch konfiguriert. Überprüfen Sie die Netzwerkverbindung zwischen den Clustern.

- **Verbindung abschaltenRemoteNode**

  Ein Remote-Knoten ist entweder getrennt oder falsch konfiguriert. Überprüfen Sie die Netzwerkverbindung zwischen den Nodes.

- **DemconnectedSnapMirrorEndpoint**

  Ein Remote-SnapMirror-Endpunkt wird getrennt oder falsch konfiguriert. Überprüfen Sie die Netzwerkverbindung zwischen dem Cluster und dem Remote-SnapMirrorEndpoint.

- **Auffahrt verfügbar**

Ein oder mehrere Laufwerke sind im Cluster verfügbar. Im Allgemeinen sollten alle Cluster alle Laufwerke hinzugefügt werden und keine im Status „verfügbar“. Sollte dieser Fehler unerwartet auftreten, wenden Sie sich an den NetApp Support.

Um diesen Fehler zu beheben, fügen Sie alle verfügbaren Laufwerke zum Speicher-Cluster hinzu.

- * Auffahrt nicht möglich*

  Das Cluster gibt diesen Fehler zurück, wenn ein oder mehrere Laufwerke ausgefallen sind und einer der folgenden Bedingungen anzeigt:

  - Der Laufwerksmanager kann nicht auf das Laufwerk zugreifen.
  - Der Slice- oder Block-Service ist zu oft ausgefallen, vermutlich aufgrund von Lese- oder Schreibfehlern des Laufwerks und kann nicht neu gestartet werden.
  - Das Laufwerk fehlt.
  - Der Master-Service für den Node ist nicht verfügbar (alle Laufwerke im Node gelten als fehlend/ausgefallen).
  - Das Laufwerk ist gesperrt und der Authentifizierungsschlüssel für das Laufwerk kann nicht erworben werden.
  - Das Laufwerk ist gesperrt, und der Entsperrvorgang schlägt fehl. So lösen Sie dieses Problem:
  - Überprüfen Sie die Netzwerkverbindung für den Node.
  - Ersetzen Sie das Laufwerk.
  - Stellen Sie sicher, dass der Authentifizierungsschlüssel verfügbar ist.
- **DriveHealthFault**

  Die SMART-Integritätsprüfung auf einem Laufwerk ist fehlgeschlagen, sodass die Funktionen des Laufwerks verringert werden. Es gibt einen kritischen Schweregrad für diesen Fehler:

  - Laufwerk mit serieller Verbindung: <Seriennummer> in Steckplatz: <Node-Steckplatz><Laufwerksfach> hat die INTELLIGENTE allgemeine Integritätsprüfung nicht bestanden. Um diesen Fehler zu beheben, ersetzen Sie das Laufwerk.
- **DriveWearFault**

  Die Restlebensdauer eines Laufwerks ist unter die Schwellenwerte gesunken, funktioniert aber immer noch.Es gibt zwei mögliche Schweregrade für diesen Fehler: Kritisch und Warnung:

  - Laufwerk mit serieller Verbindung: <Seriennummer> im Steckplatz: <Node-Steckplatz><Laufwerk-Steckplatz> verfügt über einen kritischen Verschleiß.
  - Laufwerk mit serieller Verbindung: <Seriennummer> im Steckplatz: <Node-Steckplatz><Laufwerksfach> verfügt über geringe Verschleißreserven. Um diesen Fehler zu beheben, tauschen Sie das Laufwerk bald aus.
- * DuplicateClusterMasterCandidates*

  Es wurden mehr als ein Master-Kandidat für Speichercluster erkannt. Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **EnableDriveSecurityFailed**

  Das Cluster ist so konfiguriert, dass es Laufwerkssicherheit (Verschlüsselung im Ruhezustand) benötigt, die Laufwerkssicherheit konnte jedoch auf mindestens einem Laufwerk nicht aktiviert werden. Dieser

Fehler wird mit dem Schweregrad „`Warnung`“ protokolliert.

Um diesen Fehler zu beheben, überprüfen Sie die Fehlerdetails aus dem Grund, warum die Laufwerksicherheit nicht aktiviert werden konnte. Mögliche Gründe sind:

- Der Verschlüsselungsschlüssel konnte nicht erworben werden. Untersuchen Sie das Problem mit dem Zugriff auf den Schlüssel oder den externen Schlüsselserver.
- Der Vorgang zum Aktivieren ist auf dem Laufwerk fehlgeschlagen. Stellen Sie fest, ob der falsche Schlüssel möglicherweise erfasst wurde. Wenn keiner dieser Gründe den Fehler Gründe hat, muss das Laufwerk möglicherweise ausgetauscht werden.

Sie können versuchen, ein Laufwerk wiederherzustellen, das die Sicherheit nicht erfolgreich aktiviert, selbst wenn der richtige Authentifizierungsschlüssel angegeben ist. Entfernen Sie die Laufwerke aus dem System, indem Sie sie auf verfügbar verschieben, löschen Sie sie sicher auf dem Laufwerk, und verschieben Sie sie wieder in aktiv.

- **EnsembleDegraded**

  Die Netzwerk-Konnektivität oder -Stromversorgung wurde auf einen oder mehrere der Ensemble-Knoten verloren.

  Um diesen Fehler zu beheben, stellen Sie die Netzwerkverbindung oder den Netzstrom wieder her.

- **Ausnahme**

  Ein Fehler wurde gemeldet, der sich nicht auf einen Routinefehler ausstellt. Diese Fehler werden nicht automatisch aus der Fehlerwarteschlange gelöscht. Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **AusfallenSpaceTooFull**

  Ein Blockservice reagiert nicht auf Datenschreibanfragen. Dadurch verfügt der Slice Service über keinen freien Speicherplatz zum Speichern ausgefallener Schreibvorgänge.

  Um diesen Fehler zu beheben, stellen Sie die Funktion zur Wiederherstellung von Blockdiensten wieder her, damit Schreibvorgänge normal fortgesetzt werden und der fehlerhafte Speicherplatz aus dem Schichtdienst entfernt werden kann.

- **FanSensor**

  Ein Lüftersensor ist ausgefallen oder fehlt.

  Um diesen Fehler zu beheben, ersetzen Sie eine fehlerhafte Hardware.

- **Fiber ChannelAccessDegraded**

  Ein Fibre Channel-Node reagiert nicht auf andere Nodes im Storage-Cluster über einen bestimmten Zeitraum. In diesem Status gilt der Node als nicht ansprechbar und generiert einen Cluster-Fehler. Überprüfen Sie die Netzwerkverbindung.

- **FaserChannelAccessUnverfügbar**

  Alle Fibre-Channel-Nodes reagieren nicht mehr. Die Node-IDs werden angezeigt. Überprüfen Sie die Netzwerkverbindung.

- **FiberChannelActiveIxL**

  Die Anzahl der iXL-Nexus nähert sich dem unterstützten Limit von 8000 aktiven Sitzungen pro Fibre-Channel-Node.

  - Best Practice-Grenze ist 5500.
  - Warngrenze ist 7500.
  - Die maximale Obergrenze (nicht erzwungen) beträgt 8192. Um diesen Fehler zu beheben, reduzieren Sie die Anzahl der iXL Nexus unter dem Best Practice Limit von 5500.

- **Fiber ChannelConfig**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - An einem PCI-Steckplatz befindet sich ein unerwarteter Fibre Channel-Port.
  - Es gibt ein unerwartetes Fibre Channel HBA-Modell.
  - Ein Problem mit der Firmware eines Fibre Channel HBA ist aufgetreten.
  - Ein Fibre-Channel-Port ist nicht online.
  - Bei der Konfiguration von Fibre Channel Passthrough müssen hartnäckige Probleme aufgetreten sein. Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **FiberChannelIOPS**

  Die IOPS-Gesamtzahl nähert sich dem IOPS-Limit für Fibre Channel Nodes im Cluster. Die Grenzen sind:

  - FC0025: 50.000 IOPS bei 4-KB-Blockgröße pro Fibre Channel Node.
  - FCN001: Grenzwert von 625.000 OPS bei einer Blockgröße von 4 KB pro Fibre Channel Node. Um diesen Fehler zu beheben, verteilen Sie die Last auf alle verfügbaren Fibre Channel Nodes.

- **FiberChannelStaticIxL**

  Die Anzahl der iXL-Nexus nähert sich dem unterstützten Limit von 16000 statischen Sitzungen pro Fibre-Channel-Node.

  - Best Practice-Grenze ist 11000.
  - Warngrenze ist 15000.
  - Die maximale Obergrenze (erzwungen) ist 16384. Um diesen Fehler zu beheben, reduzieren Sie die Anzahl der iXL Nexus unter dem Best Practice Limit von 11000.

- **DateiSystemkapazitätNiedrig**

  Auf einem der Dateisysteme ist nicht genügend Platz vorhanden.

  Um diesen Fehler zu beheben, fügen Sie dem Dateisystem mehr Kapazität hinzu.

- **FipsDrivesMismatch**

  Ein Laufwerk ohne FIPS wurde physisch in einen FIPS-fähigen Storage-Node eingesetzt oder ein FIPS-Laufwerk wurde physisch in einen Storage-Node außerhalb von FIPS eingesetzt. Pro Node wird ein einziger Fehler generiert und alle betroffenen Laufwerke aufgelistet.

  Um diesen Fehler zu beheben, entfernen oder ersetzen Sie das nicht übereinstimmende Laufwerk oder die betreffenden Laufwerke.

- **FipsDriveOutOfCompliance**

  Das System hat erkannt, dass die Verschlüsselung im Ruhezustand nach Aktivierung der FIPS-Festplattenfunktion deaktiviert wurde. Dieser Fehler wird auch generiert, wenn die FIPS-Laufwerksfunktion aktiviert ist und ein Laufwerk oder ein Node außerhalb von FIPS im Storage-Cluster vorhanden ist.

  Um diesen Fehler zu beheben, aktivieren Sie die Verschlüsselung im Ruhezustand oder entfernen Sie die nicht-FIPS-Hardware aus dem Storage-Cluster.

- **FipsSelfTestFailure**

  Das FIPS-Subsystem hat während des Self-Tests einen Ausfall erkannt.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **HardwareConfigMismatch**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Die Konfiguration stimmt nicht mit der Knotendefinition überein.
  - Für diesen Node-Typ gibt es eine falsche Laufwerksgröße.
  - Es wurde ein nicht unterstütztes Laufwerk erkannt. Ein möglicher Grund ist, dass die installierte Element-Version dieses Laufwerk nicht erkennt. Es wird empfohlen, die Element Software auf diesem Node zu aktualisieren.
  - Es stimmt nicht überein, dass die Laufwerk-Firmware nicht stimmt.
  - Der Status für die Laufwerksverschlüsselung stimmt nicht mit dem Node überein. Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **IdPCertificateExpiration**

  Das SSL-Zertifikat des Dienstanbieters des Clusters zur Verwendung mit einem Drittanbieter-Identitätsanbieter (IdP) nähert sich dem Ablaufdatum oder ist bereits abgelaufen. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Schweregrad	Beschreibung
Warnung	Das Zertifikat läuft innerhalb von 30 Tagen ab.
Fehler	Das Zertifikat läuft innerhalb von 7 Tagen ab.
Kritisch	Das Zertifikat läuft innerhalb von 3 Tagen ab oder ist bereits abgelaufen.

  Um diesen Fehler zu beheben, aktualisieren Sie das SSL-Zertifikat, bevor es abläuft. Verwenden Sie die UpdateIdpConfiguration API-Methode mit `refreshCertificateExpirationTime=true` Um das aktualisierte SSL-Zertifikat bereitzustellen.

- **Inkonsistenz BondModes**

  Die Bond-Modi auf dem VLAN-Gerät fehlen. Dieser Fehler zeigt den erwarteten Bond-Modus und den derzeit verwendeten Bond-Modus an.

- **Unconsistent Interface Konfiguration**

  Die Schnittstellenkonfiguration ist inkonsistent.

  Um diesen Fehler zu beheben, stellen Sie sicher, dass die Node-Schnittstellen im Storage-Cluster konsistent konfiguriert sind.

- **Inkonsistent Mtus**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Bond1G-Diskrepanz: Inkonsistente MTUs wurden an Bond1G-Schnittstellen erkannt.
  - Bond10G-Diskrepanz: Inkonsistente MTUs wurden an Bond10G-Schnittstellen erkannt. Dieser Fehler zeigt den betreffenden Node oder die betreffenden Knoten zusammen mit dem zugehörigen MTU-Wert an.

- **UnstimmigeDie Routenregeln**

  Die Routingregeln für diese Schnittstelle sind inkonsistent.

- **Inkonsistent SubnetMasken**

  Die Netzwerkmaske auf dem VLAN-Gerät stimmt nicht mit der intern aufgezeichneten Netzwerkmaske für das VLAN überein. Dieser Fehler zeigt die erwartete Netzwerkmaske und die aktuell verwendete Netzwerkmaske an.

- **IncorrectBondPortCount**

  Die Anzahl der Bond-Ports ist falsch.

- **InvalidConfiguredFiberChannelNodeCount**

  Eine der beiden erwarteten Fibre-Channel-Node-Verbindungen ist beeinträchtigt. Dieser Fehler wird angezeigt, wenn nur ein Fibre-Channel-Knoten verbunden ist.

  Um diesen Fehler zu beheben, überprüfen Sie die Cluster-Netzwerkkonnektivität und die Netzwerkverkabelung und überprüfen Sie, ob Services ausgefallen sind. Falls keine Netzwerk- oder Serviceprobleme auftreten, wenden Sie sich an den NetApp Support, um einen Fibre Channel-Node zu ersetzen.

- **IrqBalanceFailed**

  Beim Versuch, Interrupts auszugleichen, ist eine Ausnahme aufgetreten.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **KmZertifizierungFault**
  - Das Zertifikat der Root Certification Authority (CA) nähert sich dem Ablaufdatum.

    Um diesen Fehler zu beheben, erwerben Sie ein neues Zertifikat von der Root CA mit Ablaufdatum mindestens 30 Tage aus und verwenden Sie ModifyKeyServerkmip, um das aktualisierte Root CA-Zertifikat bereitzustellen.

  - Das Clientzertifikat nähert sich dem Ablaufdatum.

Um diesen Fehler zu beheben, erstellen Sie einen neuen CSR mit GetClientCertificateSigningRequest, lassen Sie ihn unterzeichnen, um sicherzustellen, dass das neue Ablaufdatum mindestens 30 Tage beträgt, und verwenden Sie ModifyKeyServerkmip, um das auslaufende KMIP-Clientzertifikat durch das neue Zertifikat zu ersetzen.

- Das Zertifikat der Root Certification Authority (CA) ist abgelaufen.

  Um diesen Fehler zu beheben, erwerben Sie ein neues Zertifikat von der Root CA mit Ablaufdatum mindestens 30 Tage aus und verwenden Sie ModifyKeyServerkmip, um das aktualisierte Root CA-Zertifikat bereitzustellen.

- Client-Zertifikat ist abgelaufen.

  Um diesen Fehler zu beheben, erstellen Sie einen neuen CSR mit GetClientCertificateSigningRequest, lassen Sie ihn unterzeichnen, um sicherzustellen, dass das neue Ablaufdatum mindestens 30 Tage beträgt, und verwenden Sie ModifyKeyServerkmip, um das abgelaufene KMIP-Clientzertifikat durch das neue Zertifikat zu ersetzen.

- Fehler bei der Root Certification Authority (CA)-Zertifizierung.

  Um diesen Fehler zu beheben, überprüfen Sie, ob das richtige Zertifikat bereitgestellt wurde und, falls erforderlich, das Zertifikat von der Stammzertifizierungsstelle erneut erwerben. Verwenden Sie ModifyKeyServerkmip, um das richtige KMIP-Client-Zertifikat zu installieren.

- Fehler beim Client-Zertifikat.

  Um diesen Fehler zu beheben, überprüfen Sie, ob das korrekte KMIP-Client-Zertifikat installiert ist. Die Root-CA des Client-Zertifikats sollte auf dem EKS installiert werden. Verwenden Sie ModifyKeyServerkmip, um das richtige KMIP-Client-Zertifikat zu installieren.

- **KmipServerFault**
  - Verbindungsfehler

    Um diesen Fehler zu beheben, überprüfen Sie, ob der externe Schlüsselserver aktiv ist und über das Netzwerk erreichbar ist. Verwenden Sie TestKeyServerKimp und TestKeyProviderKmip, um Ihre Verbindung zu testen.

  - Authentifizierungsfehler

    Um diesen Fehler zu beheben, überprüfen Sie, ob die richtige Root-CA- und KMIP-Client-Zertifikate verwendet werden und ob der private Schlüssel und das KMIP-Client-Zertifikat übereinstimmen.

  - Serverfehler

    Um diesen Fehler zu beheben, überprüfen Sie die Details auf den Fehler. Möglicherweise ist aufgrund des zurückgegebenen Fehlers eine Fehlerbehebung auf dem externen Schlüsselserver erforderlich.

- * MemoryEccThreshold*

  Es wurden eine große Anzahl von korrigierbaren oder nicht korrigierbaren ECC-Fehlern erkannt. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Ereignis	Schweregrad	Beschreibung

Ein einzelnes DIMM cErrorCount erreicht cDimmCorrectableErrWarnThreshold.	Warnung	Korrigierbare ECC-Speicherfehler über dem Schwellenwert auf DIMM: <Prozessor> <DIMM Slot>
Ein einzelnes DIMM cErrorCount bleibt über cDimmCorrectableErrWarnThreshold bis cErrorFaultTimer für das DIMM abläuft.	Fehler	Korrektur von ECC-Speicherfehlern über dem Schwellenwert auf DIMM: <Processor> <DIMM>
Ein Speicher-Controller meldet cErrorCount über cMemCtlrCorrectableErrWarnThreshold und cMemCtlrCorrectableErrWarnDauer wird angegeben.	Warnung	Korrigierbare ECC-Speicherfehler oberhalb des Schwellenwerts für Speicher-Controller: <Prozessor> <Speicher-Controller>
Ein Speicher-Controller meldet cErrorCount über cMemCtlrCorrectableErrWarnThreshold bis cErrorFaultTimer für den Speicher-Controller abläuft.	Fehler	Korrektur von ECC-Speicherfehlern über dem Schwellenwert auf DIMM: <Processor> <DIMM>
Ein einzelnes DIMM meldet einen uErrorCount über Null, aber kleiner als cDimmUncorrectTableErrFaultThreshold.	Warnung	Nicht korrigierbarer ECC-Speicherfehler auf DIMM: <Prozessor> <DIMM Slot> erkannt
Ein einzelnes DIMM meldet einen uErrorCount von mindestens cDimmUncorrectTableErrFaultThreshold.	Fehler	Nicht korrigierbarer ECC-Speicherfehler auf DIMM: <Prozessor> <DIMM Slot> erkannt
Ein Speicher-Controller meldet einen uErrorCount über Null, aber kleiner als cMemCtlrUncorregictErrFaultThreshold.	Warnung	Nicht korrigierbarer ECC-Speicherfehler auf Speichercontroller: <Prozessor> <Speichercontroller> erkannt
Ein Speicher-Controller meldet einen uErrorCount von mindestens cMemCtlrUncorregictErrFaultThreshold.	Fehler	Nicht korrigierbarer ECC-Speicherfehler auf Speichercontroller: <Prozessor> <Speichercontroller> erkannt

Um diesen Fehler zu beheben, wenden Sie sich an den NetApp Support.

- **SpeichernUserageThreshold**

Die Speicherauslastung ist über dem Normalwert. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Weitere Informationen zum Fehlertyp finden Sie in der Überschrift **Details** im Fehlerfehler.

Schweregrad	Beschreibung
Warnung	Der Systemspeicher ist schwach.
Fehler	Der Systemspeicher ist sehr gering.
Kritisch	Der Systemspeicher wird vollständig verbraucht.

Um diesen Fehler zu beheben, wenden Sie sich an den NetApp Support.

- * MetadataClusterFull*

  Es ist nicht ausreichend freier Speicherplatz für Metadaten vorhanden, um einen Ausfall eines einzelnen Nodes zu unterstützen. Weitere Informationen zu Cluster-Auslastungsstufen finden Sie in der GetClusterFullThreshold API-Methode. Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Stage3Low (Warnung): Benutzerdefinierter Schwellenwert wurde überschritten. Passen Sie Cluster-Volleinstellungen an oder fügen Sie weitere Nodes hinzu.
  - Stage4Critical (Fehler): Es gibt nicht genügend Speicherplatz zur Wiederherstellung nach einem Ausfall eines 1 Node. Das Erstellen von Volumes, Snapshots und Klonen ist nicht zulässig.
  - Stage5CompletelyConsumed (kritisch)1; es sind keine Schreibzugriffe oder neue iSCSI-Verbindungen zulässig. Aktuelle iSCSI-Verbindungen werden beibehalten. Schreibzugriffe scheitern, bis mehr Kapazität dem Cluster hinzugefügt wird. Löschen oder Löschen von Daten oder Hinzufügen weiterer Nodes Löschen oder löschen Sie Volumes, um diesen Fehler zu beheben, oder fügen Sie dem Storage-Cluster einen weiteren Storage-Node hinzu.
- **MtuCheckFailure**

  Ein Netzwerkgerät ist nicht für die richtige MTU-Größe konfiguriert.

  Um diesen Fehler zu beheben, stellen Sie sicher, dass alle Netzwerkschnittstellen und Switch-Ports für Jumbo Frames konfiguriert sind (MTUs mit einer Größe von bis zu 9000 Byte).

- **NetworkConfig**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Eine erwartete Schnittstelle ist nicht vorhanden.
  - Es ist eine doppelte Schnittstelle vorhanden.
  - Eine konfigurierte Schnittstelle ist ausgefallen.
  - Ein Netzwerkneustart ist erforderlich. Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.
- **NoVerfügbarVirtualNetzwerkIPAddresses**

  Im Block der IP-Adressen sind keine virtuellen Netzwerkadressen verfügbar.

- VirtualNetworkID # TAG(#) hat keine Speicher-IP-Adressen. Dem Cluster können keine weiteren Nodes hinzugefügt werden. Um diesen Fehler zu beheben, fügen Sie dem Block der virtuellen Netzwerkadressen weitere IP-Adressen hinzu.

- **NodeHardwareFault (Netzwerkschnittstelle <Name> ist ausgefallen oder das Kabel ist nicht angeschlossen)**

  Eine Netzwerkschnittstelle ist entweder ausgefallen oder das Kabel ist nicht angeschlossen.

  Um diesen Fehler zu beheben, überprüfen Sie die Netzwerkverbindung für den Knoten oder Knoten.

- **NodeHardwareFault (Laufwerksverschlüsselungsstatus entspricht dem Verschlüsselungsstatus des Node für das Laufwerk in Steckplatz <Node-Steckplatz><Laufwerkseinschub>)**

  Ein Laufwerk entspricht nicht den Verschlüsselungsfunktionen des in installierten Storage-Nodes.

- **NodeHardwareFault (Falscher <Laufwerkstyp> Laufwerksgröße <tatsächliche Größe> für das Laufwerk in Steckplatz <Node-Steckplatz><Laufwerkseinschub> für diesen Node-Typ - erwartete <erwartete Größe>)**

  Ein Storage-Node enthält ein Laufwerk, das die falsche Größe für diesen Node hat.

- **NodeHardwareFault (nicht unterstütztes Laufwerk in Steckplatz <Node Slot><Drive Slot> gefunden; Laufwerksstatistiken und Integritätsinformationen sind nicht verfügbar)**

  Ein Storage-Node enthält ein Laufwerk, das nicht unterstützt wird.

- **NodeHardwareFault (das Laufwerk in Slot <Node Slot><Drive Slot> sollte die Firmware-Version <erwartete Version> verwenden, wird aber nicht unterstützte Version <tatsächliche Version> verwenden)**

  Ein Speicherknoten enthält ein Laufwerk, auf dem eine nicht unterstützte Firmware-Version ausgeführt wird.

- **NoteWartungs-Modus**

  Ein Node wurde im Wartungsmodus versetzt. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Schweregrad	Beschreibung
Warnung	Gibt an, dass sich der Node noch im Wartungsmodus befindet.
Fehler	Zeigt an, dass der Wartungsmodus nicht deaktiviert wurde, wahrscheinlich aufgrund von fehlgeschlagenen oder aktiven Standardys.

  Um diesen Fehler zu beheben, deaktivieren Sie den Wartungsmodus nach Abschluss der Wartung. Wenn der Fehler auf der Fehlerebene weiterhin besteht, wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **NodeOffline**

  Element Software kann nicht mit dem angegebenen Node kommunizieren. Überprüfen Sie die

Netzwerkverbindung.

- **NotusingLACPBondMode**

  LACP Bonding-Modus ist nicht konfiguriert.

  Um diesen Fehler zu beheben, verwenden Sie LACP Bonding bei der Implementierung von Storage-Nodes. Es kann zu Performance-Problemen kommen, wenn LACP nicht aktiviert und ordnungsgemäß konfiguriert ist.

- **NtpServerUnerreichbar**

  Das Storage-Cluster kann nicht mit dem angegebenen NTP-Server oder den angegebenen Servern kommunizieren.

  Um diesen Fehler zu beheben, überprüfen Sie die Konfiguration für den NTP-Server, das Netzwerk und die Firewall.

- **NtpTimeNotInSync**

  Der Unterschied zwischen der Storage-Cluster-Zeit und der angegebenen NTP-Serverzeit ist zu groß. Der Speichercluster kann die Differenz nicht automatisch korrigieren.

  Um diesen Fehler zu beheben, verwenden Sie NTP-Server, die intern zu Ihrem Netzwerk sind, anstatt die Installationsstandards. Wenn Sie interne NTP-Server verwenden und das Problem weiterhin besteht, wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **NvramDeviceStatus**

  Ein NVRAM-Gerät weist einen Fehler auf, ist ausgefallen oder ist ausgefallen. Dieser Fehler weist folgende Schweregrade auf:

Schweregrad	Beschreibung
Warnung	Die Hardware hat eine Warnung erkannt. Dieser Zustand kann vorübergehend sein, z. B. eine Temperaturwarnung. • NvmLifetimeFehler • NvmLifetimeStatus • EnergiengySourceLifetimeStatus • EnergiengySourceTemperatureStatus • WarningThresholdExceped

Fehler	Die Hardware hat einen Fehler oder kritischen Status erkannt. Der Cluster-Master versucht, das Slice-Laufwerk aus dem Betrieb zu entfernen (dies erzeugt ein Ereignis zum Entfernen des Laufwerks). Wenn sekundäre Schichtdienste nicht verfügbar sind, wird das Laufwerk nicht entfernt. Zusätzlich zu den Warnungsebenen-Fehlern zurückgegebene Fehler: • Der Mount-Punkt für NVRAM-Gerät ist nicht vorhanden. • Die NVRAM-Gerätepartition ist nicht vorhanden. • Die NVRAM-Gerätepartition ist vorhanden, aber nicht angehängt.
Kritisch	Die Hardware hat einen Fehler oder kritischen Status erkannt. Der Cluster-Master versucht, das Slice-Laufwerk aus dem Betrieb zu entfernen (dies erzeugt ein Ereignis zum Entfernen des Laufwerks). Wenn sekundäre Schichtdienste nicht verfügbar sind, wird das Laufwerk nicht entfernt. • Persistenz verloren • ArmStatusSaveNArmed • CsaveStatusfehler

Ersetzen Sie alle fehlerhaften Hardware im Node. Falls das Problem dadurch nicht behoben werden kann, wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **PowerSupplyError**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Es ist kein Netzteil vorhanden.
  - Ein Netzteil ist fehlgeschlagen.
  - Ein Netzteileingang fehlt oder außerhalb des zulässigen Bereichs liegt. Um diesen Fehler zu beheben, überprüfen Sie, ob alle Knoten mit redundanter Stromversorgung versorgt werden. Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **ProvisionedSpaceTooFull**

  Die insgesamt bereitgestellte Kapazität des Clusters ist zu voll.

  Um diesen Fehler zu beheben, fügen Sie mehr bereitgestellten Speicherplatz hinzu oder löschen und löschen Sie Volumes.

- **EntferntRepAsyncDelayExceeded**

  Die konfigurierte asynchrone Verzögerung der Replikation wurde überschritten. Überprüfen Sie die Netzwerkverbindung zwischen Clustern.

- **EntfernteRepClusterFull**

  Die Remote-Replikation der Volumes wurde angehalten, da der Ziel-Storage-Cluster zu voll ist.

  Um diesen Fehler zu beheben, geben Sie Speicherplatz auf dem Ziel-Storage-Cluster frei.

- **EntfernteRepSnapshotClusterFull**

  Die Remote-Replizierung der Snapshots wurde durch die Volumes unterbrochen, weil der Ziel-Storage-Cluster zu voll ist.

  Um diesen Fehler zu beheben, geben Sie Speicherplatz auf dem Ziel-Storage-Cluster frei.

- **EntferntRepSnapshotsExceedLimit**

  Die Volumes haben die Remote-Replizierung von Snapshots angehalten, da das Ziel-Storage-Cluster-Volume seine Snapshot-Grenze überschritten hat.

  Um diesen Fehler zu beheben, erhöhen Sie die Snapshot-Grenze auf dem Ziel-Speicher-Cluster.

- **Fehler beim PlaneActionError**

  Mindestens eine der geplanten Aktivitäten wurde ausgeführt, ist aber fehlgeschlagen.

  Der Fehler wird gelöscht, wenn die geplante Aktivität erneut ausgeführt wird und erfolgreich ist, wenn die geplante Aktivität gelöscht wird oder wenn die Aktivität angehalten und fortgesetzt wird.

- **SensorReadingFailed**

  Der Selbsttest des Baseboard Management Controller (BMC) ist fehlgeschlagen oder ein Sensor konnte nicht mit dem BMC kommunizieren.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **ServiceNotRunning**

  Ein erforderlicher Dienst wird nicht ausgeführt.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **SliceServiceTooFull**

  Einem Schichtdienst ist zu wenig provisionierte Kapazität zugewiesen.

  Um diesen Fehler zu beheben, fügen Sie mehr bereitgestellte Kapazität hinzu.

- **SchliceServiceUngesund**

  Das System hat erkannt, dass ein Schichtdienst ungesund ist und ihn automatisch stillsetzt.

  - Schweregrad = Warnung: Es werden keine Maßnahmen ergriffen. Dieser Warnzeitraum läuft in 6 Minuten ab.
  - Schweregrad = Fehler: Das System setzt Daten automatisch zurück und repliziert seine Daten auf andere gesunde Laufwerke. Prüfen Sie auf Probleme mit der Netzwerkverbindung und Hardwarefehler. Es gibt weitere Fehler, wenn bestimmte Hardwarekomponenten ausgefallen sind. Der Fehler wird gelöscht, wenn der Schichtdienst verfügbar ist oder wenn der Dienst deaktiviert wurde.

- **Sshenenabled**

  Der SSH-Service ist auf einem oder mehreren Nodes im Storage-Cluster aktiviert.

  Um diesen Fehler zu beheben, deaktivieren Sie den SSH-Service auf dem entsprechenden Node oder Nodes oder wenden Sie sich an den NetApp Support, um Unterstützung zu erhalten.

- **SslCertificateExpiration**

  Das mit diesem Knoten verknüpfte SSL-Zertifikat nähert sich dem Ablaufdatum oder ist abgelaufen. Dieser Fehler nutzt die folgenden Schweregrade auf der Grundlage der Dringlichkeit:

Schweregrad	Beschreibung
Warnung	Das Zertifikat läuft innerhalb von 30 Tagen ab.
Fehler	Das Zertifikat läuft innerhalb von 7 Tagen ab.
Kritisch	Das Zertifikat läuft innerhalb von 3 Tagen ab oder ist bereits abgelaufen.

  Um diesen Fehler zu beheben, erneuern Sie das SSL-Zertifikat. Wenden Sie sich bei Bedarf an den NetApp Support, um Hilfe zu erhalten.

- * Stranddecacity*

  Ein einzelner Node verursacht mehr als die Hälfte der Storage-Cluster-Kapazität.

  Um die Datenredundanz aufrechtzuerhalten, reduziert das System die Kapazität des größten Node, sodass einige seiner Blockkapazitäten ungenutzt (nicht verwendet) sind.

  Fügen Sie zur Behebung dieses Fehlers weitere Laufwerke zu vorhandenen Speicher-Nodes hinzu oder fügen Sie dem Cluster Storage-Nodes hinzu.

- **TempSensor**

  Ein Temperatursensor meldet höhere Temperaturen als normale Temperaturen. Dieser Fehler kann in Verbindung mit PowerSupplyError oder FanSensor Fehlern ausgelöst werden.

  Um diesen Fehler zu beheben, prüfen Sie, ob Luftstrombehinderungen in der Nähe des Storage-Clusters vorhanden sind. Wenden Sie sich bei Bedarf an den NetApp Support, um Hilfe zu erhalten.

- **Upgrade**

  Ein Upgrade läuft seit mehr als 24 Stunden.

  Setzen Sie das Upgrade fort, oder wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **UnresponsiveService**

  Ein Dienst reagiert nicht mehr.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **VirtualNetworkConfig**

  Dieser Cluster-Fehler gibt eine der folgenden Bedingungen an:

  - Eine Schnittstelle ist nicht vorhanden.
  - Ein falscher Namespace auf einer Schnittstelle.
  - Eine falsche Netzmaske ist vorhanden.
  - Eine falsche IP-Adresse ist vorhanden.
  - Eine Schnittstelle ist nicht verfügbar und wird nicht ausgeführt.
  - Es gibt eine überflüssige Schnittstelle auf einem Knoten. Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

- **VolumesDegradiert**

  Die Replikation und Synchronisierung der sekundären Volumes ist nicht abgeschlossen. Die Meldung wird gelöscht, wenn die Synchronisierung abgeschlossen ist.

- **VolumesOffline**

  Ein oder mehrere Volumes im Storage-Cluster sind offline. Der Fehler **volumeDegraded** ist ebenfalls vorhanden.

  Wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

Zeigen Sie die Node-Performance-Aktivitäten an

Sie können Performance-Aktivitäten für jeden Node in einem grafischen Format anzeigen. Diese Information bietet Echtzeitstatistiken für CPU und Lese-/Schreib-I/O-Vorgänge pro Sekunde (IOPS) für jedes Laufwerk des Node. Das Auslastungsdiagramm wird alle fünf Sekunden aktualisiert, und das Laufwerksstatistiken-Diagramm aktualisiert alle zehn Sekunden.

1. Klicken Sie Auf **Cluster** > **Knoten**.
2. Klicken Sie auf **Aktionen** für den Knoten, den Sie anzeigen möchten.
3. Klicken Sie Auf **Details Anzeigen**.

Sie können bestimmte Punkte in der Zeit auf den Linien- und Balkendiagrammen sehen, indem Sie den Cursor über die Linie oder den Balken positionieren.

Anzeigen der Volume-Performance

Sie können detaillierte Performance-Informationen für alle Volumes im Cluster anzeigen. Sie können die Informationen nach der Volume-ID oder einer der Performance-Spalten sortieren. Sie können die Informationen auch nach bestimmten Kriterien filtern.

Sie können ändern, wie oft das System Performanceinformationen auf der Seite aktualisiert, indem Sie auf die Liste **Aktualisieren alle** klicken und einen anderen Wert auswählen. Das Standard-Aktualisierungsintervall ist 10 Sekunden, wenn das Cluster weniger als 1000 Volumes hat, andernfalls beträgt die Standardeinstellung 60

Sekunden. Wenn Sie einen Wert von „nie“ wählen, ist die automatische Aktualisierung der Seite deaktiviert.

Sie können die automatische Aktualisierung durch Klicken auf **Aktivieren der automatischen Aktualisierung** wieder aktivieren.

1. Wählen Sie in der Element UI die Option **Berichterstellung** > **Volume Performance**.
2. Klicken Sie in der Liste Volume auf das Aktionen-Symbol für ein Volume.
3. Klicken Sie Auf **Details Anzeigen**.

   Unten auf der Seite wird ein Fach mit allgemeinen Informationen zum Volume angezeigt.

4. Um weitere Informationen zum Volumen anzuzeigen, klicken Sie auf **Weitere Details**.

   Das System zeigt detaillierte Informationen sowie Performance-Diagramme für das Volume an.

Weitere Informationen

Volume Performance im Detail

Volume Performance im Detail

Auf der Seite Volume Performance auf der Registerkarte Reporting in der Element UI können Sie Performancestatistiken der Volumes anzeigen.

In der folgenden Liste werden die Details beschrieben, die Ihnen zur Verfügung stehen:

- **ID**

  Die vom System generierte ID für das Volume.

- **Name**

  Der Name, der dem Volume bei seiner Erstellung gegeben wurde.

- **Konto**

  Der Name des Kontos, das dem Volume zugewiesen wurde.

- **Zugriffsgruppen**

  Der Name der Zugriffsgruppe oder der Gruppen des Volumes, der das Volume angehört.

- **Volume-Nutzung**

  Ein Prozentwert, der beschreibt, wie viel der Client das Volume verwendet.

  Mögliche Werte:

  - 0 = der Client verwendet das Volume nicht
  - 100 = der Client verwendet das Maximum
  - >100 = der Kunde verwendet den Burst

- **IOPS insgesamt**

Gesamtzahl der derzeit ausgeführten IOPS (Lese- und Schreibvorgänge) gegenüber dem Volume

- **Lese-IOPS**

  Gesamtzahl der Lese-IOPS, die derzeit auf dem Volume ausgeführt wird

- **Schreib-IOPS**

  Die Gesamtzahl der momentan ausgeführten Schreib-IOPS gegenüber dem Volume.

- **Gesamtdurchsatz**

  Der aktuell ausgeführte Gesamtdurchsatz (Lese- und Schreibvorgänge) gegenüber dem Volume.

- **Lesedurchsatz**

  Gesamtmenge des aktuell ausgeführten Lese-Durchsatzes gegenüber dem Volume.

- **Schreibdurchsatz**

  Der Gesamtdurchsatz, der derzeit für das Volume ausgeführt wird.

- **Gesamte Latenz**

  Die durchschnittliche Zeit in Mikrosekunden, die Lese- und Schreibvorgänge auf einem Volume abzuschließen.

- **Leselatenz**

  Die durchschnittliche Zeit in Mikrosekunden, um Lesevorgänge in dem Volume in den letzten 500 Millisekunden abzuschließen.

- **Schreiblatenz**

  Der durchschnittliche Zeitaufwand in Mikrosekunden, um Schreibvorgänge in einem Volume in den letzten 500 Millisekunden abzuschließen.

- **Warteschlangentiefe**

  Die Anzahl der ausstehenden Lese- und Schreibvorgänge auf dem Volume.

- **Durchschnittliche I/O-Größe**

  Durchschnittliche Größe in Byte der letzten I/O-Vorgänge für das Volume in den letzten 500 Millisekunden.

Anzeigen von iSCSI-Sitzungen

Sie können die iSCSI-Sitzungen anzeigen, die mit dem Cluster verbunden sind. Sie können die Informationen filtern, um nur die gewünschten Sitzungen einzubeziehen.

1. Wählen Sie in der Element UI die Option **Reporting** > **iSCSI-Sitzungen**.
2. Klicken Sie zum Anzeigen der Filterkriterien auf **Filter**.

Weitere Informationen

Details zur iSCSI-Sitzung

Details zur iSCSI-Sitzung

Sie können Informationen zu den iSCSI-Sitzungen anzeigen, die mit dem Cluster verbunden sind.

In der folgenden Liste werden die Informationen beschrieben, die Sie zu den iSCSI-Sitzungen finden können:

- **Knoten**

  Der Node, der die primäre Metadatenpartition für das Volume hostet.

- **Konto**

  Der Name des Kontos, zu dem das Volume gehört. Wenn der Wert leer ist, wird ein Strich (-) angezeigt.

- **Lautstärke**

  Der auf dem Node angegebene Volume-Name.

- **Volumen-ID**

  ID des Volumes, das mit der Ziel-IQN verknüpft ist.

- **Initiator-ID**

  Eine vom System generierte ID für den Initiator.

- **Initiator-Alias**

  Ein optionaler Name für den Initiator, der es einfacher macht, in einer langen Liste den Initiator zu finden.

- **Initator IP**

  Die IP-Adresse des Endpunkts, der die Sitzung initiiert.

- **Initiator-IQN**

  Der IQN des Endpunkts, der die Sitzung initiiert.

- **Ziel-IP**

  Die IP-Adresse des Node, der das Volume hostet.

- **Ziel-IQN**

  Der IQN des Volumes.

- **Erstellt Am**

  Datum, an dem die Sitzung eingerichtet wurde.

Zeigen Sie Fibre-Channel-Sitzungen an

Sie können die Fibre Channel-Sitzungen (FC) anzeigen, die mit dem Cluster verbunden sind. Sie können Informationen so filtern, dass nur die Verbindungen berücksichtigt werden, die im Fenster angezeigt werden sollen.

1. Wählen Sie in der Element-UI die Option **Reporting** > **FC-Sitzungen**.
2. Klicken Sie zum Anzeigen der Filterkriterien auf **Filter**.

Weitere Informationen

Details zur Fibre Channel-Sitzung

Details zur Fibre Channel-Sitzung

Sie können Informationen zu den aktiven Fibre Channel-Sitzungen (FC) finden, die mit dem Cluster verbunden sind.

In der folgenden Liste werden die Informationen beschrieben, die Sie über die mit dem Cluster verbundenen FC-Sitzungen finden:

- **Knoten-ID**

  Der Node, der die Sitzung für die Verbindung hostet.

- **Knotenname**

  Vom System generierter Node-Name.

- **Initiator-ID**

  Eine vom System generierte ID für den Initiator.

- **Initiator WWPN**

  Der weltweite Port-Name des Initiierenden.

- **Initiator-Alias**

  Ein optionaler Name für den Initiator, der es einfacher macht, in einer langen Liste den Initiator zu finden.

- **Ziel-WWPN**

  Der weltweite Zielname des Ports.

- **Volume Access Group**

  Name der Zugriffsgruppe des Volumes, der die Sitzung angehört.

- **Volume Access Group ID**

  Vom System generierte ID für die Zugriffsgruppe.

Fehlerbehebung bei Laufwerken

Fehlerhafte Solid State-Laufwerke (SSD) können durch ein Ersatzlaufwerk ersetzt werden. SSDs für SolidFire Storage-Nodes sind Hot-Swap-fähig. Wenn Sie vermuten, dass eine SSD ausgefallen ist, wenden Sie sich an den NetApp Support, um den Fehler zu überprüfen und gehen Sie durch das entsprechende Lösungsverfahren. NetApp Support bietet Ihnen auch Ersatzlaufwerk nach Ihren Service Level Agreements.

So kann ein ausgefallenes Laufwerk eines aktiven Nodes entfernt und durch ein neues SSD-Laufwerk von NetApp ersetzt werden. Es wird nicht empfohlen, nicht ausgefallene Laufwerke in einem aktiven Cluster zu entfernen.

Sie sollten die von NetApp Support vorgeschlagenen vor-Ort-Ersatzteile aufrecht erhalten, um bei einem Ausfall einen sofortigen Austausch des Laufwerks zu ermöglichen.

> Wenn Sie zu Testzwecken einen Laufwerksausfall simulieren, indem Sie ein Laufwerk von einem Node entfernen, müssen Sie 30 Sekunden warten, bevor Sie das Laufwerk wieder in den Laufwerkschacht einsetzen.

Wenn ein Laufwerk ausfällt, verteilt Double Helix die Daten auf dem Laufwerk auf die Nodes, die im Cluster verbleiben. Mehrere Laufwerkausfälle auf demselben Node stellen kein Problem dar, da die Element Software vor zwei Kopien von Daten auf demselben Node schützt. Ein ausgefallenes Laufwerk führt zu den folgenden Ereignissen:

- Daten werden vom Laufwerk migriert.
- Die Gesamtkapazität des Clusters wird nach der Kapazität des Laufwerks verringert.
- Double Helix Datensicherung stellt sicher, dass zwei gültige Kopien der Daten vorhanden sind.

> SolidFire Storage-Systeme unterstützen das Entfernen eines Laufwerks nicht, wenn zu wenig Storage für die Datenmigration erforderlich ist.

Finden Sie weitere Informationen

- Entfernen ausgefallener Laufwerke aus dem Cluster
- Grundlegende Fehlersuche bei MDSS-Laufwerken
- Entfernen Sie MDSS-Laufwerke
- "Austausch von Laufwerken für SolidFire Storage-Nodes"
- "Austausch von Laufwerken für Storage-Nodes der Serie H600S"
- "H410S und H610S Hardware-Informationen"
- "Hardwareinformationen zur SF-Series"

Entfernen ausgefallener Laufwerke aus dem Cluster

Das SolidFire-System setzt ein Laufwerk in den Status „ausgefallen“, wenn die Selbstdiagnose des Laufwerks den Node angibt, an dem es ausgefallen ist, oder ob die Kommunikation mit dem Laufwerk fünf oder anderthalb Minuten lang unterbrochen wird. Das System zeigt eine Liste der ausgefallenen Laufwerke an. Sie müssen ein

ausgefallenes Laufwerk von der Liste ausgefallener Laufwerke in der NetApp Element-Software entfernen.

Laufwerke in der Liste **Alerts** werden als **blockServiceUnHealthy** angezeigt, wenn ein Knoten offline ist. Wenn der Node und seine Laufwerke beim Neustart innerhalb von fünf und anderthalb Minuten wieder online sind, werden die Laufwerke automatisch aktualisiert und fortgesetzt, wenn die aktiven Laufwerke im Cluster wieder verfügbar sind.

1. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke**.
2. Klicken Sie auf **fehlgeschlagen**, um die Liste der fehlgeschlagenen Laufwerke anzuzeigen.
3. Notieren Sie sich die Steckplatznummer des ausgefallenen Laufwerks.

   Sie benötigen diese Informationen, um das ausgefallene Laufwerk im Chassis zu finden.

4. Entfernen Sie die ausgefallenen Laufwerke mithilfe einer der folgenden Methoden:

Option	Schritte
Um einzelne Laufwerke zu entfernen	a. Klicken Sie auf **Aktionen** für das Laufwerk, das Sie entfernen möchten. b. Klicken Sie Auf **Entfernen**.
Um mehrere Laufwerke zu entfernen	a. Wählen Sie alle Laufwerke aus, die Sie entfernen möchten, und klicken Sie auf **Massenaktionen**. b. Klicken Sie Auf **Entfernen**.

Grundlegende Fehlersuche bei MDSS-Laufwerken

Metadaten (oder Slice)-Laufwerke können wiederhergestellt werden, indem sie zu dem Cluster hinzugefügt werden, wenn ein oder beide Metadaten-Laufwerke ausfallen. Sie können den Wiederherstellungsvorgang in der NetApp Element-Benutzeroberfläche ausführen, wenn die MDSS-Funktion bereits auf dem Knoten aktiviert ist.

Wenn es bei einem oder beiden Metadatenlaufwerken in einem Node zu einem Ausfall kommt, wird der Slice-Service heruntergefahren und Daten von beiden Laufwerken werden auf unterschiedlichen Laufwerken im Node gesichert.

In den folgenden Szenarien werden mögliche Fehler-Szenarien beschrieben und grundlegende Empfehlungen zur Behebung des Problems bereitgestellt:

Systemscheibe schlägt fehl

- In diesem Szenario wird der Steckplatz 2 überprüft und in einen verfügbaren Status zurückgeführt.
- Das Systemschichtlaufwerk muss neu befüllt werden, bevor der Schichtdienst wieder in den Online-Modus versetzt werden kann.
- Sie sollten das System-Slice-Laufwerk ersetzen, wenn das System-Slice-Laufwerk verfügbar ist, fügen Sie das Laufwerk und das Steckplatz-2-Laufwerk gleichzeitig hinzu.

Sie können das Laufwerk in Steckplatz 2 nicht selbst als Metadatenlaufwerk hinzufügen. Sie müssen beide Laufwerke gleichzeitig zum Node hinzufügen.

Steckplatz 2 fällt aus

- In diesem Szenario wird das Systemschichtlaufwerk überprüft und in einen verfügbaren Zustand zurückgeführt.
- Sie sollten Steckplatz 2 durch ein Ersatzlaufwerk ersetzen, wenn Steckplatz 2 verfügbar ist, fügen Sie das SystemSlice-Laufwerk und das Laufwerk Steckplatz 2 gleichzeitig hinzu.

System-Slice-Laufwerk und Steckplatz 2 schlägt fehl

- Sie sollten beide Systemscheiben-Laufwerke und Steckplatz 2 durch ein Ersatzlaufwerk ersetzen. Wenn beide Laufwerke verfügbar sind, fügen Sie das Systemlaufwerk und das Laufwerk Steckplatz 2 gleichzeitig hinzu.

Reihenfolge der Vorgänge

- Ersetzen Sie das ausgefallene Hardwarelaufwerk durch ein Ersatzlaufwerk (ersetzen Sie beide Laufwerke, wenn beide ausgefallen sind).
- Fügen Sie wieder Laufwerke zum Cluster hinzu, wenn sie wieder gefüllt wurden und sich in einem verfügbaren Zustand befinden.

Überprüfung des Betriebs

- Überprüfen Sie, ob die Laufwerke in Steckplatz 0 (oder intern) und Steckplatz 2 in der Liste „Aktive Laufwerke“ als Metadatenlaufwerke identifiziert werden.
- Vergewissern Sie sich, dass der gesamte Schichtausgleich abgeschlossen ist (es sind mindestens 30 Minuten lang keine weiteren Verschieben von Slices im Ereignisprotokoll vorhanden).

Finden Sie weitere Informationen

Fügen Sie MDSS-Laufwerke hinzu

Fügen Sie MDSS-Laufwerke hinzu

Sie können ein zweites Metadatenlaufwerk auf einem SolidFire-Knoten hinzufügen, indem Sie das Blocklaufwerk in Steckplatz 2 in ein Slice-Laufwerk konvertieren. Dies wird durch die Aktivierung der MDSS-Funktion (Multi-Drive Slice Service) erreicht. Um diese Funktion zu aktivieren, müssen Sie sich an den NetApp Support wenden.

Wenn Sie ein Slice-Laufwerk in einen verfügbaren Zustand bringen, muss möglicherweise ein ausgefallenes Laufwerk durch ein neues oder ein neues Ersatzlaufwerk ersetzt werden. Sie müssen das System-Slice-Laufwerk gleichzeitig hinzufügen, wenn Sie das Laufwerk für Steckplatz 2 hinzufügen. Wenn Sie versuchen, das Slice-Laufwerk für Steckplatz 2 allein oder vor dem Hinzufügen des Slice-Laufwerks hinzuzufügen, wird das System einen Fehler generieren.

1. Klicken Sie Auf **Cluster** > **Laufwerke**.
2. Klicken Sie auf **verfügbar**, um die Liste der verfügbaren Laufwerke anzuzeigen.
3. Wählen Sie die zu addieren Slice-Laufwerke aus.

4. Klicken Sie Auf **Massenaktionen**.
5. Klicken Sie Auf **Hinzufügen**.
6. Bestätigen Sie auf der Registerkarte * Aktive Laufwerke*, dass die Laufwerke hinzugefügt wurden.

Entfernen Sie MDSS-Laufwerke

Sie können die MDSS-Laufwerke (Slice Service) mit mehreren Laufwerken entfernen. Dieser Vorgang gilt nur, wenn der Knoten über mehrere Slice-Laufwerke verfügt.

> Wenn das System-Slice-Laufwerk und das Steckplatz-2-Laufwerk ausfallen, schaltet das System die Services ab und entfernt die Laufwerke. Wenn kein Ausfall auftritt und Sie die Laufwerke entfernen, müssen beide Laufwerke gleichzeitig entfernt werden.

1. Klicken Sie Auf **Cluster** > **Laufwerke**.
2. Klicken Sie auf der Registerkarte **Available** Drives auf das Kontrollkästchen für die zu entfernenden Slice Drives.
3. Klicken Sie Auf **Massenaktionen**.
4. Klicken Sie Auf **Entfernen**.
5. Bestätigen Sie die Aktion.

Fehlerbehebung für Nodes

Sie können Nodes zu Wartungs- oder Austauschzwecken aus einem Cluster entfernen. Sie sollten die NetApp Element-UI oder -API verwenden, um Nodes zu entfernen, bevor Sie sie in den Offline-Modus versetzen.

Ein Überblick über das Verfahren zum Entfernen von Storage-Nodes:

- Stellen Sie sicher, dass im Cluster genügend Kapazität verfügbar ist, um eine Kopie der Daten auf dem Node zu erstellen.
- Entfernen Sie Laufwerke aus dem Cluster mithilfe der UI oder der RemoveDrives API-Methode.

  Daher werden Daten im System von Laufwerken des Node auf andere Laufwerke im Cluster migriert. Die Dauer dieses Prozesses hängt davon ab, wie viele Daten migriert werden müssen.

- Entfernen Sie den Node aus dem Cluster.

Beachten Sie die folgenden Überlegungen, bevor Sie einen Node herunterfahren oder hochfahren:

- Das Herunterfahren von Nodes und Clustern birgt Risiken, wenn die Performance nicht ordnungsgemäß erbracht wird.

  Das Herunterfahren eines Node sollte unter Anleitung von NetApp Support erfolgen.

- Wenn ein Node unter jeder Art von Herunterfahren länger als 5.5 Minuten ausgefallen ist, beginnt die Double Helix Datensicherung mit der Aufgabe, einzelne replizierte Blöcke auf einen anderen Node zu schreiben, um die Daten zu replizieren. In diesem Fall wenden Sie sich an den NetApp Support, um Hilfe bei der Analyse des ausgefallenen Nodes zu erhalten.
- Um einen Knoten sicher neu zu starten oder herunterzufahren, können Sie den API-Befehl Herunterfahren

verwenden.

- Wenn ein Node sich in einem „down“ oder „Off“ befindet, müssen Sie den NetApp Support kontaktieren, bevor Sie ihn wieder in den Online-Status versetzen.
- Nachdem ein Node wieder online geschaltet wurde, müssen Sie die Laufwerke je nach Dauer des Service zurück zum Cluster hinzufügen.

Finden Sie weitere Informationen

"Austausch eines fehlerhaften SolidFire-Chassis"

"Austausch eines fehlerhaften H600S-Series-Knotens"

Schalten Sie ein Cluster aus

Gehen Sie wie folgt vor, um ein gesamtes Cluster herunterzufahren.

Schritte

1. (Optional) Wenden Sie sich an den NetApp Support, um Hilfe beim Abschluss der ersten Schritte zu erhalten.
2. Vergewissern Sie sich, dass alle I/O-Vorgänge angehalten wurden.
3. Trennen Sie alle iSCSI-Sitzungen:
   a. Navigieren Sie zur Management Virtual IP (MVIP)-Adresse auf dem Cluster, um die Element-UI zu öffnen.
   b. Beachten Sie die in der Liste Knoten aufgeführten Knoten.
   c. Führen Sie die Shutdown-API-Methode mit der Stopp-Option aus, die für jede Node-ID im Cluster angegeben ist.

> Wenn Sie das Cluster neu starten, müssen Sie bestimmte Schritte durchführen, um zu überprüfen, ob alle Nodes online sind:
>
> 1. Stellen Sie sicher, dass alle kritischen Schweregrad und `volumesOffline` Clusterfehler wurden behoben.
> 2. Warten Sie 10 bis 15 Minuten, bis sich das Cluster absetzen lässt.
> 3. Starten Sie, um die Hosts für den Zugriff auf die Daten aufzurufen.
>
> Wenn Sie beim Einschalten der Knoten mehr Zeit einplanen und überprüfen möchten, ob sie nach der Wartung ordnungsgemäß sind, wenden Sie sich an den technischen Support, um Hilfe bei der Verzögerung der Datensynchronisierung zu erhalten, um unnötige bin-Synchronisierung zu vermeiden.

Weitere Informationen

"Ordnungsgemäß Herunterfahren und Einschalten eines NetApp SolidFire/HCI Storage-Clusters"

Storage-Nodes: Dienstprogramme pro Node unterstützen

Sie können die Dienstprogramme pro Node verwenden, um Netzwerkprobleme zu beheben, wenn die Standard-Monitoring-Tools der NetApp Element-Software nicht genügend Informationen zur Fehlerbehebung enthalten. Dienstprogramme pro Node

bieten spezifische Informationen und Tools, die Sie bei der Fehlerbehebung bei Netzwerkproblemen zwischen Nodes oder mit dem Management-Node unterstützen.

Weitere Informationen

- Über die UI pro Node können Sie auf Einstellungen pro Node zugreifen
- Details zu den Netzwerkeinstellungen in der Benutzeroberfläche pro Node
- Details zu den Cluster-Einstellungen erhalten Sie über die UI pro Node
- Führen Sie Systemtests über die UI pro Node aus
- Führen Sie Systemdienstprogramme über die UI pro Node aus

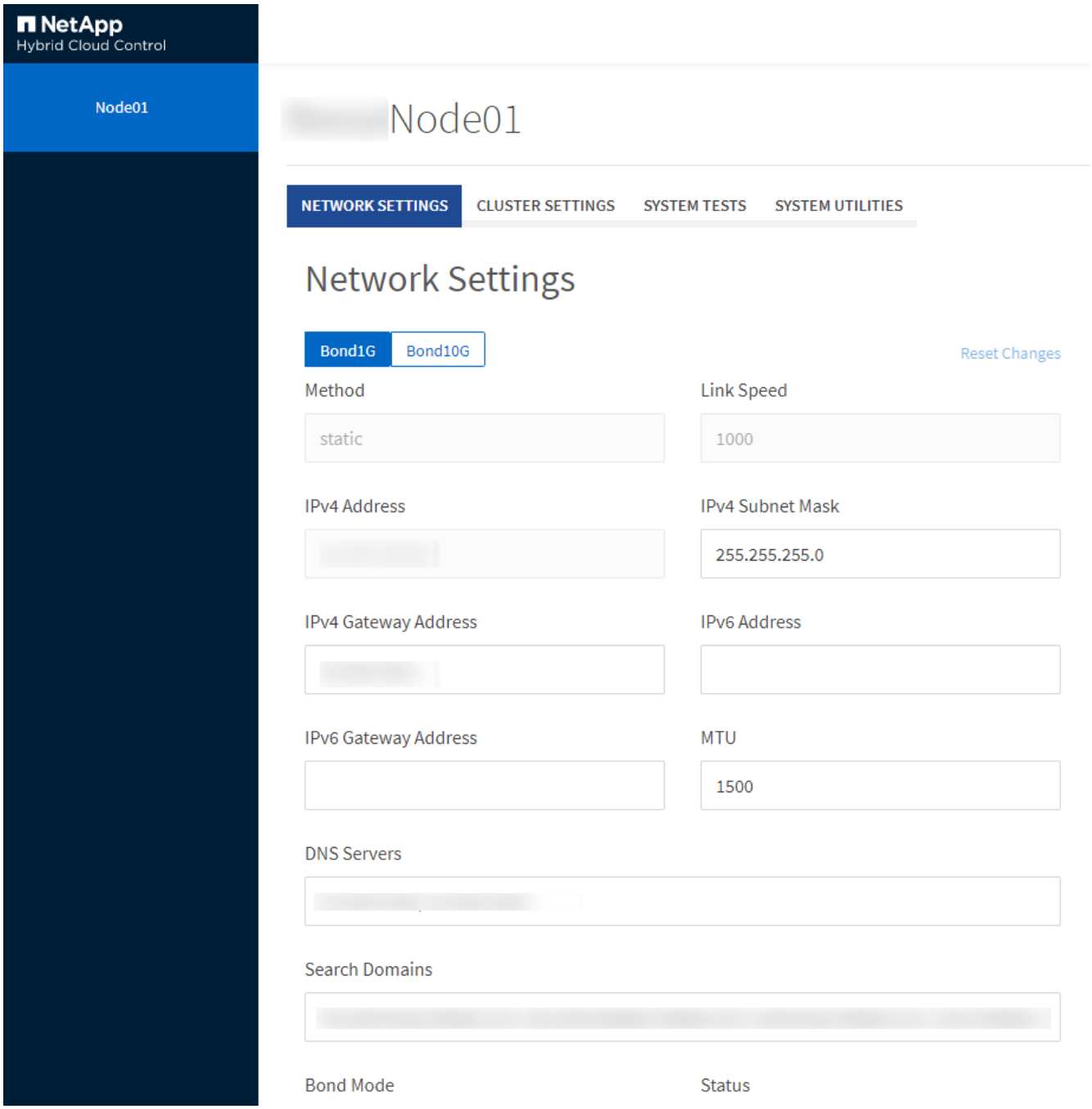
Über die UI pro Node können Sie auf Einstellungen pro Node zugreifen

Nach Eingabe der Management-Node-IP und Authentifizierung haben Sie in der Benutzeroberfläche per Node Zugriff auf Netzwerkeinstellungen, Cluster-Einstellungen sowie Systemtests und Dienstprogramme.

Wenn Sie die Einstellungen für einen Node in einem aktiven Status ändern möchten, der Teil eines Clusters ist, müssen Sie sich als Cluster-Administrator-Benutzer einloggen.

> Sie sollten Nodes jeweils einzeln konfigurieren oder ändern. Sie sollten sicherstellen, dass die angegebenen Netzwerkeinstellungen den erwarteten Effekt haben und dass das Netzwerk stabil und gut funktioniert, bevor Sie Änderungen an einem anderen Node vornehmen.

1. Öffnen Sie die UI pro Node mit einer der folgenden Methoden:
   - Geben Sie die Management-IP-Adresse gefolgt von :442 in einem Browser-Fenster ein, und melden Sie sich mit einem Admin-Benutzernamen und -Passwort an.
   - Wählen Sie in der Element UI **Cluster** > **Nodes** aus und klicken Sie auf den Link Management-IP-Adresse für den Knoten, den Sie konfigurieren oder ändern möchten. Im geöffneten Browser-Fenster können Sie die Einstellungen des Node bearbeiten.



Details zu den Netzwerkeinstellungen in der Benutzeroberfläche pro Node

Sie können die Netzwerkeinstellungen des Storage-Nodes ändern, um dem Node einen neuen Satz an Netzwerkattributen zuzuweisen.

Wenn Sie sich beim Knoten anmelden, werden auf der Seite **Netzwerkeinstellungen** die Netzwerkeinstellungen für einen Speicherknoten angezeigt (https://<node IP>:442/hcc/Node/Network-settings). Sie können entweder **Bond1G** (Management) oder **Bond10G** (Storage) Einstellungen auswählen. In der folgenden Liste werden die Einstellungen beschrieben, die Sie ändern können, wenn sich ein Speicherknoten im Status „verfügbar“, „Ausstehend“ oder „aktiv“ befindet:

- **Methode**

  Die Methode zum Konfigurieren der Schnittstelle. Mögliche Methoden:

- Loopback: Wird verwendet, um die IPv4-Loopback-Schnittstelle zu definieren.
- Manuell: Wird verwendet, um Schnittstellen zu definieren, für die keine Konfiguration standardmäßig erfolgt.
- dhcp: Wird verwendet, um eine IP-Adresse über DHCP zu erhalten.
- Statisch: Zur Definition von Ethernet-Schnittstellen mit statisch zugewiesenen IPv4-Adressen.

- **Verbindungsgeschwindigkeit**

  Die von der virtuellen NIC ausgehandelte Geschwindigkeit.

- * IPv4-Adresse*

  Die IPv4-Adresse für das eth0-Netzwerk.

- **IPv4-Subnetzmaske**

  Adressbereiche des IPv4-Netzwerks.

- * IPv4 Gateway-Adresse*

  Netzwerkadresse des Routers für das Senden von Paketen aus dem lokalen Netzwerk.

- * IPv6-Adresse*

  Die IPv6-Adresse für das eth0-Netzwerk.

- * IPv6 Gateway-Adresse*

  Netzwerkadresse des Routers für das Senden von Paketen aus dem lokalen Netzwerk.

- **MTU**

  Größte Paketgröße, die ein Netzwerkprotokoll übertragen kann. Muss größer als oder gleich 1500 sein. Wenn Sie eine zweite Speicher-NIC hinzufügen, sollte der Wert 9000 sein.

- **DNS-Server**

  Für die Cluster-Kommunikation verwendete Netzwerkschnittstelle.

- **Domänen Suchen**

  Suche nach zusätzlichen MAC-Adressen, die dem System zur Verfügung stehen.

- **Bond-Modus**

  Dies kann einer der folgenden Modi sein:

  - ActivePassive (Standard)
  - ALB
  - LACP

- **Status**

  Mögliche Werte:

- UpAndRunning
- Runter
- Hoch

- **Virtual Network Tag**

  Das Tag wurde beim Erstellen des virtuellen Netzwerks zugewiesen.

- **Routen**

  Statische Routen zu bestimmten Hosts oder Netzwerken über die zugewiesene Schnittstelle, die die Routen für die Verwendung konfiguriert sind.

Details zu den Cluster-Einstellungen erhalten Sie über die UI pro Node

Sie können die Cluster-Einstellungen für einen Storage-Node nach der Cluster-Konfiguration überprüfen und den Node-Hostnamen ändern.

In der folgenden Liste werden die Clustereinstellungen für einen Speicherknoten beschrieben, die auf der Seite **Cluster-Einstellungen** der Benutzeroberfläche pro Node angezeigt werden (https://<node IP>:442/hcc/Node/Cluster-settings).

- * Rolle*

  Rolle, die der Node im Cluster hat. Mögliche Werte:

  - Storage: Storage oder Fibre Channel-Node
  - Management: Node ist ein Management-Node.

- **Hostname**

  Der Name des Node.

- * Cluster*

  Der Name des Clusters.

- **Cluster Mitgliedschaft**

  Status des Node. Mögliche Werte:

  - Verfügbar: Der Node ist keinem Cluster-Namen zugeordnet und ist noch nicht Teil eines Clusters.
  - Ausstehend: Der Node ist konfiguriert und kann einem bestimmten Cluster hinzugefügt werden. Für den Zugriff auf den Node ist keine Authentifizierung erforderlich.
  - PendingActive: Das System installiert gerade kompatible Software auf dem Knoten. Nach Abschluss der Migration wird der Node in den Status „aktiv“ verschoben.
  - Aktiv: Der Knoten nimmt an einem Cluster Teil. Zum Ändern des Node ist eine Authentifizierung erforderlich.

- **Version**

  Version der Element Software, die auf dem Node ausgeführt wird

- **Ensemble**

  Knoten, die Teil des Datenbankensembles sind.

- **Knoten-ID**

  ID wird zugewiesen, wenn dem Cluster ein Node hinzugefügt wird.

- * Clusterschnittstelle*

  Für die Cluster-Kommunikation verwendete Netzwerkschnittstelle.

- **Management-Schnittstelle**

  Management-Netzwerkschnittstelle. Dies ist standardmäßig Bond1G, kann aber auch Bond10G verwenden.

- **Storage-Schnittstelle**

  Storage-Netzwerk-Schnittstelle mit Bond10G.

- **Verschlüsselungsfähig**

  Gibt an, ob der Node die Laufwerkverschlüsselung unterstützt.

Führen Sie Systemtests über die UI pro Node aus

Sie können Änderungen an den Netzwerkeinstellungen testen, nachdem Sie sie zur Netzwerkkonfiguration übergeben haben. Sie können die Tests durchführen, um sicherzustellen, dass der Storage-Node stabil ist und ohne Probleme online geschaltet werden kann.

Sie haben sich bei der UI pro Node für den Storage-Node angemeldet.

1. Klicken Sie Auf **Systemtests**.
2. Klicken Sie neben dem Test, den Sie ausführen möchten, auf **Test ausführen** oder wählen Sie **Alle Tests ausführen**.

   Alle Testvorgänge können zeitaufwändig sein und sollten nur Richtung NetApp Support ausgeführt werden.

   - **Angeschlossenes Ensemble Testen**

     Testet und überprüft die Verbindung zu einem Datenbankensemble. Standardmäßig verwendet der Test das Ensemble für den Cluster, dem der Knoten zugeordnet ist. Alternativ können Sie auch ein anderes Ensemble zur Prüfung der Konnektivität bereitstellen.

   - * Testen Sie Connect Mvip*

     Sendet eine Pings der angegebenen MVIP-Adresse (Management Virtual IP) und führt dann einen einfachen API-Aufruf an das MVIP aus, um die Konnektivität zu überprüfen. Standardmäßig verwendet der Test das MVIP für das Cluster, dem der Node zugeordnet ist.

- * Testen Sie Connect Svip*

  Pings der angegebenen virtuellen Speicher-IP-Adresse (SVIP) mit ICMP-Paketen (Internet Control Message Protocol), die mit der auf dem Netzwerkadapter festgelegten Maximum Transmission Unit (MTU)-Größe übereinstimmen. Er stellt dann eine Verbindung zum SVIP als iSCSI-Initiator her. Standardmäßig verwendet der Test das SVIP für das Cluster, dem der Node zugeordnet ist.

- **Hardware-Konfiguration Testen**

  Testet die Richtigkeit aller Hardware-Konfigurationen, validiert die richtigen Firmware-Versionen und bestätigt, dass alle Laufwerke installiert und ordnungsgemäß ausgeführt werden. Dies ist das gleiche wie bei den werkseitigen Tests.

  Dieser Test ist ressourcenintensiv und sollte nur auf Anfrage des NetApp Supports ausgeführt werden.

- * Testen Sie Lokale Konnektivität*

  Testet die Verbindung zu allen anderen Knoten im Cluster, indem an jeden Knoten die Cluster-IP (CIP) pinging. Dieser Test wird nur auf einem Node angezeigt, wenn der Node Teil eines aktiven Clusters ist.

- **Test Lokalisieren Cluster**

  Überprüft, ob der Node das in der Cluster-Konfiguration angegebene Cluster finden kann.

- **Netzwerk-Konfiguration Testen**

  Stellt sicher, dass die konfigurierten Netzwerkeinstellungen mit den im System verwendeten Netzwerkeinstellungen übereinstimmen. Dieser Test dient nicht zur Erkennung von Hardwarefehlern, wenn ein Node aktiv an einem Cluster teilnimmt.

- **Ping Testen**

  Gibt eine angegebene Liste von Hosts aus oder, wenn keine angegeben werden, erstellt dynamisch eine Liste aller registrierten Nodes im Cluster und pings für einfache Konnektivität.

- **Remote-Verbindung Testen**

  Testet die Verbindung zu allen Knoten in Remote-gekoppelten Clustern durch Ping-Signal der Cluster-IP (CIP) an jedem Knoten. Dieser Test wird nur auf einem Node angezeigt, wenn der Node Teil eines aktiven Clusters ist.

Führen Sie Systemdienstprogramme über die UI pro Node aus

Über die UI pro Node kann der Storage-Node Supportpakete erstellen oder löschen, Konfigurationseinstellungen für Laufwerke zurücksetzen und Netzwerk- oder Cluster-Services neu starten.

Sie haben sich bei der UI pro Node für den Storage-Node angemeldet.

1. Klicken Sie Auf **Systemdienstprogramme**.
2. Klicken Sie auf die Schaltfläche für das Systemdienstprogramm, das Sie ausführen möchten.

- **Steuerleistung**

  Neubooten, aus- und wieder einschalten oder den Node herunterfahren.

  > Dieser Vorgang führt zu einem vorübergehenden Verlust der Netzwerkverbindung.

  Geben Sie die folgenden Parameter an:

  - Aktion: Optionen umfassen Neustart und Anhalten (Ausschalten).
  - Aufwachsverzögerung: Alle zusätzlichen Zeit, bevor der Node wieder online geht.

- **Node Logs Sammeln**

  Erstellt ein Supportpaket unter dem Verzeichnis /tmp/Bundles des Node.

  Geben Sie die folgenden Parameter an:

  - Bundle-Name: Eindeutiger Name für jedes erstellte Support-Bundle. Wenn kein Name angegeben wird, werden „Supportbundle“ und der Node-Name als Dateiname verwendet.
  - Zusätzliche Args: Dieser Parameter wird dem skript sf_Make_Support_Bundle zugeführt. Dieser Parameter sollte nur auf Anfrage des NetApp Support verwendet werden.
  - Timeout sec: Geben Sie die Anzahl der Sekunden an, die auf jede einzelne Ping-Antwort warten sollen.

- **Node Logs Löschen**

  Löscht alle aktuellen Supportpakete auf dem Knoten, die mit **Cluster Support Bundle erstellen** oder der CreateSupportBundle API-Methode erstellt wurden.

- **Laufwerke Zurücksetzen**

  Initialisiert die Laufwerke und entfernt alle auf dem Laufwerk vorhandenen Daten. Sie können das Laufwerk in einem vorhandenen Knoten oder einem aktualisierten Knoten wiederverwenden.

  Geben Sie den folgenden Parameter an:

  - Laufwerke: Liste der Gerätenamen (keine Fahrerkennungen) zum Zurücksetzen.

- **Netzwerk-Konfiguration Zurücksetzen**

  Unterstützt die Behebung von Netzwerkkonfigurationsproblemen für einen einzelnen Knoten und setzt die Netzwerkkonfiguration eines einzelnen Knotens auf die Werkseinstellungen zurück.

- **Knoten Zurücksetzen**

  Setzt einen Knoten auf die Werkseinstellungen zurück. Alle Daten werden entfernt, die Netzwerkeinstellungen für den Node jedoch während dieses Vorgangs erhalten. Nodes können nur zurückgesetzt werden, wenn sie einem Cluster nicht zugewiesen sind und sich im verfügbaren Status befinden.

  > Bei Verwendung dieser Option werden alle Daten, Pakete (Software-Upgrades), Konfigurationen und Protokolldateien vom Knoten gelöscht.

- **Netzwerk Neu Starten**

Startet alle Netzwerkdienste auf einem Node neu.

> Dieser Vorgang kann zu einem vorübergehenden Verlust der Netzwerkverbindung führen.

- **Neustart Service**

  Startet die Element Softwareservices auf einem Node neu.

  > Dieser Vorgang kann zu einer temporären Node-Serviceunterbrechung führen. Sie sollten diesen Vorgang nur auf Anweisung des NetApp Supports durchführen.

  Geben Sie die folgenden Parameter an:

  - Dienst: Dienstname, der neu gestartet werden soll.
  - Aktion: Aktion, die auf dem Dienst ausgeführt werden soll. Die Optionen umfassen Start, Stopp und Neustart.

Arbeiten Sie mit dem Management-Node

Sie können den Management-Node (mNode) verwenden, um Systemservices zu aktualisieren, Cluster-Assets und -Einstellungen zu managen, Systemtests und Dienstprogramme auszuführen, Active IQ für das System-Monitoring zu konfigurieren und den NetApp Support-Zugriff zur Fehlerbehebung zu aktivieren.

> Als Best Practice wird nur ein Management Node mit einer VMware vCenter Instanz verknüpft, sodass nicht dieselben Storage- und Computing-Ressourcen oder vCenter Instanzen in mehreren Management Nodes definiert werden müssen.

Siehe "Dokumentation des Management-Node" Finden Sie weitere Informationen.

Erläuterung der Cluster-Auslastungsebenen

Der Cluster, auf dem Element Software ausgeführt wird, generiert Cluster-Fehler, um den Storage-Administrator zu warnen, wenn die Kapazität des Clusters knapp wird. Es gibt drei Ebenen der Cluster-Fülle, die alle in der NetApp Element UI angezeigt werden: Warnung, Fehler und kritisch.

Das System verwendet den BlockClusterFull-Fehlercode, um vor der Speicherfülle des Clusterblocks zu warnen. Sie können die Schweregrade für die Cluster-Fülle über die Registerkarte Meldungen der Element UI anzeigen.

Die folgende Liste enthält Informationen zum Schweregrad BlockClusterFull:

- **Warnung**

  Dies ist eine vom Kunden konfigurierbare Warnung, die angezeigt wird, wenn sich die Blockgröße des Clusters dem Fehlergrad nähert. Diese Stufe wird standardmäßig auf drei Prozent unter der Fehlerebene festgelegt und kann über die Element-UI und -API optimiert werden. Sie müssen so schnell wie möglich zusätzliche Kapazität hinzufügen oder Kapazität freisetzen.

- **Fehler**

  Wenn sich das Cluster in diesem Status befindet und ein Node verloren geht, ist nicht genügend Kapazität im Cluster vorhanden, um die Double Helix Datensicherung wiederherzustellen. Erstellung neuer Volumes, Klone und Snapshots werden allesamt gesperrt, während sich das Cluster in diesem Zustand befindet. Dies ist kein sicherer oder empfohlener Status für ein Cluster in. Sie müssen zusätzliche Kapazität hinzufügen oder Kapazität sofort freisetzen.

- * Kritisch*

  Dieser kritische Fehler ist aufgetreten, da das Cluster zu 100 Prozent verbraucht wird. Die Lösung befindet sich im schreibgeschützten Zustand und es können keine neuen iSCSI-Verbindungen zum Cluster hergestellt werden. Wenn Sie diese Phase erreichen, müssen Sie sofort freisetzen oder mehr Kapazität hinzufügen.

Das System verwendet den MetadaClusterFull Fehlercode, um über die Speicherfülle des Clusters zu warnen. Sie können die Cluster-Metadaten-Storage-Fülle im Abschnitt Cluster-Kapazität auf der Übersichtsseite der Registerkarte Berichterstellung in der Element UI anzeigen.

Die folgende Liste enthält Informationen zu den Schweregraden für MetadataClusterFull:

- **Warnung**

  Dies ist eine vom Kunden konfigurierbare Warnung, die angezeigt wird, wenn sich die Metatdatenkapazität des Clusters dem Schweregrad „Fehler“ nähert. Standardmäßig wird diese Ebene auf drei Prozent unter der Fehlerebene gesetzt und kann über die Element-API optimiert werden. Sie müssen so schnell wie möglich zusätzliche Kapazität hinzufügen oder Kapazität freisetzen.

- **Fehler**

  Wenn sich das Cluster in diesem Status befindet und ein Node verloren geht, ist nicht genügend Kapazität im Cluster vorhanden, um die Double Helix Datensicherung wiederherzustellen. Erstellung neuer Volumes, Klone und Snapshots werden allesamt gesperrt, während sich das Cluster in diesem Zustand befindet. Dies ist kein sicherer oder empfohlener Status für ein Cluster in. Sie müssen zusätzliche Kapazität hinzufügen oder Kapazität sofort freisetzen.

- * Kritisch*

  Dieser kritische Fehler ist aufgetreten, da das Cluster zu 100 Prozent verbraucht wird. Die Lösung befindet sich im schreibgeschützten Zustand und es können keine neuen iSCSI-Verbindungen zum Cluster hergestellt werden. Wenn Sie diese Phase erreichen, müssen Sie sofort freisetzen oder mehr Kapazität hinzufügen.

Folgendes gilt für Cluster-Schwellenwerte mit zwei Nodes:

- Metadaten-Fehler liegt 20 % unter dem kritischen Wert.
- Unter dem kritischen Block-Auslastungsfehler liegt ein Block-Laufwerk (einschließlich ungenutzter Kapazität). Das bedeutet, dass es sich um zwei Blocklaufwerke handelt, die weniger kritisch sind.