Management des Systems

Element Software

NetApp
March 01, 2023

Inhaltsverzeichnis

Management des Systems

Sie können Ihr System in der Element UI verwalten. Dies ermöglicht die Multi-Faktor-Authentifizierung, das Managen von Cluster-Einstellungen, unterstützt FIPS (Federal Information Processing Standards) und nutzt externes Verschlüsselungsmanagement.

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

Finden Sie weitere Informationen

- "Seite „SolidFire und Element Ressourcen“"
- "NetApp Element Plug-in für vCenter Server"

Multi-Faktor-Authentifizierung aktivieren

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

Richten Sie die Multi-Faktor-Authentifizierung ein

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

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

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

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

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

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

3. Konfigurieren Sie die SAML-Behauptungen auf dem IdP eines Drittanbieters so, dass das Attribut „ `NameID`“ verwendet wird, dass ein Benutzer für die Prüfprotokollierung eindeutig identifiziert wird und dass

Single Logout ordnungsgemäß funktioniert.

4. Erstellen Sie ein oder mehrere Cluster-Administrator-Benutzerkonten, die von einem Drittanbieter-IdP zur Autorisierung authentifiziert wurden, indem Sie die folgende API-Methode aufrufen:`AddIdpClusterAdmin`

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

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

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

Weitere Informationen

- "Seite „SolidFire und Element Ressourcen“"
- "NetApp Element Plug-in für vCenter Server"

Zusätzliche Informationen für Multi-Faktor-Authentifizierung

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

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

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

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

Weitere Informationen

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

Konfigurieren Sie Cluster-Einstellungen

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

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

Optionen

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

Weitere Informationen

- "Seite „SolidFire und Element Ressourcen“"
- "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. Für ESDS-Cluster (SolidFire Enterprise SDS) ist die Softwareverschlüsselung im Ruhezustand standardmäßig aktiviert.

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

- "Ressourcen-Seite zu NetApp SolidFire"
- "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.

Diese Funktion ist in SolidFire Enterprise SDS-Clustern nicht verfügbar.

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.

Diese Funktion ist in SolidFire Enterprise SDS-Clustern nicht verfügbar.

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

- "Seite „SolidFire und Element Ressourcen“"
- "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

- "Seite „SolidFire und Element Ressourcen“"
- "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

- "Seite „SolidFire und Element Ressourcen“"
- "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"

Nodes können zu SolidFire Enterprise SDS-Clustern (SolidFire ESDS) oder zu NetApp HCI Appliances hinzugefügt werden.

SolidFire ESDS-Knoten werden mit einem Node-Typ-Präfix von „`SFC`“ gekennzeichnet, z. B. „`s F.c100.`“

Schritte

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

   Wenn der Vorgang zum Hinzufügen von Knoten (sowohl SolidFire-ESDS als auch nicht-SolidFire-ESDS-Knoten) abgeschlossen ist, werden sie in der Liste Aktive Knoten angezeigt. Bis dahin werden die ausstehenden Knoten in der Liste „Ausstehend aktiv“ angezeigt.

   Bei Knoten, die keine SolidFire ESDS-Knoten sind, installiert SolidFire die Element Softwareversion des Clusters auf den ausstehenden Knoten, 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

- "Seite „SolidFire und Element Ressourcen“"
- "NetApp Element Plug-in für vCenter Server"

Managen Sie virtuelle Netzwerke

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

Weitere Informationen

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

Fügen Sie ein virtuelles Netzwerk hinzu

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

Was Sie benötigen

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

Für diese Konfiguration müssen Sie die folgenden Kriterien berücksichtigen:

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

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

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

Schritte

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

Details zum virtuellen Netzwerk anzeigen

Schritte

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

Aktivieren Sie virtuelles Routing und Forwarding

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

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

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

Weitere Informationen

Fügen Sie ein virtuelles Netzwerk hinzu

Bearbeiten eines virtuellen Netzwerks

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

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

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

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

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

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

virtuelle Netzwerk hinzuzufügen.

6. Wählen Sie **Änderungen Speichern**.

Link zur Fehlerbehebung in KB-Artikeln

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

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

VRF-VLANs bearbeiten

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

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

Löschen Sie ein virtuelles Netzwerk

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

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

Weitere Informationen

Bearbeiten eines virtuellen Netzwerks

Erstellen eines Clusters, das FIPS-Laufwerke unterstützt

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

- "Vermeiden Sie das Kombinieren von Nodes für FIPS-Laufwerke"
- "Verschlüsselung für Daten im Ruhezustand aktivieren"
- "Ermitteln, ob Nodes für die FIPS-Laufwerksfunktion bereit sind"

- "Aktivierung der FIPS-Laufwerksfunktion"
- "Prüfen Sie den FIPS-Laufwerksstatus"
- "Fehlerbehebung für die FIPS-Laufwerksfunktion"

Vermeiden Sie das Kombinieren von Nodes für FIPS-Laufwerke

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

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

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

Verschlüsselung für Daten im Ruhezustand aktivieren

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

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

Weitere Informationen

- Aktivieren und Deaktivieren der Verschlüsselung für ein Cluster
- "Seite „SolidFire und Element Ressourcen“"
- "NetApp Element Plug-in für vCenter Server"

Ermitteln, ob Nodes für die FIPS-Laufwerksfunktion bereit sind

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

Der resultierende Bericht zeigt einen der folgenden Status an:

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

Schritte

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

```
GetFipsReport
```

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

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

Weitere Informationen

- "Seite „SolidFire und Element Ressourcen“"
- "NetApp Element Plug-in für vCenter Server"

Aktivierung der FIPS-Laufwerksfunktion

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

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

Schritt

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

```
EnableFeature params: FipsDrives
```

Weitere Informationen

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

Prüfen Sie den FIPS-Laufwerksstatus

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

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

```
GetFeatureStatus
```

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

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

Weitere Informationen

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

Fehlerbehebung für die FIPS-Laufwerksfunktion

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

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

Weitere Informationen

- Cluster-Fehlercodes
- "Storage-Management mit der Element API"
- "Seite „SolidFire und Element Ressourcen“"
- "NetApp Element Plug-in für vCenter Server"

Aktivieren Sie FIPS 140-2 für HTTPS auf dem Cluster

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

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

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

Weitere Informationen finden Sie unter Element API Informationen.

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

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

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

Weitere Informationen

- SSL-Chiffren
- "Storage-Management mit der Element API"
- "Seite „SolidFire und Element Ressourcen“"
- "NetApp Element Plug-in für vCenter Server"

SSL-Chiffren

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

Die folgenden Listen enthalten die von der Element-Software unterstützten Standard-SSL-Chiffren (Secure Socket Layer) und die SSL-Chiffren, die unterstützt werden, wenn der FIPS 140-2-Modus aktiviert ist:

- **FIPS 140-2 deaktiviert**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A

TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) – C

TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) – A

TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) – A

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (RSA 2048) - A

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (RSA 2048) - A

TLS_RSA_WITH_IDEA_CBC_SHA (RSA 2048) - A

TLS_RSA_WITH_RC4_128_MD5 (RSA 2048) – C

TLS_RSA_WITH_RC4_128_SHA (RSA 2048) – C

TLS_RSA_WITH_SEED_CBC_SHA (RSA 2048) - A

- **FIPS 140-2 aktiviert**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECT571R1) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECT571R1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECT571R1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECT571R1) - A

TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) – C

TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) – A

TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) – A

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A

Weitere Informationen

Aktivieren Sie FIPS 140-2 für HTTPS auf dem Cluster

Erste Schritte mit externem Verschlüsselungsmanagement

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

Nur Softwareverschlüsselung im Ruhezustand ist für SolidFire Enterprise SDS Cluster verfügbar.

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

Weitere Informationen

- "CreateCluster API, die zur Aktivierung der Softwareverschlüsselung im Ruhezustand verwendet werden kann"
- "Ressourcen-Seite zu NetApp SolidFire"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

Externes Verschlüsselungsmanagement einrichten

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

Was Sie benötigen

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

Schritte

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

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

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

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

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

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

Weitere Informationen

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

Verschlüsselung der Software beim Rest-Master-Schlüssel

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

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

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

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

Was Sie benötigen

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

Schritte

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

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

3. Kopieren Sie die `asyncHandle` Wert aus dem `RekeySoftwareEncryptionAtRestMasterKey`

Befehlsantwort.

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

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

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

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

Weitere Informationen

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

Wiederherstellen von nicht zugänglichen oder ungültigen Authentifizierungsschlüsseln

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

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

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

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

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

Schritte zum Löschen:

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

Siehe "Cluster-Fehlercodes" Finden Sie weitere Informationen.

Befehle für externes Verschlüsselungsmanagement-API

Liste aller zur Verwaltung und Konfiguration von EKM verfügbaren APIs.

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

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

Wird zur Definition der spezifischen Details externer kundeneigener Server verwendet:

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

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

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

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