Konfigurieren Sie Cluster-Einstellungen

Element Software

NetApp
April 17, 2024

This PDF was generated from https://docs.netapp.com/de-de/element-software/storage/task_system_manage_cluster_enable_and_disable_encryption_for_a_cluster.html on April 17, 2024. Always check docs.netapp.com for the latest.

Inhalt

Konfigurieren Sie Cluster-Einstellungen . . . 1
Weitere Informationen . . . 1
Aktivieren und deaktivieren Sie die Verschlüsselung für ein Cluster im Ruhezustand . . . 1
Legen Sie den Schwellenwert für den vollen Cluster fest . . . 3
Aktivieren und deaktivieren Sie den Zugriff auf den Support . . . 3
Banner für Nutzungsbedingungen verwalten . . . 3
Legen Sie das Network Time Protocol fest . . . 5
SNMP managen . . . 6
Verwalten Sie Laufwerke . . . 8
Managen von Nodes . . . 10
Zeigen Sie Details zu Fibre Channel-Ports an . . . 13
Managen Sie virtuelle Netzwerke . . . 14

Konfigurieren Sie Cluster-Einstellungen

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

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

Optionen

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

Weitere Informationen

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

Aktivieren und deaktivieren Sie die Verschlüsselung für ein Cluster im Ruhezustand

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

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

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

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

Was Sie benötigen

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

Überprüfen Sie den Status der Verschlüsselung im Ruhezustand

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

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

Optionen

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

Hardwarebasierte Verschlüsselung für Daten im Ruhezustand

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

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

Softwarebasierte Verschlüsselung im Ruhezustand aktivieren

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

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

Deaktivieren Sie die hardwarebasierte Verschlüsselung für Daten im Ruhezustand

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

Weitere Informationen

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

Legen Sie den Schwellenwert für den vollen Cluster fest

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

Was Sie benötigen

Sie müssen über Administratorrechte für den Cluster verfügen.

Schritte

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

Weitere Informationen

"Wie werden die BlockSpace Schwellenwerte für Element berechnet"

Aktivieren und deaktivieren Sie den Zugriff auf den Support

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

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

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

Banner für Nutzungsbedingungen verwalten

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

Optionen

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

Aktivieren Sie das Banner für Nutzungsbedingungen

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

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

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

   Überschreiten Sie maximal 4096 Zeichen.

3. Klicken Sie Auf **Aktivieren**.

Bearbeiten Sie den Banner für Nutzungsbedingungen

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

Was Sie benötigen

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

Schritte

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

   Überschreiten Sie maximal 4096 Zeichen.

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

Deaktivieren Sie den Banner für die Nutzungsbedingungen

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

Was Sie benötigen

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

Schritte

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

Legen Sie das Network Time Protocol fest

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

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

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

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

Konfigurieren Sie NTP auf dem Cluster, um auf einen lokalen NTP-Server zu verweisen. Sie können die IP-Adresse oder den FQDN-Hostnamen verwenden. Der NTP-Standardserver zum Erstellungszeitpunkt des Clusters ist auf us.pool.ntp.org eingestellt. Es kann jedoch nicht immer eine Verbindung zu diesem Standort hergestellt werden, abhängig vom physischen Standort des SolidFire Clusters.

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

Sie können bis zu fünf verschiedene NTP-Server eingeben.

Sie können IPv4- und IPv6-Adressen verwenden.

Was Sie benötigen

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

Schritte

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

Weitere Informationen

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

Konfigurieren Sie das Cluster, um NTP-Broadcasts abzuhören

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

Was Sie benötigen

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

Schritte

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

Weitere Informationen

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

SNMP managen

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

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

Sie können IPv4- und IPv6-Adressen verwenden.

SNMP-Details

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

- **SNMP MIBs**

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

- **Allgemeine SNMP-Einstellungen**

  Sie können SNMP aktivieren oder deaktivieren. Nachdem Sie SNMP aktiviert haben, können Sie wählen, welche Version verwendet werden soll. Wenn Sie Version 2 verwenden, können Sie Anfragesteller

hinzufügen, und wenn Sie Version 3 verwenden, können Sie USM-Benutzer einrichten.

- **SNMP-Trap-Einstellungen**

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

Konfigurieren eines SNMP-Anforderers

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

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

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

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

Weitere Informationen

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

Konfigurieren eines SNMP-USM-Benutzers

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

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

Konfigurieren Sie SNMP-Traps

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

überwachen.

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

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

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

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

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

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

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

Schritte

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

Verwalten Sie Laufwerke

Jeder Node enthält mindestens ein physisches Laufwerk, für das ein Teil der Daten für

das Cluster gespeichert wird. Das Cluster verwendet die Kapazität und Performance des Laufwerks, nachdem das Laufwerk erfolgreich zu einem Cluster hinzugefügt wurde. Sie können die Element UI zum Managen von Laufwerken verwenden.

Finden Sie weitere Informationen

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

Laufwerke für Details

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

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

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

- **Fahrausweis**

  Die dem Laufwerk zugewiesene sequenzielle Nummer.

- **Knoten-ID**

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

- **Knotenname**

  Der Name des Knotens, der das Laufwerk beherbergt.

- **Slot**

  Die Steckplatznummer, in der sich das Laufwerk befindet.

- * Kapazität*

  Die Größe des Laufwerks, in GB.

- **Seriell**

  Die Seriennummer des Laufwerks.

- **Tragen Sie Rest**

  Die Verschleißanzeige.

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

oder schließen und neu laden, um die Informationen zu aktualisieren.

- **Typ**

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

Managen von Nodes

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

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

Weitere Informationen

Fügen Sie einem Cluster einen Node hinzu

Fügen Sie einem Cluster einen Node hinzu

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

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

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

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

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

Sie können NetApp HCI Appliances Nodes hinzufügen.

Schritte

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

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

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

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

   Der Node wird in der Liste der aktiven Nodes angezeigt.

Weitere Informationen

Node-Versionierung und -Kompatibilität

Node-Versionierung und -Kompatibilität

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

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

- **Major**

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

- **Klein**

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

- **Mikro**

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

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

Kapazität des Clusters in einer gemischten Node-Umgebung

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

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

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

Je nach Element Softwareversion werden die folgenden SF-Series Storage-Nodes nicht unterstützt:

Beginnt mit…	Storage-Node nicht unterstützt…
Element 12.7	• SF2405 • SF9608
Element 12.0	• SF3010 • SF6010 • SF9010

Wenn Sie versuchen, einen dieser Knoten auf eine nicht unterstützte Elementversion zu aktualisieren, wird ein Fehler angezeigt, der angibt, dass dieser Knoten nicht von Element 12.x unterstützt wird

Zeigen Sie Node-Details an

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

Schritte

1. Klicken Sie Auf **Cluster** > **Knoten**.
2. Um die Details für einen bestimmten Knoten anzuzeigen, klicken Sie auf das Symbol **Aktionen** für einen Knoten.

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

Zeigen Sie Details zu Fibre Channel-Ports an

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

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

Schritte

1. Klicken Sie auf **Cluster** > **FC-Ports**.
2. Um Informationen auf dieser Seite zu filtern, klicken Sie auf **Filter**.
3. Überprüfen Sie die Details:
   - **Knoten-ID**: Der Knoten, der die Sitzung für die Verbindung hostet.
   - **Knotenname**: Vom System generierter Knotenname.
   - **Steckplatz**: Steckplatznummer, wo sich der Fibre Channel-Port befindet.
   - **HBA-Port**: Physischer Port am Fibre Channel Host Bus Adapter (HBA).
   - **WWNN**: Der World Wide Node Name.

- **WWPN**: Der weltweite Zielname des Ports.
- **Switch WWN**: Der weltweite Name des Fibre Channel Switch.
- **Port State**: Aktueller Zustand des Ports.
- **NPort-ID**: Die Node-Port-ID auf der Fibre Channel Fabric.
- **Geschwindigkeit**: Die ausgehandelte Fibre Channel-Geschwindigkeit. Folgende Werte sind möglich:
  - 4 Gbit/s
  - 8 Gbit/s
  - 16 Gbit/s

Weitere Informationen

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

Managen Sie virtuelle Netzwerke

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

Weitere Informationen

- Fügen Sie ein virtuelles Netzwerk hinzu
- Aktivieren Sie virtuelles Routing und Forwarding
- Bearbeiten eines virtuellen Netzwerks
- VRF-VLANs bearbeiten
- Löschen Sie ein virtuelles Netzwerk

Fügen Sie ein virtuelles Netzwerk hinzu

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

Was Sie benötigen

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

Für diese Konfiguration müssen Sie die folgenden Kriterien berücksichtigen:

- Bei VLANs, die nicht VRF-aktiviert sind, müssen sich Initiatoren in demselben Subnetz wie das SVIP befinden.

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

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

Schritte

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

Details zum virtuellen Netzwerk anzeigen

Schritte

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

Aktivieren Sie virtuelles Routing und Forwarding

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

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

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

Weitere Informationen

Fügen Sie ein virtuelles Netzwerk hinzu

Bearbeiten eines virtuellen Netzwerks

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

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

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

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

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

1. Wählen Sie **Cluster** > **Netzwerk**.
2. Wählen Sie das Aktionen-Symbol für das zu bearbeitende VLAN aus.
3. Wählen Sie **Bearbeiten**.
4. Geben Sie im Dialogfeld **VLAN bearbeiten** die neuen Attribute für das VLAN ein.

5. Wählen Sie **Einen Block hinzufügen** aus, um einen nicht kontinuierlichen Block mit IP-Adressen für das virtuelle Netzwerk hinzuzufügen.
6. Wählen Sie **Änderungen Speichern**.

Link zur Fehlerbehebung in KB-Artikeln

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

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

VRF-VLANs bearbeiten

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

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

Löschen Sie ein virtuelles Netzwerk

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

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

Weitere Informationen

Bearbeiten eines virtuellen Netzwerks

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.