



Storage einrichten

Element Software

NetApp
March 01, 2023

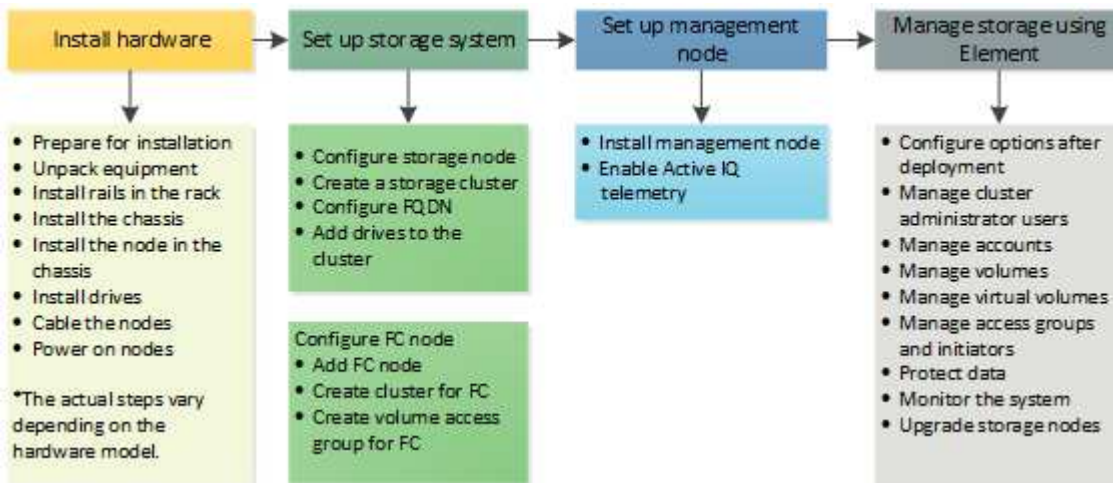
Inhaltsverzeichnis

- Setup-Übersicht 1
- Weitere Informationen 1
- Einrichten eines Clusters mit Element Storage Nodes 1
- Einrichten eines Clusters mit Fibre Channel Nodes 7
- Ermitteln der zu installierenden SolidFire-Komponenten 11
- Richten Sie einen Management-Node ein 12
- Konfigurieren Sie vollständig qualifizierten Domännennamen Web UI-Zugriff 12
- Was kommt als Nächstes 17

Setup-Übersicht

An diesem Punkt sollten Sie die Hardware installiert haben. Die Hardware beinhaltet auch die Element Software.

Als Nächstes müssen Sie das Storage-System für Ihre Umgebung einrichten. Sie können ein Cluster mit Storage-Nodes oder Fibre Channel Nodes einrichten und es über Element Software managen, nachdem Sie Nodes in einer Höheneinheit installiert und verkabeln und dann wieder einschalten.



Schritte zur Einrichtung von Speicher

1. Wählen Sie eine der folgenden Optionen:
 - "Richten Sie ein Cluster mit Storage Nodes ein"
 - "Richten Sie das Cluster mit Fibre Channel Nodes ein"
2. "Ermitteln der zu installierenden SolidFire-Komponenten"
3. "Einrichten eines Management-Node und Aktivieren der Active IQ Telemetrie"

Weitere Informationen

- "Erfahren Sie mehr über die nächsten Schritte zur Storage-Nutzung"
- "Seite „SolidFire und Element Ressourcen“"

Einrichten eines Clusters mit Element Storage Nodes

Sie können ein Cluster mit Storage-Nodes einrichten und mithilfe von Element Software managen, nachdem Sie Nodes in einer Höheneinheit installiert und verkabeln und dann wieder einschalten. Anschließend können Sie zusätzliche Komponenten in Ihrem Speichersystem installieren und konfigurieren.

Schritte

1. "Konfigurieren Sie einen Storage-Node"
2. "Erstellen eines Storage-Clusters"
3. "Melden Sie sich bei der Benutzeroberfläche der Element Software an"

4. "Fügen Sie dem Cluster Laufwerke hinzu"
5. "Ermitteln der zu installierenden SolidFire-Komponenten"
6. "Richten Sie einen Management-Node ein"

Weitere Informationen

- "Seite „SolidFire und Element Ressourcen“"

Konfigurieren Sie einen Storage-Node

Sie müssen einzelne Nodes konfigurieren, bevor Sie sie einem Cluster hinzufügen können. Nachdem Sie einen Knoten in einer Rack-Einheit installiert und verkabeln und einschalten, können Sie die Knotennetzeinstellungen über die UI pro Node oder die Node Terminal User Interface (TUI) konfigurieren. Stellen Sie sicher, dass Sie über die erforderlichen Netzwerkkonfigurationsinformationen für den Node verfügen, bevor Sie fortfahren.

Es gibt zwei Optionen für die Konfiguration von Speicher-Nodes:

- **UI pro Node:** Verwenden Sie die Pro-Node-Benutzeroberfläche (https://<node_management_IP>:442) So konfigurieren Sie die Node-Netzeinstellungen.
- **TUI:** Verwenden Sie die Node Terminal User Interface (TUI), um den Knoten zu konfigurieren.

Sie können einem Cluster keinen Node mit DHCP-zugewiesenen IP-Adressen hinzufügen. Über die DHCP-IP-Adresse können Sie den Node zunächst in der UI, der TUI oder der API pro Node konfigurieren. Während dieser Erstkonfiguration können Sie statische IP-Adressinformationen hinzufügen, damit Sie den Node zu einem Cluster hinzufügen können.

Nach der Erstkonfiguration können Sie mit der Management-IP-Adresse des Node auf den Node zugreifen. Anschließend können Sie die Node-Einstellungen ändern, zu einem Cluster hinzufügen oder einen Cluster mit dem Node erstellen. Zudem können Sie mithilfe von Element Software-API-Methoden einen neuen Node konfigurieren.



Ab Element Version 11.0 können Nodes mit IPv4, IPv6 oder beiden Adressen für ihr Managementnetzwerk konfiguriert werden. Dies gilt sowohl für Storage-Nodes als auch für Management-Nodes, mit Ausnahme von Management-Node 11.3 und höher, der IPv6 nicht unterstützt. Wenn Sie ein Cluster erstellen, kann für das MVIP nur eine einzelne IPv4- oder IPv6-Adresse verwendet werden, und der entsprechende Adresstyp muss auf allen Knoten konfiguriert werden.

Konfigurieren Sie einen Storage-Node über die UI pro Node

Sie können Nodes über die Benutzeroberfläche pro Node konfigurieren.

Über diese Aufgabe

- Sie können den Node so konfigurieren, dass er eine IPv4- oder eine IPv6-Adresse hat.
- Sie benötigen die in der TUI angezeigte DHCP-Adresse, um auf einen Knoten zugreifen zu können. Sie können einem Cluster keine DHCP-Adressen verwenden, um einen Node hinzuzufügen.



Sie sollten die Management-Schnittstellen (Bond1G) und Storage-Schnittstellen (Bond10G) für separate Subnetze konfigurieren. Bond1G- und Bond10G-Schnittstellen für dasselbe Subnetz verursachen Routing-Probleme, wenn Storage Traffic über die Bond1G-Schnittstelle gesendet wird. Wenn Sie dasselbe Subnetz für Management und Storage-Verkehr verwenden müssen, konfigurieren Sie den Management-Traffic manuell, um die Bond10G-Schnittstelle zu verwenden. Dies können Sie für jeden Knoten mithilfe der **Cluster-Einstellungen**-Seite der Pro-Node-Benutzeroberfläche tun.

Schritte

1. Geben Sie in einem Browser-Fenster die DHCP-IP-Adresse eines Node ein.

Sie müssen die Erweiterung hinzufügen : 442 Um auf den Node zuzugreifen, z. B. <https://172.25.103.6:442>.

Die Registerkarte **Network Settings** wird mit dem Abschnitt **Bond1G** geöffnet.

2. Geben Sie die 1G-Verwaltungsnetzwerkeinstellungen ein.
3. Klicken Sie Auf **Änderungen Übernehmen**.
4. Klicken Sie auf **Bond10G**, um die Einstellungen des 10G-Speichernetzwerks anzuzeigen.
5. Geben Sie die Einstellungen für das 10G-Speichernetzwerk ein.
6. Klicken Sie Auf **Änderungen Übernehmen**.
7. Klicken Sie Auf **Cluster-Einstellungen**.
8. Geben Sie den Hostnamen für das 10G-Netzwerk ein.
9. Geben Sie den Cluster-Namen ein.



Dieser Name muss der Konfiguration für alle Nodes hinzugefügt werden, bevor ein Cluster erstellt werden kann. Alle Nodes in einem Cluster müssen identische Cluster-Namen aufweisen. Bei Cluster-Namen wird die Groß-/Kleinschreibung berücksichtigt.

10. Klicken Sie Auf **Änderungen Übernehmen**.

Konfigurieren Sie über die TUI einen Storage-Node

Über die Terminal User Interface (TUI) können Sie die Erstkonfiguration neuer Knoten vornehmen.

Sie sollten die Bond1G (Management)- und Bond10G (Storage)-Schnittstellen für separate Subnetze konfigurieren. Bond1G- und Bond10G-Schnittstellen für dasselbe Subnetz verursachen Routing-Probleme, wenn Storage Traffic über die Bond1G-Schnittstelle gesendet wird. Wenn Sie dasselbe Subnetz für Management und Storage-Verkehr verwenden müssen, konfigurieren Sie den Management-Traffic manuell, um die Bond10G-Schnittstelle zu verwenden. Dies können Sie für jeden Knoten mithilfe der Seite **Cluster > Knoten** der Element-Benutzeroberfläche tun.

Schritte

1. Schließen Sie eine Tastatur und einen Monitor an den Knoten an, und schalten Sie den Knoten ein.

Das NetApp Storage Main Menu der TUI erscheint auf dem tty1 Terminal.



Wenn der Knoten den Konfigurationsserver nicht erreichen kann, zeigt die TUI eine Fehlermeldung an. Überprüfen Sie die Verbindung des Konfigurationsservers oder die Netzwerkverbindung, um den Fehler zu beheben.

2. Wählen Sie **Netzwerk > Netzwerkkonfiguration**.



Um durch das Menü zu navigieren, drücken Sie die nach-oben- oder nach-unten-Taste. Um zu einer anderen Schaltfläche oder zu den Feldern von den Schaltflächen zu wechseln, drücken Sie **Tab**. Um zwischen Feldern zu navigieren, verwenden Sie die nach-oben- oder nach-unten-Pfeiltasten.

3. Wählen Sie **Bond1G (Management)** oder **Bond10G (Storage)** aus, um die 1G- und 10G-Netzwerkeinstellungen für den Node zu konfigurieren.
4. Drücken Sie für die Felder „Bond Mode“ und „Status“ die Taste **Tab**, um die Schaltfläche „Hilfe“ auszuwählen und die verfügbaren Optionen zu ermitteln.

Alle Nodes in einem Cluster müssen identische Cluster-Namen aufweisen. Bei Cluster-Namen wird die Groß-/Kleinschreibung berücksichtigt. Wenn im Netzwerk ein DHCP-Server mit verfügbaren IP-Adressen ausgeführt wird, wird im Feld Adresse die 1-GbE-Adresse angezeigt.

5. Drücken Sie **Tab**, um die **OK**-Taste auszuwählen und die Änderungen zu speichern.

Der Node wird in einen ausstehenden Status versetzt, und er kann einem vorhandenen oder einem neuen Cluster hinzugefügt werden.

Weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Erstellen eines Storage-Clusters

Sie können ein Storage-Cluster erstellen, nachdem Sie alle einzelnen Nodes konfiguriert haben. Wenn Sie ein Cluster erstellen, wird automatisch ein Cluster-Administrator-Benutzerkonto für Sie erstellt. Der Clusteradministrator verfügt über die Berechtigung zum Verwalten aller Clusterattribute und kann andere Cluster-Administratorkonten erstellen.

Was Sie benötigen

- Sie haben den Management-Node installiert.
- Sie haben alle einzelnen Nodes konfiguriert.

Über diese Aufgabe

Während der Konfiguration eines neuen Node werden jedem Node 1-GB- oder 10-GB-Management-IP-Adressen (MIP) zugewiesen. Sie müssen eine der bei der Konfiguration erstellten Node-IP-Adressen verwenden, um die Seite Neues Cluster erstellen zu öffnen. Die verwendete IP-Adresse hängt vom Netzwerk ab, das Sie für das Cluster-Management ausgewählt haben.






Wenn Sie Cluster-weit aktivieren möchten "[Softwareverschlüsselung für Daten im Ruhezustand](#)" Bei SolidFire All-Flash-Storage-Clustern müssen Sie dies während der Cluster-Erstellung tun. Ab Element 12.5 müssen Sie während der Cluster-Erstellung in der UI „Cluster erstellen“ die Softwareverschlüsselung im Ruhezustand aktivieren. Für Element 12.3.x und früher müssen Sie den Cluster mithilfe der erstellen "[CreateCluster erstellen](#)" API-Methode und ändern Sie den `enableSoftwareVerschlüsselungAtRest`-Parameter in `true`. Die Softwareverschlüsselung im Ruhezustand ist für SolidFire ESDS Cluster standardmäßig aktiviert. Bei All-Flash-Storage-Clustern von SolidFire und SolidFire ESDS-Clustern kann die Verschlüsselung von Software im Ruhezustand auf dem Cluster nicht deaktiviert werden. Das können Sie "[Aktivieren und deaktivieren Sie](#)" Hardwarebasierte Verschlüsselung für Daten im Ruhezustand nach der Cluster-Erstellung

Beim Erstellen eines neuen Clusters müssen folgende Aspekte berücksichtigt werden:



- Wenn Sie Storage-Nodes in einem gemeinsam genutzten Chassis nutzen, sollte möglicherweise der Entwurf für eine Ausfallsicherung auf Chassis-Ebene mithilfe der Schutz-Domänen-Funktion in Betracht gezogen werden.
- Wenn ein freigegebenes Gehäuse nicht verwendet wird, können Sie ein benutzerdefiniertes Schutz-Domain-Layout definieren.

Schritte

1. Geben Sie in einem Browser-Fenster ein `https://MIP:443`, wobei MIP die Management-Node-IP-Adresse ist.
2. Geben Sie unter Erstellen eines neuen Clusters die folgenden Informationen ein:
 - Management-VIP: Routingfähige virtuelle IP im 1-GbE- oder 10-GbE-Netzwerk für Netzwerk-Management-Aufgaben.
 -  Sie können ein neues Cluster mit einer IPv4- oder IPv6-Adresse erstellen.
 - iSCSI (Storage) VIP: Virtuelle IP im 10-GbE-Netzwerk für Storage und iSCSI-Erkennung.
 -  Sie können den MVIP-, SVIP- oder Cluster-Namen nicht ändern, nachdem Sie den Cluster erstellt haben.
 - Benutzername: Der primäre Clusteradministrator-Benutzername für authentifizierten Zugriff auf das Cluster. Sie müssen den Benutzernamen für die zukünftige Referenz speichern.
 -  Sie können Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern für den Benutzernamen und das Passwort verwenden.
 - Passwort: Passwort für authentifizierten Zugriff auf das Cluster. Sie müssen das Kennwort für die spätere Referenz speichern. Standardmäßig ist die zwei-Wege-Datensicherung aktiviert. Sie können diese Einstellung nicht ändern.
3. Lesen Sie die Endbenutzer-Lizenzvereinbarung und wählen Sie **Ich stimme zu**.
4. **Optional**: Stellen Sie in der Liste Knoten sicher, dass die Kontrollkästchen für Knoten, die nicht im Cluster enthalten sein sollen, nicht ausgewählt sind.
5. Wählen Sie **Cluster Erstellen**.

Das System kann je nach Anzahl der Nodes im Cluster mehrere Minuten dauern, bis der Cluster erstellt

wurde. In einem ordnungsgemäß konfigurierten Netzwerk sollte ein kleines Cluster mit fünf Nodes weniger als eine Minute dauern. Nach dem Erstellen des Clusters wird das Fenster Erstellen eines neuen Clusters an die MVIP-URL-Adresse für den Cluster umgeleitet und die Element-UI angezeigt.

Finden Sie weitere Informationen

- ["Storage-Management mit der Element API"](#)
- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Greifen Sie auf die Benutzeroberfläche der Element Software zu

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

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

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

Schritte

1. Folgenden Optionen wählbar:

- IPv6: Geben Sie ein `https://[IPv6_MVIP_address]`. Beispiel:

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

- IPv4: Geben Sie ein `https://[IPv4_MVIP_address]`. Beispiel:

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

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

Finden Sie weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Fügen Sie Laufwerke zu einem Cluster hinzu

Wenn Sie dem Cluster einen Node hinzufügen oder neue Laufwerke in einem vorhandenen Node installieren, werden die Laufwerke automatisch nach Verfügbarkeit registriert. Sie müssen die Laufwerke zum Cluster entweder über die Element-UI oder -API hinzufügen, bevor sie am Cluster teilnehmen können.

Laufwerke werden in der Liste Verfügbare Laufwerke nicht angezeigt, wenn folgende Bedingungen vorliegen:

- Laufwerke befinden sich im Status „aktiv“, „Entfernen“, „Löschen“ oder „Fehlgeschlagen“.
- Der Knoten, von dem das Laufwerk Teil ist, befindet sich im Status „Ausstehend“.

Schritte

1. Wählen Sie in der Element-Benutzeroberfläche **Cluster > Laufwerke** aus.
2. Klicken Sie auf **verfügbar**, um die Liste der verfügbaren Laufwerke anzuzeigen.
3. Führen Sie einen der folgenden Schritte aus:
 - Um einzelne Laufwerke hinzuzufügen, klicken Sie auf das **Aktionen** -Symbol für das Laufwerk, das Sie hinzufügen möchten, und klicken Sie auf **Hinzufügen**.
 - Um mehrere Laufwerke hinzuzufügen, aktivieren Sie die Kontrollkästchen der Laufwerke, die hinzugefügt werden sollen, klicken Sie auf **Massenaktionen** und klicken Sie auf **Hinzufügen**.

```
== Find more information
* https://www.netapp.com/data-storage/solidfire/documentation[SolidFire and Element Resources page^]
* https://docs.netapp.com/us-en/vcp/index.html[NetApp Element Plug-in for vCenter Server^]
```

Einrichten eines Clusters mit Fibre Channel Nodes

Sie können ein Cluster mit Fibre Channel Nodes einrichten und es mithilfe der Element Software managen, nachdem Sie Nodes in einer Höheneinheit installiert und verkabeln und dann wieder einschalten. Anschließend können Sie zusätzliche Komponenten in Ihrem Speichersystem installieren und konfigurieren.

Schritte

1. ["Konfigurieren Sie einen Fibre Channel-Node"](#)
2. ["Erstellen Sie ein neues Cluster mit Fibre Channel Nodes"](#)
3. ["Fügen Sie einem Cluster Fibre Channel Nodes hinzu"](#)
4. ["Einrichten von Zonen für Fibre Channel-Nodes"](#)
5. ["Erstellen einer Volume-Zugriffsgruppe für Fibre Channel-Clients"](#)
6. ["Ermitteln der zu installierenden SolidFire-Komponenten"](#)
7. ["Richten Sie einen Management-Node ein"](#)

Weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)

Konfigurieren Sie einen Fibre Channel-Node

Mit Fibre Channel Nodes können Sie das Cluster mit einer Fibre Channel-Netzwerkstruktur verbinden. Fibre Channel Nodes werden paarweise hinzugefügt und im

aktiv/aktiv-Modus betrieben (alle Nodes verarbeiten aktiv den Datenverkehr für das Cluster). Cluster, die Element Softwareversion 9.0 und höher ausführen, unterstützen bis zu vier Nodes. Cluster mit früheren Versionen unterstützen maximal zwei Nodes.

Sie müssen sicherstellen, dass die folgenden Bedingungen erfüllt sind, bevor Sie einen Fibre Channel-Node konfigurieren:

- Mindestens zwei Fibre Channel Nodes sind mit Fibre Channel Switches verbunden.
- Alle SolidFire Fibre Channel-Ports sollten mit Ihrem Fibre Channel Fabric verbunden sein. Die vier SolidFire-Bond10G-Netzwerkverbindungen sollten an eine LACP-Bond-Gruppe auf Switch-Ebene angeschlossen werden. Dies ermöglicht die beste Gesamt-Performance der Fibre Channel-Systeme.
- Prüfen und Validieren aller Best Practices für Fibre Channel Cluster in diesem NetApp Knowledge Base Artikel

["Best Practice für SolidFire FC Cluster"](#)

Für Fibre Channel Nodes und Storage Nodes sind die Schritte für Netzwerk- und Cluster-Konfiguration identisch.

Wenn Sie einen neuen Cluster mit Fibre Channel Nodes und SolidFire Storage Nodes erstellen, sind die WWPN-Adressen (Worldwide Port Name) für die Nodes in der Element UI verfügbar. Sie können die WWPN-Adressen verwenden, um den Fibre Channel-Switch zu Zone.

WWPNs sind im System registriert, wenn Sie ein neues Cluster mit Nodes erstellen. In der Element UI finden Sie die WWPN-Adressen in der Spalte WWPN der Registerkarte FC-Ports, auf die Sie über die Registerkarte Cluster zugreifen.

Weitere Informationen

[Fügen Sie einem Cluster Fibre Channel Nodes hinzu](#)

[Erstellen Sie ein neues Cluster mit Fibre Channel Nodes](#)

Erstellen Sie ein neues Cluster mit Fibre Channel Nodes

Sie können ein neues Cluster erstellen, nachdem Sie die einzelnen Fibre Channel Nodes konfiguriert haben. Wenn Sie ein Cluster erstellen, wird automatisch ein Cluster-Administrator-Benutzerkonto für Sie erstellt. Der Clusteradministrator verfügt über die Berechtigung zum Verwalten aller Clusterattribute und kann andere Cluster-Administratorkonten erstellen.

Während der Konfiguration eines neuen Node werden jedem Node 1-GB- oder 10-GB-Management-IP-Adressen (MIP) zugewiesen. Sie müssen eine der bei der Konfiguration erstellten Node-IP-Adressen verwenden, um die Seite Neues Cluster erstellen zu öffnen. Die verwendete IP-Adresse hängt vom Netzwerk ab, das Sie für das Cluster-Management ausgewählt haben.

Was Sie benötigen

Sie haben die einzelnen Fibre Channel Nodes konfiguriert.

Schritte

1. Geben Sie in einem Browserfenster eine Knoten-MIP-Adresse ein.

2. Geben Sie unter Erstellen eines neuen Clusters die folgenden Informationen ein:

- Management-VIP: Routingfähige virtuelle IP im 1-GbE- oder 10-GbE-Netzwerk für Netzwerk-Management-Aufgaben.
- iSCSI (Storage) VIP: Virtuelle IP im 10-GbE-Netzwerk für Storage und iSCSI-Erkennung.



Sie können SVIP nicht ändern, nachdem Sie das Cluster erstellt haben.

- Benutzername: Der primäre Clusteradministrator-Benutzername für authentifizierten Zugriff auf das Cluster. Sie müssen den Benutzernamen für die zukünftige Referenz speichern.



Sie können Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern für den Benutzernamen verwenden.

- Passwort: Passwort für authentifizierten Zugriff auf das Cluster. Sie müssen den Benutzernamen für die zukünftige Referenz speichern. Standardmäßig ist die zwei-Wege-Datensicherung aktiviert. Sie können diese Einstellung nicht ändern.

3. Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Ich stimme zu**.

4. **Optional:** Stellen Sie in der Liste Knoten sicher, dass die Kontrollkästchen für Knoten, die nicht im Cluster enthalten sein sollen, nicht ausgewählt sind.

5. Klicken Sie Auf **Cluster Erstellen**.

Das System kann je nach Anzahl der Nodes im Cluster mehrere Minuten dauern, bis der Cluster erstellt wurde. In einem ordnungsgemäß konfigurierten Netzwerk sollte ein kleines Cluster mit fünf Nodes weniger als eine Minute dauern. Nach dem Erstellen des Clusters wird das Fenster Erstellen eines neuen Clusters an die MVIP-URL-Adresse für den Cluster umgeleitet und die Web-UI angezeigt.

Weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Fügen Sie einem Cluster Fibre Channel Nodes hinzu

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

Die Softwareversion auf jedem Fibre Channel-Knoten in einem Cluster muss kompatibel sein. Wenn Sie einem Cluster einen Fibre Channel Node hinzufügen, installiert das Cluster nach Bedarf die Cluster-Version des Elements auf dem neuen Node.

Schritte

1. Wählen Sie **Cluster > Knoten**.
2. Klicken Sie auf **Ausstehend**, um die Liste der ausstehenden Knoten anzuzeigen.
3. Führen Sie einen der folgenden Schritte aus:

- Um einzelne Knoten hinzuzufügen, klicken Sie auf das Symbol **Aktionen** für den Knoten, den Sie hinzufügen möchten.
- Um mehrere Knoten hinzuzufügen, aktivieren Sie das Kontrollkästchen der Knoten, die hinzugefügt werden sollen, und dann **Massenaktionen**.



Wenn der Node, den Sie hinzufügen, eine andere Version des Elements als die im Cluster ausgeführte Version hat, aktualisiert der Cluster den Node asynchron an die Version des Elements, das auf dem Cluster-Master ausgeführt wird. Nach der Aktualisierung des Node wird er sich automatisch dem Cluster hinzugefügt. Während dieses asynchronen Prozesses befindet sich der Knoten im hängenden Zustand aktiv.

4. Klicken Sie Auf **Hinzufügen**.

Der Node wird in der Liste der aktiven Nodes angezeigt.

Weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Einrichten von Zonen für Fibre Channel-Nodes

Wenn Sie einen neuen Cluster mit Fibre Channel-Nodes und SolidFire-Storage-Nodes erstellen, sind die WWPN-Adressen (Worldwide Port Name) für die Nodes in der Web-Benutzeroberfläche verfügbar. Sie können die WWPN-Adressen verwenden, um den Fibre Channel-Switch zu Zone.

WWPNs sind im System registriert, wenn Sie ein neues Cluster mit Nodes erstellen. In der Element UI finden Sie die WWPN-Adressen in der Spalte WWPN der Registerkarte FC-Ports, auf die Sie über die Registerkarte Cluster zugreifen.

Weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Erstellen einer Volume-Zugriffsgruppe für Fibre Channel-Clients

Volume-Zugriffsgruppen ermöglichen die Kommunikation zwischen Fibre Channel Clients und Volumes auf einem SolidFire Storage-System. Das Zuordnen von Fibre Channel-Client-Initiatoren (WWPN) zu den Volumes einer Volume-Zugriffsgruppe ermöglicht den sicheren Daten-I/O zwischen einem Fibre Channel-Netzwerk und einem SolidFire Volume.

Sie können auch iSCSI-Initiatoren zu einer Volume-Zugriffsgruppe hinzufügen. Dadurch können die Initiatoren auf dieselben Volumes in der Volume-Zugriffsgruppe zugreifen.

Schritte

1. Klicken Sie Auf **Verwaltung > Zugriffsgruppen**.

2. Klicken Sie Auf **Zugriffsgruppe Erstellen**.
3. Geben Sie im Feld **Name** einen Namen für die Zugriffsgruppe des Volumes ein.
4. Wählen Sie die Fibre Channel-Initiatoren aus der Liste **Unbound Fibre Channel Initiatoren** aus, und fügen Sie sie hinzu.



Sie können Initiatoren zu einem späteren Zeitpunkt hinzufügen oder löschen.

5. **Optional:** Wählen und fügen Sie einen iSCSI-Initiator aus der Liste **Initiatoren** hinzu.
6. So hängen Sie Volumes an die Zugriffsgruppe an:
 - a. Wählen Sie ein Volume aus der Liste **Volumes** aus.
 - b. Klicken Sie Auf **Volumen Anhängen**.
7. Klicken Sie Auf **Zugriffsgruppe Erstellen**.

Weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Ermitteln der zu installierenden SolidFire-Komponenten

Vielleicht möchten Sie je nach Konfiguration und Bereitstellung prüfen, welche SolidFire Komponenten wie Management-Node, Active IQ und NetApp Monitoring Agent (NMA) installiert werden sollten.

In der folgenden Tabelle sind die zusätzlichen Komponenten aufgeführt und gibt an, ob diese installiert werden sollen.

Komponente	Standalone SolidFire Storage-Cluster	NetApp HCI Cluster
Management-Node	Empfehlenswert	Standardmäßig installiert, erforderlich
Active IQ	Empfohlen*	Empfohlen*
NetApp Monitoring Agent	Nicht unterstützt	Empfehlenswert

*Active IQ ist für kapazitätslizenzierte SolidFire Storage Cluster erforderlich.

Schritte

1. Ermitteln Sie, welche Komponenten installiert werden sollen.
2. Führen Sie die Installation gemäß der durch ["Installieren Sie den Management-Node"](#) Verfahren.



Verwenden Sie zum Einrichten von Active IQ den `--telemetry_active` Parameter im Setup-Skript, um die Datenerfassung für die Analyse durch Active IQ zu ermöglichen.

3. Informationen zu NetApp Monitoring Agent finden Sie hier ["Verfahren"](#).

Finden Sie weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Richten Sie einen Management-Node ein

Sie können den NetApp Element Software-Management-Node (mNode) installieren, um Upgrades durchzuführen und Systemservices bereitzustellen, Cluster-Ressourcen und -Einstellungen zu managen, Systemtests und Dienstprogramme auszuführen und den NetApp Support-Zugriff zur Fehlerbehebung zu aktivieren.

1. Siehe ["Installieren Sie den Management-Node"](#) Dokumentation.



Verwenden Sie zum Einrichten von Active IQ den `--telemetry_active` Parameter im Setup-Skript, um die Datenerfassung für die Analyse durch Active IQ zu ermöglichen.

Weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Konfigurieren Sie vollständig qualifizierten Domännennamen Web UI-Zugriff

Mit SolidFire All-Flash-Speicher mit NetApp Element Software 12.2 oder höher können Sie unter Verwendung des vollständig qualifizierten Domain-Namens (FQDN) auf Webschnittstellen des Speicherclusters zugreifen. Wenn Sie den FQDN für den Zugriff auf Webbenutzerschnittstellen wie die Element-Web-UI, die Benutzeroberfläche per Node oder die Management-Node-Benutzeroberfläche verwenden möchten, müssen Sie zuerst eine Speichercluster-Einstellung hinzufügen, um den vom Cluster verwendeten FQDN zu identifizieren.

Durch diesen Prozess kann das Cluster eine Anmeldesitzung ordnungsgemäß umleiten und die Integration in externe Services wie Schlüsselmanager und Identitätsanbieter für die Multi-Faktor-Authentifizierung verbessern.

Was Sie benötigen

- Diese Funktion erfordert Element 12.2 oder höher.
- Für die Konfiguration dieser Funktion mit NetApp Hybrid Cloud Control REST-APIs sind Management-Services 2.15 oder höher erforderlich.
- Für die Konfiguration dieser Funktion mit der NetApp Hybrid Cloud Control UI sind Management-Services ab 2.19 erforderlich.
- Zur Verwendung VON REST-APIs müssen Sie einen Management-Node mit Version 11.5 oder höher

bereitgestellt haben.

- Sie benötigen vollqualifizierte Domain-Namen für den Management-Node und jeden Storage-Cluster, die korrekt zur Management Node-IP-Adresse und den einzelnen Storage-Cluster-IP-Adressen auflösen.

Über NetApp Hybrid Cloud Control und DIE REST-API können Sie den FQDN-Webbenutzerzugriff konfigurieren oder entfernen. Sie können auch Fehler bei falsch konfigurierten FQDNs beheben.

- [Konfigurieren Sie den FQDN-Web-UI-Zugriff mit NetApp Hybrid Cloud Control](#)
- [Konfigurieren Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API](#)
- [Entfernen Sie FQDN Web-UI-Zugriff mit NetApp Hybrid Cloud Control](#)
- [Entfernen Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API](#)
- [Fehlerbehebung](#)

Konfigurieren Sie den FQDN-Web-UI-Zugriff mit NetApp Hybrid Cloud Control

Schritte

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

```
https://<ManagementNodeIP>
```

2. Melden Sie sich bei NetApp Hybrid Cloud Control an, indem Sie die Anmeldedaten des Storage-Cluster-Administrators bereitstellen.
3. Wählen Sie das Menüsymbol oben rechts auf der Seite aus.
4. Wählen Sie **Konfigurieren**.
5. Wählen Sie im Fenster **vollqualifizierte Domänennamen** die Option **Einrichtung** aus.
6. Geben Sie im daraufhin angezeigten Fenster die FQDNs für den Managementknoten und jeden Speichercluster ein.
7. Wählen Sie **Speichern**.

Im Fensterbereich **Fully Qualified Domain Names** werden alle Speichercluster mit dem zugehörigen MVIP und FQDN aufgelistet.



Nur verbundene Speichercluster mit dem FQDN-Satz werden im Fensterbereich **vollqualifizierte Domänennamen** aufgeführt.

Konfigurieren Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API

Schritte

1. Stellen Sie sicher, dass die Element-Speicherknoten und der mNode für die Netzwerkumgebung richtig konfiguriert sind, damit FQDNs in der Umgebung aufgelöst werden können. Um DNS einzustellen, wechseln Sie zur Benutzeroberfläche für Speicherknoten pro Knoten und zum Managementknoten und wählen Sie dann **Netzwerkeinstellungen > Managementnetzwerk** aus.
 - a. UI pro Node für Storage-Nodes: https://<storage_node_management_IP>:442
 - b. UI pro Node für den Management-Node: https://<management_node_IP>:442

2. Ändern Sie die Storage-Cluster-Einstellungen mithilfe der Element API.
- a. Greifen Sie auf die Element API zu, und erstellen Sie mithilfe der die folgende Clusterschnittstelle "**CreateClusterSchnittstellenPräferenz**" API-Methode, Einfügen des Clusters MVIP FQDN für den Vorzugswert:

- Name: `mvip_fqdn`
- Wert: Fully Qualified Domain Name for the Cluster MVIP

In diesem Beispiel ist FQDN=`storagecluster.my.org`:

```
https://<Cluster_MVIP>/json-rpc/12.2?  
method=CreateClusterInterfacePreference&name=mvip_fqdn&value=storageclus  
ter.my.org
```

3. Ändern Sie die Management-Node-Einstellungen mit der REST-API auf dem Management-Node:

- a. Rufen Sie die REST-API-UI für den Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/2/`

Beispiel:

```
https://<management_node_IP>/mnode/2/
```

- a. Klicken Sie auf **authorize** oder ein Schloss-Symbol und geben Sie den Cluster-Benutzernamen und das Passwort ein.
- b. Geben Sie die Client-ID als ein `mnode-client`.
- c. Klicken Sie auf **autorisieren**, um die Sitzung zu starten und dann das Fenster zu schließen.
- d. Wählen Sie in der Liste Server die Option aus `mnode2`.
- e. Klicken Sie auf **GET /settings**.
- f. Klicken Sie auf **Probieren Sie es aus**.
- g. Klicken Sie Auf **Ausführen**.
- h. Notieren Sie alle Proxyeinstellungen, die im Antwortkörper gemeldet wurden.
 - i. Klicken Sie auf **PUT/settings**.
 - j. Klicken Sie auf **Probieren Sie es aus**.
- k. Geben Sie im Bereich Text anfordern den Management-Node FQDN als Wert für das ein `mnode_fqdn` Parameter.
 - l. Geben Sie alle Proxy-Einstellungswerte ein, die Sie zuvor in den verbleibenden Parametern im Anforderungskörper aufgezeichnet haben. Wenn Sie die Proxyparameter leer lassen oder nicht in den Text der Anforderung aufnehmen, werden die vorhandenen Proxyeinstellungen entfernt.
- m. Klicken Sie Auf **Ausführen**.

Entfernen Sie FQDN Web-UI-Zugriff mit NetApp Hybrid Cloud Control

Mit diesem Verfahren können Sie den FQDN-Webzugriff für den Managementknoten und die Speichercluster entfernen.

Schritte

1. Wählen Sie im Fenster **vollqualifizierte Domännennamen** die Option **Bearbeiten** aus.
2. Löschen Sie im resultierenden Fenster den Inhalt im Textfeld **FQDN**.
3. Wählen Sie **Speichern**.

Das Fenster wird geschlossen, und der FQDN wird nicht mehr im Bereich **Fully Qualified Domain Names** aufgeführt.

Entfernen Sie den FQDN-Webbenutzerzugriff mithilfe der REST-API

Schritte

1. Ändern Sie die Storage-Cluster-Einstellungen mithilfe der Element API.
 - a. Greifen Sie auf die Element API zu und löschen Sie mithilfe der die folgende Clusterschnittstelle `DeleteClusterInterfacePreference` API-Methode:

- Name: `mvip_fqdn`

Beispiel:

```
https://<Cluster_MVIP>/json-rpc/12.2?method=DeleteClusterInterfacePreference&name=mvip_fqdn
```

2. Ändern Sie die Management-Node-Einstellungen mit der REST-API auf dem Management-Node:
 - a. Rufen Sie die REST-API-UI für den Management-Node auf, indem Sie die IP-Adresse des Management-Node, gefolgt von, eingeben `/mnode/2/`. Beispiel:

```
https://<management_node_IP>/mnode/2/
```

- b. Wählen Sie **authorize** oder ein Schloss-Symbol aus und geben Sie den Benutzernamen und das Kennwort des Element Clusters ein.
- c. Geben Sie die Client-ID als ein `mnode-client`.
- d. Wählen Sie **autorisieren**, um eine Sitzung zu starten.
- e. Schließen Sie das Fenster.
- f. Wählen Sie **PUT /settings**.
- g. Wählen Sie **Probieren Sie es aus**.
- h. Geben Sie im Bereich des Anforderungskörpers keinen Wert für das ein `mnode_fqdn` Parameter. Geben Sie außerdem an, ob der Proxy verwendet werden soll (`true` Oder `false`) Für die `use_proxy` Parameter.

```

{
  "mnode_fqdn": "",
  "use_proxy": false
}

```

i. Wählen Sie **Ausführen**.

Fehlerbehebung

Wenn FQDNs falsch konfiguriert sind, können Sie Probleme beim Zugriff auf den Managementknoten, einen Speichercluster oder beide haben. Verwenden Sie die folgenden Informationen, um die Fehlerbehebung zu unterstützen.

Problem	Ursache	Auflösung
<ul style="list-style-type: none"> • Beim Versuch, entweder mit dem FQDN auf den Management-Node oder den Speicher-Cluster zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse nicht entweder beim Management-Node oder beim Storage-Cluster einloggen. 	Der FQDN des Managementknoten und der FQDN des Speicherclusters sind beide falsch konfiguriert.	Verwenden Sie die REST-API-Anweisungen auf dieser Seite, um die FQDN-Einstellungen des Management-Nodes und Speicherclusters zu entfernen und erneut zu konfigurieren.
<ul style="list-style-type: none"> • Beim Versuch, auf den Speicher-Cluster-FQDN zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse nicht entweder beim Management-Node oder beim Storage-Cluster einloggen. 	Der FQDN des Managementknoten ist richtig konfiguriert, der Speichercluster-FQDN ist jedoch falsch konfiguriert.	Mithilfe der REST-API-Anweisungen auf dieser Seite können Sie die FQDN-Einstellungen des Speicherclusters entfernen und erneut konfigurieren
<ul style="list-style-type: none"> • Beim Versuch, auf den Verwaltungsknoten FQDN zuzugreifen, wird ein Browserfehler angezeigt. • Sie können sich mit einer IP-Adresse beim Management-Node und Storage-Cluster einloggen. 	Der FQDN des Managementknoten ist falsch konfiguriert, der Speichercluster-FQDN ist jedoch korrekt konfiguriert.	Melden Sie sich bei NetApp Hybrid Cloud Control an, um die FQDN-Einstellungen des Managementknoten in der UI zu korrigieren, oder VERWENDEN Sie die REST-API-Anweisungen auf dieser Seite, um die Einstellungen zu korrigieren.

Weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Was kommt als Nächstes

Nachdem Sie Element Software eingerichtet haben, managen Sie Storage, indem Sie einige der folgenden Optionen ausführen:

- ["Greifen Sie auf die Benutzeroberfläche der Element Software zu"](#)
- ["Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen"](#)
- ["Konten verwalten"](#)
- ["Management des Systems"](#)
- ["Management von Volumes und virtuellen Volumes"](#)
- ["Sichern Sie Ihre Daten"](#)
- ["Fehler im System beheben"](#)

Weitere Informationen

- ["Seite „SolidFire und Element Ressourcen“"](#)
- ["Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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