Installation und Verwendung von SolidFire Enterprise SDS

Element Software

NetApp
March 01, 2023

Inhaltsverzeichnis

Installation und Verwendung von SolidFire Enterprise SDS

Lesen Sie, wie Sie SolidFire Enterprise SDS installieren und verwenden.

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Erste Schritte mit NetApp SolidFire Enterprise SDS

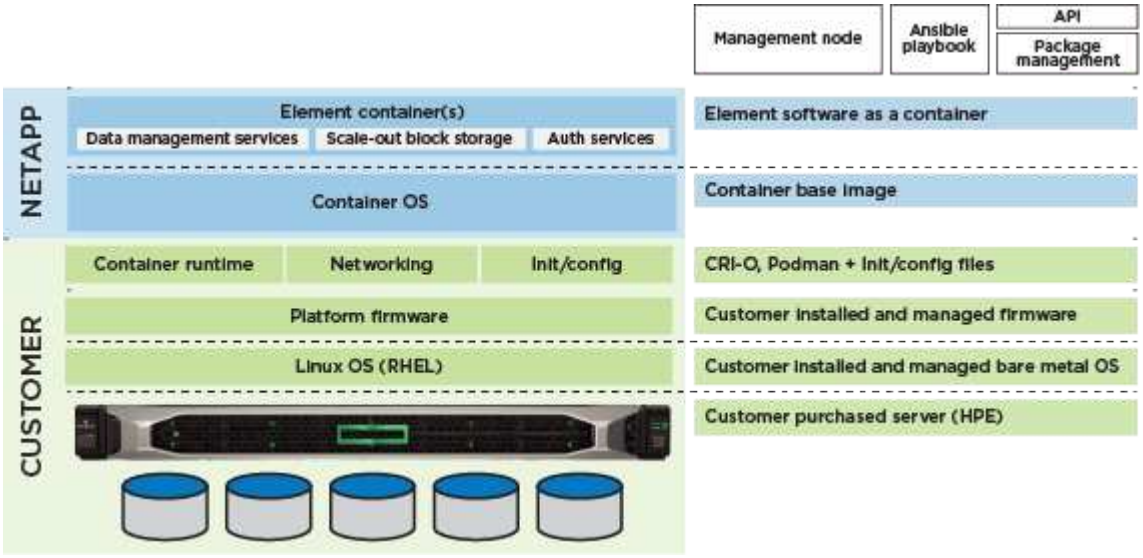
NetApp SolidFire Enterprise SDS (ESDS) bietet die Vorteile der Scale-Out-Technologie von SolidFire und der NetApp Element Software-Datenservices auf der Hardware Ihrer Wahl, die der Referenzkonfiguration für SolidFire ESDS entspricht. SolidFire ESDS stellt die NetApp Element-Software unabhängig von der zugrunde liegenden Hardware bereit. So können Sie sämtliche Funktionen der Elemente entweder auf einer NetApp Appliance oder auf einem Allzweck-Server nutzen, der mit der NetApp Referenzkonfiguration konform ist.

Hauptmerkmale von SolidFire ESDS

- Ermöglicht die Installation und Ausführung von Element Software über Container.
- Bietet Storage-Funktionen und Zuverlässigkeit der Enterprise-Klasse auf vorab validierten Standard-Serverplattformen. Sie können Produktions-Workloads ausführen, nachdem Sie die SolidFire ESDS-Software auf der vorgegebenen x86-Serverplattform und den zugrunde liegenden Komponenten (CPU, Arbeitsspeicher, SSD-Laufwerke, Cache, Netzwerk, Firmware) gemäß der veröffentlichten Referenzkonfiguration im "NetApp Interoperabilitäts-Matrix-Tool (IMT)".
- Bietet Softwareverschlüsselung für Daten im Ruhezustand. Mithilfe der Softwareverschlüsselung können alle auf die SSDs in einem Storage-Cluster geschriebenen Daten verschlüsselt werden. Dies bietet eine primäre Verschlüsselungsschicht in SolidFire ESDS-Knoten, die keine Self-Encrypting Drives (SEDs) enthalten.
- Ermöglicht mithilfe von Quality-of-Service-Richtlinien (QoS) eine vorhersehbare Cluster-Performance.

- Unterstützt Cluster mit vier bis 40 Nodes.
- Mit dem Term Capacity License Modell lizenziert.
- Nutzt ein neues Modell für Support durch Support-Vereinbarungen mit Technologiepartnern.

Mit SolidFire ESDS bietet NetApp Container für Element, das Sie auf Standard-Hardware ausführen können, die die erforderlichen Anforderungen erfüllt. Sie bringen Ihren eigenen Server mit einem bereits installierten Betriebssystem. Kunden verwenden ein Automatisierungs-Tool wie Ansible, um die Compliance-Prüfung vor der Installation auszuführen und den SolidFire ESDS zu installieren. Im Rahmen Ihrer Vorinstallationsaufgaben sollten Sie den Management-Node installieren, der die Protokollbündelsammlung sowie andere Services wie SolidFire AIQ unterstützt. Hier ist ein Überblick über die Architektur, der die verschiedenen Komponenten der ESDS-Umgebung von SolidFire anzeigt:



Sie sind für die Konfiguration, Überwachung und Verwaltung des Lebenszyklus der Plattform sowie für die Konfiguration der Netzwerkschnittstellen und Routing-Tabellen verantwortlich.

Einige Funktionen der NetApp Element-Software gelten nicht für SolidFire ESDS. Native Element Funktionen für herkömmliche SolidFire Storage Nodes wie Hardware-Monitoring, Firmware-Updates, Verschlüsselung als Rest (OHR) mit Self-Encrypting Drives (SEDs) und Fibre Channel sind für SolidFire ESDS deaktiviert.

- Externes Verschlüsselungsmanagement (EKM)
- Hardware-Verschlüsselung
- Multi-Drive Slice Service (MDSS)
- Hardware-Überwachung, Aktualisierungen der Host-Plattform (z. B. Treiber, Firmware- und Betriebssystempakete) und Fibre Channel

Schnellstartinformationen

Hier finden Sie eine Reihe von Anweisungen für die Installation von SolidFire ESDS "Hier".

Lizenzrichtlinien

SolidFire ESDS unterliegt dem NetApp Term Capacity License Modell.

Hier finden Sie eine allgemeine Übersicht über die Richtlinien dieses Modells:

- Softwarekosten sind abhängig von der Rohkapazität (Größe der Laufwerke, also die Anzahl der Laufwerke im Node oder Cluster). Somit lassen sich die Softwarekosten für dieses Modell leicht vorhersagen.
- Sie benötigen keinen Softwarelizenzschlüssel. Sie erhalten auf dem Auftrag eine Master-Seriennummer für die Software, die im Dokumentenkit enthalten ist, das Sie nach der Bestellung erhalten. Sie müssen diese Master-Seriennummer behalten, da sie für den Support verwendet wird.

Weitere Informationen finden Sie unter "Kaufmodelle für NetApp HCI und SolidFire".

Schnittstellen zur Installation und Verwendung von SolidFire ESDS

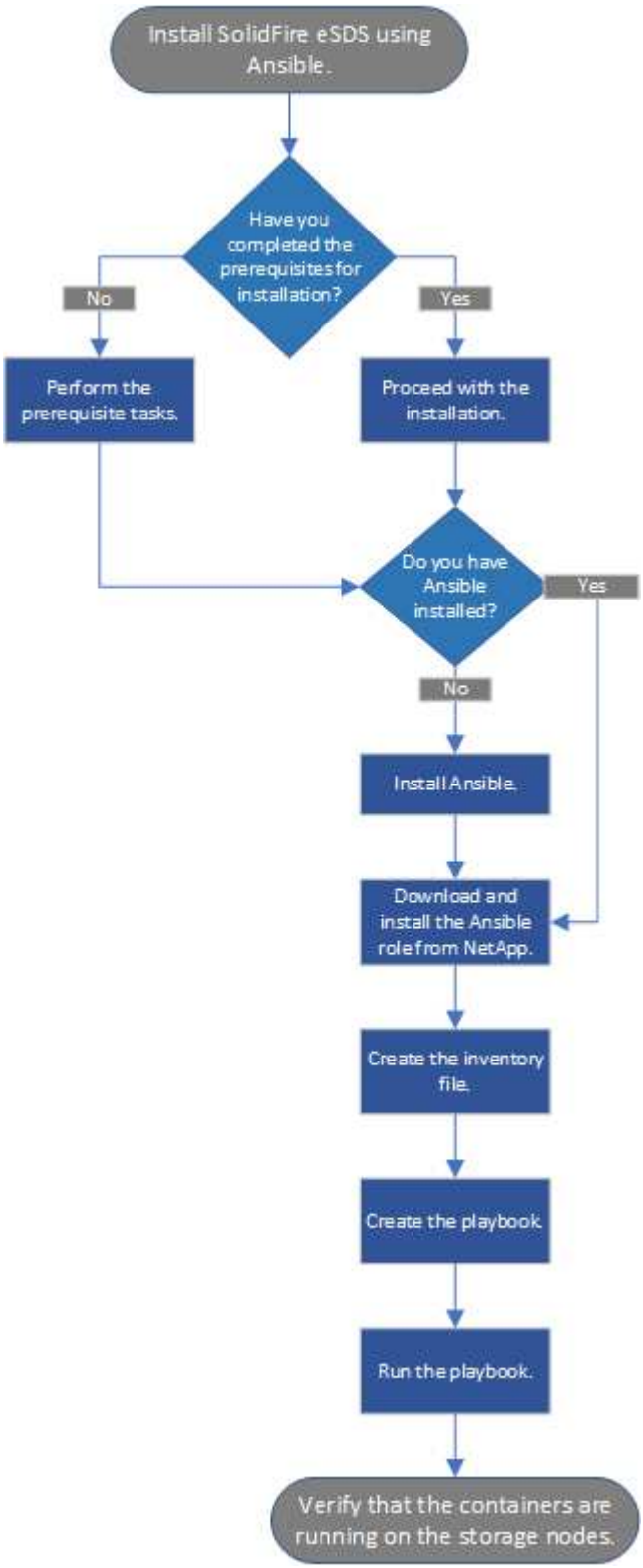
Hier ist eine Liste der Tools und Schnittstellen, die Sie für die Installation, Überwachung und Verwaltung von SolidFire ESDS verwenden:

Tool/Schnittstelle	Wer verwendet den Storage	Beschreibung
Ansible-Compliance-Überprüfung, Rolle	Kunde	Überprüfen, ob die Plattform mit der in angegebenen Referenzkonfiguration übereinstimmt "NetApp Interoperabilitäts-Matrix-Tool (Anmeldung erforderlich)". Sie sollten dies vor der Installation von SolidFire ESDS tun.
Ansible-Installationsrolle	Kunde	Zur Installation von SolidFire ESDS.
Management-Node	Kunde	Für Protokollsammlung und Management-Services wie AIQ
NetApp Hybrid Cloud Control	Kunde, NetApp Support	Für die Cluster-Erstellung und das Management pro Node sowie die Erfassung von Protokollen vom Management-Node.
Hewlett Packard Enterprise (HPE) Integrated Lights Out (iLO)	Kunde, HPE Support	Zum Erfassen von Daten über Ereignisse und Status für die Ursachenanalyse.
Dell Integrated Dell Remote Access Controller (iDRAC)	Kunde, Dell Support	Zum Erfassen von Daten über Ereignisse und Status für die Ursachenanalyse.
NetApp Element Software-UI	Kunde	Für das Management von ESDS-Speicherclustern von SolidFire.
Active IQ	Kunde, NetApp Support	Für das Monitoring des Cluster-Systemzustands.
Eine Sammlung	NetApp Support	Für zusätzliche Protokollerfassung.

Übersicht über die Installation

Sie können SolidFire ESDS mit einem Automatisierungs-Tool wie Ansible installieren.

Hier ein grundlegender Überblick über die Installation mit Ansible:



Dynamische Node-Bewertung

Mit der in Element 12.3.1 eingeführten dynamischen Knotenbewertung können Sie 24 unterstützte CPUs pro ESDS-Plattform nutzen, im Gegensatz zum heutigen Modell einer einzigen CPU pro Plattform.

Die dynamische Knotenbewertung wird auf allen Plattformen unterstützt, die derzeit auf ESDS unterstützt werden: DL360, DL380 und R640.

Bei der ersten Version der dynamischen Node-Bewertung beträgt die maximale IOPS eines jeden Node 100.000 IOPS.

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Führen Sie die erforderlichen Aufgaben für die Installation aus

Vor der Installation von SolidFire ESDS stellen Sie sicher, dass Ihre Umgebung die Konfigurations-, IP-Adressierung- und Netzwerkanforderungen erfüllt.

Installieren Sie die erforderliche Hardware

- Installieren Sie den unterstützten Server. Siehe "NetApp Interoperabilitäts-Matrix (Anmeldung erforderlich)" Finden Sie weitere Informationen.
- Stellen Sie sicher, dass Ihre Hardwarekonfiguration ausgewogen ist und alle Kanäle gefüllt sind. Weitere Informationen zur Maximierung der Bandbreite finden Sie im "KB-Artikel" (anmeldung erforderlich).

Konfigurieren Sie den Host (Knoten)

- Installieren Sie Red hat Package Manager auf Basis der unterstützten Versionen, die in aufgeführt sind "NetApp Interoperabilitäts-Matrix (Anmeldung erforderlich)".
- Konfigurieren Sie einen NTP-Server (Network Time Protocol) für die Verwendung mit allen Hosts im Netzwerk.
- Wenn Sie das Installationsziel auswählen, wählen Sie das Optionsfeld aus, um die Partitionierung des Dateisystems manuell zu konfigurieren. Verwenden Sie auf der Seite **Manuelle Partitionierung** die Schaltflächen **+** und **-**, um vorhandene Partitionen zu entfernen und neue Partitionen zu erstellen und diese nach den hier aufgeführten Empfehlungen zu dimensionieren. Mit dem Standard-LVM-Partitionierungsschema können Sie bei Bedarf die Größe später problemlos ändern.

> Standardmäßig wählt Red hat Package Manager aus `xfs` Als Standarddateisystem für die Partitionen, die Sie manuell erstellen. Sie sollten es in ändern `ext4`, Mit Ausnahme des `/boot` Und `swap` Partitionen: Ihr `/boot` Die Partition sollte verwendet werden `ext2`.

Wenn Ihr SATA-Laufwerk 250 GB beträgt, befolgen Sie die unten empfohlene Partition. Wenn Ihre SATA-Festplatte mehr Speicherplatz hat, können Sie die Partitionsgrößen /opt und /var erhöhen.

Partition	Größe
/Boot	1 GB

Partition	Größe
/Opt	50 GB
/Var	50 GB
Austauschen	4 GB
/Zu Hause	5 GB
/	Mindestens 10 GB
/Usr	Mindestens 10 GB

Der `/dev/sdb` Die Festplatte wird von keinem Prozess verwendet.

- Deaktivieren Sie RAID für /Boot.
- Wählen Sie auf dem Bildschirm Softwareauswahl, auf dem Sie bestimmte zu installierende Pakete auswählen, basierend auf Ihrer Red hat Package Manager-Version **Server** oder **Infrastructure Server** aus.
- Gehen Sie nach dem ersten Start wie folgt vor:
  - Installieren Sie Red hat Subscription Manager und aktivieren Sie die folgenden Repositories:

```
rhel-7-server-ansible-2.9-rpms
rhel-7-server-optional-rpms
rhel-7-server-extras-rpms
```

  - Aktivieren Sie SSH auf Ihren Knoten.
  - Wenn Sie IPv6 deaktivieren möchten, befolgen Sie die in diesem Schritt beschriebenen Schritte "KB-Artikel (Anmeldung erforderlich)".

Installieren Sie die erforderliche Software

- Installation von Ansible, Git, Podman und Python 3.0

Für Element 12.5 hängt die unterstützte Podman-Version von Ihrer Red hat Package Manager-Version ab:

Red hat Package Manager-Version	Podman-Version
7.x	1.6.4
8.1, 8.2, 8.3 und 8.4	3.1.x, 3.2.x, 3.3.x, 3.4.1 und 3.4.2 Sobald verfügbar, empfiehlt NetApp, Sicherheitsupdates für Ihre Podman-Version zu akzeptieren.

Überprüfen Sie, ob Ihre Konfiguration den Anforderungen von NetApp für die Installation von SolidFire ESDS entspricht

- Verwenden Sie die in aufgeführte SolidFire-ESDS-Konfiguration "NetApp Interoperabilitäts-Matrix-Tool (IMT)" Als Referenz zu dienen.

Wenn Sie sich bei Problemen im Zusammenhang mit dem SolidFire ESDS an den NetApp Support wenden, stellt der Support zunächst sicher, dass die Plattform den im IMT aufgeführten Referenzkonfigurationen für ESDS von SolidFire entspricht. Wenn der Support feststellt, dass die zugrunde liegende Plattform nicht der Referenzkonfiguration entspricht, unterstützt Sie die Ausrichtung der nicht konformen Firmware-, Software- und/oder Hardwarekomponenten auf die entsprechenden Versionen im IMT.

- Führen Sie eine Compliance-Prüfung für SolidFire ESDS durch.

a. Führen Sie die aus `ansible-galaxy install` Befehl zum Installieren des `nar_solidfire_sds_compliance` Rolle:

```
ansible-galaxy install git+https://github.com/NetApp-Automation/nar_solidfire_sds_compliance.git
```

Sie können die Rolle auch manuell installieren, indem Sie sie aus dem kopieren "NetApp GitHub Repository" Und die Rolle in das zu setzen `~/.ansible/roles` Verzeichnis. NetApp stellt eine README-Datei zur Verfügung, die Informationen zur Ausführung einer Rolle enthält.

Stellen Sie sicher, dass Sie immer die neuesten Versionen der Rollen herunterladen.

b. Verschieben Sie die Rollen, die Sie heruntergeladen haben, in einem Verzeichnis, von dem aus sie installiert wurden.

```
$ mv ~/.ansible/roles/ansible/nar_solidfire_sds_* ~/.ansible/roles/
```

c. Führen Sie die aus `ansible-galaxy role list` Befehl, um sicherzustellen, dass Ansible für die Verwendung der neuen Rollen konfiguriert ist.

```
- nar_solidfire_sds_install, (unknown version)
- nar_solidfire_sds_upgrade, (unknown version)
- ansible, (unknown version)
- nar_solidfire_sds_compliance, (unknown version)
- nar_solidfire_cluster_config, (unknown version)
- nar_solidfire_sds_uninstall, (unknown version)
```

d. Erstellen Sie das Playbook für die Compliance-Überprüfung.

e. Führen Sie das Playbook zur Compliance-Überprüfung aus, wie im folgenden Beispiel dargestellt:

```
$ ansible-playbook -i yourinventory.yml yourplaybook.yml
```

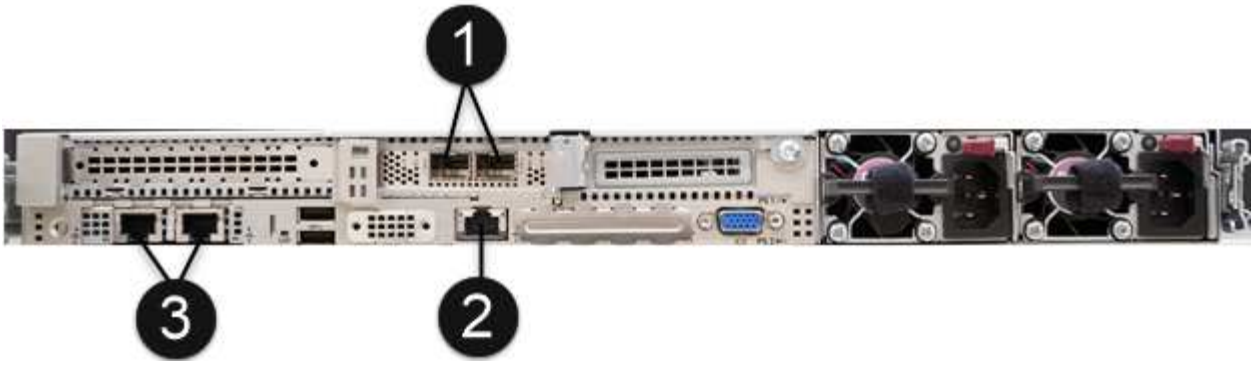
Selbst wenn Sie das ESDS-System von SolidFire nutzen, sollten Sie die Compliance-Prüfung regelmäßig durchführen, um sicherzustellen, dass Ihr System konform ist. In einigen Fällen fordert Sie der NetApp Support von Ihnen, die Compliance-Überprüfung auszuführen, um Probleme zu diagnostizieren und zu beheben.

Anforderungen an Netzwerk- und IP-Adressen verstehen

- Machen Sie sich mit der Konfiguration und Verwaltung von Netzwerken und Netzwerkschnittstellen in Red hat Package Manager vertraut. Siehe "Red hat-Dokumentation".
- Konfigurieren Sie Ihr Netzwerk gemäß den hier angegebenen IP-Anforderungen:

Komponente	IP-Adresse des Storage-Netzwerks	IP-Adresse des Managementnetzwerks	Summe # der IP-Adressen
Storage-Node	1	1	2 pro Node
Management-Node	(Optional) 1	1	1 pro Cluster im Speichernetzwerk + 1 pro Cluster im Managementnetzwerk + 1 FQDN pro Cluster für den Management-Node
Storage-Cluster	Nr. 1 Speicher-IP (SVIP)	1 Management-IP (MVIP)	2 pro Storage Cluster

- Konfigurieren Sie das Storage-Netzwerk auf 25-GbE-Ethernet-Switches und das Management-Netzwerk auf 10-GbE-Switches. Siehe folgende Verkabelungsabbildung:



Element	Beschreibung
1	Ports für das Storage-Netzwerk
2	Port für IPMI
3	Ports für das Management-Netzwerk

Die hier angegebene Abbildung soll als Beispiel dienen. Ihre tatsächliche Hardware kann sich abhängig vom Server, den Sie haben, unterscheiden.

- Ändern Sie den MTU-Switch-Port in 9216 Byte.

Erlauben Sie bestimmte Ports durch die Firewall Ihres Rechenzentrums

- Wenn `firewalld` Ist auf dem Speicherknoten aktiviert, auf dem Red hat Package Manager ausgeführt wird, stellen Sie sicher, dass die folgenden Ports geöffnet sind, so dass Sie das System Remote verwalten können, Clients außerhalb Ihres Rechenzentrums eine Verbindung zu Ressourcen herstellen können und sicherstellen können, dass interne Dienste ordnungsgemäß funktionieren:

Quelle	Ziel	Port	Beschreibung
MIP-Speicher-Node	Management-Node	80 TCP/UDP	Cluster-Upgrades
SNMP-Server	MIP-Speicher-Node	161 UDP	SNMP-Abfrage
System Administrator-PC	Management-Node	442 TCP	HTTPS-UI-Zugriff auf den Management-Node
System Administrator-PC	MIP-Speicher-Node	442 TCP	HTTPS-UI-Zugriff auf Storage-Node
ISCSI-Clients	Storage Cluster MVIP	443 TCP	(Optional) UI- und API-Zugriff
Management-Node	monitoring.solidfire.com	443 TCP	Berichterstellung für den Storage-Cluster an Active IQ

Quelle	Ziel	Port	Beschreibung
MIP-Speicher-Node	Remote Storage Cluster MVIP	443 TCP	Kommunikation über die Verbindung des Remote-Replikationsclusters
MIP-Speicher-Node	MIP für Remote-Storage-Node	443 TCP	Kommunikation über die Verbindung des Remote-Replikationsclusters
SolidFire ESDS sfapp	UI- und API-Zugriff pro Node, um ein Cluster zu erstellen	2010 UDP	Cluster-Beacon (Erkennung von Nodes, die zu einem Cluster hinzugefügt werden sollen)
ISCSI-Clients	Storage Cluster SVIP	3260 TCP	ISCSI-Kommunikation des Clients
ISCSI-Clients	Speicher-Cluster SIP	3260 TCP	ISCSI-Kommunikation des Clients
SOAP-Server	SolidFire ESDS sfapp	7627 TCP	SOAP-Webservices
System Administrator-PC	1. A.	8080 TCP	Kommunikation für Systemadministratoren
VCenter Server	Management-Node	8443 TCP	VCenter Plug-in QoSSIOC-Service

Die Ports 2181, 2182 und 2183 sind für die verteilte Elementdatenbank erforderlich und werden bei der Installation von SolidFire ESDS dynamisch aus dem Elementcontainer geöffnet.

- Verwenden Sie folgende Befehle, um die oben genannten Ports zu öffnen:

```
systemctl start firewalld
firewall-cmd --permanent --add-service=snmp
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=80/udp
firewall-cmd --permanent --add-port=442-443/tcp
firewall-cmd --permanent --add-port=442-443/udp
firewall-cmd --permanent --add-port=2010/udp
firewall-cmd --permanent --add-source-port=2010/udp
firewall-cmd --permanent --add-port=3260/tcp
firewall-cmd --permanent --add-port=7627/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=8443/tcp
firewall-cmd --reload
```

Konfigurieren Sie Ihr Hostnetzwerk

- Konfigurieren Sie das Hostnetzwerk mit "Best Practices in sich vereint" Wird bereitgestellt.

> Führen Sie die Schritte durch, um Ihr Hostnetzwerk so zu konfigurieren, dass eine erfolgreiche Installation von SolidFire ESDS sichergestellt ist.

*** Zusätzliche Anforderungen erfüllen***

- Installieren Sie eine Datensammlung, die von NetApp Support für die Erfassung der Host-Protokolle verwendet wird. Sie können eine Collect von installieren "Hier". Sie benötigen ein NetApp Konto, um auf den Download zugreifen zu können. Sie können auch das One Collect Installation Guide und die Versionshinweise am selben Ort finden.

> Sie müssen einen Collect herunterladen und installieren, um einen optimalen Support erhalten zu können.

- Installieren Sie den Management-Node für die Protokollerfassung und um NetApp Support-Zugriff zur Fehlerbehebung zu aktivieren. Informationen zu Management-Node und Installationsschritten finden Sie unter "Hier".

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Überlegungen bei der Netzwerkkonfiguration

Vor der Installation von SolidFire ESDS sollten Sie die erforderlichen Netzwerke auf den Speicherknoten einrichten, auf denen RHEL ausgeführt wird. Sie sind für das Netzwerk-Routing in Ihrer Umgebung verantwortlich. Sie können die Best Practices, die als Framework zur Verfügung gestellt werden, verwenden.

- Verwenden Sie gebundene oder geteamte Schnittstellen.
- Verwenden Sie die gleichen Schnittstellennamen für alle Knoten im Cluster (z. B. Team-Management für die Managementoberfläche jedes Node und Team-stg für die Storage-Schnittstelle jedes Node).
- Stellen Sie sicher, dass NetworkManager ausgeführt wird.
- Stellen Sie sicher, dass das Paket „NetworkManager-Dispatcher-Routing-Rules“ auf allen Storage-Nodes für richtlinienbasiertes Routing installiert ist.
- Siehe "Best Practices für die Netzwerk- und Netzwerkwartung bei NetApp SolidFire Storage-Systemen".
- Konfigurieren Sie das Management- und die Storage-Netzwerke auf jedem Node so, dass mehrere redundante physische Schnittstellen über Bond oder Team-Konfigurationen verwendet werden.

Weitere Informationen zur Netzwerkbildung finden Sie unter "Konfiguration der Netzwerk-Teaming". Standardmäßig sind alle Storage-Node-10-GbE-Schnittstellen mit einer Maximum Transmission Unit (MTU) von 9000 Byte aktiviert. Für optimale Performance konfigurieren Sie alle Server-seitigen Storage-Schnittstellen mit derselben MTU wie die NetApp SolidFire Storage-Nodes. Sie sollten Netzwerk-Switches so konfigurieren, dass eine MTU von mindestens 9016 Byte oder mehr unterstützt wird, um den Jumbo Frame Overhead und die ordnungsgemäße Weiterleitung über das Netzwerk zu berücksichtigen. Wenn Sie diese Konfiguration ändern möchten, um eine niedrigere MTU-Einstellung zu unterstützen, wenden Sie sich an den NetApp Support.

In der folgenden Tabelle finden Sie Informationen zu den Speicher- und Verwaltungsnetzwerken, die SolidFire ESDS für die verschiedenen Arten von Datenverkehr benötigt:

Netzwerktyp	Beschreibung
Datennetzwerk Storage-Netzwerk	• Umfasst den gesamten Storage-/iSCSI-Datenverkehr. • Sie können weitergeleitet werden, wenn Sie Hosts bereitstellen möchten, die sich auf einem anderen Layer-3-Netzwerk befinden, oder wenn Sie Daten zwischen Clustern replizieren möchten. • Sollte mit Netzwerkschnittstellen auf derselben Layer 2 Broadcast-Domäne konfiguriert sein.
Managementnetzwerk	• Umfasst den gesamten Verwaltungsverkehr. • Kann geroutet werden, wenn Sie über ein anderes Layer 3-Netzwerk auf die Cluster-API oder -UI zugreifen möchten. • Sollte mit Netzwerkschnittstellen auf derselben Layer 2 Broadcast-Domäne konfiguriert sein. • Sollte mit einer Netzwerkschnittstellenkarte mit einer MTU von mindestens 1500 Bytes konfiguriert werden.

Beispiele und Tipps zur Konfiguration des Hostnetzwerks finden Sie unter "Hier".

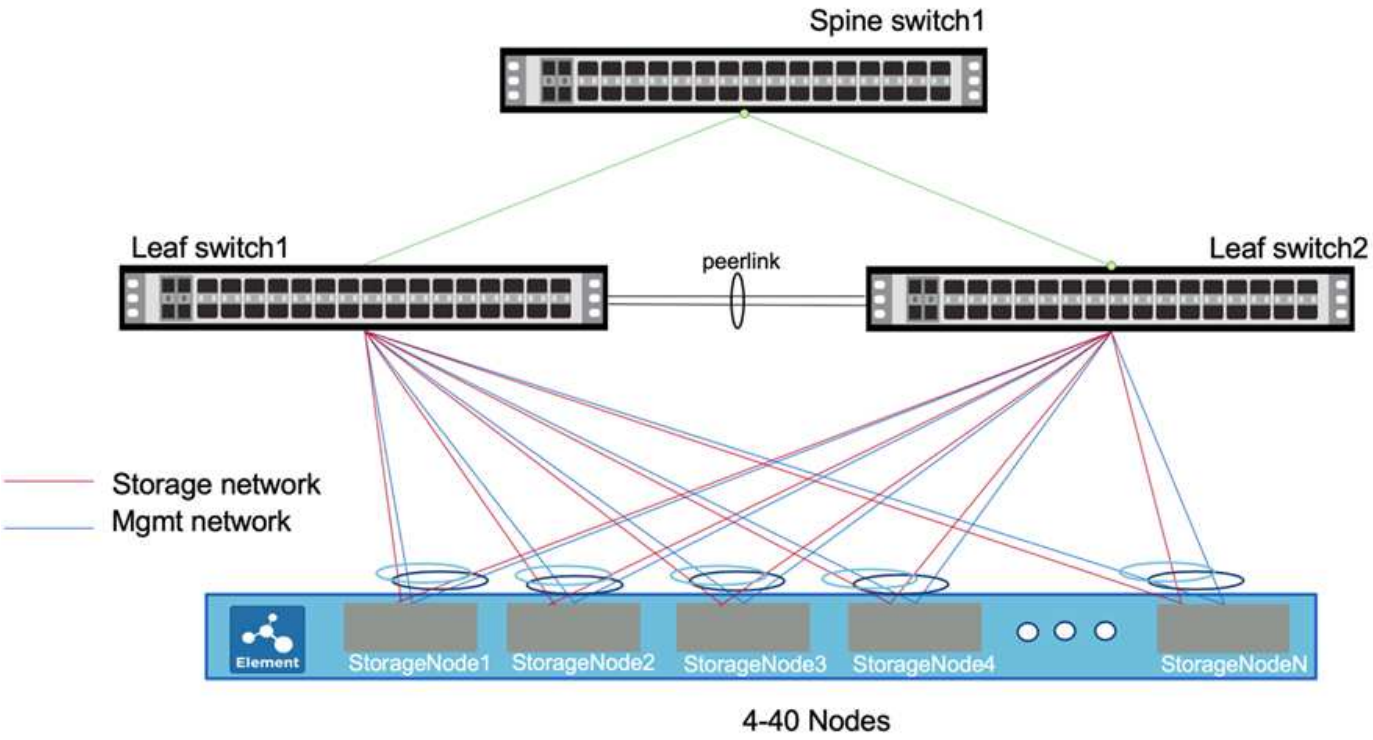
Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Konfigurieren Sie das Hostnetzwerk

Verwenden Sie die Beispiele und Tipps, die Sie zur Konfiguration des Hostnetzwerkes verwenden, bevor Sie SolidFire ESDS installieren.

Hier ist eine Beispiel für eine Netzwerkkonfiguration:



In diesem Beispiel sind zwei Schnittstellen auf dem Storage-Node Netzwerk "Team" Aus Redundanzgründen mit dem Managementnetzwerk verbunden. Ebenso werden zwei zusätzliche Schnittstellen miteinander kombiniert und mit dem Storage-Netzwerk verbunden.

Jede Schnittstelle hat eine Konfigurationsdatei namens ifcfg-<Interface-Name>X, wobei X die Nummer der Schnittstelle ist, beginnend mit null oder 1 je nach verwendeter Namenskonvention. Die Konfigurationsdateien werden beim ersten Erstellen der Schnittstellen erstellt. Für jede der beiden physischen Schnittstellen, die mit dem Storage-Netzwerk verbunden sind, sollte bereits eine Konfigurationsdatei vorhanden sein. Für jede der beiden physischen Schnittstellen, die mit dem Management-Netzwerk verbunden sind, sollte auch eine Konfigurationsdatei vorhanden sein. Die Schnittstellenkonfigurationsdateien sind im Verzeichnis /etc/sysconfig/Network-scripts abgelegt. Siehe "Schnittstellenkonfigurationsdateien".

In den hier angegebenen Beispielen sind die Namen der Storage- und Managementoberfläche für HPE-Server angegeben. Wenn Sie einen Dell-Server haben, unterscheiden sich die Schnittstellennamen. Die Namen der Speicherschnittstelle für den Dell-Server lauten em1 und em2. Die Namen der Managementoberfläche für den Dell-Server sind p3p1 und p3p2.

Schritte

1. Installieren `NetworkManager-dispatcher-routing-rules` Paket und stellen Sie sicher, dass die entsprechenden Repositorys konfiguriert sind.
2. Konfigurieren Sie Ihren Netzwerk-Switch mithilfe der Dokumentation des Switch-Anbieters. Genaue Anweisungen zum Konfigurieren des MLAG-Protokolls (Multi-Chassis Link Aggregation Group) und dem Link Aggregation Control Protocol (LACP) finden Sie in der Dokumentation Ihres Switch-Anbieters.

   Es wird empfohlen, LACP Fallback zu konfigurieren und LACP Individual Port Suspension Verhalten durch Ausführen zu deaktivieren `no lacp suspend-individual`. So kann der AccessPoint Link auch ohne LACP-Pakete bei Fehlkonfigurationen übertragen werden.

3. Bearbeiten Sie die beiden Konfigurationsdateien für die physischen Schnittstellen, die mit dem Storage-Netzwerk verbunden sind. Verwenden Sie hierfür das folgende Beispiel: Jumbo-Frame-Einstellung im Storage-Netzwerk wird dringend empfohlen, ist jedoch nicht erforderlich. In diesem unten stehenden Beispiel ist der Name des Speicherinterface ens2f0 und der Name des Speicherteams team10G:

   IN allen hier aufgeführten Beispielkonfigurationen VERWENDEN NAME und GERÄT dieselben Werte. Sie können verschiedene Werte verwenden, wenn Sie dies tun.

   ```
   # cat /etc/sysconfig/network-scripts/ifcfg-ens2f0
   # 10G Team Physical Port to Storage Network
   NAME=ens2f0
   DEVICE=ens2f0
   ONBOOT=yes
   TEAM_MASTER=team10G
   DEVICETYPE=TeamPort
   MTU=9000
   ```

4. Bearbeiten Sie die beiden Konfigurationsdateien für die mit dem Managementnetzwerk verbundenen Schnittstellen anhand des folgenden Beispiels. In diesem Beispiel lautet der Name der Management-Schnittstelle eno5 und der Name des Management-Teams team1G:

   ```
   # cat ifcfg-eno5
   # 1G Team Physical Port to Management Network
   NAME=eno5
   DEVICE=eno5
   ONBOOT=yes
   TEAM_MASTER=team1G
   DEVICETYPE=TeamPort
   ```

5. Erstellen Sie die Team Interface-Datei für das Storage Team anhand des folgenden Beispiels. In diesem Beispiel heißt das Team team10G. Sie befindet sich auf dem Storage-Netzwerk mit dem Network Teaming lacp Läufer.

Für Storage-Schnittstellen wird die aktiv/aktiv-Konfiguration empfohlen. Diese Konfiguration erfordert ein zusätzliches aktiv/aktiv-MLAG-Protokoll (Multi-Chassis Link Aggregation Group) und das Link Aggregation Control Protocol (LACP) für die Konfiguration auf den Switches. Diese Konfiguration erfordert das "Network Teaming lacp Runner".

```
# cat /etc/sysconfig/network-scripts/ifcfg-team10G
# IPADDR= "SIP"
# GATEWAY= "SIP_GATEWAY"
# Pick one TEAM_CONFIG, activebackup or lacp
# note that lacp require changing switch port to lacp as well

TEAM_CONFIG="{\"runner\": {\"name\": \"lacp\"}, \"link_watch\":
{\"name\": \"ethtool\"}}"
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=no
IPV4_FAILURE_FATAL=no
IPV6INIT=no
NAME=team10G
DEVICE=team10G
ONBOOT=yes
DEVICETYPE=Team
IPADDR=192.0.2.2
PREFIX=24
GATEWAY=192.0.2.1
NM_CONTROLLED=yes
MTU=9000
```

6. Erstellen Sie die Team-Interface-Datei für das Management-Team anhand des folgenden Beispiels. In diesem Beispiel heißt das Team team1G. Er befindet sich im Managementnetzwerk, auf dem der Network Teaming activeBackup Runner ausgeführt wird.

Die aktiv/Passiv-Konfiguration wird für Management-Schnittstellen empfohlen, allerdings können Sie auch die aktiv/aktiv-Konfiguration verwenden. Auf den Lamellenschaltern sind keine zusätzlichen Konfigurationen erforderlich. Diese Konfiguration verwendet das "Network Teaming activeBackup Runner".

```
# cat /etc/sysconfig/network-scripts/ifcfg-team1G
# IPADDR= "MIP"
# GATEWAY= "MIP_GATEWAY"
# DNS1= "DNS"
# Pick one TEAM_CONFIG, activebackup or lacp
# note that lacp require changing switch port to lacp as well

TEAM_CONFIG="{\"runner\": {\"name\": \"activebackup\"}, \"link_watch\":
{\"name\": \"ethtool\"}}"
#TEAM_CONFIG="{ \"runner\": {\"name\": \"lacp\", \"active\": true,
\"fast_rate\": true }}"
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=team1G
DEVICE=team1G
ONBOOT=yes
DEVICETYPE=Team
IPADDR=198.51.100.2
PREFIX=24
GATEWAY=198.51.100.1
DNS1=198.51.100.250
NM_CONTROLLED=yes
```

7. Bearbeiten Sie das `/etc/iproute2/rt_tables` Datei zum Aktivieren einer neuen Routing-Tabelle mithilfe des folgenden Beispieles. Diese Datei definiert die Zuordnungen, die anstelle von Indexnummern die Namen der Routing-Tabelle verwenden sollen, um auf eine bestimmte Tabelle zu verweisen. Im folgenden Beispiel kann die neue Speicherroutingtabelle team10G mit ihrem Index (20) oder ihrem Namen (team10G) aufgerufen werden:

```
# cat /etc/iproute2/rt_tables
#
# reserved values
#
255local
254main
253default
0unspec

20   team10G
```

8. Im folgenden Beispiel können Sie Routen zur Routing-Tabelle für den Speicherdatenverkehr hinzufügen. Diese Routing-Tabelle weist auf das Speichernetzwerk als Standard-Gateway hin und muss für iSCSI-Datenverkehr verwendet werden. Im folgenden Beispiel lautet der Name der geteam10G Schnittstelle.

> Sie sollten ersetzen `$storage_network`, `$storage_if_name src`, `$SIP table`, `$routing_table_name`, `$storage_default_gw dev`, `$storage_if_name src`, `$SIP table`, und `$routing_table_name` Mit Ihren eigenen Werten.

```
# cat /etc/sysconfig/network-scripts/route-team10G
$storage_network/24 dev $storage_if_name src $SIP table
$routing_table_name
default via $storage_default_gw dev $storage_if_name src $SIP table \
$routing_table_name
```

9. Fügen Sie Policy-based Routing hinzu, um die neue Routing-Tabelle zu verwenden, die Sie erstellt haben, wenn der Traffic aus dem SIP oder SVIP stammt. Verwenden Sie das folgende Beispiel und ersetzen Sie durch Ihre eigenen Werte:

```
# cat /etc/sysconfig/network-scripts/rule-team10G
from $SIP table
$routing_table_name
```

10. Starten Sie das Netzwerk neu, um alle Änderungen zu übernehmen.

```
# systemctl restart network.service
```

11. Um die richtlinienbasierten Routing-Regeln zu prüfen, führen Sie den aus `ip rule show` Befehl.
12. Um die Routing-Tabelle zu überprüfen, führen Sie den aus `ip route show table` Befehl.

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"

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

Installieren Sie SolidFire ESDS mit Ansible

Sie können SolidFire ESDS mit einem Automatisierungs-Tool wie Ansible installieren. Wenn Sie mit Ansible vertraut sind, können Sie ein Ansible-Playbook erstellen, das mehrere Aufgaben umfasst, wie z. B. das Installieren von SolidFire ESDS und das Erstellen eines Clusters.

Was Sie benötigen

- Sie haben Ansible auf Ihrem lokalen Server installiert, indem Sie die Anweisungen befolgen "Hier".
- Sie haben sich mit Ansible-Rollen vertraut gemacht. Siehe "Hier".
- Sie haben alle aufgeführten Vorraussaufgaben ausgeführt "Hier".
- Sie haben eine Compliance-Prüfung für SolidFire ESDS durchgeführt. Anweisungen zum Ausführen der Compliance-Prüfung finden Sie unter "Hier".

Über diese Aufgabe

Verwenden Sie Ansible Vault für sensible Informationen, z. B. Passwörter, anstatt nur Klartext zu verwenden. Weitere Informationen finden Sie unter den folgenden Links:

- "Verwendung Von Ansible Vault"
- "So bauen Sie Ihren Bestand auf"

Sie sollten alle erforderlichen Variablen in Ihrer Bestandsdatei und nicht im Playbook angeben.

Schritte

1. Führen Sie die aus `ansible-galaxy install` Befehl zum Installieren des `nar_solidfire_sds_install` Rolle:

   ```
   ansible-galaxy install git+https://github.com/NetApp-
   Automation/nar_solidfire_sds_install.git
   ```

   Sie können die Rolle auch manuell installieren, indem Sie sie aus dem kopieren "NetApp GitHub Repository" Und die Rolle in das zu setzen `~/.ansible/roles` Verzeichnis. NetApp stellt eine README-Datei zur Verfügung, die Informationen zur Ausführung einer Rolle enthält.

   Stellen Sie sicher, dass Sie immer die neuesten Versionen der Rollen herunterladen.

2. Verschieben Sie die Rollen, die Sie heruntergeladen haben, in einem Verzeichnis, von dem aus sie installiert wurden.

   ```
   $ mv ~/.ansible/roles/ansible/nar_solidfire_sds_* ~/.ansible/roles/
   ```

3. Führen Sie die aus `ansible-galaxy role list` Befehl, um sicherzustellen, dass Ansible für die Verwendung der neuen Rollen konfiguriert ist.

```
$ ansible-galaxy role list
# ~/.ansible/roles
- nar_solidfire_sds_install, (unknown version)
- nar_solidfire_sds_upgrade, (unknown version)
- ansible, (unknown version)
- nar_solidfire_sds_compliance, (unknown version)
- nar_solidfire_cluster_config, (unknown version)
- nar_solidfire_sds_uninstall, (unknown version)
```

Die mit Rollen verknüpfte README-Datei enthält eine Liste aller erforderlichen und optionalen Variablen, die Sie wie unten gezeigt definieren sollten:

Sie sollten diese Variablen in der Bestandsdatei definieren, die Sie im nächsten Schritt erstellen.

4. Erstellen Sie die Bestandsdatei in Ihrem Ansible-Arbeitsverzeichnis.

In der Bestandsdatei sollten Sie alle Hosts (Knoten) einschließen, auf denen Sie SolidFire ESDS installieren möchten. Mit der Bestandsdatei kann das Playbook (das Sie im nächsten Schritt erstellen) mehrere Hosts mit einem einzigen Befehl verwalten. Außerdem sollten Sie Variablen wie Benutzername und Passwort für Ihre Storage Nodes, Namen der Managementoberfläche und der Storage-Schnittstelle usw. definieren.

Achten Sie darauf, dass Sie diese Richtlinien für die Bestandsdatei befolgen: **Verwenden Sie die richtigen Schreibweisen für Gerätenamen.** Verwenden Sie die korrekte Formatierung in der Datei. **Stellen Sie sicher, dass es nur ein Cache-Gerät gibt.** Verwenden Sie eine Liste zur Angabe von Storage_Devices.

In den hier angegebenen Beispielen sind die Namen der Storage- und Managementoberfläche für HPE-Server angegeben. Wenn Sie einen Dell-Server haben, lautet der Name des Cache-Geräts nvme1n1. Für Dell-Server ist mgmt_iface team1G und Storage_iface team10G.

Unten ist eine Beispieldatei für den Bestand dargestellt. Es umfasst vier Storage-Nodes. Ersetzen Sie in diesem Beispiel **Speicherknoten MIP** durch die MIP-Adressen für Ihre Speicherknoten und ersetzen Sie *

Mit Benutzername und Passwort für Ihre Speicherknoten.

```
all:
    hosts:
        storage node MIP:
        storage node MIP:
        storage node MIP:
        storage node MIP:
    vars:
        ansible_connection: ssh
        ansible_ssh_common_args: -o StrictHostKeyChecking=no
        ansible_user: *****
        ansible_ssh_pass: *****
        solidfire_element_rpm: http://sf-
artifactory.solidfire.net/artifactory/crux/solidfire-element-**.*.*.***-
*.***.x86_64.rpm
        mgmt_iface: "team0"
        storage_iface: "team1"
        storage_devices:
          - "/dev/nvme0n1"
          - "/dev/nvme1n1"
          - "/dev/nvme2n1"
          - "/dev/nvme3n1"
          - "/dev/nvme4n1"
          - "/dev/nvme5n1"
          - "/dev/nvme6n1"
          - "/dev/nvme7n1"
          - "/dev/nvme8n1"
        cache_devices:
          - "/dev/nvme9n1"
```

5. Anpingen der Hosts (Nodes), die Sie in der Bestandsdatei definiert haben, um zu überprüfen, ob Ansible mit ihnen kommunizieren kann.
6. Laden Sie die Red hat Package Manager (RPM)-Datei in das Dateiverzeichnis auf einem lokalen Webserver herunter, auf den der Server mit Ansible und den Speicherknoten zugreifen kann.
7. Erstellen des Ansible-Playbook Wenn Sie bereits über ein Playbook verfügen, können Sie es bearbeiten. Sie können die Beispiele in der von NetApp zur Verfügung gegebenen README-Datei verwenden.
8. Installieren Sie SolidFire ESDS, indem Sie das Playbook ausführen, das Sie im vorherigen Schritt erstellt haben:

```
$ ansible-playbook -i inventory.yaml sample_playbook.yaml
```

Ersetzen Sie **sample_Playbook.yaml** mit dem Namen Ihres Playbooks und **Inventory.yaml** mit dem Namen Ihrer Bestandsdatei. Durch Ausführen des Playbook wird der erstellt `sf_sds_config.yaml` Datei auf jedem Knoten, der in Ihrer Bestandsdatei aufgeführt ist. Er installiert außerdem den SolidFire-Service

auf jedem Storage Node und startet ihn. Finden Sie weitere Informationen zu `sf_sds_config.yaml`, Siehe "Hier".

9. Überprüfen Sie die Ansible-Ausgabe in der Konsole, um sicherzustellen, dass der SolidFire-Service auf jedem Node gestartet wurde.

   Es folgt ein Beispiel für die Ausgabe:

```
TASK [nar_solidfire_sds_install : Ensure the SolidFire eSDS service is
started]
**********************************************************************
*********************

changed: [10.61.68.52]

changed: [10.61.68.54]

changed: [10.61.68.51]

changed: [10.61.68.53]



PLAY RECAP
**********************************************************************
**********************************************************************
******************

10.61.68.51                : ok=12   changed=3    unreachable=0
failed=0    skipped=10   rescued=0    ignored=0

10.61.68.52                : ok=12   changed=3    unreachable=0
failed=0    skipped=10   rescued=0    ignored=0

10.61.68.53                : ok=12   changed=3    unreachable=0
failed=0    skipped=10   rescued=0    ignored=0

10.61.68.54                : ok=12   changed=3    unreachable=0
failed=0    skipped=10   rescued=0    ignored=0
```

10. Um zu überprüfen, ob der SolidFire-Service richtig gestartet wurde, führen Sie das aus `systemctl status solidfire` Befehl und Prüfung auf `Active:active (exited)` … In der Ausgabe.

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Ausführung von Aufgaben nach der Installation

Konfigurieren Sie nach der Installation von SolidFire ESDS den Clusternamen auf jedem SolidFire ESDS-Knoten. Anschließend können Sie einen SolidFire ESDS-Cluster erstellen.

Über diese Aufgabe

Hier finden Sie einen Überblick über die Aufgaben, die Sie nach der Installation von SolidFire ESDS ausführen sollten:

- Konfigurieren Sie den Cluster-Namen
- Legen Sie den Lizenzschlüssel fest
- Erstellen eines Clusters
- Fügen Sie dem Cluster Laufwerke hinzu

> Sie können den Link:https://github.com/NetApp-Automation/nar_solidfire_cluster_config verwenden[`nar_solidfire_cluster_config`^] Ansible-Rolle von NetApp zur Durchführung der Schritte nach der Installation Wenn Sie es manuell ausführen möchten, lesen Sie die unten beschriebenen Schritte.

Konfigurieren Sie den Cluster-Namen

Sie sollten den Cluster-Namen auf jedem SolidFire ESDS-Knoten konfigurieren, bevor Sie den Node zu einem Cluster hinzufügen können. Dazu ist entweder die UI pro Node oder die Element API erforderlich.

> Sie können den Cluster-Namen nicht ändern, nachdem das Cluster erstellt wurde.

Schritte

1. Wählen Sie eine der folgenden Optionen:
   - Verwenden Sie die UI pro Node:
     i. Öffnen Sie die Management-Node-UI pro Node: `https://<node_mip>:442`.
     ii. Wählen Sie **Cluster-Einstellungen** und geben Sie den Cluster-Namen ein.
     iii. Wählen Sie **Änderungen Anwenden**.
   - Verwenden Sie den Link:./API/reference_element_api_setclusterconfig.html[`SetClusterConfig`^] API-Methode.

     Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`cluster`	Konfigurationsattribute, die während dieses Methodenaufrufs geändert werden sollten. Nur die Felder, die geändert werden sollen, müssen dieser Methode als Mitglieder in diesem Parameter hinzugefügt werden.	Cluster	Keine	Nein

Das folgende Anforderungsbeispiel ist verfügbar:

```
{
   "method": "SetClusterConfig",
   "params": {
      "cluster": {
         "name": "myhost",
         "mipi": "Bond10G"
      },
    "id" : 1
   }
}
```

Legen Sie den Lizenzschlüssel fest

Wenn Sie einen SolidFire ESDS-Cluster erstellen, benötigen Sie die Lizenzschlüsselinformationen. Der NetApp Support benötigt außerdem die Lizenzschlüsselinformationen, die bei der Problembehebung helfen. Der Lizenzschlüssel für den SolidFire ESDS-Cluster besteht aus der Bestellnummer des Clusters kombiniert mit der Seriennummer und aktiviert das von Ihnen erworbene Kapazitätszeitlizenzmodell.

Über diese Aufgabe

Sie können das verwenden `SetLicenseKey` Methode zum Festlegen des Lizenzschlüssels für den SolidFire ESDS-Speicher-Cluster. Der `SetLicenseKey` Die Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`orderNumber`	Die neue Bestellnummer für diesen Storage Cluster.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
`serialNumber`	Die neue Seriennummer für diesen Storage-Cluster.	Zeichenfolge	Keine	Ja.

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
`orderNumber`	Die neue Bestellnummer des Storage Clusters.	Zeichenfolge
`serialNumber`	Die neue Seriennummer des Storage-Clusters.	Zeichenfolge

Schritt

1. Verwenden Sie die `SetLicenseKey` API-Methode, wie im folgenden Beispiel dargestellt:

   Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

```
{
  "method": "SetLicenseKey",
  "params": {
    "orderNumber": "33601",
    "serialNumber": "30G56E3WV"   },
   "id" : 1
}
```

   Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
   "result" : {
      "serialNumber": "30G56E3WV",
      "orderNumber": "33601"
     }
   }
}
```

Erstellen eines Clusters

Nachdem Sie den Cluster-Namen auf jedem SolidFire ESDS-Speicherknoten konfiguriert haben, können Sie entweder über die UI pro Node oder die Element-API ein Cluster erstellen.

Die Softwareverschlüsselung im Ruhezustand ist für SolidFire ESDS Cluster standardmäßig aktiviert. Wenn Sie die Standardeinstellung ändern möchten, sollten Sie dies tun, wenn Sie das Cluster mit der erstellen `CreateCluster` API-Methode.

Schritte

1. Wählen Sie eine der folgenden Optionen:

   - Verwenden Sie die UI pro Node:

     i. Öffnen Sie die Management-Node-UI pro Node: `https://<node_mip>:442*`.

     ii. Wählen Sie im linken Navigationsmenü die Option **Cluster erstellen** aus.

     iii. Aktivieren Sie die Kontrollkästchen für die Nodes. Die SolidFire ESDS-Knoten werden als SFc100 angezeigt.

     iv. Geben Sie folgende Informationen ein: Benutzername, Passwort, Management Virtual IP (MVIP)-Adresse, Speicher Virtual IP (SVIP)-Adresse, Software-Bestellnummer und Seriennummer.

     Sie können die MVIP- und SVIP-Adressen nach dem Erstellen des Clusters nicht ändern. Die Verwendung derselben IP-Adressen für MVIP und SVIP wird nicht unterstützt.

     Sie können den anfänglichen Cluster-Administrator-Benutzernamen nicht ändern.

     Wenn Sie die Bestellnummer und Seriennummer nicht angeben, schlägt der Vorgang zum Erstellen des Clusters fehl.

     i. Bestätigen Sie, dass Sie die NetApp Endbenutzer-Lizenzvereinbarung gelesen haben.

     ii. Wählen Sie **Cluster Erstellen**.

     iii. Um zu überprüfen, ob ein Cluster erstellt wurde, melden Sie sich bei dem Cluster an: `http://mvip_ip`.

     iv. Vergewissern Sie sich, dass ClusterName, SVIP, MVIP, Anzahl der Nodes und Elementversion korrekt sind.

   - Verwenden Sie den Link:./API/reference_element_api_createcluster.html[`CreateCluster`^] API-Methode.

     Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`acceptEula`	Geben Sie an, dass Sie die Endnutzer-Lizenzvereinbarung akzeptieren, wenn Sie dieses Cluster erstellen. Um die EULA zu akzeptieren, setzen Sie diesen Parameter auf „true“.	boolesch	Keine	Ja.
`attributes`	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
`enableSoftwareEncryptionAtRest`	Aktivieren Sie diesen Parameter, um eine softwarebasierte Verschlüsselung im Ruhezustand zu verwenden. Standardmäßig auf SolidFire ESDS-Clustern auf „true“ gesetzt. Standardmäßig auf allen anderen Clustern auf false gesetzt.	boolesch	Richtig	Nein
`mvip`	Fließende (virtuelle) IP-Adresse für den Cluster im Managementnetzwerk.	Zeichenfolge	Keine	Ja.
`nodes`	CIP/SIP-Adressen der ersten Knotengruppe, die den Cluster einrichten. Die IP-Adresse dieses Node muss in der Liste enthalten sein.	String-Array	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
`orderNumber`	Alphanumerische Auftragsnummer. Erforderlich für SolidFire ESDS.	Zeichenfolge	Keine	Nein (hardwarebasierte Plattformen) Ja (softwarebasierte Plattformen)
`password`	Anfängliches Passwort für das Cluster-Administratorkonto .	Zeichenfolge	Keine	Ja.
`serialNumber`	Neunstellige alphanumerische Seriennummer. Erforderlich für SolidFire ESDS.	Zeichenfolge	Keine	Nein (hardwarebasierte Plattformen) Ja (softwarebasierte Plattformen)
`svip`	Fließende (virtuelle) IP-Adresse für den Cluster im Storage-Netzwerk (iSCSI).	Zeichenfolge	Keine	Ja.
`username`	Benutzername für den Cluster-Administrator.	Zeichenfolge	Keine	Ja.

Siehe folgende Beispielanforderung:

```
{
  "method": "CreateCluster",
  "params": {
    "acceptEula": true,
    "mvip": "10.0.3.1",
    "svip": "10.0.4.1",
    "repCount": 2,
    "username": "Admin1",
    "password": "9R7ka4rEPa2uREtE",
    "attributes": {
      "clusteraccountnumber": "axdf323456"
    },
    "nodes": [
      "10.0.2.1",
      "10.0.2.2",
      "10.0.2.3",
      "10.0.2.4"
    ]
  },
  "id": 1
}
```

Weitere Informationen zu dieser Methode finden Sie unter Link:API/reference_element_api_createcluster.html[`CreateCluster`^].

Fügen Sie dem Cluster Laufwerke hinzu

Sie sollten Laufwerke zu Ihrem SolidFire ESDS-Cluster hinzufügen, damit sie am Cluster teilnehmen können. Dazu wird entweder die Element UI oder die APIs verwendet.

Schritte

1. Wählen Sie eine der folgenden Optionen:

   - Verwenden Sie die Element-UI:
     i. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke**.
     ii. Wählen Sie **verfügbar**, um die Liste der verfügbaren Laufwerke anzuzeigen.
     iii. Um einzelne Laufwerke hinzuzufügen, wählen Sie das Symbol **Aktionen** für das Laufwerk, das Sie hinzufügen möchten, und wählen Sie dann **Hinzufügen**.
     iv. Um mehrere Laufwerke hinzuzufügen, aktivieren Sie die Kontrollkästchen für die Laufwerke, die hinzugefügt werden sollen, wählen Sie **Massenaktionen** und dann **Hinzufügen** aus.
     v. Vergewissern Sie sich, dass die Laufwerke hinzugefügt werden und die Cluster-Kapazität wie erwartet ist.
   - Verwenden Sie die[`AddDrives`^] API-Methode.

     Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`drives`	Informationen über die einzelnen Laufwerke, die dem Cluster hinzugefügt werden sollen. Mögliche Werte: • DriveID: Die ID des Laufwerks, das hinzugefügt werden soll (Integer). • Typ: Der Typ des hinzufügenden Laufwerks (String). Gültige Werte sind „Slice“, „Block“ oder „Volume“. Wenn keine Angabe erfolgt, weist das System den korrekten Typ zu.	JSON-Objekt-Array	Keine	Ja (Typ ist optional)

Hier ein Beispiel für Anfragen:

```
{
  "id": 1,
  "method": "AddDrives",
  "params": {
    "drives": [
      {
        "driveID": 1,
        "type": "slice"
      },
      {
        "driveID": 2,
        "type": "block"
      },
      {
        "driveID": 3,
        "type": "block"
      }
    ]
  }
}
```

Weitere Informationen zu dieser API-Methode finden Sie unter Link:./API/reference_element_api_adddrives.html[`AddDrives`^].

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Aktualisieren Sie die Cluster

Mit Ansible können Sie ein unterbrechungsfreies Rolling Upgrade auf Ihrem SolidFire ESDS Cluster durchführen. Verwenden der `nar_solidfire_sds_upgrade` Rolle von NetApp, Ansible führt Rolling Upgrades für einen Node gleichzeitig durch, während alle Volumes von der Datenverfügbarkeit profitieren.

Was Sie benötigen

Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind, bevor Sie ein Upgrade durchführen:

- Es gibt keine Cluster-Fehler in der Element UI.
- Die Bestandsdatei ist mit den aktuellen Informationen zu den RPM-Dateiaufbau und Details zu Cluster-Mitgliedsknoten auf dem neuesten Stand.
- Die Hosts werden in der Bestandsdatei unter Verwendung von IP-Adressen definiert (und nicht vollständig qualifizierten Domänennamen [FQDNs]).

Das Upgrade schlägt fehl, wenn Sie die Hosts mithilfe von FQDNs definieren.

- Die Hosts werden in der Bestandsdatei anhand des Formats im folgenden Beispiel definiert:

```
hosts:
  10.117.136.26:
  10.117.136.27:
```

- Die Anzahl der Knoten in Ihrer Bestandsdatei ist identisch mit der Anzahl der Knoten im Cluster, die Sie aktualisieren. Wenn eine Anzahl nicht stimmt, schlägt das Upgrade-Verfahren mit einem Fehler fehl, der dem folgenden Beispiel ähnelt: `"Cluster 10.194.79.151 consists of more nodes than what has been specified for upgrade!"`
- Die Bestandsdatei hat die folgenden Variablen angegeben: sf_mgmt_virt_ip (MVIP), sf_Cluster_admin_username, sf_Cluster_admin_passwd und solidfire_Element_rpm (Pfad zur neuen RPM-Datei).

Upgrade-Übersicht

Hier eine Übersicht über die Ereignisse während des Upgrades:

- Die in der Bestandsdatei eingegebenen Informationen werden validiert.
- Node-Informationen werden erfasst.
- RPM wird auf allen Knoten installiert, die in der Bestandsdatei enthalten sind.
- Nachdem die RPM auf jedem Knoten installiert wurde, wird jeder SolidFire-ESDS-Knoten nacheinander aktualisiert. Jeder Node wird automatisch im Wartungsmodus versetzt. Sie müssen den Wartungsmodus nicht manuell aktivieren, wenn Sie das Upgrade-Playbook ausführen.
- Nachdem der erste Knoten in den Wartungsmodus versetzt wurde, werden die auf diesem SolidFire ESDS-Knoten gehosteten Volumes auf die übrigen ESDS-Knoten des SolidFire-Knotens im Cluster Failover ausgeführt.
- Der SolidFire-Dienst wird neu gestartet, um die neueste Version der Anwendung abzuholen.
- Für den Node ist der Wartungsmodus deaktiviert, und das Cluster wartet auf die Wiederherstellung des Node.
- Sobald der Node wieder online geschaltet wurde, wird das Cluster ausgeglichen.
- Der gleiche Prozess wird für alle Nodes im Cluster wiederholt.
- Nach dem Upgrade aller Nodes wird im Cluster die aktuelle Version angezeigt.

Wenn während des Upgrades oder des Clusters ein Fehler auftritt, wird das Upgrade nicht angehalten. Sie wird in dem Umfang fortgeführt, in dem sie eine Liste aller Knoten ausdruckt, die erfolgreich und nicht erfolgreich aktualisiert wurden. Nachdem Sie Fehler behoben haben, können Sie das Playbook erneut ausführen oder die Datei ablehnen, um den Upgrade-Prozess abzuschließen.

Wenn das Upgrade aufgrund eines Fehlers fehlschlägt, sollten Sie es beheben und das Upgrade fortsetzen. Das Cluster bleibt bis zum Abschluss des Upgrades im Upgrade-Status. Wenn die Störung nicht durch Element behoben wird, während sich das Cluster im Upgrade-Status befindet, sollten Sie sich an den NetApp Support wenden. Abhängig von der Art der Störung und wenn es sicher ist, dies zu tun, Support kann Sie anweisen, die hinzuzufügen `yes_i_want_to_ignore_cluster_faults` Variable Einstellung für Ihr Upgrade-Playbook und Re-Ausführen von Playbook auf „true“. Versuchen Sie dies nicht ohne Beratung mit dem Support.

Schritte

1. Führen Sie die aus `ansible-galaxy install` Befehl zum Installieren des `nar_solidfire_sds_upgrade` Rolle:

```
ansible-galaxy install git+https://github.com/NetApp-
Automation/nar_solidfire_sds_upgrade.git
```

Sie können die Rolle auch manuell installieren, indem Sie sie aus dem kopieren "NetApp GitHub Repository" Und die Rolle in das zu setzen `~/.ansible/roles` Verzeichnis. NetApp stellt eine README-Datei zur Verfügung, die Informationen zur Ausführung einer Rolle enthält.

Stellen Sie sicher, dass Sie immer die neuesten Versionen der Rollen herunterladen.

2. Verschieben Sie die Rollen, die Sie heruntergeladen haben, in einem Verzeichnis, von dem aus sie installiert wurden.

```
$ mv ~/.ansible/roles/ansible/nar_solidfire_sds_* ~/.ansible/roles/
```

3. Führen Sie den ansible-Galaxie-Rollenlistenbefehl aus, um sicherzustellen, dass Ansible für die Verwendung der neuen Rollen konfiguriert ist.

```
$ ansible-galaxy role list
# ~/.ansible/roles
- nar_solidfire_sds_install, (unknown version)
- nar_solidfire_sds_upgrade, (unknown version)
- ansible, (unknown version)
- nar_solidfire_sds_compliance, (unknown version)
- nar_solidfire_cluster_config, (unknown version)
- nar_solidfire_sds_uninstall, (unknown version)
```

4. Erstellen Sie das Playbook für Upgrades. Wenn Sie bereits über ein Playbook verfügen und dieses verwenden möchten, müssen Sie sicherstellen, dass Sie das angeben `nar_solidfire_sds_upgrade` Rolle in diesem Playbook.
5. Führen Sie das Playbook aus:

```
$ ansible-playbook -i inventory.yaml playbook_upgrade_sample.yaml
```

Der hier verwendete Playbook-Name ist ein Beispiel. Sie sollten es durch den Namen Ihres Playbooks ersetzen.

Durch Ausführen des Playbooks werden die in der Bestandsdatei eingegebenen Informationen validiert und die RPM wird auf allen im Bestand aufgeführten Nodes installiert. Sie können die Ansible-Ausgabe überprüfen, um sicherzustellen, dass jeder Node aktualisiert wird.

6. Überprüfen Sie nach Abschluss des Upgrades jeden Node, um sicherzustellen, dass die neue Version über die Element UI oder die Cluster-API ausgeführt wird.

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Monitoring der Cluster

Sie können die Performance Ihrer SolidFire ESDS Cluster überwachen und den Bestand über die Benutzeroberfläche von NetApp Hybrid Cloud Control anzeigen. Sie können auch Protokolle zur Fehlerbehebung über die Benutzeroberfläche von NetApp Hybrid Cloud Control erfassen.

Die folgenden Links führen zu den Informationen zum Monitoring Ihrer Cluster in der Benutzeroberfläche von NetApp Hybrid Cloud Control:

- "Zeigen Sie Ihren Bestand auf der Seite Knoten an"
- "Überwachung von Volumes auf Ihrem Storage-Cluster"

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

SolidFire ESDS-Speicher managen

Nach der Installation von SolidFire ESDS in Ihren Storage Clustern können Sie die Storage-Cluster über Element UI, Element APIs oder das NetApp Element Plug-in für vCenter Server verwalten.

Im Folgenden finden Sie die Links zu Inhalten für verschiedene Storage-Management-Aufgaben:

- "Verwenden Sie grundlegende Optionen in der UI für Element Software"
- "Arbeiten Sie mit Konten, die CHAP verwenden"
- "Arbeiten mit Volumes"

Außerdem können Sie hier Informationen über das Anwenden einer QoS-Richtlinie auf Volumes abrufen.

- "Arbeiten mit virtuellen Volumes"
- "Arbeiten Sie mit Volume-Zugriffsgruppen und -Initiatoren"
- "Arbeiten Sie mit Snapshots"
- "Erste Schritte mit externem Verschlüsselungsmanagement" *NEU!*
- "Externes Verschlüsselungsmanagement einrichten" *NEU!*
- "Remote-Replizierung zwischen Clustern"
- "Backup und Restore von Volumes"
- "Storage-Management mit Element APIs"
- "Fehler im System beheben"
- "Übersicht über das NetApp Element Plug-in für vCenter Server"

Über die Übersichtsseite können Sie zu bestimmten Aufgaben navigieren.

Element-APIs auf SolidFire ESDS-Clustern verwenden

- **Software-Verschlüsselung im Ruhezustand Verbesserungen**: Bei der Erstellung eines SolidFire Enterprise SDS Storage-Clusters standardmäßig aktivierte Erweiterungen für die Softwareverschlüsselung im Ruhezustand wurden mit Element 12.3 eingeführt. Diese Funktion verschlüsselt alle auf den SSDs gespeicherten Daten in den Storage-Nodes und verursacht nur eine sehr geringe Beeinträchtigung der Client-I/O (~2 %) auf die Performance. Die folgenden Element-API-Methoden beziehen sich auf die Softwareverschlüsselung im Ruhezustand (siehe "Dokumentation der Element API" Weitere Informationen zu den einzelnen Methoden):
  - `CreateCluster`
  - `DisableEncryptionAtRest`
  - `EnableEncryptionAtRest`
  - `GetSoftwareEncryptionAtRestInfo`
  - `RekeySoftwareEncryptionAtRestMasterKey`
- **Fähigkeit, eine maximale Anzahl von Snapshots zu definieren**: Mit Element 12.3 wurden Verbesserungen der Funktion zur Snapshot-Aufbewahrung eingeführt. Die folgenden APIs wurden geändert, um diese Erweiterung zu unterstützen (siehe "Dokumentation der Element API" Weitere Informationen zu den einzelnen Methoden):
  - `CreateVolume`
  - `ModifyVolume`
  - `CreateSnapshot`
  - `CreateSchedule`
  - `ModifyGroupSnapshot`
  - `ModifySchedule`
  - `ModifySnapshot`
  - `CreateGroupSnapshot`

- **Informationen zu Element Software Patches**: Der `GetPatchInfo` Die in Element 12.3 eingeführte Methode liefert Informationen über auf einem Storage-Node installierte Element Software-Patches. Siehe "Dokumentation der Element API" Entsprechende Details.
- **Statistiken für jede Netzwerkschnittstelle auf einem Knoten**: Der `ListNetworkInterfaceStats` Mit der in Element 12.3 eingeführten Methode können Sie Statistiken auflisten, wie z. B. die Anzahl der heruntergelassenen Pakete und verschiedene Arten von Fehlern für jede Netzwerkschnittstelle auf einem Knoten. Diese API-Methode ist für die Verwendung auf einzelnen Nodes gedacht. Für den Zugriff auf einzelne Nodes ist eine Benutzer-ID und Passwort-Authentifizierung erforderlich. Sie können diese Methode jedoch im Cluster verwenden, wenn der Parameter Force im Methodenaufruf den Wert „true“ angegeben hat. Wenn der Parameter auf dem Cluster verwendet wird, werden die Netzwerkstatistiken für alle Schnittstellen aufgeführt. Siehe "Dokumentation der Element API" Entsprechende Details.
- **APIs eingeführt und aktualisiert in Element 12.2 zur Unterstützung von SolidFire ESDS**: In Element 12.2 wurden mehrere neue APIs eingeführt, die Sie auf SolidFire ESDS Clustern verwenden können.

Hier finden Sie eine Liste der neuen APIs in Element 12.2:

- Link:../API/reference_element_api_getlicensekey.html[`GetLicenseKey`^]
- Link:../API/reference_element_api_setlicensekey.html[`SetLicenseKey`^]
- Link:../API/reference_element_api_enablemaintenancemode.html[`EnableMaintenanceMode`^]
- Link:../API/reference_element_api_disablemaintenancemode.html[`DisableMaintenanceMode`^]

Die folgenden 12.2 APIs wurden aktualisiert, um SolidFire ESDS-Cluster zu unterstützen:

- Link:../API/reference_element_api_addnodes.html[`AddNodes`^]
- Link:../API/reference_element_api_createcluster.html[`CreateCluster`^]

> Neue Parameter, `OrderNumber`, `SerialNumber`, und `enableSoftwareEncryptionAtRest` Wurden der hinzugefügt `CreateCluster` Methode in Element Software 12.2. Sie sollten diese Parameter angeben, während Sie diese API-Methode zum Erstellen eines Clusters verwenden, nachdem Sie SolidFire ESDS installiert haben.

- **Element 12.2 APIs nicht unterstützt auf SolidFire ESDS Clustern**: Hier ist eine Liste von Element 12.2 APIs, die auf SolidFire ESDS Clustern nicht unterstützt werden:
- `ListClusterInterfacePreferences`
- `ListNodeStats`
- `DisableSsh`
- `DisableClusterSsh`
- `EnableClusterSsh`
- `EnableSsh`
- `GetIpmiConfig`
- `GetIpmiInfo`
- `GetSshInfo`
- `ListNetworkInterfaces`

- `ResetNode`
- `RestartNetworking`
- `ResetNetworkConfig`
- `SetConfig`
- `SetNetworkConfig`
- `DisableBmcColdReset`
- `EnableBmcColdReset`
- `SetNtpInfo`
- `TestAddressAvailability`

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Deinstallieren Sie SolidFire ESDS auf dem Knoten

Sie können einen Knoten, auf dem Sie SolidFire ESDS installiert haben, durch Entfernen von SolidFire ESDS auf dem Knoten * zurücksetzen. Zum Reaktivieren von SolidFire ESDS auf dem Knoten sollten Sie alle Installationsschritte durchführen.

Sie können den Link:https://github.com/NetApp-Automation/nar_solidfire_sds_uninstall verwenden[`nar_solidfire_sds_uninstall`^] Ansible-Rolle von NetApp zur Durchführung des Vorgangs Wenn Sie SolidFire ESDS auf dem Knoten manuell entfernen möchten, lesen Sie die folgenden Schritte.

Schritte

1. Entfernen Sie Laufwerke aus dem Cluster mithilfe der Element-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.

2. Entfernen Sie den Knoten mithilfe der Element-UI oder der aus dem Cluster[`RemoveNodes`^] API-Methode.
3. Verwenden Sie SSH, um eine Verbindung zum Node herzustellen, der aus dem Cluster entfernt wird.
4. Entfernen Sie SolidFire ESDS wie folgt aus dem Knoten:

   ```
   yum remove solidfire-element
   ```

5. Entfernen Sie persistente Daten aus dem Verzeichnis wie folgt:

```
rm -rf /opt/sf
```

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

ESDS von SolidFire warten

Informationen über die Verwendung des Wartungsmodus und den Austausch der Laufwerke in den ESDS-Clustern von SolidFire finden Sie.

- "Holen Sie sich den Lizenzschlüssel"
- "Verwenden Sie den Wartungsmodus auf SolidFire ESDS Clustern"
- "Ersetzen Sie Laufwerke für HPE DL380"
- "Ersetzen Sie Laufwerke für HPE DL360"
- "Ersetzen Sie die Laufwerke für Dell R640"
- "Sammelt Containerprotokolle"
- "Links zu KB-Artikeln zur Fehlerbehebung"
- "Inhalt der datei sf_sds_config.yaml"

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Holen Sie sich den Lizenzschlüssel

Die Lizenzschlüsselinformationen für den SolidFire ESDS-Cluster sollten bereitgestellt werden, bevor Sie sich bei der Behebung von Problemen an den NetApp Support wenden. Der Lizenzschlüssel für den SolidFire ESDS-Cluster besteht aus der Bestellnummer des Clusters kombiniert mit der Seriennummer.

Sie können das verwenden `GetLicenseKey` Methode zum Abrufen der Lizenzschlüsselinformationen für den SolidFire ESDS-Speicher-Cluster. Der `GetLicenseKey` Methode hat keine Eingabeparameter. Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
`orderNumber`	Die neue Bestellnummer des Storage Clusters.	Zeichenfolge
`serialNumber`	Die neue Seriennummer des Storage-Clusters.	Zeichenfolge

Schritt

1. Führen Sie die aus `GetLicenseKey` API-Methode, wie im folgenden Beispiel dargestellt:

   Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

   ```
   {
      "method": "GetLicenseKey",
      "params": {
      },
      "id": 1
   }
   ```

   Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

   ```
   {
      "id" : 1,
      "result" : {
         "serialNumber": "30G56E3WV",
         "orderNumber": "33601"
        }
      }
   }
   ```

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Verwenden Sie den Wartungsmodus auf SolidFire ESDS Clustern

Wenn Sie einen Storage Node für Wartungsarbeiten, wie z. B. Software-Upgrades oder Host-Reparaturen, offline schalten müssen, können Sie die Auswirkungen auf den Rest des Storage-Clusters durch Aktivierung des Wartungsmodus für diesen Node auf ein Minimum minimieren.

Wenn Sie den aktuellen Status des Wartungsmodus auf Ihrem Knoten überprüfen möchten, verwenden Sie den Link:./API/reference_element_api_listactivenodes.html[`ListActiveNodes`^] API-Methode. Das Node-Objekt enthält eine `maintenanceMode` Parameter, der den aktuellen Status des Wartungsmodus auf dem Node angibt.

Stellen Sie sicher, dass Sie die Wartung durchführen, sobald der Wartungsmodus aktiviert ist. Verlassen Sie den Node nicht mehr als erforderlich im Wartungsmodus.

Sie können einen Storage Node nur in den Wartungsmodus versetzen, wenn der Node ordnungsgemäß ist (keine Blockierung von Cluster-Fehlern) und das Storage Cluster einem Ausfall einzelner Nodes gegenüber

tolerant ist. Nachdem Sie den Wartungsmodus für einen gesunden und toleranten Node aktiviert haben, wird der Node nicht sofort migriert. Er wird überwacht, bis die folgenden Bedingungen erfüllt sind:

- Alle auf dem Node gehosteten Volumes haben einen Failover durchgeführt, und der Node hostet für jedes Volume nicht mehr als primärer Volume.
- Jedem Failover eines Volumes wird ein temporärer Standby-Node zugewiesen.

Nachdem diese Kriterien erfüllt sind, wird der Node in den Wartungsmodus versetzt. Wenn diese Kriterien innerhalb von fünf Minuten nicht erfüllt werden, wechselt der Node in den Wartungsmodus.

Wenn Sie den Wartungsmodus für einen Storage-Node deaktivieren, wird der Node überwacht, bis die folgenden Bedingungen erfüllt sind:

- Alle Daten werden vollständig zum Node repliziert.
- Alle blockierenden Cluster-Fehler werden behoben.
- Alle temporären Standby-Node-Zuweisungen für die auf dem Node gehosteten Volumes wurden deaktiviert.

Nachdem diese Kriterien erfüllt sind, wird der Node aus dem Wartungsmodus migriert. Wenn diese Kriterien nicht innerhalb einer Stunde erfüllt werden, kann der Node nicht in den Wartungsmodus wechseln.

Mögliche Szenarien bei Verwendung des Wartungsmodus

- Wenn sich ein Node im Wartungsmodus befindet, ihn jedoch noch nicht neu gebootet wurde und/oder keine Wartung durchgeführt wurde oder Wartungsarbeiten durchgeführt wurden, und der Node wieder verfügbar ist und sich in einem ordnungsgemäßen Zustand befindet, der Wartungsmodus nicht deaktiviert ist, Und ein weiterer Node ausfällt. Der Wartungsmodus auf dem ersten Node wird automatisch deaktiviert.
- Wenn sich einer der Nodes im Wartungsmodus befindet und ein anderer Node gleichzeitig ausfällt, kommt es zu einem Ausfall. Sie müssen warten, bis der Node im Wartungsmodus wieder online geschaltet wird.
- Wenn Sie einen Knoten, der ein Mitglied eines Ensembles ist, für einen langen Zeitraum in den Wartungsmodus versetzen, wird das System ihn automatisch aus dem Ensemble entfernen, wenn andere Knoten an seiner Stelle hinzugefügt werden können.

Aktivieren Sie den Wartungsmodus

Sie können den Wartungsmodus mit aktivieren `EnableMaintenanceMode` API-Methode. Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`forceWithUnresolvedFaults`	Aktivierung des Wartungsmodus für diesen Node erzwingen, selbst wenn Cluster-Fehler blockiert sind.	boolesch	Falsch	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
`nodes`	Die Liste der Node-IDs, die in den Wartungsmodus versetzt werden sollen. Es wird nur jeweils ein Node unterstützt.	Integer-Array	Keine	Ja.
`perMinutePrimarySwapLimit`	Die Anzahl der primären Schichten, die pro Minute ausgetauscht werden sollen. Wenn nicht angegeben, werden alle primären Schichten gleichzeitig ausgetauscht.	Ganzzahl	Keine	Nein
`timeout`	Gibt an, wie lange der Wartungsmodus aktiviert bleiben soll, bevor er automatisch deaktiviert wird. Formatiert als Zeitzeichenfolge (z. B. HH:mm:ss). Wenn nicht angegeben, bleibt der Wartungsmodus aktiviert, bis er explizit deaktiviert ist.	Zeichenfolge	Keine	Nein

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
`asyncHandle`	Sie können das verwenden `GetAsyncResult` Nutzen Sie diese Methode, um diese Async zu abrufen und zu bestimmen, wann die Transition des Wartungsmodus abgeschlossen ist.	Ganzzahl

Name	Beschreibung	Typ
`currentMode`	Der aktuelle Status des Wartungsmodus des Node. Mögliche Werte: • Deaktiviert: Es wurde keine Wartung angefordert. • FailedToRecover: Der Knoten konnte nicht aus dem Wartungsmodus wiederherstellen. • RecoveringFromMaintenance: Der Knoten wird gerade vom Wartungsmodus wiederhergestellt. • VorbereitungForMaintenance: Es werden Maßnahmen ergriffen, um einen Knoten vorzubereiten, der gewartet werden soll. • ReadyForMaintenance: Der Knoten ist zur Durchführung der Wartung bereit.	Wartungsmodus (String)
`requestedMode`	Der angeforderte Wartungsmodus des Node. Mögliche Werte: • Deaktiviert: Es wurde keine Wartung angefordert. • FailedToRecover: Der Knoten konnte nicht aus dem Wartungsmodus wiederherstellen. • RecoveringFromMaintenance: Der Knoten wird gerade vom Wartungsmodus wiederhergestellt. • VorbereitungForMaintenance: Es werden Maßnahmen ergriffen, um einen Knoten vorzubereiten, der gewartet werden soll. • ReadyForMaintenance: Der Knoten ist zur Durchführung der Wartung bereit.	Wartungsmodus (String)

Deaktivieren des Wartungsmodus

Sie können den Wartungsmodus mit deaktivieren `DisableMaintenanceMode` API-Methode. Diese Methode verfügt über den folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
`nodes`	Liste der Storage-Node-IDs, die den Wartungsmodus nicht verlassen sollen	Integer-Array	Keine	Ja.

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
`asyncHandle`	Sie können das verwenden `GetAsyncResult` Nutzen Sie diese Methode, um diese Async zu abrufen und zu bestimmen, wann die Transition des Wartungsmodus abgeschlossen ist.	Ganzzahl
`currentMode`	Der aktuelle Status des Wartungsmodus des Node. Mögliche Werte: • Deaktiviert: Es wurde keine Wartung angefordert. • FailedToRecover: Der Knoten konnte nicht aus dem Wartungsmodus wiederherstellen. • Unerwartete: Der Node wurde offline gefunden, war aber im deaktivierten Modus. • RecoveringFromMaintenance: Der Knoten wird gerade vom Wartungsmodus wiederhergestellt. • VorbereitungForMaintenance: Es werden Maßnahmen ergriffen, um einen Knoten vorzubereiten, der gewartet werden soll. • ReadyForMaintenance: Der Knoten ist zur Durchführung der Wartung bereit.	Wartungsmodus (String)

Name	Beschreibung	Typ
`requestedMode`	Der angeforderte Wartungsmodus des Node. Mögliche Werte: • Deaktiviert: Es wurde keine Wartung angefordert. • FailedToRecover: Der Knoten konnte nicht aus dem Wartungsmodus wiederherstellen. • Unerwartete: Der Node wurde offline gefunden, war aber im deaktivierten Modus. • RecoveringFromMaintenance: Der Knoten wird gerade vom Wartungsmodus wiederhergestellt. • VorbereitungForMaintenance: Es werden Maßnahmen ergriffen, um einen Knoten vorzubereiten, der gewartet werden soll. • ReadyForMaintenance: Der Knoten ist zur Durchführung der Wartung bereit.	Wartungsmodus (String)

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Ersetzen Sie Laufwerke für HPE DL380

Wählen Sie aus den hier aufgeführten Verfahren, um ein Laufwerk proaktiv zu ersetzen, ein Laufwerk nach dem Ausfall zu ersetzen und ein Cache-Laufwerk zu ersetzen. Ein Metadatenlaufwerk oder ein Blocklaufwerk im SolidFire ESDS-Cluster ersetzen. Auf der Seite Element UI **Cluster > Laufwerke** werden die Informationen zum Laufwerksverschleiß angezeigt.

- Ersetzen Sie ein Laufwerk proaktiv
- Tauschen Sie ein fehlerhaftes Laufwerk aus
- Ersetzen Sie ein Cache-Laufwerk

Ersetzen Sie ein Laufwerk proaktiv

Führen Sie dieses Verfahren durch, wenn Sie ein Metadatenlaufwerk oder ein Blocklaufwerk im SolidFire ESDS-Cluster proaktiv ersetzen möchten. Auf der Seite Element UI **Cluster** > **Drives** werden die

Informationen zum Laufwerksverschleiß angezeigt.

Was Sie benötigen

- Stellen Sie über die NetApp Element Software-UI sicher, dass der Cluster in einem guten Zustand ist und es keine Warnungen oder Cluster-Fehler gibt. Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.
- Stellen Sie sicher, dass auf dem Cluster keine aktiven Jobs ausgeführt werden.
- Stellen Sie sicher, dass Sie sich mit allen Schritten vertraut gemacht haben.
- Stellen Sie sicher, dass Sie die erforderlichen Vorsichtsmaßnahmen treffen, um elektrostatische Entladung (ESD) beim Umgang mit Laufwerken zu verhindern.

Schritte

1. Führen Sie die folgenden Schritte in der Element UI aus:
   a. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke** > **aktiv**.
   b. Wählen Sie das Laufwerk aus, das Sie ersetzen möchten.
   c. Notieren Sie sich die Seriennummer des Laufwerks. Dies hilft Ihnen dabei, die entsprechende BayID in der IPMI-Schnittstelle des Knotens zu finden (in diesem Fall HPE Integrated Lights-Out oder iLO).
   d. Wählen Sie **Massenaktionen** > **Entfernen**. Nachdem Sie das Laufwerk entfernt haben, wechselt das Laufwerk in den Zustand **Entfernen**. Er bleibt eine Weile im Status **Entfernen** und wartet darauf, dass die Daten auf dem Laufwerk synchronisiert oder auf die übrigen Laufwerke im Cluster verteilt werden. Nach dem Entfernen des Laufwerks wechselt das Laufwerk in den Status **verfügbar**.
2. Gehen Sie wie folgt vor, um den Laufwerkschacht des zu ersetzenden Laufwerks zu finden:
   a. Melden Sie sich bei der IPMI-Schnittstelle des Knotens an (in diesem Fall iLO).
   b. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.
   c. Ordnen Sie die Seriennummer, die Sie im vorherigen Schritt angegeben haben, mit dem überein, was auf dem Bildschirm angezeigt wird.
   d. Suchen Sie nach der Steckplatznummer, die mit der Seriennummer aufgeführt ist. Dies ist der physische Steckplatz, aus dem Sie das Laufwerk entfernen müssen.
3. Nachdem Sie das Laufwerk identifiziert haben, entfernen Sie es nun physisch wie folgt:
   a. Identifizieren Sie die Antriebsbox.

      Das folgende Bild zeigt die Vorderseite des Servers mit den Laufwerken:

   b. Drücken Sie den Netzschalter des Laufwerks, das Sie ersetzen möchten. Die LED blinkt 5-10 Sekunden lang und stoppt.
   c. Nachdem die LED nicht mehr blinkt und das Laufwerk ausgeschaltet ist, entfernen Sie es vom Server, indem Sie die rote Taste drücken und die Verriegelung ziehen.

Stellen Sie sicher, dass Sie Laufwerke sehr sorgfältig behandeln.

Nachdem Sie das Laufwerk physisch entfernt haben, ändert sich der Laufwerkszustand in der Element-UI in **failed**.

4. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke** > **fehlgeschlagen**.
5. Wählen Sie das Symbol unter **Aktionen** und dann **Entfernen** aus.

   Jetzt können Sie das neue Laufwerk im Knoten installieren.

6. Notieren Sie sich die Seriennummer des neuen Laufwerks.
7. Setzen Sie das Ersatzlaufwerk ein, indem Sie das Laufwerk vorsichtig mit der Verriegelung in den Schacht schieben und die Verriegelung schließen. Das Laufwerk wird eingeschaltet, wenn es richtig eingesetzt wird.
8. Führen Sie die folgenden Schritte durch, um die neuen Laufwerkdetails in iLO zu überprüfen:
   a. Melden Sie sich bei iLO an.
   b. Wählen Sie **Information** > **Integriertes Management-Protokoll**. Sie sehen ein Ereignis, das für das hinzugefügte Laufwerk protokolliert ist.
   c. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.
   d. Blättern Sie, bis Sie Informationen über den Schacht finden, in dem Sie das Laufwerk ersetzt haben.
   e. Überprüfen Sie, ob die Seriennummer auf dem Bildschirm mit der Seriennummer des neuen Laufwerks übereinstimmt, das Sie ersetzt haben.
9. Fügen Sie die neuen Laufwerksinformationen in das hinzu `sf_sds_config.yaml` Datei für den Knoten, in dem Sie das Laufwerk ersetzt haben.

   Der `sf_sds_config.yaml` Datei wird in gespeichert `/opt/sf/`. Diese Datei enthält alle Informationen über die Laufwerke im Node. Jedes Mal, wenn Sie ein Laufwerk ersetzen, müssen Sie die Ersatzlaufwerk-Informationen in dieser Datei eingeben. Weitere Informationen zu dieser Datei finden Sie unter "Inhalt der datei sf_sds_config.yaml".

   a. Stellen Sie mit PuTTY eine SSH-Verbindung zum Knoten her.
   b. Geben Sie im Fenster PuTTY-Konfiguration den Knoten MIP im Feld **Hostname (oder IP-Adresse)** ein.
   c. Wählen Sie **Offen**.
   d. Melden Sie sich im sich öffnenden Terminalfenster mit Ihrem Benutzernamen und Passwort an.
   e. Führen Sie die aus `# cat /opt/sf/sf_sds_config.yaml` Befehl zum Auflisten des Inhalts der Datei.
   f. Ersetzen Sie die Einträge im `dataDevices` Oder `cacheDevices` Listen für das Laufwerk, das Sie durch die neuen Laufwerksinformationen ersetzt haben.
   g. Laufen `# systemctl start solidfire-update-drives`.

      Nach der Ausführung dieses Befehls wird die Bash-Eingabeaufforderung angezeigt. Danach sollten Sie zur Element UI wechseln, um das Laufwerk zum Cluster hinzuzufügen. Die Element-UI zeigt eine Warnmeldung für ein neues Laufwerk an, das verfügbar ist.

10. Wählen Sie **Cluster** > **Laufwerke** > **Verfügbar**.

Sie sehen die Seriennummer des neuen Laufwerks, das Sie installiert haben.

11. Wählen Sie das Symbol unter **Aktionen** und dann **Hinzufügen** aus.
12. Aktualisieren Sie die Element-UI, nachdem der Synchronisationsauftrag für den Block abgeschlossen ist. Sie sehen, dass die Warnung über das verfügbare Laufwerk gelöscht wurde, wenn Sie auf die Seite **ausgeführte Aufgaben** auf der Registerkarte **Reporting** der Element-Benutzeroberfläche zugreifen.

Tauschen Sie ein fehlerhaftes Laufwerk aus

Wenn das SolidFire ESDS-Cluster über ein fehlerhaftes Laufwerk verfügt, zeigt die Element-UI eine Warnmeldung an. Bevor Sie das Laufwerk aus dem Cluster entfernen, überprüfen Sie den Grund für Fehler, indem Sie die Informationen in der IPMI-Schnittstelle für Ihren Node/Server anzeigen. Diese Schritte sind anwendbar, wenn Sie ein Block-Laufwerk oder ein Metadaten-Laufwerk ersetzen.

Was Sie benötigen

- Überprüfen Sie in der NetApp Element-Software-UI, ob das Laufwerk ausgefallen ist. Element zeigt eine Warnmeldung an, wenn ein Laufwerk ausfällt. Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.
- Stellen Sie sicher, dass Sie sich mit allen Schritten vertraut gemacht haben.
- Stellen Sie sicher, dass Sie die erforderlichen Vorsichtsmaßnahmen treffen, um elektrostatische Entladung (ESD) beim Umgang mit Laufwerken zu verhindern.

Schritte

1. Entfernen Sie das ausgefallene Laufwerk mithilfe der Element UI wie folgt aus dem Cluster:
   a. Wählen Sie **Cluster** > **Laufwerke** > **Fehlgeschlagen**.
   b. Notieren Sie den Node-Namen und die Seriennummer des ausgefallenen Laufwerks.
   c. Wählen Sie das Symbol unter **Aktionen** und dann **Entfernen** aus. Wenn Sie Warnungen über den Dienst sehen, der mit dem Laufwerk verbunden ist, warten Sie, bis die bin-Synchronisierung abgeschlossen ist, und entfernen Sie dann das Laufwerk.
2. Führen Sie die folgenden Schritte durch, um den Laufwerkausfall zu überprüfen und die protokollierten Ereignisse anzuzeigen, die mit dem Laufwerksausfall verbunden sind:
   a. Melden Sie sich bei der IPMI-Schnittstelle des Knotens an (in diesem Fall iLO).
   b. Wählen Sie **Information** > **Integriertes Management-Protokoll**. Hier ist der Grund für den Laufwerksausfall (z. B. SSDWOROut) und den Standort aufgeführt. Es wird auch ein Ereignis angezeigt, das den Status des Laufwerks angibt.
   c. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.
   d. Überprüfen Sie die verfügbaren Informationen über das ausgefallene Laufwerk. Der Status des ausgefallenen Laufwerks lautet **degradiert**.
3. Entfernen Sie das Laufwerk wie folgt physisch:

   a. Identifizieren Sie das Laufwerk im Gehäuse.

      Das folgende Bild zeigt die Vorderseite des Servers mit den Laufwerken:

a. Drücken Sie den Netzschalter des Laufwerks, das Sie ersetzen möchten. Die LED blinkt 5-10 Sekunden lang und stoppt.

b. Nachdem die LED nicht mehr blinkt und das Laufwerk ausgeschaltet ist, entfernen Sie es vom Server, indem Sie die rote Taste drücken und die Verriegelung ziehen.

Stellen Sie sicher, dass Sie Laufwerke sehr sorgfältig behandeln.

4. Setzen Sie das Ersatzlaufwerk ein, indem Sie das Laufwerk vorsichtig mit der Verriegelung in den Schacht schieben und die Verriegelung schließen. Das Laufwerk wird eingeschaltet, wenn es richtig eingesetzt wird.
5. Überprüfen Sie die neuen Laufwerkdetails in iLO:
   a. Wählen Sie **Information** > **Integriertes Management-Protokoll**. Sie sehen ein Ereignis, das für das hinzugefügte Laufwerk protokolliert ist.
   b. Aktualisieren Sie die Seite, um die Ereignisse anzuzeigen, die für das neue Laufwerk, das Sie hinzugefügt haben, protokolliert wurden.
6. Überprüfen Sie den Zustand Ihres Speichersystems in iLO:
   a. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.
   b. Blättern Sie, bis Sie Informationen über den Schacht finden, in dem Sie das neue Laufwerk installiert haben.
   c. Notieren Sie sich die Seriennummer.
7. Fügen Sie die neuen Laufwerksinformationen in das hinzu `sf_sds_config.yaml` Datei für den Knoten, in dem Sie das Laufwerk ersetzt haben.

   Der `sf_sds_config.yaml` Datei wird in gespeichert `/opt/sf/`. Diese Datei enthält alle Informationen über die Laufwerke im Node. Jedes Mal, wenn Sie ein Laufwerk ersetzen, müssen Sie die Ersatzlaufwerk-Informationen in dieser Datei eingeben. Weitere Informationen zu dieser Datei finden Sie unter "Inhalt der datei sf_sds_config.yaml".

   a. Stellen Sie mit PuTTY eine SSH-Verbindung zum Knoten her.
   b. Geben Sie im Fenster PuTTY-Konfiguration den Knoten MIP im Feld **Hostname (oder IP-Adresse)** ein.
   c. Wählen Sie **Offen**.
   d. Melden Sie sich im sich öffnenden Terminalfenster mit Ihrem Benutzernamen und Passwort an.
   e. Führen Sie die aus `# cat /opt/sf/sf_sds_config.yaml` Befehl zum Auflisten des Inhalts der Datei.
   f. Ersetzen Sie die Einträge im `dataDevices` Oder `cacheDevices` Listen für das Laufwerk, das Sie durch die neuen Laufwerksinformationen ersetzt haben.
   g. Laufen `# systemctl start solidfire-update-drives`.

Nach der Ausführung dieses Befehls wird die Bash-Eingabeaufforderung angezeigt. Danach sollten Sie zur Element UI wechseln, um das Laufwerk zum Cluster hinzuzufügen. Die Element-UI zeigt eine Warnmeldung für ein neues Laufwerk an, das verfügbar ist.

8. Wählen Sie **Cluster** > **Laufwerke** > **Verfügbar**.

   Sie sehen die Seriennummer des neuen Laufwerks, das Sie installiert haben.

9. Wählen Sie das Symbol unter **Aktionen** und dann **Hinzufügen** aus.
10. Aktualisieren Sie die Element-UI, nachdem der Synchronisationsauftrag für den Block abgeschlossen ist. Sie sehen, dass die Warnung über das verfügbare Laufwerk gelöscht wurde, wenn Sie auf die Seite **ausgeführte Aufgaben** auf der Registerkarte **Reporting** der Element-Benutzeroberfläche zugreifen.

Ersetzen Sie ein Cache-Laufwerk

Führen Sie dieses Verfahren durch, wenn Sie das Cache-Laufwerk im SolidFire ESDS-Cluster ersetzen möchten. Das Cache-Laufwerk ist mit Metadaten-Services verknüpft. Auf der Seite Element UI **Cluster** > **Drives** werden die Informationen zum Laufwerksverschleiß angezeigt.

Was Sie benötigen

- Stellen Sie über die NetApp Element Software-UI sicher, dass der Cluster in einem guten Zustand ist und es keine Warnungen oder Cluster-Fehler gibt. Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.
- Stellen Sie sicher, dass auf dem Cluster keine aktiven Jobs ausgeführt werden.
- Stellen Sie sicher, dass Sie sich mit allen Schritten vertraut gemacht haben.
- Vergewissern Sie sich, dass Sie die Metadaten-Services von der Element UI entfernen.
- Stellen Sie sicher, dass Sie die erforderlichen Vorsichtsmaßnahmen treffen, um elektrostatische Entladung (ESD) beim Umgang mit Laufwerken zu verhindern.

Schritte

1. Führen Sie die folgenden Schritte in der Element UI aus:
   a. Wählen Sie in der Element-UI die Option **Cluster** > **Nodes** > **aktiv** aus.
   b. Notieren Sie sich die Node-ID und die Management-IP-Adresse des Nodes, in dem Sie das Cache-Laufwerk ersetzen.
   c. Wenn das Cache-Laufwerk gesund ist und Sie es proaktiv ersetzen, wählen Sie **Aktive Laufwerke**, suchen Sie das Metadatenlaufwerk und entfernen Sie es aus der UI.

      Nachdem Sie es entfernt haben, geht das Metadatenlaufwerk zuerst in den **removing** Status und dann in **available**.

   d. Wenn Sie nach dem Ausfall des Cache-Laufwerks einen Austausch durchführen, befindet sich das Metadatenlaufwerk im Status **verfügbar** und wird unter **Cluster** > **Laufwerke** > **verfügbar** aufgelistet.
   e. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke** > **aktiv**.
   f. Wählen Sie das Metadatenlaufwerk aus, das dem NodeName zugeordnet ist, wo Sie das Cache-Laufwerk ersetzen möchten.
   g. Wählen Sie **Massenaktionen** > **Entfernen**. Nachdem Sie das Laufwerk entfernt haben, wechselt das Laufwerk in den Zustand **Entfernen**. Er bleibt eine Weile im Status **Entfernen** und wartet darauf, dass die Daten auf dem Laufwerk synchronisiert oder auf die übrigen Laufwerke im Cluster verteilt werden. Nach dem Entfernen des Laufwerks wechselt das Laufwerk in den Status **verfügbar**.

2. Führen Sie die folgenden Schritte durch, um den Laufwerkschacht des Cache-Laufwerks zu finden, das Sie ersetzen:
   a. Melden Sie sich bei der IPMI-Schnittstelle des Knotens an (in diesem Fall iLO).
   b. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.
   c. Suchen Sie das Cache-Laufwerk.

      Cache-Laufwerke haben weniger Kapazität als Storage-Laufwerke.

   d. Suchen Sie nach der Steckplatznummer, die für das Cache-Laufwerk aufgeführt ist. Dies ist der physische Steckplatz, aus dem Sie das Laufwerk entfernen müssen.
3. Nachdem Sie das Laufwerk identifiziert haben, entfernen Sie es nun physisch wie folgt:
   a. Identifizieren Sie die Antriebsbox.

      Das folgende Bild zeigt die Vorderseite des Servers mit den Laufwerken:

   b. Drücken Sie den Netzschalter des Laufwerks, das Sie ersetzen möchten. Die LED blinkt 5-10 Sekunden lang und stoppt.
   c. Nachdem die LED nicht mehr blinkt und das Laufwerk ausgeschaltet ist, entfernen Sie es vom Server, indem Sie die rote Taste drücken und die Verriegelung ziehen.

      Stellen Sie sicher, dass Sie Laufwerke sehr sorgfältig behandeln.

   Nachdem Sie das Laufwerk physisch entfernt haben, ändert sich der Laufwerkszustand in der Element-UI in **failed**.
4. Notieren Sie sich die HPE Modellnummer und die ISN (Seriennummer) des neuen Cache-Laufwerks.
5. Setzen Sie das Ersatzlaufwerk ein, indem Sie das Laufwerk vorsichtig mit der Verriegelung in den Schacht schieben und die Verriegelung schließen. Das Laufwerk wird eingeschaltet, wenn es richtig eingesetzt wird.
6. Führen Sie die folgenden Schritte durch, um die neuen Laufwerkdetails in iLO zu überprüfen:
   a. Melden Sie sich bei iLO an.
   b. Wählen Sie **Information** > **Integriertes Management-Protokoll**. Sie sehen ein Ereignis, das für das hinzugefügte Laufwerk protokolliert ist.
   c. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.
   d. Blättern Sie, bis Sie Informationen über den Schacht finden, in dem Sie das Laufwerk ersetzt haben.
   e. Überprüfen Sie, ob die Seriennummer auf Ihrem Bildschirm mit der Seriennummer des neuen Laufwerks übereinstimmt, das Sie installiert haben.

7. Fügen Sie die Informationen zum neuen Cache-Laufwerk in das ein `sf_sds_config.yaml` Datei für den Knoten, in dem Sie das Laufwerk ersetzt haben.

   Der `sf_sds_config.yaml` Datei wird in gespeichert `/opt/sf/`. Diese Datei enthält alle Informationen über die Laufwerke im Node. Jedes Mal, wenn Sie ein Laufwerk ersetzen, sollten Sie die Informationen zum Ersatzlaufwerk in dieser Datei eingeben. Weitere Informationen zu dieser Datei finden Sie unter "Inhalt der datei sf_sds_config.yaml".

   a. Stellen Sie mit PuTTY eine SSH-Verbindung zum Knoten her.

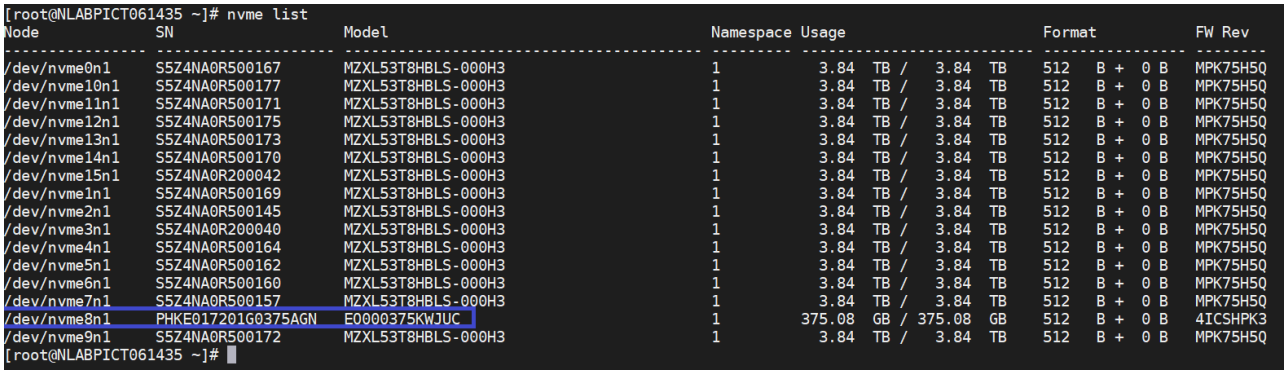
   b. Geben Sie im Konfigurationsfenster von PuTTY die Knoten-MIP-Adresse (die Sie zuvor von der Element UI zur Kenntnis genommen haben) im Feld **Hostname (oder IP-Adresse)** ein.

   c. Wählen Sie **Offen**.

   d. Melden Sie sich im sich öffnenden Terminalfenster mit Ihrem Benutzernamen und Passwort an.

   e. Führen Sie die aus `nvme list` Befehl zum Auflisten der NMVe-Geräte.

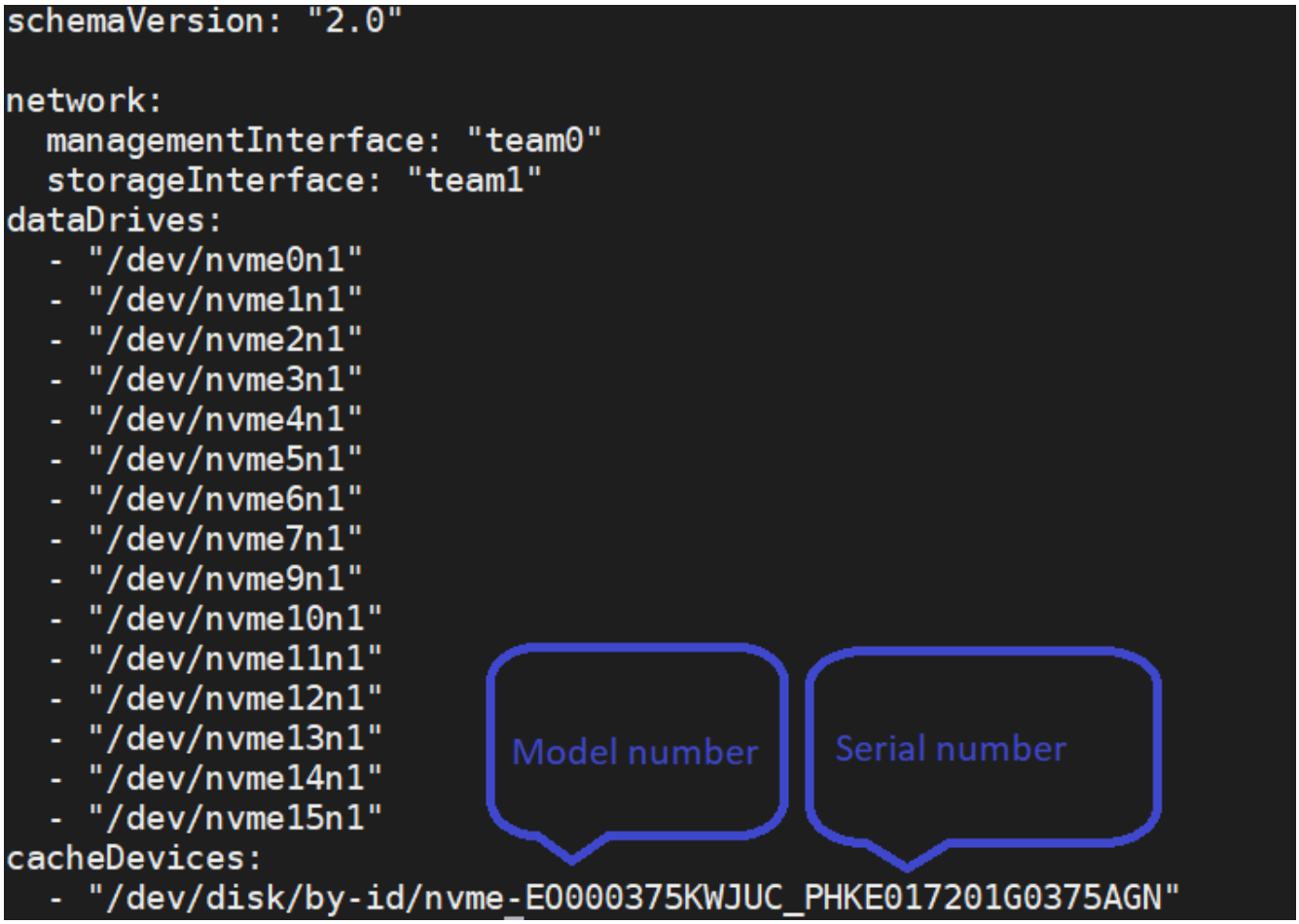
      Sie können die Modellnummer und die Seriennummer des neuen Cache-Laufwerks sehen. Die folgende Beispielausgabe finden Sie unter:



```
[root@NLABPICT061435 ~]# nvme list
Node             SN                   Model                                    Namespace Usage                      Format           FW Rev
---------------- -------------------- ---------------------------------------- --------- -------------------------- ---------------- --------
/dev/nvme0n1     S5Z4NA0R500167       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme10n1    S5Z4NA0R500177       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme11n1    S5Z4NA0R500171       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme12n1    S5Z4NA0R500175       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme13n1    S5Z4NA0R500173       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme14n1    S5Z4NA0R500170       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme15n1    S5Z4NA0R200042       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme1n1     S5Z4NA0R500169       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme2n1     S5Z4NA0R500145       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme3n1     S5Z4NA0R200040       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme4n1     S5Z4NA0R500164       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme5n1     S5Z4NA0R500162       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme6n1     S5Z4NA0R500160       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme7n1     S5Z4NA0R500157       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
/dev/nvme8n1     PHKE017201G0375AGN   E0000375KWJUC                            1         375.08  GB / 375.08  GB    512   B +  0 B   4ICSHPK3
/dev/nvme9n1     S5Z4NA0R500172       MZXL53T8HBLS-000H3                       1           3.84  TB /   3.84  TB    512   B +  0 B   MPK75H5Q
[root@NLABPICT061435 ~]#
```

   f. Fügen Sie die Informationen zum neuen Cache-Laufwerk in hinzu `/opt/sf/sf_sds_config.yaml`.

      Sie sollten die Modellnummer und Seriennummer des vorhandenen Cache-Laufwerks durch die entsprechenden Informationen für das neue Cache-Laufwerk ersetzen. Das folgende Beispiel zeigt:



a. Speichern Sie die `/opt/sf/sf_sds_config.yaml` Datei:

8. Führen Sie die für Sie relevanten Schritte für das Szenario aus:

Szenario	Schritte
Das neue eingelegte Cache-Laufwerk wird angezeigt, nachdem Sie den ausgeführt haben `nvme list` Befehl	a. Laufen `# systemctl restart solidfire`. Dies dauert etwa drei Minuten. b. Prüfen Sie die `solidfire` Status durch Ausführen `system status solidfire`. c. Fahren Sie mit Schritt 9 fort.
Das neue eingelegte Cache-Laufwerk wird nicht angezeigt, nachdem Sie den ausgeführt haben `nvme list` Befehl	a. Booten Sie den Node neu. b. Überprüfen Sie, nachdem der Node neu gebootet wurde, dass der `solidfire` Dienste werden ausgeführt, indem Sie sich beim Knoten (mit PuTTY) anmelden und den ausführen `system status solidfire` Befehl. c. Fahren Sie mit Schritt 9 fort.

Neustart `solidfire` Oder beim Neubooten des Node werden einige Cluster-Fehler verursacht, die in etwa fünf Minuten behoben werden.

9. Fügen Sie in der Element UI das Metadatenlaufwerk hinzu, das Sie entfernt haben:
    a. Wählen Sie **Cluster** > **Laufwerke** > **Verfügbar**.
    b. Wählen Sie das Symbol unter Aktionen aus, und wählen Sie **Hinzufügen**.
10. Aktualisieren Sie die Element-UI, sobald der Synchronisationsauftrag für den Block abgeschlossen ist.

    Es wird angezeigt, dass die Meldung über das verfügbare Laufwerk zusammen mit anderen Cluster-Fehlern beseitigt wurde.

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Ersetzen Sie Laufwerke für HPE DL360

Wählen Sie aus den hier aufgeführten Verfahren, um ein Laufwerk proaktiv zu ersetzen, ein Laufwerk nach dem Ausfall zu ersetzen und ein Cache-Laufwerk zu ersetzen. Ein Metadatenlaufwerk oder ein Blocklaufwerk im SolidFire ESDS-Cluster ersetzen. Auf der Seite Element UI **Cluster > Laufwerke** werden die Informationen zum Laufwerksverschleiß angezeigt.

- Ersetzen Sie ein Laufwerk proaktiv
- Tauschen Sie ein fehlerhaftes Laufwerk aus
- Ersetzen Sie ein Cache-Laufwerk

Ersetzen Sie ein Laufwerk proaktiv

Führen Sie dieses Verfahren durch, wenn Sie ein Metadatenlaufwerk oder ein Blocklaufwerk im SolidFire ESDS-Cluster proaktiv ersetzen möchten. Auf der Seite Element UI **Cluster** > **Drives** werden die Informationen zum Laufwerksverschleiß angezeigt.

Was Sie benötigen

- Stellen Sie über die NetApp Element Software-UI sicher, dass der Cluster in einem guten Zustand ist und es keine Warnungen oder Cluster-Fehler gibt. Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.
- Stellen Sie sicher, dass auf dem Cluster keine aktiven Jobs ausgeführt werden.
- Stellen Sie sicher, dass Sie sich mit allen Schritten vertraut gemacht haben.
- Stellen Sie sicher, dass Sie die erforderlichen Vorsichtsmaßnahmen treffen, um elektrostatische Entladung (ESD) beim Umgang mit Laufwerken zu verhindern.

Schritte

1. Führen Sie die folgenden Schritte in der Element UI aus:
    a. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke** > **aktiv**.
    b. Wählen Sie das Laufwerk aus, das Sie ersetzen möchten.
    c. Notieren Sie sich die Seriennummer des Laufwerks. Dies hilft Ihnen dabei, die entsprechende BayID in der IPMI-Schnittstelle des Knotens zu finden (in diesem Fall HPE Integrated Lights-Out oder iLO).

d. Wählen Sie **Massenaktionen** > **Entfernen**. Nachdem Sie das Laufwerk entfernt haben, wechselt das Laufwerk in den Zustand **Entfernen**. Er bleibt eine Weile im Status **Entfernen** und wartet darauf, dass die Daten auf dem Laufwerk synchronisiert oder auf die übrigen Laufwerke im Cluster verteilt werden. Nach dem Entfernen des Laufwerks wechselt das Laufwerk in den Status **verfügbar**.

2. Gehen Sie wie folgt vor, um den Laufwerkschacht des zu ersetzenden Laufwerks zu finden:
   a. Melden Sie sich bei der IPMI-Schnittstelle des Knotens an (in diesem Fall iLO).
   b. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.
   c. Ordnen Sie die Seriennummer, die Sie im vorherigen Schritt angegeben haben, mit dem überein, was auf dem Bildschirm angezeigt wird.
   d. Suchen Sie nach der Steckplatznummer, die mit der Seriennummer aufgeführt ist. Dies ist der physische Steckplatz, aus dem Sie das Laufwerk entfernen müssen.
3. Nachdem Sie das Laufwerk identifiziert haben, entfernen Sie es nun physisch wie folgt:
   a. Identifizieren Sie den Laufwerkschacht.

      Das folgende Bild zeigt die Vorderseite des Servers mit der Nummerierung des Laufwerksschachts auf der linken Seite des Bildes:

   b. Drücken Sie den Netzschalter des Laufwerks, das Sie ersetzen möchten. Die LED blinkt 5-10 Sekunden lang und stoppt.
   c. Nachdem die LED nicht mehr blinkt und das Laufwerk ausgeschaltet ist, entfernen Sie es vom Server, indem Sie die rote Taste drücken und die Verriegelung ziehen.

      Stellen Sie sicher, dass Sie Laufwerke sehr sorgfältig behandeln.

   Nachdem Sie das Laufwerk physisch entfernt haben, ändert sich der Laufwerkszustand in der Element-UI in **failed**.

4. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke** > **fehlgeschlagen**.
5. Wählen Sie das Symbol unter **Aktionen** und dann **Entfernen** aus.

   Jetzt können Sie das neue Laufwerk im Knoten installieren.

6. Notieren Sie sich die Seriennummer des neuen Laufwerks.
7. Setzen Sie das Ersatzlaufwerk ein, indem Sie das Laufwerk vorsichtig mit der Verriegelung in den Schacht schieben und die Verriegelung schließen. Das Laufwerk wird eingeschaltet, wenn es richtig eingesetzt wird.
8. Führen Sie die folgenden Schritte durch, um die neuen Laufwerkdetails in iLO zu überprüfen:
   a. Melden Sie sich bei iLO an.
   b. Wählen Sie **Information** > **Integriertes Management-Protokoll**. Sie sehen ein Ereignis, das für das hinzugefügte Laufwerk protokolliert ist.
   c. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.

d. Blättern Sie, bis Sie Informationen über den Schacht finden, in dem Sie das Laufwerk ersetzt haben.

e. Überprüfen Sie, ob die Seriennummer auf dem Bildschirm mit der Seriennummer des neuen Laufwerks übereinstimmt, das Sie ersetzt haben.

9. Fügen Sie die neuen Laufwerksinformationen in das hinzu `sf_sds_config.yaml` Datei für den Knoten, in dem Sie das Laufwerk ersetzt haben.

   Der `sf_sds_config.yaml` Datei wird in gespeichert `/opt/sf/`. Diese Datei enthält alle Informationen über die Laufwerke im Node. Jedes Mal, wenn Sie ein Laufwerk ersetzen, müssen Sie die Ersatzlaufwerk-Informationen in dieser Datei eingeben. Weitere Informationen zu dieser Datei finden Sie unter "Inhalt der datei sf_sds_config.yaml".

   a. Stellen Sie mit PuTTY eine SSH-Verbindung zum Knoten her.

   b. Geben Sie im Fenster PuTTY-Konfiguration den Knoten MIP im Feld **Hostname (oder IP-Adresse)** ein.

   c. Wählen Sie **Offen**.

   d. Melden Sie sich im sich öffnenden Terminalfenster mit Ihrem Benutzernamen und Passwort an.

   e. Führen Sie die aus `# cat /opt/sf/sf_sds_config.yaml` Befehl zum Auflisten des Inhalts der Datei.

   f. Ersetzen Sie die Einträge im `dataDevices` Oder `cacheDevices` Listen für das Laufwerk, das Sie durch die neuen Laufwerksinformationen ersetzt haben.

   g. Laufen `# systemctl start solidfire-update-drives`.

      Nach der Ausführung dieses Befehls wird die Bash-Eingabeaufforderung angezeigt. Danach sollten Sie zur Element UI wechseln, um das Laufwerk zum Cluster hinzuzufügen. Die Element-UI zeigt eine Warnmeldung für ein neues Laufwerk an, das verfügbar ist.

10. Wählen Sie **Cluster** > **Laufwerke** > **Verfügbar**.

    Sie sehen die Seriennummer des neuen Laufwerks, das Sie installiert haben.

11. Wählen Sie das Symbol unter **Aktionen** und dann **Hinzufügen** aus.

12. Aktualisieren Sie die Element-UI, nachdem der Synchronisationsauftrag für den Block abgeschlossen ist. Sie sehen, dass die Warnung über das verfügbare Laufwerk gelöscht wurde, wenn Sie auf die Seite **ausgeführte Aufgaben** auf der Registerkarte **Reporting** der Element-Benutzeroberfläche zugreifen.

Tauschen Sie ein fehlerhaftes Laufwerk aus

Wenn das SolidFire ESDS-Cluster über ein fehlerhaftes Laufwerk verfügt, zeigt die Element-UI eine Warnmeldung an. Bevor Sie das Laufwerk aus dem Cluster entfernen, überprüfen Sie den Grund für Fehler, indem Sie die Informationen in der IPMI-Schnittstelle für Ihren Node/Server anzeigen. Diese Schritte sind anwendbar, wenn Sie ein Block-Laufwerk oder ein Metadaten-Laufwerk ersetzen.

Was Sie benötigen

- Überprüfen Sie in der NetApp Element-Software-UI, ob das Laufwerk ausgefallen ist. Element zeigt eine Warnmeldung an, wenn ein Laufwerk ausfällt. Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.
- Stellen Sie sicher, dass Sie sich mit allen Schritten vertraut gemacht haben.
- Stellen Sie sicher, dass Sie die erforderlichen Vorsichtsmaßnahmen treffen, um elektrostatische Entladung (ESD) beim Umgang mit Laufwerken zu verhindern.

Schritte

1. Entfernen Sie das ausgefallene Laufwerk mithilfe der Element UI wie folgt aus dem Cluster:
   a. Wählen Sie **Cluster** > **Laufwerke** > **Fehlgeschlagen**.
   b. Notieren Sie den Node-Namen und die Seriennummer des ausgefallenen Laufwerks.
   c. Wählen Sie das Symbol unter **Aktionen** und dann **Entfernen** aus. Wenn Sie Warnungen über den Dienst sehen, der mit dem Laufwerk verbunden ist, warten Sie, bis die bin-Synchronisierung abgeschlossen ist, und entfernen Sie dann das Laufwerk.
2. Führen Sie die folgenden Schritte durch, um den Laufwerkausfall zu überprüfen und die protokollierten Ereignisse anzuzeigen, die mit dem Laufwerksausfall verbunden sind:
   a. Melden Sie sich bei der IPMI-Schnittstelle des Knotens an (in diesem Fall iLO).
   b. Wählen Sie **Information** > **Integriertes Management-Protokoll**. Hier ist der Grund für den Laufwerksausfall (z. B. SSDWOROut) und den Standort aufgeführt. Es wird auch ein Ereignis angezeigt, das den Status des Laufwerks angibt.
   c. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.
   d. Überprüfen Sie die verfügbaren Informationen über das ausgefallene Laufwerk. Der Status des ausgefallenen Laufwerks lautet **degradiert**.
3. Entfernen Sie das Laufwerk wie folgt physisch:
   a. Identifizieren Sie die Laufwerkssteckplatznummer im Gehäuse.

      Das folgende Bild zeigt die Vorderseite des Servers mit der Nummerierung des Laufwerksschachts auf der linken Seite des Bildes:

   a. Drücken Sie den Netzschalter des Laufwerks, das Sie ersetzen möchten. Die LED blinkt 5-10 Sekunden lang und stoppt.
   b. Nachdem die LED nicht mehr blinkt und das Laufwerk ausgeschaltet ist, entfernen Sie es vom Server, indem Sie die rote Taste drücken und die Verriegelung ziehen.

      Stellen Sie sicher, dass Sie Laufwerke sehr sorgfältig behandeln.

4. Setzen Sie das Ersatzlaufwerk ein, indem Sie das Laufwerk vorsichtig mit der Verriegelung in den Schacht schieben und die Verriegelung schließen. Das Laufwerk wird eingeschaltet, wenn es richtig eingesetzt wird.
5. Überprüfen Sie die neuen Laufwerkdetails in iLO:
   a. Wählen Sie **Information** > **Integriertes Management-Protokoll**. Sie sehen ein Ereignis, das für das hinzugefügte Laufwerk protokolliert ist.
   b. Aktualisieren Sie die Seite, um die Ereignisse anzuzeigen, die für das neue Laufwerk, das Sie hinzugefügt haben, protokolliert wurden.
6. Überprüfen Sie den Zustand Ihres Speichersystems in iLO:
   a. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.

b. Blättern Sie, bis Sie Informationen über den Schacht finden, in dem Sie das neue Laufwerk installiert haben.

c. Notieren Sie sich die Seriennummer.

7. Fügen Sie die neuen Laufwerksinformationen in das hinzu `sf_sds_config.yaml` Datei für den Knoten, in dem Sie das Laufwerk ersetzt haben.

   Der `sf_sds_config.yaml` Datei wird in gespeichert `/opt/sf/`. Diese Datei enthält alle Informationen über die Laufwerke im Node. Jedes Mal, wenn Sie ein Laufwerk ersetzen, müssen Sie die Ersatzlaufwerk-Informationen in dieser Datei eingeben. Weitere Informationen zu dieser Datei finden Sie unter "Inhalt der datei sf_sds_config.yaml".

   a. Stellen Sie mit PuTTY eine SSH-Verbindung zum Knoten her.

   b. Geben Sie im Fenster PuTTY-Konfiguration den Knoten MIP im Feld **Hostname (oder IP-Adresse)** ein.

   c. Wählen Sie **Offen**.

   d. Melden Sie sich im sich öffnenden Terminalfenster mit Ihrem Benutzernamen und Passwort an.

   e. Führen Sie die aus `# cat /opt/sf/sf_sds_config.yaml` Befehl zum Auflisten des Inhalts der Datei.

   f. Ersetzen Sie die Einträge im `dataDevices` Oder `cacheDevices` Listen für das Laufwerk, das Sie durch die neuen Laufwerksinformationen ersetzt haben.

   g. Laufen `# systemctl start solidfire-update-drives`.

      Nach der Ausführung dieses Befehls wird die Bash-Eingabeaufforderung angezeigt. Danach sollten Sie zur Element UI wechseln, um das Laufwerk zum Cluster hinzuzufügen. Die Element-UI zeigt eine Warnmeldung für ein neues Laufwerk an, das verfügbar ist.

8. Wählen Sie **Cluster** > **Laufwerke** > **Verfügbar**.

   Sie sehen die Seriennummer des neuen Laufwerks, das Sie installiert haben.

9. Wählen Sie das Symbol unter **Aktionen** und dann **Hinzufügen** aus.

10. Aktualisieren Sie die Element-UI, nachdem der Synchronisationsauftrag für den Block abgeschlossen ist. Sie sehen, dass die Warnung über das verfügbare Laufwerk gelöscht wurde, wenn Sie auf die Seite **ausgeführte Aufgaben** auf der Registerkarte **Reporting** der Element-Benutzeroberfläche zugreifen.

Ersetzen Sie ein Cache-Laufwerk

Führen Sie dieses Verfahren durch, wenn Sie das Cache-Laufwerk im SolidFire ESDS-Cluster ersetzen möchten. Das Cache-Laufwerk ist mit Metadaten-Services verknüpft. Auf der Seite Element UI **Cluster** > **Drives** werden die Informationen zum Laufwerksverschleiß angezeigt.

Was Sie benötigen

- Stellen Sie über die NetApp Element Software-UI sicher, dass der Cluster in einem guten Zustand ist und es keine Warnungen oder Cluster-Fehler gibt. Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.
- Stellen Sie sicher, dass auf dem Cluster keine aktiven Jobs ausgeführt werden.
- Stellen Sie sicher, dass Sie sich mit allen Schritten vertraut gemacht haben.
- Vergewissern Sie sich, dass Sie die Metadaten-Services von der Element UI entfernen.

- Stellen Sie sicher, dass Sie die erforderlichen Vorsichtsmaßnahmen treffen, um elektrostatische Entladung (ESD) beim Umgang mit Laufwerken zu verhindern.

Schritte

1. Führen Sie die folgenden Schritte in der Element UI aus:
   a. Wählen Sie in der Element-UI die Option **Cluster** > **Nodes** > **aktiv** aus.
   b. Notieren Sie sich die Node-ID und die Management-IP-Adresse des Nodes, in dem Sie das Cache-Laufwerk ersetzen.
   c. Wenn das Cache-Laufwerk gesund ist und Sie es proaktiv ersetzen, wählen Sie **Aktive Laufwerke**, suchen Sie das Metadatenlaufwerk und entfernen Sie es aus der UI.

      Nachdem Sie es entfernt haben, geht das Metadatenlaufwerk zuerst in den **removing** Status und dann in **available**.

   d. Wenn Sie nach dem Ausfall des Cache-Laufwerks einen Austausch durchführen, befindet sich das Metadatenlaufwerk im Status **verfügbar** und wird unter **Cluster** > **Laufwerke** > **verfügbar** aufgelistet.
   e. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke** > **aktiv**.
   f. Wählen Sie das Metadatenlaufwerk aus, das dem NodeName zugeordnet ist, wo Sie das Cache-Laufwerk ersetzen möchten.
   g. Wählen Sie **Massenaktionen** > **Entfernen**. Nachdem Sie das Laufwerk entfernt haben, wechselt das Laufwerk in den Zustand **Entfernen**. Er bleibt eine Weile im Status **Entfernen** und wartet darauf, dass die Daten auf dem Laufwerk synchronisiert oder auf die übrigen Laufwerke im Cluster verteilt werden. Nach dem Entfernen des Laufwerks wechselt das Laufwerk in den Status **verfügbar**.
2. Führen Sie die folgenden Schritte durch, um den Laufwerkschacht des Cache-Laufwerks zu finden, das Sie ersetzen:
   a. Melden Sie sich bei der IPMI-Schnittstelle des Knotens an (in diesem Fall iLO).
   b. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.
   c. Suchen Sie das Cache-Laufwerk.

      Cache-Laufwerke haben weniger Kapazität als Storage-Laufwerke.

   d. Suchen Sie nach der Steckplatznummer, die für das Cache-Laufwerk aufgeführt ist. Dies ist der physische Steckplatz, aus dem Sie das Laufwerk entfernen müssen.
3. Nachdem Sie das Laufwerk identifiziert haben, entfernen Sie es nun physisch wie folgt:
   a. Identifizieren Sie den Laufwerkschacht.

      Das folgende Bild zeigt die Vorderseite des Servers mit der Nummerierung des Laufwerksschachts auf der linken Seite des Bildes:

   b. Drücken Sie den Netzschalter des Laufwerks, das Sie ersetzen möchten. Die LED blinkt 5-10 Sekunden lang und stoppt.
   c. Nachdem die LED nicht mehr blinkt und das Laufwerk ausgeschaltet ist, entfernen Sie es vom Server,

indem Sie die rote Taste drücken und die Verriegelung ziehen.

Stellen Sie sicher, dass Sie Laufwerke sehr sorgfältig behandeln.

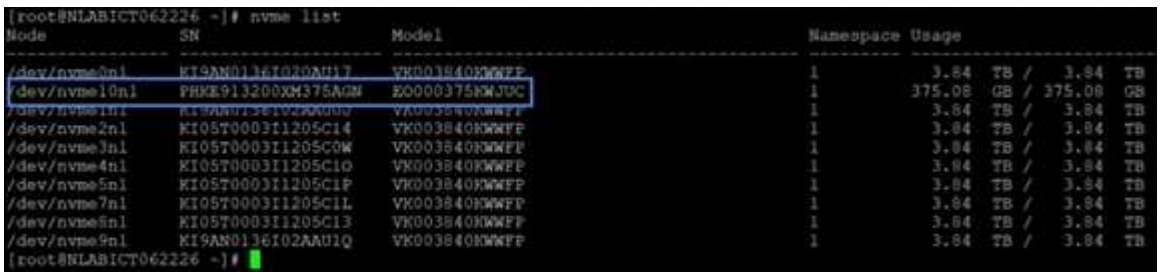
Nachdem Sie das Laufwerk physisch entfernt haben, ändert sich der Laufwerkszustand in der Element-UI in **failed**.

4. Notieren Sie sich die HPE Modellnummer und die ISN (Seriennummer) des neuen Cache-Laufwerks.
5. Setzen Sie das Ersatzlaufwerk ein, indem Sie das Laufwerk vorsichtig mit der Verriegelung in den Schacht schieben und die Verriegelung schließen. Das Laufwerk wird eingeschaltet, wenn es richtig eingesetzt wird.
6. Führen Sie die folgenden Schritte durch, um die neuen Laufwerkdetails in iLO zu überprüfen:
   a. Melden Sie sich bei iLO an.
   b. Wählen Sie **Information** > **Integriertes Management-Protokoll**. Sie sehen ein Ereignis, das für das hinzugefügte Laufwerk protokolliert ist.
   c. Wählen Sie in der linken Navigationsleiste die Option **Systeminformationen** aus, und wählen Sie dann **Speicherung** aus.
   d. Blättern Sie, bis Sie Informationen über den Schacht finden, in dem Sie das Laufwerk ersetzt haben.
   e. Überprüfen Sie, ob die Seriennummer auf Ihrem Bildschirm mit der Seriennummer des neuen Laufwerks übereinstimmt, das Sie installiert haben.
7. Fügen Sie die Informationen zum neuen Cache-Laufwerk in das ein `sf_sds_config.yaml` Datei für den Knoten, in dem Sie das Laufwerk ersetzt haben.

   Der `sf_sds_config.yaml` Datei wird in gespeichert `/opt/sf/`. Diese Datei enthält alle Informationen über die Laufwerke im Node. Jedes Mal, wenn Sie ein Laufwerk ersetzen, sollten Sie die Informationen zum Ersatzlaufwerk in dieser Datei eingeben. Weitere Informationen zu dieser Datei finden Sie unter "Inhalt der datei sf_sds_config.yaml".

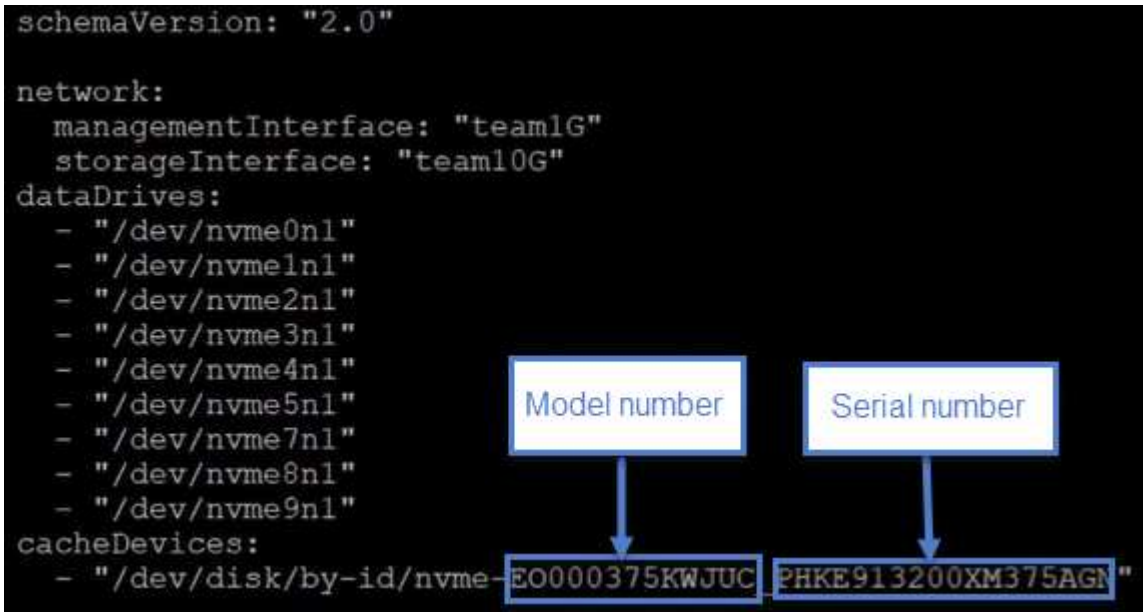
   a. Stellen Sie mit PuTTY eine SSH-Verbindung zum Knoten her.
   b. Geben Sie im Konfigurationsfenster von PuTTY die Knoten-MIP-Adresse (die Sie zuvor von der Element UI zur Kenntnis genommen haben) im Feld **Hostname (oder IP-Adresse)** ein.
   c. Wählen Sie **Offen**.
   d. Melden Sie sich im sich öffnenden Terminalfenster mit Ihrem Benutzernamen und Passwort an.
   e. Führen Sie die aus `nvme list` Befehl zum Auflisten der NMVe-Geräte.

      Sie können die Modellnummer und die Seriennummer des neuen Cache-Laufwerks sehen. Die folgende Beispielausgabe finden Sie unter:



   f. Fügen Sie die Informationen zum neuen Cache-Laufwerk in hinzu `/opt/sf/sf_sds_config.yaml`.

Sie sollten die Modellnummer und Seriennummer des vorhandenen Cache-Laufwerks durch die entsprechenden Informationen für das neue Cache-Laufwerk ersetzen. Das folgende Beispiel zeigt:



a. Speichern Sie die `/opt/sf/sf_sds_config.yaml` Datei:

8. Führen Sie die für Sie relevanten Schritte für das Szenario aus:

Szenario	Schritte
Das neue eingelegte Cache-Laufwerk wird angezeigt, nachdem Sie den ausgeführt haben `nvme list` Befehl	a. Laufen `# systemctl restart solidfire`. Dies dauert etwa drei Minuten. b. Prüfen Sie die `solidfire` Status durch Ausführen `system status solidfire`. c. Fahren Sie mit Schritt 9 fort.
Das neue eingelegte Cache-Laufwerk wird nicht angezeigt, nachdem Sie den ausgeführt haben `nvme list` Befehl	a. Booten Sie den Node neu. b. Überprüfen Sie, nachdem der Node neu gebootet wurde, dass der `solidfire` Dienste werden ausgeführt, indem Sie sich beim Knoten (mit PuTTY) anmelden und den ausführen `system status solidfire` Befehl. c. Fahren Sie mit Schritt 9 fort.

Neustart `solidfire` Oder beim Neubooten des Node werden einige Cluster-Fehler verursacht, die in etwa fünf Minuten behoben werden.

9. Fügen Sie in der Element UI das Metadatenlaufwerk hinzu, das Sie entfernt haben:
   a. Wählen Sie **Cluster** > **Laufwerke** > **Verfügbar**.
   b. Wählen Sie das Symbol unter Aktionen aus, und wählen Sie **Hinzufügen**.
10. Aktualisieren Sie die Element-UI, sobald der Synchronisationsauftrag für den Block abgeschlossen ist.

Es wird angezeigt, dass die Meldung über das verfügbare Laufwerk zusammen mit anderen Cluster-Fehlern beseitigt wurde.

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Ersetzen Sie die Laufwerke für Dell R640

Wählen Sie aus den hier aufgeführten Verfahren, um ein Laufwerk proaktiv zu ersetzen, ein Laufwerk nach dem Ausfall zu ersetzen und ein Cache-Laufwerk zu ersetzen. Ein Metadatenlaufwerk oder ein Blocklaufwerk im SolidFire ESDS-Cluster ersetzen. Auf der Seite Element UI **Cluster > Laufwerke** werden die Informationen zum Laufwerksverschleiß angezeigt.

- Ersetzen Sie ein Laufwerk proaktiv
- Tauschen Sie ein fehlerhaftes Laufwerk aus
- Ersetzen Sie ein Cache-Laufwerk

Ersetzen Sie ein Laufwerk proaktiv

Führen Sie dieses Verfahren durch, wenn Sie ein Metadatenlaufwerk oder ein Blocklaufwerk im SolidFire ESDS-Cluster proaktiv ersetzen möchten. Auf der Seite Element UI **Cluster** > **Drives** werden die Informationen zum Laufwerksverschleiß angezeigt.

Was Sie benötigen

- Stellen Sie über die NetApp Element Software-UI sicher, dass der Cluster in einem guten Zustand ist und es keine Warnungen oder Cluster-Fehler gibt. Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.
- Stellen Sie sicher, dass auf dem Cluster keine aktiven Jobs ausgeführt werden.
- Stellen Sie sicher, dass Sie sich mit allen Schritten vertraut gemacht haben.
- Stellen Sie sicher, dass Sie die erforderlichen Vorsichtsmaßnahmen treffen, um elektrostatische Entladung (ESD) beim Umgang mit Laufwerken zu verhindern.

Schritte

1. Führen Sie die folgenden Schritte in der Element UI aus:
   a. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke** > **aktiv**.
   b. Wählen Sie das Laufwerk aus, das Sie ersetzen möchten.
   c. Notieren Sie sich die Seriennummer des Laufwerks. Auf diese Weise können Sie die entsprechende Steckplatznummer des Laufwerks im Integrated Dell Remote Access Controller (iDRAC) finden.
   d. Wählen Sie **Massenaktionen** > **Entfernen**. Nachdem Sie das Laufwerk entfernt haben, wechselt das Laufwerk in den Zustand **Entfernen**. Er bleibt eine Weile im Status **Entfernen** und wartet darauf, dass die Daten auf dem Laufwerk synchronisiert oder auf die übrigen Laufwerke im Cluster verteilt werden. Nach dem Entfernen des Laufwerks wechselt das Laufwerk in den Status **verfügbar**.
2. Gehen Sie wie folgt vor, um den Laufwerkschacht des zu ersetzenden Laufwerks zu finden:

a. Melden Sie sich an der IPMI-Schnittstelle des Knotens an (iDRAC in diesem Fall).
b. Wählen Sie im Menü * Storage* aus und wählen Sie dann **physische Festplatten**.
c. Um die Seriennummer des Laufwerks zu finden, wählen Sie das **+** -Symbol neben jedem PCIe SSD aus.
d. Ordnen Sie die auf dem Bildschirm angezeigte Seriennummer mit den in der Element-UI angegebenen Seriennummern zu.
e. Suchen Sie nach der Steckplatznummer, die mit der Seriennummer aufgeführt ist.

   Dies ist der physische Steckplatz, aus dem Sie das Laufwerk entfernen sollten.

3. Nachdem Sie das Laufwerk identifiziert haben, entfernen Sie es nun physisch wie folgt:
   a. Identifizieren Sie die Laufwerkssteckplatznummer im Gehäuse.

      Das folgende Bild zeigt die Vorderseite des Servers mit der für jedes Laufwerk angezeigten Steckplatznummerierung:

   b. Drücken Sie die Taste auf dem Laufwerk.

      Die Verriegelung tritt aus.

   c. Ziehen Sie das Laufwerk physisch aus dem Steckplatz heraus.

      Stellen Sie sicher, dass Sie Laufwerke sehr sorgfältig behandeln.

   Nachdem Sie das Laufwerk physisch entfernt haben, ändert sich der Laufwerkszustand in der Element-UI in **failed**.

4. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke** > **fehlgeschlagen**.
5. Wählen Sie das Symbol unter **Aktionen** und dann **Entfernen** aus.

   Jetzt können Sie das neue Laufwerk im Knoten installieren.

6. Notieren Sie sich die Seriennummer des neuen Laufwerks.
7. Setzen Sie das Ersatzlaufwerk ein, indem Sie das Laufwerk vorsichtig mit der Verriegelung in den Schacht schieben und die Verriegelung schließen. Das Laufwerk wird eingeschaltet, wenn es richtig eingesetzt wird.
8. Führen Sie die folgenden Schritte durch, um die neuen Laufwerkdetails in iDRAC zu überprüfen:
   a. Melden Sie sich am iDRAC an.
   b. Wählen Sie **Wartung** > **Systemereignisprotokoll**.

      Sie sehen ein Ereignis, das für das hinzugefügte Laufwerk protokolliert ist.

   c. Wählen Sie im Menü * Storage* aus und wählen Sie dann **physische Festplatten**.
   d. Vergewissern Sie sich, dass das neue Laufwerk, das Sie eingesetzt haben, in dem entsprechenden Steckplatz in der UI angezeigt wird.

e. Um die Seriennummer des Laufwerks zu finden, wählen Sie das **+** -Symbol neben jedem PCIe SSD aus.

9. Fügen Sie die neuen Laufwerksinformationen in das hinzu `sf_sds_config.yaml` Datei für den Knoten, in dem Sie das Laufwerk ersetzt haben.

   Der `sf_sds_config.yaml` Datei wird in gespeichert `/opt/sf/`. Diese Datei enthält alle Informationen über die Laufwerke im Node. Jedes Mal, wenn Sie ein Laufwerk ersetzen, müssen Sie die Ersatzlaufwerk-Informationen in dieser Datei eingeben. Weitere Informationen zu dieser Datei finden Sie unter "Inhalt der datei sf_sds_config.yaml".

   a. Stellen Sie mit PuTTY eine SSH-Verbindung zum Knoten her.
   b. Geben Sie im Fenster PuTTY-Konfiguration den Knoten MIP im Feld **Hostname (oder IP-Adresse)** ein.
   c. Wählen Sie **Offen**.
   d. Melden Sie sich im sich öffnenden Terminalfenster mit Ihrem Benutzernamen und Passwort an.
   e. Führen Sie die aus `# cat /opt/sf/sf_sds_config.yaml` Befehl zum Auflisten des Inhalts der Datei.
   f. Ersetzen Sie die Einträge im `dataDevices` Oder `cacheDevices` Listen für das Laufwerk, das Sie durch die neuen Laufwerksinformationen ersetzt haben.
   g. Laufen `# systemctl start solidfire-update-drives`.

      Nach der Ausführung dieses Befehls wird die Bash-Eingabeaufforderung angezeigt. Danach sollten Sie zur Element UI wechseln, um das Laufwerk zum Cluster hinzuzufügen. Die Element-UI zeigt eine Warnmeldung für ein neues Laufwerk an, das verfügbar ist.

10. Wählen Sie **Cluster** > **Laufwerke** > **Verfügbar**.

    Sie sehen die Seriennummer des neuen Laufwerks, das Sie installiert haben.

11. Wählen Sie das Symbol unter **Aktionen** und dann **Hinzufügen** aus.
12. Aktualisieren Sie die Element-UI, nachdem der Synchronisationsauftrag für den Block abgeschlossen ist. Sie sehen, dass die Warnung über das verfügbare Laufwerk gelöscht wurde, wenn Sie auf die Seite **ausgeführte Aufgaben** auf der Registerkarte **Reporting** der Element-Benutzeroberfläche zugreifen.

Tauschen Sie ein fehlerhaftes Laufwerk aus

Wenn das SolidFire ESDS-Cluster über ein fehlerhaftes Laufwerk verfügt, zeigt die Element-UI eine Warnmeldung an. Bevor Sie das Laufwerk aus dem Cluster entfernen, überprüfen Sie den Grund für Fehler, indem Sie die Informationen in der IPMI-Schnittstelle für Ihren Node/Server anzeigen. Diese Schritte sind anwendbar, wenn Sie ein Block-Laufwerk oder ein Metadaten-Laufwerk ersetzen.

Was Sie benötigen

- Überprüfen Sie in der NetApp Element-Software-UI, ob das Laufwerk ausgefallen ist. Element zeigt eine Warnmeldung an, wenn ein Laufwerk ausfällt. Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.
- Stellen Sie sicher, dass Sie sich mit allen Schritten vertraut gemacht haben.
- Stellen Sie sicher, dass Sie die erforderlichen Vorsichtsmaßnahmen treffen, um elektrostatische Entladung (ESD) beim Umgang mit Laufwerken zu verhindern.

Schritte

1. Entfernen Sie das ausgefallene Laufwerk mithilfe der Element UI wie folgt aus dem Cluster:
   a. Wählen Sie **Cluster** > **Laufwerke** > **Fehlgeschlagen**.
   b. Notieren Sie den Node-Namen und die Seriennummer des ausgefallenen Laufwerks.
   c. Wählen Sie das Symbol unter **Aktionen** und dann **Entfernen** aus. Wenn Sie Warnungen über den Dienst sehen, der mit dem Laufwerk verbunden ist, warten Sie, bis die bin-Synchronisierung abgeschlossen ist, und entfernen Sie dann das Laufwerk.
2. Führen Sie die folgenden Schritte durch, um den Laufwerkausfall zu überprüfen und die protokollierten Ereignisse anzuzeigen, die mit dem Laufwerksausfall verbunden sind:
   a. Melden Sie sich an der IPMI-Schnittstelle des Knotens an (IDRAC in diesem Fall).
   b. Wählen Sie **Wartung** > **Systemereignisprotokoll** aus, um den Grund für den Laufwerksfehler zu sehen (z. B. SSDWOROut oder Laufwerk nicht richtig eingesetzt).

      Sie können auch ein Ereignis mit dem Status des Laufwerks sehen.

   c. Wählen Sie im Menü * Storage* aus und wählen Sie dann **physische Festplatten**.
   d. Suchen Sie die Steckplatznummer des ausgefallenen Laufwerks mithilfe der Seriennummer, die Sie in der Element UI angegeben haben.
3. Entfernen Sie das Laufwerk wie folgt physisch:
   a. Identifizieren Sie die Laufwerkssteckplatznummer im Gehäuse.

      Das folgende Bild zeigt die Vorderseite des Servers mit der für jedes Laufwerk angezeigten Steckplatznummerierung:

   a. Drücken Sie die Taste auf dem Laufwerk.

      Die Verriegelung tritt aus.

   b. Ziehen Sie das Laufwerk physisch aus dem Steckplatz heraus.

      Stellen Sie sicher, dass Sie Laufwerke sehr sorgfältig behandeln.

4. Setzen Sie das Ersatzlaufwerk ein, indem Sie das Laufwerk mithilfe der Verriegelung vorsichtig in den Steckplatz schieben und die Verriegelung schließen.

   Das Laufwerk wird eingeschaltet, wenn es richtig eingesetzt wird.

5. Überprüfen Sie die neuen Laufwerkdetails im iDRAC:
   a. Wählen Sie **Wartung** > **Systemereignisprotokoll**. Sie sehen ein Ereignis, das für das hinzugefügte Laufwerk protokolliert ist.
   b. Wählen Sie im Menü * Storage* aus und wählen Sie dann **physische Festplatten**.
   c. Vergewissern Sie sich, dass das neue Laufwerk, das Sie eingesetzt haben, in dem entsprechenden Steckplatz in der UI angezeigt wird.
   d. Um die Seriennummer des Laufwerks zu finden, wählen Sie das **+** -Symbol neben jedem PCIe SSD aus.

6. Fügen Sie die neuen Laufwerksinformationen in das hinzu `sf_sds_config.yaml` Datei für den Knoten, in dem Sie das Laufwerk ersetzt haben.

   Der `sf_sds_config.yaml` Datei wird in gespeichert `/opt/sf/`. Diese Datei enthält alle Informationen über die Laufwerke im Node. Jedes Mal, wenn Sie ein Laufwerk ersetzen, müssen Sie die Ersatzlaufwerk-Informationen in dieser Datei eingeben. Weitere Informationen zu dieser Datei finden Sie unter "Inhalt der datei sf_sds_config.yaml".

   a. Stellen Sie mit PuTTY eine SSH-Verbindung zum Knoten her.
   b. Geben Sie im Fenster PuTTY-Konfiguration den Knoten MIP im Feld **Hostname (oder IP-Adresse)** ein.
   c. Wählen Sie **Offen**.
   d. Melden Sie sich im sich öffnenden Terminalfenster mit Ihrem Benutzernamen und Passwort an.
   e. Führen Sie die aus `# cat /opt/sf/sf_sds_config.yaml` Befehl zum Auflisten des Inhalts der Datei.
   f. Ersetzen Sie die Einträge im `dataDevices` Oder `cacheDevices` Listen für das Laufwerk, das Sie durch die neuen Laufwerksinformationen ersetzt haben.
   g. Laufen `# systemctl start solidfire-update-drives`.

      Nach der Ausführung dieses Befehls wird die Bash-Eingabeaufforderung angezeigt. Danach sollten Sie zur Element UI wechseln, um das Laufwerk zum Cluster hinzuzufügen. Die Element-UI zeigt eine Warnmeldung für ein neues Laufwerk an, das verfügbar ist.

7. Wählen Sie **Cluster** > **Laufwerke** > **Verfügbar**.

   Sie sehen die Seriennummer des neuen Laufwerks, das Sie installiert haben.

8. Wählen Sie das Symbol unter **Aktionen** und dann **Hinzufügen** aus.
9. Aktualisieren Sie die Element-UI, nachdem der Synchronisationsauftrag für den Block abgeschlossen ist. Sie sehen, dass die Warnung über das verfügbare Laufwerk gelöscht wurde, wenn Sie auf die Seite **ausgeführte Aufgaben** auf der Registerkarte **Reporting** der Element-Benutzeroberfläche zugreifen.

Ersetzen Sie ein Cache-Laufwerk

Führen Sie dieses Verfahren durch, wenn Sie das Cache-Laufwerk im SolidFire ESDS-Cluster ersetzen möchten. Das Cache-Laufwerk ist mit Metadaten-Services verknüpft. Auf der Seite Element UI **Cluster** > **Drives** werden die Informationen zum Laufwerksverschleiß angezeigt.

Was Sie benötigen

- Stellen Sie über die NetApp Element Software-UI sicher, dass der Cluster in einem guten Zustand ist und es keine Warnungen oder Cluster-Fehler gibt. Sie können über die Management Virtual IP (MVIP)-Adresse des primären Cluster-Knotens auf die Element-UI zugreifen.
- Stellen Sie sicher, dass auf dem Cluster keine aktiven Jobs ausgeführt werden.
- Stellen Sie sicher, dass Sie sich mit allen Schritten vertraut gemacht haben.
- Vergewissern Sie sich, dass Sie die Metadaten-Services von der Element UI entfernen.
- Stellen Sie sicher, dass Sie die erforderlichen Vorsichtsmaßnahmen treffen, um elektrostatische Entladung (ESD) beim Umgang mit Laufwerken zu verhindern.

Schritte

1. Führen Sie die folgenden Schritte in der Element UI aus:
   a. Wählen Sie in der Element-UI die Option **Cluster** > **Nodes** > **aktiv** aus.
   b. Notieren Sie sich die Node-ID und die Management-IP-Adresse des Nodes, in dem Sie das Cache-Laufwerk ersetzen.
   c. Wenn das Cache-Laufwerk gesund ist und Sie es proaktiv ersetzen, wählen Sie **Aktive Laufwerke**, suchen Sie das Metadatenlaufwerk und entfernen Sie es aus der UI.

      Nachdem Sie es entfernt haben, geht das Metadatenlaufwerk zuerst in den **removing** Status und dann in **available**.

   d. Wenn Sie nach dem Ausfall des Cache-Laufwerks einen Austausch durchführen, befindet sich das Metadatenlaufwerk im Status **verfügbar** und wird unter **Cluster** > **Laufwerke** > **verfügbar** aufgelistet.
   e. Wählen Sie in der Element UI die Option **Cluster** > **Laufwerke** > **aktiv**.
   f. Wählen Sie das Metadatenlaufwerk aus, das dem NodeName zugeordnet ist, wo Sie das Cache-Laufwerk ersetzen möchten.
   g. Wählen Sie **Massenaktionen** > **Entfernen**. Nachdem Sie das Laufwerk entfernt haben, wechselt das Laufwerk in den Zustand **Entfernen**. Er bleibt eine Weile im Status **Entfernen** und wartet darauf, dass die Daten auf dem Laufwerk synchronisiert oder auf die übrigen Laufwerke im Cluster verteilt werden. Nach dem Entfernen des Laufwerks wechselt das Laufwerk in den Status **verfügbar**.
2. Führen Sie die folgenden Schritte durch, um den Laufwerkschacht des Cache-Laufwerks zu finden, das Sie ersetzen:
   a. Melden Sie sich an der IPMI-Schnittstelle des Knotens an (iDRAC in diesem Fall).
   b. Wählen Sie im Menü * Storage* aus und wählen Sie dann **physische Festplatten**.
   c. Suchen Sie das Cache-Laufwerk.

      Cache-Laufwerke haben eine geringere Kapazität (375 GB) als Speicherlaufwerke und sind PCIe-SSDs.

   d. Suchen Sie nach der Steckplatznummer, die für das Cache-Laufwerk aufgeführt ist.

      Dies ist der physische Steckplatz, aus dem Sie das Laufwerk entfernen sollten.
3. Nachdem Sie das Laufwerk identifiziert haben, entfernen Sie es nun physisch wie folgt:
   a. Identifizieren Sie die Laufwerkssteckplatznummer im Gehäuse.

      Das folgende Bild zeigt die Vorderseite des Servers mit der für jedes Laufwerk angezeigten Steckplatznummerierung:

   b. Drücken Sie die Taste auf dem Laufwerk.

      Die Verriegelung tritt aus.

   c. Ziehen Sie das Laufwerk physisch aus dem Steckplatz heraus.

Stellen Sie sicher, dass Sie Laufwerke sehr sorgfältig behandeln.

Nachdem Sie das Laufwerk physisch entfernt haben, ändert sich der Laufwerkszustand in der Element-UI in **failed**.

4. Notieren Sie sich die Modellnummer und die ISN (Seriennummer) des neuen Cache-Laufwerks.
5. Setzen Sie das Ersatzlaufwerk ein, indem Sie das Laufwerk mithilfe der Verriegelung vorsichtig in den Steckplatz schieben und die Verriegelung schließen.

   Das Laufwerk wird eingeschaltet, wenn es richtig eingesetzt wird.

6. Führen Sie die folgenden Schritte durch, um die neuen Laufwerkdetails in iDRAC zu überprüfen:
   a. Wählen Sie **Wartung** > **Systemereignisprotokoll**. Sie sehen ein Ereignis, das für das hinzugefügte Laufwerk protokolliert ist.
   b. Wählen Sie im Menü * Storage* aus und wählen Sie dann **physische Festplatten**.
   c. Vergewissern Sie sich, dass das neue Laufwerk, das Sie eingesetzt haben, in dem entsprechenden Steckplatz in der UI angezeigt wird.
   d. Um die Seriennummer des Laufwerks zu finden, wählen Sie das **+** -Symbol neben jedem PCIe SSD aus.
7. Fügen Sie die Informationen zum neuen Cache-Laufwerk in das ein `sf_sds_config.yaml` Datei für den Knoten, in dem Sie das Laufwerk ersetzt haben.

   Der `sf_sds_config.yaml` Datei wird in gespeichert `/opt/sf/`. Diese Datei enthält alle Informationen über die Laufwerke im Node. Jedes Mal, wenn Sie ein Laufwerk ersetzen, sollten Sie die Informationen zum Ersatzlaufwerk in dieser Datei eingeben. Weitere Informationen zu dieser Datei finden Sie unter "Inhalt der datei sf_sds_config.yaml".

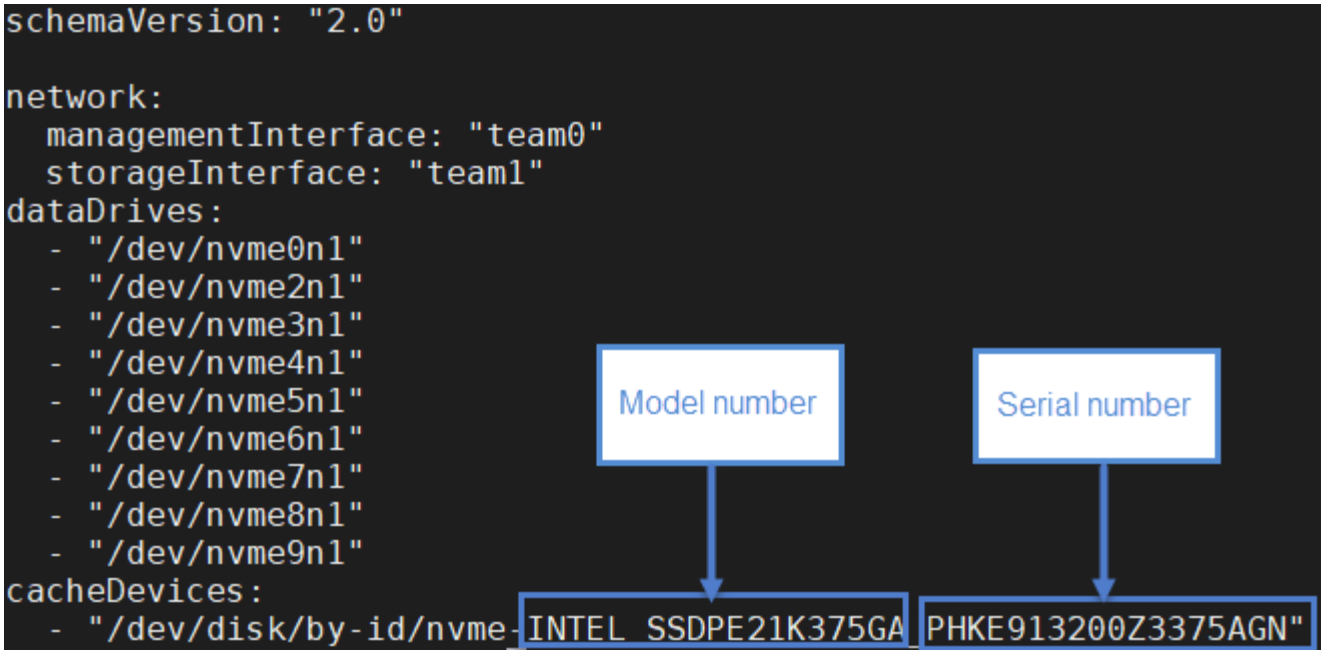
   a. Stellen Sie mit PuTTY eine SSH-Verbindung zum Knoten her.
   b. Geben Sie im Konfigurationsfenster von PuTTY die Knoten-MIP-Adresse (die Sie zuvor von der Element UI zur Kenntnis genommen haben) im Feld **Hostname (oder IP-Adresse)** ein.
   c. Wählen Sie **Offen**.
   d. Melden Sie sich im sich öffnenden Terminalfenster mit Ihrem Benutzernamen und Passwort an.
   e. Führen Sie die aus `nvme list` Befehl zum Auflisten der NMVe-Geräte.

      Sie können die Modellnummer und die Seriennummer des neuen Cache-Laufwerks sehen. Die folgende Beispielausgabe finden Sie unter:

```
Node             SN                   Model                                    Namespace Usage                      Format           FW Rev
---------------- -------------------- ---------------------------------------- --------- -------------------------- ---------------- --------
/dev/nvme0n1     PHLJ029506A54P0DGN   INTEL SSDPE2KX040T8                      1           4.00  TB /   4.00  TB    512   B +  0 B   VDV10131
/dev/nvme1n1     PHKE914000063 75AGN  INTEL SSDPE21K375GA                      1         375.08  GB / 375.08  GB    512   B +  0 B   E2010435
/dev/nvme2n1     PHLJ030004VJ4P0DGN   INTEL SSDPE2KX040T8                      1           4.00  TB /   4.00  TB    512   B +  0 B   VDV10131
/dev/nvme3n1     PHLJ029507NB4P0DGN   INTEL SSDPE2KX040T8                      1           4.00  TB /   4.00  TB    512   B +  0 B   VDV10131
/dev/nvme4n1     PHLJ030004W84P0DGN   INTEL SSDPE2KX040T8                      1           4.00  TB /   4.00  TB    512   B +  0 B   VDV10131
/dev/nvme5n1     PHLJ030101RS4P0DGN   INTEL SSDPE2KX040T8                      1           4.00  TB /   4.00  TB    512   B +  0 B   VDV10131
/dev/nvme6n1     PHLJ029509QX4P0DGN   INTEL SSDPE2KX040T8                      1           4.00  TB /   4.00  TB    512   B +  0 B   VDV10131
/dev/nvme7n1     PHLJ030101S44P0DGN   INTEL SSDPE2KX040T8                      1           4.00  TB /   4.00  TB    512   B +  0 B   VDV10131
/dev/nvme8n1     PHLJ029509QZ4P0DGN   INTEL SSDPE2KX040T8                      1           4.00  TB /   4.00  TB    512   B +  0 B   VDV10131
/dev/nvme9n1     PHLJ030101RW4P0DGN   INTEL SSDPE2KX040T8                      1           4.00  TB /   4.00  TB    512   B +  0 B   VDV10131
```

   f. Fügen Sie die Informationen zum neuen Cache-Laufwerk in hinzu `/opt/sf/sf_sds_config.yaml`.

      Sie sollten die Modellnummer und Seriennummer des vorhandenen Cache-Laufwerks durch die entsprechenden Informationen für das neue Cache-Laufwerk ersetzen. Das folgende Beispiel zeigt:



a. Speichern Sie die `/opt/sf/sf_sds_config.yaml` Datei:

8. Führen Sie die für Sie relevanten Schritte für das Szenario aus:

Szenario	Schritte
Das neue eingelegte Cache-Laufwerk wird angezeigt, nachdem Sie den ausgeführt haben `nvme list` Befehl	a. Laufen `# systemctl restart solidfire`. Dies dauert etwa drei Minuten. b. Prüfen Sie die `solidfire` Status durch Ausführen `system status solidfire`. c. Fahren Sie mit Schritt 9 fort.
Das neue eingelegte Cache-Laufwerk wird nicht angezeigt, nachdem Sie den ausgeführt haben `nvme list` Befehl	a. Booten Sie den Node neu. b. Überprüfen Sie, nachdem der Node neu gebootet wurde, dass der `solidfire` Dienste werden ausgeführt, indem Sie sich beim Knoten (mit PuTTY) anmelden und den ausführen `system status solidfire` Befehl. c. Fahren Sie mit Schritt 9 fort.

Neustart `solidfire` Oder beim Neubooten des Node werden einige Cluster-Fehler verursacht, die in etwa fünf Minuten behoben werden.

9. Fügen Sie in der Element UI das Metadatenlaufwerk hinzu, das Sie entfernt haben:
   a. Wählen Sie **Cluster** > **Laufwerke** > **Verfügbar**.
   b. Wählen Sie das Symbol unter Aktionen aus, und wählen Sie **Hinzufügen**.
10. Aktualisieren Sie die Element-UI, sobald der Synchronisationsauftrag für den Block abgeschlossen ist.

    Es wird angezeigt, dass die Meldung über das verfügbare Laufwerk zusammen mit anderen Cluster-Fehlern beseitigt wurde.

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Sammelt Containerprotokolle

Erfahren Sie mehr über die ESDS-Container von SolidFire und wo Sie die zugehörigen Protokolle abrufen können. Die hier angegebenen Informationen sollen Ihnen bei den ersten Schritten helfen, Protokolle zur Fehlerbehebung zu sammeln. Am besten engagieren "NetApp Support", Wo ausgebildete Ingenieure gut vertraut mit Protokollanalyse kann helfen, Probleme zu lösen.

SolidFire ESDS umfasst die folgenden Container:

- Element Container (`element`): Beherbergt alle Element-Services in einem einzelnen Container.
- Element auth Container (`element_auth`): Bietet Multi-Faktor-Authentifizierung (MFA) und Session-Authentifizierungs-Tokens für die Management-UIs.
- Netzwerk-Watchdog-Container (`sfnetwd`): Bietet Heartbeat-Überwachung der lokalen Elementinstanz und Failover der virtuellen IPs (MVIP und SVIP).

Um über SSH auf die Container auf einem ESDS-Knoten zuzugreifen, sollte der Eigentümer des Knotens SSH aktivieren und die Anmeldedaten angeben. Nachdem Sie SSH-Zugriff auf das Host-System haben, können Sie den Status eines oder mehrerer Container mithilfe der überprüfen `podman ps` Befehl. Siehe das folgende Beispiel:

```
# podman ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
f6b8817c024a localhost/solidfire-element:12.2.0.777 --config /sf/etc/...
11 seconds ago Up 10 seconds ago sfnetwd
c3fed6141259 localhost/solidfire-auth:12.2.0.777 --config /sf/etc/... 11
seconds ago Up 11 seconds ago element_auth
1ffa8289c701 localhost/solidfire-element:12.2.0.777 --config /sf/etc/...
12 seconds ago Up 12 seconds ago element
#
```

Wenn einer der Container nicht verfügbar ist oder nicht ausgeführt wird, verwenden Sie Podman nicht, um die Container direkt zu steuern (Stopp oder Start). Element Software wird über das gesteuert `solidfire systemd` Serviceeinheit. Dieser Service verwendet `elementctl` Zur Orchestrierung der Software, die in den drei Element Containern ausgeführt wird Wird Verwendet `systemctl` Um den SolidFire Service auf dem Host zu steuern, ist die empfohlene und unterstützte Methode zum Starten und Stoppen der Element Software auf einem beliebigen Node. Allerdings sollten die Vorgänge auf einem Live-Cluster nur unter den Anleitungen des Supports ausgeführt werden.

Alle Protokolle im Zusammenhang mit SolidFire ESDS finden Sie in `/var/log/solidfire/` Auf dem Host, der über Container-Instanzen hinweg erhalten bleibt. Dieses Verzeichnis enthält die Protokolle aus dem Elementcontainer und enthält das `element_auth/` Und `sfnetwd/` Unterverzeichnisse, die die Protokolle aus

dem enthalten `element_auth` Und `sfnetwd` Container. Innerhalb eines Containers können Sie bei auf Container-spezifische Protokolle zugreifen `/var/log`.

Verwenden Sie die Benutzeroberfläche von NetApp Hybrid Cloud Control zum Erfassen von Protokollen

Sie können Protokolle zusammen, die an den NetApp Support gesendet werden, um Hilfe bei der Diagnose von Problemen mit Ihren SolidFire ESDS Clustern zu erhalten.

Beachten Sie bei der Protokollsammlung die folgenden Überlegungen:

- Verwenden Sie keine Podman-Befehle, um Protokolle zu sammeln.
- NetApp Support verwendet eine Erfassung für die Erfassung der Host-Protokolle. Für einen optimalen Support sollten Sie eine Collect installiert haben.

Schritte

1. Öffnen Sie die IP-Adresse des Management-Node in einem Webbrowser. Beispiel:

   ```
   https://[management node IP address]
   ```

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie im Dashboard oben rechts das Menü aus.
4. Wählen Sie **Protokolle Sammeln**.
5. Wählen Sie im Dropdown-Menü **Datumsbereich** einen Datumsbereich aus, um festzulegen, welche Daten die Protokolle enthalten sollen.

   Wenn Sie ein benutzerdefiniertes Startdatum angeben, können Sie das Datum auswählen, um den Datumsbereich zu beginnen. Protokolle werden von diesem Datum bis zur aktuellen Zeit gesammelt.

6. Wählen Sie im Abschnitt **Protokollsammlung** den Speicher-Cluster oder bestimmte Speicherknoten aus.
7. Wählen Sie **Protokolle sammeln**, um die Protokollsammlung zu starten.

   Die Protokollerfassung wird im Hintergrund ausgeführt, und auf der Seite wird der Fortschritt angezeigt.

   > ⓘ Abhängig von den gesammelten Protokollen bleibt der Fortschrittsbalken möglicherweise für einige Minuten bei einem bestimmten Prozentsatz oder läuft an einigen Punkten sehr langsam voran.

8. Wählen Sie **Protokolle herunterladen**, um das Protokollpaket herunterzuladen.

   Das Protokollpaket befindet sich in einem komprimierten UNIX `.tgz` Dateiformat.

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Links zu KB-Artikeln zur Fehlerbehebung

Finden Sie die Links zu den Knowledgebase-Artikeln, um Hilfe bei der Fehlerbehebung Ihres SolidFire ESDS-Systems zu erhalten.

- "So machen Sie Schnittstellennamen für alle Nodes in einem Cluster gleich (Anmeldung erforderlich)"
- "Ändern der MTU-Größe (Anmeldung erforderlich)"
- "So lösen Sie Probleme mit dem Absturz von Podman-Containern (Anmeldung erforderlich)"
- "Deaktivieren von IPv6 für SolidFire ESDS (Anmeldung erforderlich)"
- "So ändern Sie die gebundenen Schnittstellen in einem ESDS-Cluster während der Produktion (Anmeldung erforderlich)"

Dies ist keine umfassende Liste. Sie können die durchsuchen "Knowledgebase" Für weitere Artikel.

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Inhalt der datei sf_sds_config.yaml

Jeder Node verfügt über eine `sf_sds_config.yaml` Datei, die die Liste der Hardware enthält, die Sie angeben, die von den ESDS-Diensten von SolidFire verwendet werden soll. Nachdem Sie ein Laufwerk ersetzt haben, sollten Sie die Informationen zum Ersatzlaufwerk in dieser Datei für den Node hinzufügen, von dem Sie das Laufwerk ersetzt haben. Diese Datei wird in gespeichert `/opt/sf/`. Diese Datei enthält alle Informationen über die Laufwerke im Node. Sie sollten die Details des neuen Laufwerks in dieser Datei jedes Mal eingeben, wenn Sie ein neues Laufwerk hinzufügen.

Hier finden Sie den **erforderlichen** Inhalt der Datei:

Taste	Standard	Typ	Beschreibung
SchemaVersion	„2.0“	Zeichenfolge	Die Nummer der Schemaversion für die Datei.
Netzwerk	1. A.	Liste	Zulässige Werte: ManagementInterface,StorageInterface

Taste	Standard	Typ	Beschreibung
Management-Schnittstelle	„Team0“	Zeichenfolge	Der Name der vorkonfigurierten, redundanten Hostbetriebnetzwerkschnittstelle, die für den Management- und Cluster-Managementdatenverkehr verwendet werden soll.
Storage Interface	„team1“	Zeichenfolge	Der Name der vorkonfigurierten, redundanten Hostbetriebssystem-Netzwerkschnittstelle für den Speichernetzwerkdatenverkehr (iSCSI-Datenverkehr).
Datenlaufwerke	1. A.	Liste	Die Liste der Host-Betriebssystempfade zu physischen Speichergeräten, die von SolidFire ESDS verwendet werden. Sie können dies als vollständige Pfade zum Block- oder NVME-Gerät angeben. Die folgenden vollständigen Pfadbeispiele werden unterstützt: /Dev/Disk/by-id/wwn-xxxx-xxxx-xxxx-BEISPIEL, /dev/Disk/by-UUID/nvme-xxxx-xxxxx-EXAMPLE und /dev/sda1

Taste	Standard	Typ	Beschreibung
Cache-Geräte	1. A.	Liste	Der Host-OS-Pfad zum physischen Gerät, das von SolidFire ESDS als Cache-Gerät verwendet wird. Sie sollten es als Listeneintrag angeben. Das folgende Beispiel zeigt einen unterstützten vollständigen Pfad: /Dev/Disk/by-id/nvme-nvme.8086-XXXXXXX-XXXXX-XXXXX-XXXXXXXX-EXAMPLE

Weitere Informationen

- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"