管理您的系統
Element Software

NetApp
November 12, 2025

目錄

管理您的系統

管理您的系統

您可以在 Element 使用者介面中管理系統。這包括啟用多因素身份驗證、管理叢集設定、支援聯邦資訊處理標準 (FIPS) 以及使用外部金鑰管理。

- "啟用多重身份驗證"
- "配置叢集設定"
- "建立支援 FIPS 驅動器的集群"
- "開始使用外部密鑰管理"

更多資訊

- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

啟用多重身份驗證

設定多重身份驗證

多因素身份驗證 (MFA) 使用第三方身分提供者 (IdP) 透過安全性斷言標記語言 (SAML) 來管理使用者會話。 MFA 允許管理員根據需要配置其他身份驗證因素，例如密碼和短信，以及密碼和電子郵件。

您可以使用 Element API 的以下基本步驟來設定叢集以使用多因素身份驗證。

每個 API 方法的詳細資訊可以在以下位置找到： "元素 API 參考"。

1. 透過呼叫以下 API 方法並以 JSON 格式傳遞 IdP 元數據，為叢集建立新的第三方身分提供者 (IdP) 配置：`CreateIdpConfiguration`

   從第三方身分提供者 (IdP) 擷取純文字格式的身分提供者元資料。需要驗證此元數據，以確保其 JSON 格式正確。有許多 JSON 格式化應用程式可供使用，例如： https://freeformatter.com/json-escape.html.

2. 透過 spMetadataUrl 檢索叢集元數據，並透過呼叫以下 API 方法將其複製到第三方身分提供者：`ListIdpConfigurations`

   spMetadataUrl 是一個 URL，用於從叢集中檢索身分提供者 (IdP) 的元數據，以便建立信任關係。

3. 在第三方身分提供者 (IdP) 上設定 SAML 斷言，使其包含「`NameID`」屬性，以便唯一識別使用者進行稽核日誌記錄，並使單點登出功能正常運作。
4. 透過呼叫下列 API 方法，建立一個或多個由第三方身分提供者 (IdP) 進行驗證的叢集管理員使用者帳戶：`AddIdpClusterAdmin`

為了達到預期效果，IdP 叢集管理員的使用者名稱應與 SAML 屬性名稱/值對應相匹配，如下例所示：

- email=bob@company.com — 其中 IdP 配置為在 SAML 屬性中發布電子郵件地址。
- group=cluster-administrator - 其中 IdP 配置為釋放一個群組屬性，所有使用者都應該有權存取該群組屬性。請注意，出於安全考慮，SAML 屬性名稱/值對區分大小寫。

5. 透過呼叫以下 API 方法為叢集啟用 MFA： `EnableIdpAuthentication`

查找更多信息

- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

多因素身份驗證的補充訊息

關於多因素身份驗證，您應該注意以下注意事項。

- 若要刷新不再有效的身分提供者 (IdP) 證書，您需要使用非身分提供者管理員使用者呼叫下列 API 方法： `UpdateIdpConfiguration`
- MFA 與長度小於 2048 位元的憑證不相容。預設情況下，叢集上會建立一個 2048 位元 SSL 憑證。呼叫 API 方法時，應避免設定較小的憑證： `SetSSLCertificate`

如果叢集在升級前使用的憑證小於 2048 位，則升級至 Element 12.0 或更高版本後，必須將叢集憑證更新為 2048 位元或更高版本的憑證。

- IdP 管理員使用者不能直接用於進行 API 呼叫（例如，透過 SDK 或 Postman），也不能用於其他整合（例如，OpenStack Cinder 或 vCenter 外掛程式）。如果需要建立具有這些權限的用戶，請新增 LDAP 叢集管理員用戶或本機叢集管理員用戶。

查找更多信息

- "使用 Element API 管理存儲"
- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

配置叢集設定

啟用和停用叢集的靜態資料加密

使用SolidFire集群，您可以加密儲存在集群驅動器上的所有靜態資料。您可以使用下列任一方式啟用對自加密磁碟機 (SED) 的叢集層級保護"靜態資料採用硬體或軟體加密"。

您可以使用 Element UI 或 API 啟用靜態硬體加密。啟用靜態資料硬體加密功能不會影響叢集的效能或效率。您只能使用 Element API 啟用靜態軟體加密。

在叢集建立期間，預設不會啟用基於硬體的靜態加密，可以透過 Element UI 啟用和停用。

對於SolidFire全快閃儲存集群，必須在建立集群期間啟用靜態軟體加密，且集群建立後不能停用靜態軟體加密。

你需要什麼

- 您擁有叢集管理員權限，可以啟用或變更加密設定。
- 對於基於硬體的靜態加密，在變更加密設定之前，您已確保叢集處於健康狀態。
- 如果要停用加密，則必須有兩個節點參與叢集才能存取金鑰以停用磁碟機上的加密。

檢查靜態加密狀態

若要查看叢集上靜態加密和/或靜態軟體加密的目前狀態，請使用下列方法："獲取集群資訊"方法。你可以使用"取得靜態軟體加密訊息"獲取集群用於加密靜態資料的資訊的方法。

Element軟體使用者介面儀表板 `https://<MVIP>/`目前僅顯示基於硬體的加密的靜態加密狀態。

選項

- [啟用基於硬體的靜態資料加密]
- [啟用靜態資料軟體加密]
- [停用靜態資料的硬體加密]

啟用基於硬體的靜態資料加密

若要使用外部金鑰管理配置啟用靜態加密，您必須透過以下方式啟用靜態加密："API" 。啟用使用現有 Element UI 按鈕後，將恢復使用內部產生的金鑰。

1. 從元素使用者介面中，選擇“集群”>“設定”。
2. 選擇“啟用靜態資料加密”。

啟用靜態資料軟體加密

軟體靜態加密在叢集上啟用後無法停用。

1. 在叢集建立期間，運行"建立集群方法"和 `enableSoftwareEncryptionAtRest`設定為 `true`。

停用靜態資料的硬體加密

1. 從元素使用者介面中，選擇“集群”>“設定”。
2. 選擇“停用靜態資料加密”。

查找更多信息

- "SolidFire和 Element 軟體文檔"
- "NetApp SolidFire和 Element 產品早期版本的文檔"

設定集群滿閾值

您可以使用下列步驟變更系統產生區塊簇已滿警告的等級。此外，您可以使用 ModifyClusterFullThreshold API 方法來變更系統產生區塊或元資料警告的等級。

你需要什麼

您必須擁有叢集管理員權限。

步驟

1. 點選“集群”>“設定”。
2. 在叢集完全設定部分，輸入百分比，表示在 Helix 無法從節點故障中恢復之前剩餘容量為 _% 時發出警告警報。
3. 點選「儲存變更」。

查找更多信息

"元素的區塊空間閾值是如何計算的"

啟用和停用磁碟區負載平衡

從 Element 12.8 開始，您可以使用磁碟區負載平衡，根據每個磁碟區的實際 IOPS 而不是 QoS 策略中配置的最小 IOPS，在節點之間平衡磁碟區。您可以使用 Element UI 或 API 啟用和停用磁碟區負載平衡（預設為停用狀態）。

步驟

1. 選擇“集群”>“設定”。
2. 在「叢集特定」部分，變更卷負載平衡的狀態：

   啟用磁碟區負載平衡

   選擇“啟用基於實際 IOPS 的負載平衡”，並確認您的選擇。

   停用卷宗負載平衡：

   選擇“停用基於實際 IOPS 的負載平衡”，並確認您的選擇。

3. （可選）選擇「報告」>「概覽」以確認「實際 IOPS 餘額」的狀態變更。您可能需要向下捲動叢集健康資訊才能查看狀態。

查找更多信息

- "使用 API 啟用卷負載平衡"
- "使用 API 停用卷負載平衡"
- "建立和管理磁碟區 QoS 策略"

啟用和停用支援訪問

您可以啟用支援存取權限，以便暫時允許NetApp支援人員透過 SSH 存取儲存節點進行故障排除。

您必須擁有叢集管理員權限才能變更支援存取權限。

1. 點選“集群”>“設定”。
2. 在「啟用/停用支援存取權限」部分，輸入您希望允許支援人員存取的持續時間（以小時為單位）。
3. 點選「啟用支援存取權限」。
4. *可選：*若要停用支援存取權限，請按一下「停用支援存取權限」。

管理使用條款橫幅

您可以啟用、編輯或設定包含使用者訊息的橫幅。

選項

[啟用「使用條款」橫幅] [編輯使用條款橫幅] [停用「使用條款」橫幅]

啟用「使用條款」橫幅

您可以啟用「使用條款」橫幅，該橫幅會在使用者登入 Element UI 時顯示。當使用者點擊橫幅時，會出現一個文字對話框，其中包含您為叢集配置的訊息。橫幅可以隨時關閉。

您必須擁有叢集管理員權限才能啟用使用條款功能。

1. 點選「使用者」>「使用條款」。
2. 在「使用條款」表單中，輸入要在「使用條款」對話方塊中顯示的文字。

   請勿超過 4096 個字元。

3. 按一下“啟用”。

編輯使用條款橫幅

您可以編輯使用者選擇「使用條款」登入橫幅時看到的文字。

你需要什麼

- 您必須擁有叢集管理員權限才能設定使用條款。
- 請確保已啟用「使用條款」功能。

步驟

1. 點選「使用者」>「使用條款」。
2. 在「使用條款」對話方塊中，編輯您想要顯示的文字。

   請勿超過 4096 個字元。

3. 點選「儲存變更」。

停用「使用條款」橫幅

您可以關閉「使用條款」橫幅。停用橫幅後，使用者在使用 Element UI 時不再需要接受使用條款。

你需要什麼

- 您必須擁有叢集管理員權限才能設定使用條款。
- 請確保已啟用“使用條款”。

步驟

1. 點選「使用者」>「使用條款」。
2. 按一下“禁用”。

設定網路時間協議

配置叢集要查詢的網路時間協定伺服器

您可以指示叢集中的每個節點向網路時間協定 (NTP) 伺服器查詢更新。叢集僅聯繫已設定的伺服器，並向這些伺服器請求 NTP 資訊。

NTP用於透過網路同步時鐘。連接到內部或外部 NTP 伺服器應該是叢集初始設定的一部分。

在叢集上設定 NTP，使其指向本機 NTP 伺服器。您可以使用 IP 位址或 FQDN 主機名稱。建立叢集時預設的 NTP 伺服器設定為 us.pool.ntp.org；但是，根據SolidFire叢集的實體位置，有時可能無法連線到此網站。

使用 FQDN 取決於各個儲存節點的 DNS 設定是否已就位並正常運作。為此，請在每個儲存節點上設定 DNS 伺服器，並透過查看「網路連接埠要求」頁面確保連接埠已開啟。

您最多可以輸入五個不同的 NTP 伺服器。

你可以同時使用 IPv4 位址和 IPv6 位址。

你需要什麼

您必須擁有叢集管理員權限才能配置此設定。

步驟

1. 在伺服器設定中設定 IP 位址和/或 FQDN 清單。
2. 確保節點上的 DNS 設定正確。
3. 點選“集群”>“設定”。
4. 在“網路時間協定設定”下，選擇“否”，即使用標準 NTP 配置。
5. 點選「儲存變更」。

查找更多信息

- "設定叢集監聽 NTP 廣播"

- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

設定叢集監聽 NTP 廣播

透過使用廣播模式，您可以指示叢集中的每個節點在網路上監聽來自特定伺服器的網路時間協定 (NTP) 廣播訊息。

NTP用於透過網路同步時鐘。連接到內部或外部 NTP 伺服器應該是叢集初始設定的一部分。

你需要什麼

- 您必須擁有叢集管理員權限才能配置此設定。
- 您必須在網路上將 NTP 伺服器設定為廣播伺服器。

步驟

1. 點選“集群”>“設定”。
2. 將使用廣播模式的 NTP 伺服器新增至伺服器清單。
3. 在網路時間協定設定中，選擇「是」以使用廣播用戶端。
4. 若要設定廣播用戶端，請在「伺服器」欄位中輸入您在廣播模式下設定的 NTP 伺服器。
5. 點選「儲存變更」。

查找更多信息

- "配置叢集要查詢的網路時間協定伺服器"
- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

管理 SNMP

了解 SNMP

您可以在叢集中設定簡單網路管理協定 (SNMP)。

您可以選擇 SNMP 請求者、選擇要使用的 SNMP 版本、識別 SNMP 基於用戶的安全模型 (USM) 用戶，並配置陷阱來監控SolidFire叢集。您也可以檢視和存取管理資訊庫文件。

> ⓘ 你可以同時使用 IPv4 位址和 IPv6 位址。

SNMP 詳細資訊

在叢集標籤的 SNMP 頁面上，您可以查看以下資訊。

- **SNMP MIB**

  您可以查看或下載的 MIB 檔案。

- 常規**SNMP**設定

  您可以啟用或停用SNMP。啟用 SNMP 後，您可以選擇要使用的版本。如果使用版本 2，您可以新增請求者；如果使用版本 3，您可以設定 USM 使用者。

- **SNMP**陷阱設定

  您可以確定要捕獲哪些陷阱。您可以為每個陷阱接收者設定主機、連接埠和團體字串。

設定 **SNMP** 請求器

啟用 SNMP 版本 2 後，您可以啟用或停用請求者，並設定請求者以接收授權的 SNMP 請求。

1. 點選選單：集群[SNMP]。
2. 在「常規 SNMP 設定」下，按一下「是」以啟用 SNMP。
3. 從“版本”清單中選擇“版本 2”。
4. 在「請求者」部分，輸入「社群字串」和「網路」資訊。

   預設情況下，團體字串為 public，網路為 localhost。您可以變更這些預設值。

5. *可選：*若要新增另一個請求者，請點選*新增請求者*並輸入*社群字串*和*網路*資訊。
6. 點選「儲存變更」。

查找更多信息

- 配置SNMP陷阱
- 使用管理資訊庫檔案查看託管對象數據

設定 **SNMP USM** 用戶

啟用 SNMP 版本 3 時，需要設定一個 USM 使用者來接收授權的 SNMP 請求。

1. 點選“集群”>“SNMP”。
2. 在「常規 SNMP 設定」下，按一下「是」以啟用 SNMP。
3. 從“版本”清單中選擇“版本 3”。
4. 在「**USM** 使用者」部分，輸入使用者名稱、密碼和密碼短語。
5. *可選：*要新增另一個 USM 用戶，請點擊*新增 USM 用戶*並輸入名稱、密碼和密碼短語。
6. 點選「儲存變更」。

配置**SNMP**陷阱

系統管理員可以使用 SNMP 陷阱（也稱為通知）來監控SolidFire叢集的運作狀況。

啟用 SNMP 陷阱後， SolidFire叢集會產生與事件日誌條目和系統警報關聯的陷阱。若要接收 SNMP 通知，您

需要選擇要產生的陷阱並確定陷阱資訊的接收者。預設情況下，不會產生任何陷阱。

1. 點選“集群”>“SNMP”。
2. 在「SNMP陷阱設定」部分，選擇系統應產生的一種或多種陷阱類型：
   - 簇故障陷阱
   - 集群已解決的故障陷阱
   - 集群事件陷阱
3. 在「**Trap Recipients**」部分，輸入接收者的主機、連接埠和團體字串資訊。
4. 可選：若要新增另一個陷阱接收者，請按一下*新增陷阱接收者*並輸入主機、連接埠和團體字串資訊。
5. 點選「儲存變更」。

使用管理資訊庫檔案查看託管對象數據

您可以檢視和下載用於定義每個受管物件的管理資訊庫 (MIB) 檔案。 SNMP 功能支援對SolidFire-StorageCluster-MIB 中定義的物件進行唯讀存取。

MIB中提供的統計數據顯示了以下系統活動：

- 聚類統計
- 成交量統計
- 按帳戶統計的交易量
- 節點統計資訊
- 其他數據，例如報告、錯誤和系統事件

該系統還支援存取包含 SF 系列產品上層存取點 (OID) 的 MIB 檔案。

步驟

1. 點選“集群”>“SNMP”。
2. 在“SNMP MIB”下，按一下要下載的 MIB 檔案。
3. 在彈出的下載視窗中，開啟或儲存 MIB 檔案。

管理驅動器

每個節點包含一個或多個實體驅動器，用於儲存叢集的一部分資料。將硬碟成功加入叢集後，叢集即可利用硬碟的容量和效能。您可以使用 Element UI 來管理驅動器。

驅動細節

「叢集」標籤上的「磁碟機」頁面提供了叢集中活動磁碟機的清單。您可以透過選擇「活動」、「可用」、「移除」、「擦除」和「失敗」標籤來篩選頁面。

首次初始化叢集時，活動磁碟機清單為空。建立新的SolidFire叢集後，您可以新增未指派給叢集且列在「可用」標籤中的磁碟機。

活動磁碟機清單中包含下列元素。

- 驅動器 **ID**

  分配給硬碟的順序編號。

- 節點 **ID**

  節點新增到叢集時分配的節點編號。

- 節點名稱

  存放驅動器的節點的名稱。

- 投幣口

  硬碟實際所在的插槽編號。

- 容量

  硬碟容量，單位為 GB。

- 序號

  硬碟的序號。

- 剩餘磨損量

  磨損程度指示器。

  儲存系統會報告每個固態硬碟 (SSD) 可用於寫入和擦除資料的大致磨損量。硬碟使用完其設計寫入和擦除週期的 5% 後，報告剩餘磨損量為 95%。系統不會自動刷新硬碟磨損資訊；您可以刷新或關閉並重新載入頁面來刷新資訊。

- 類型

  驅動類型。類型可以是區塊或元資料。

更多資訊

- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

管理節點

管理節點

您可以從叢集標籤的「節點」頁面管理SolidFire儲存和光纖通道節點。

如果新新增的節點佔叢集總容量的 50% 以上，則該節點的部分容量將停用（「閒置」），以使其符合容量規則。在增加更多儲存空間之前，這種情況將持續下去。如果新增一個非常大的節點，並且該節點也違反容量規則

，則先前被困的節點將不再被困，而新新增的節點將變為被困。為避免這種情況發生，容量應該始終成對添加。當節點發生孤立狀態時，會拋出對應的叢集故障。

查找更多信息

向叢集新增節點

向叢集新增節點

當需要更多儲存空間時，或在建立叢集之後，您可以向叢集新增節點。節點首次上電時需要初始配置。節點配置完成後，它將出現在待處理節點清單中，您可以將其新增至叢集。

叢集中每個節點上的軟體版本必須相容。在叢集新增節點時，叢集會根據需要在新節點上安裝叢集版本的NetApp Element軟體。

您可以為現有叢集新增容量較小或較大的節點。您可以為叢集新增更大容量的節點，以滿足容量成長的需求。在包含較小節點的叢集中新增較大節點時，必須成對新增。這樣就為 Double Helix 留出了足夠的空間，以便在較大的節點之一發生故障時能夠轉移資料。您可以為較大的節點叢集中新增較小的節點容量，以提高效能。

如果新新增的節點佔叢集總容量的 50% 以上，則該節點的部分容量將停用（「閒置」），以使其符合容量規則。在增加更多儲存空間之前，這種情況將持續下去。如果新增一個非常大的節點，並且該節點也違反容量規則，則先前被困的節點將不再被困，而新新增的節點將變為被困。為避免這種情況發生，容量應該始終成對添加。當節點發生故障時，會拋出 strandedCapacity 叢集故障。

"NetApp影片：按需擴充：擴展SolidFire集群"

您可以為NetApp HCI設備新增節點。

步驟

1. 選擇“集群”>“節點”。
2. 點選「待處理」查看待處理節點清單。

   新增節點的過程完成後，它們將出現在「活動節點」清單中。在此之前，待處理節點會出現在待處理活動清單中。

   當您將節點新增至叢集時， SolidFire會在待新增節點上安裝叢集的 Element 軟體版本。這可能需要幾分鐘。

3. 執行下列操作之一：
   - 若要新增單一節點，請按一下要新增的節點旁的「操作」圖示。
   - 若要新增多個節點，請選取要新增的節點的複選框，然後選擇「批次操作」。 *注意：*如果您新增的節點的 Element 軟體版本與叢集上執行的版本不同，則叢集會非同步地將該節點更新為叢集主節點上執行的 Element 軟體版本。節點更新後，會自動加入到叢集中。在此非同步過程中，節點將處於 pendingActive 狀態。
4. 按一下“新增”。

   此節點出現在活動節點清單中。

查找更多信息

Node 版本控制和相容性

Node 版本控制和相容性

節點相容性取決於節點上安裝的 Element 軟體版本。如果節點和叢集的版本不相容，Element 軟體儲存叢集會自動將節點鏡像到叢集上的 Element 軟體版本。

以下列表描述了構成 Element 軟體版本號的軟體版本重要性等級：

- 主要的

  第一個數字表示軟體版本。主版本號只有一個的節點不能加入到包含主版本號不同的節點的叢集中，也不能建立包含混合主版本節點的叢集。

- 次要的

  第二個數字表示添加到主要版本中的較小軟體功能或對現有軟體功能的增強。此元件在主版本元件內遞增，表示此增量版本與任何其他具有不同次元件的 Element 軟體增量版本並不相容。例如，11.0 與 11.1 不相容，11.1 與 11.2 也不相容。

- 微

  第三個數字表示與主版本號.次版本號所代表的 Element 軟體版本相容的修補程式（增量版本）。例如，11.0.1 與 11.0.2 相容，11.0.2 與 11.0.3 相容。

主版本號和次版本號必須匹配才能相容。微型計算機的編號不必完全匹配即可相容。

混合節點環境下的叢集容量

在叢集中可以混合使用不同類型的節點。 SF系列2405、3010、4805、6010、9605、9010、19210、38410和H系列可以在集群中共存。

H 系列包括 H610S-1、H610S-2、H610S-4 和 H410S 節點。這些節點同時支援 10GbE 和 25GbE。

最好不要將未加密節點和加密節點混用。在混合節點叢集中，任何節點的容量都不能超過叢集總容量的 33%。例如，在一個包含四個 SF 系列 4805 節點的叢集中，可以單獨新增的最大節點是 SF 系列 9605。群集容量閾值是根據此情況下最大節點可能發生的損失來計算的。

根據您的 Element 軟體版本，以下 SF 系列儲存節點不受支援：

從...開始	不支援儲存節點...
元素 12.8	• SF4805 • SF9605 • SF19210 • SF38410

從...開始	不支援儲存節點...
元素 12.7	• SF2405 • SF9608
元素 12.0	• SF3010 • SF6010 • SF9010

如果您嘗試將這些節點之一升級到不受支援的 Element 版本，您將看到一條錯誤訊息，指出 Element 12.x 不支援該節點。

查看節點詳情

您可以查看各個節點的詳細信息，例如服務標籤、驅動器詳細資訊以及使用率和驅動器統計資訊的圖形。叢集標籤的「節點」頁面提供了「版本」列，您可以在其中查看每個節點的軟體版本。

步驟

1. 點選“集群”>“節點”。
2. 要查看特定節點的詳細信息，請點擊節點的“操作”圖示。
3. 按一下“查看詳細資料”。
4. 查看節點詳細資訊：
   - 節點 **ID**：系統產生的節點 ID。
   - 節點名稱：節點的主機名稱。
   - 節點角色：節點在叢集中所扮演的角色。可能的值：
     - 叢集主節點：執行叢集範圍管理任務的節點，包含 MVIP 和 SVIP。
     - 整合節點：參與叢集的節點。根據叢集大小，整合節點的數量為 3 個或 5 個。
     - 光纖通道：叢集中的一個節點。
   - 節點類型：節點的模型類型。
   - 活動硬碟：節點中活動硬碟的數量。
   - 節點利用率：基於節點熱度的節點利用率百分比。顯示的值是 recentPrimaryTotalHeat 的百分比。從 Element 12.8 版本開始可用。
   - 管理 **IP**：指派給節點的用於 1GbE 或 10GbE 網路管理任務的管理 IP (MIP) 位址。
   - 叢集 **IP**：指派給節點的叢集 IP (CIP) 位址，用於同一叢集中節點之間的通訊。
   - 儲存 **IP**：分配給節點的儲存 IP (SIP) 位址，用於 iSCSI 網路發現和所有資料網路流量。
   - 管理 **VLAN ID**：管理局網域網路的虛擬 ID。
   - 儲存 **VLAN ID**：儲存區域網路的虛擬 ID。
   - 版本：每個節點上運行的軟體版本。

- 複製連接埠：節點上用於遠端複製的連接埠。
- 服務標籤：指派給節點的唯一服務標籤編號。
- 自訂保護域：指派給節點的自訂保護域。

查看光纖通道連接埠詳情

您可以從 FC 連接埠頁面查看光纖通道連接埠的詳細信息，例如其狀態、名稱和連接埠位址。

查看連接到叢集的光纖通道連接埠的相關資訊。

步驟

1. 點選“集群”>“FC連接埠”。
2. 若要篩選此頁面上的信息，請點選「篩選」。
3. 請查看詳細資訊：
   - 節點 **ID**：承載連線會話的節點。
   - 節點名稱：系統產生的節點名稱。
   - 插槽：光纖通道連接埠所在的插槽編號。
   - **HBA** 連接埠：光纖通道主機匯流排適配器 (HBA) 上的實體連接埠。
   - **WWNN**：全球節點名稱。
   - **WWPN**：目標全球連接埠名稱。
   - 交換器 **WWN**：光纖通道交換器的全球通用名稱。
   - 連接埠狀態：連接埠的目前狀態。
   - **nPort ID**：光纖通道架構上的節點連接埠 ID。
   - 速度：協商的光纖通道速度。可能的值如下：
     - 4Gbps
     - 8Gbps
     - 16Gbps

查找更多信息

- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

管理虛擬網絡

管理虛擬網絡

SolidFire儲存中的虛擬網路允許將位於不同邏輯網路上的多個用戶端之間的流量連接到一個叢集。透過使用 VLAN 標記，叢集的連線在網路堆疊中被隔離。

查找更多信息

- 新增虛擬網路
- 啟用虛擬路由和轉送
- 編輯虛擬網絡
- 編輯 VRF VLAN
- 刪除虛擬網絡

新增虛擬網路

您可以為叢集配置中新增的虛擬網絡，以啟用多租戶環境連接到執行 Element 軟體的叢集。

你需要什麼

- 確定將指派給叢集節點上虛擬網路的 IP 位址區塊。
- 確定一個儲存網路 IP (SVIP) 位址，該位址將用作所有NetApp Element儲存流量的端點。

對於此配置，您必須考慮以下標準：

- 未啟用 VRF 的 VLAN 要求發起方與 SVIP 位於相同子網路中。
- 啟用 VRF 的 VLAN 不需要發起方與 SVIP 位於同一子網路中，並且支援路由。
- 預設的 SVIP 不要求發起方與 SVIP 位於同一子網路中，並且支援路由。

當新增虛擬網路時，會為每個節點建立一個接口，每個介面都需要一個虛擬網路 IP 位址。建立新虛擬網路時指定的 IP 位址數量必須等於或大於叢集中的節點數量。虛擬網路位址由系統批次自動配置並指派給各個節點。您無需手動為叢集中的節點指派虛擬網路位址。

步驟

1. 點選“集群”>“網路”。
2. 點選「建立VLAN」。
3. 在「建立新 VLAN」對話方塊中，在下列欄位中輸入值：
   - **VLAN**名稱
   - **VLAN**標籤
   - **SVIP**
   - **Netmask**
   - （可選）描述
4. 輸入 **IP** 位址區塊 中 IP 位址範圍的 起始 **IP** 位址。
5. 輸入 IP 位址範圍的*大小*，即要包含在位址區塊中的 IP 位址數量。
6. 點擊「新增區塊」為該 VLAN 新增一個非連續的 IP 位址區塊。
7. 點選「建立VLAN」。

查看虛擬網路詳情

步驟

1. 點選“集群”>“網路”。
2. 查看詳細資訊。
    - **ID**：VLAN 網路的唯一 ID，由系統指派。
    - 名稱：VLAN 網路的唯一使用者指定名稱。
    - **VLAN** 標籤：建立虛擬網路時指派的 VLAN 標籤。
    - **SVIP**：指派給虛擬網路的儲存虛擬 IP 位址。
    - 子網路遮罩：此虛擬網路的子網路遮罩。
    - 網關：虛擬網路網關的唯一IP位址。必須啟用VRF。
    - **VRF** 已啟用：指示虛擬路由和轉送是否已啟用。
    - 使用的**IP**位址：用於虛擬網路的虛擬網路IP位址範圍。

啟用虛擬路由和轉送

您可以啟用虛擬路由和轉送 (VRF)，它允許路由器中存在多個路由表實例並同時工作。此功能僅適用於儲存網路。

只能在建立 VLAN 時啟用 VRF。如果要切換回非 VRF 模式，則必須刪除並重新建立 VLAN。

1. 點選“集群”>“網路”。
2. 若要在新 VLAN 上啟用 VRF，請選擇「建立 VLAN」。
    a. 請輸入新VRF/VLAN的相關資訊。請參閱「新增虛擬網路」。
    b. 選取“啟用VRF”複選框。
    c. 可選：輸入網關。
3. 點選「建立VLAN」。

查找更多信息

新增虛擬網路

編輯虛擬網絡

您可以變更 VLAN 屬性，例如 VLAN 名稱、子網路遮罩和 IP 位址區塊大小。 VLAN 的 VLAN 標籤和 SVIP 不能修改。對於非 VRF VLAN，網關屬性不是有效參數。

如果存在任何 iSCSI、遠端複製或其他網路會話，則修改可能會失敗。

管理 VLAN IP 位址範圍大小時，應注意下列限制：

- 您只能從建立 VLAN 時指派的初始 IP 位址範圍內移除 IP 位址。
- 您可以刪除在初始 IP 位址範圍之後新增的 IP 位址區塊，但不能透過刪除 IP 位址來調整 IP 位址區塊的大小。

- 當您嘗試從初始 IP 位址範圍或 IP 位址區塊中刪除叢集中節點正在使用的 IP 位址時，操作可能會失敗。
- 您無法將特定正在使用的 IP 位址重新指派給叢集中的其他節點。

您可以使用下列步驟新增 IP 位址區塊：

1. 選擇“集群”>“網路”。
2. 選擇要編輯的 VLAN 的「操作」圖示。
3. 選擇*編輯*。
4. 在「編輯 VLAN」對話方塊中，輸入 VLAN 的新屬性。
5. 選擇「新增區塊」為虛擬網路新增非連續的 IP 位址區塊。
6. 選擇“儲存變更”。

故障排除知識庫文章鏈接

連結到知識庫文章，以取得管理 VLAN IP 位址範圍的故障排除協助。

- "在 Element 叢集的 VLAN 中新增儲存節點後出現重複 IP 警告"
- "如何在 Element 中確定哪些 VLAN IP 位址正在使用以及這些 IP 位址指派給了哪些節點"

編輯 **VRF VLAN**

您可以變更 VRF VLAN 屬性，例如 VLAN 名稱、子網路遮罩、閘道和 IP 位址區塊。

1. 點選“集群”>“網路”。
2. 按一下要編輯的 VLAN 的「操作」圖示。
3. 按一下“編輯”。
4. 在「編輯 VLAN」對話方塊中輸入 VRF VLAN 的新屬性。
5. 點選「儲存變更」。

刪除虛擬網絡

您可以刪除虛擬網路物件。在刪除虛擬網路之前，必須先將位址區塊新增至另一個虛擬網路。

1. 點選“集群”>“網路”。
2. 按一下要刪除的 VLAN 旁邊的「操作」圖示。
3. 按一下“刪除”。
4. 確認訊息。

查找更多信息

編輯虛擬網絡

建立支援 FIPS 驅動器的集群

為 FIPS 驅動器功能準備元素集群

在許多客戶環境中，安全性對於解決方案的部署變得越來越重要。聯邦資訊處理標準（FIPS）是電腦安全和互通性標準。符合 FIPS 140-2 標準的靜態資料加密是整體安全解決方案的一個組成部分。

為了啟用 FIPS 驅動器功能，您應該避免將一些節點支援 FIPS 驅動器功能而其他節點不支援。

叢集被視為符合 FIPS 標準的驅動器，需符合以下條件：

- 所有硬碟均通過了FIPS認證。
- 所有節點均為FIPS驅動節點。
- 已啟用靜態資料加密 (EAR)。
- FIPS驅動功能已啟用。所有磁碟機和節點都必須具備 FIPS 功能，並且必須啟用靜態加密才能啟用 FIPS 磁碟機功能。

啟用靜態資料加密

您可以啟用和停用叢集範圍內的靜態資料加密。此功能預設未啟用。若要支援 FIPS 驅動器，必須啟用靜態加密。

1. 在NetApp Element軟體使用者介面中，按一下「叢集」>「設定」。
2. 點選「啟用靜態資料加密」。

查找更多信息

- 啟用和停用叢集加密
- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

確定節點是否已準備好使用 FIPS 磁碟機功能

您應該使用NetApp Element軟體 GetFipsReport API 方法檢查儲存叢集中的所有節點是否都已準備好支援 FIPS 磁碟機。

產生的報告顯示以下狀態之一：

- 無：節點不支援 FIPS 驅動器功能。
- 部分：節點具備 FIPS 功能，但並非所有磁碟機都是 FIPS 磁碟機。
- 就緒：節點具備 FIPS 功能，所有驅動器均為 FIPS 驅動器，或沒有驅動器。

步驟

1. 使用 Element API，輸入以下命令檢查儲存叢集中的節點和磁碟機是否支援 FIPS 磁碟機：

```
GetFipsReport
```

2. 查看結果，注意任何未顯示“就緒”狀態的節點。
3. 對於任何未顯示「就緒」狀態的節點，請檢查磁碟機是否支援 FIPS 磁碟機功能：
   - 使用 Element API，輸入： `GetHardwareList`
   - 請注意 **DriveEncryptionCapabilityType** 的值。如果是“fips”，則硬體可以支援FIPS驅動器功能。

     看詳情 `GetFipsReport` 或者 `ListDriveHardware` 在 "元素 API 參考"。
4. 如果驅動器不支援 FIPS 驅動器功能，請將硬體更換為 FIPS 硬體（節點或驅動器）。

查找更多信息

- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

啟用 **FIPS** 驅動器功能

您可以使用NetApp Element軟體啟用 FIPS 驅動器功能。 `EnableFeature` API 方法。

叢集上必須啟用靜態資料加密，且所有節點和磁碟機都必須具備 FIPS 功能，當 GetFipsReport 對所有節點顯示「就緒」狀態時，即可表示這一點。

步

1. 使用 Element API，透過輸入以下命令在所有磁碟機上啟用 FIPS：

```
EnableFeature params: FipsDrives
```

查找更多信息

- "使用 Element API 管理存儲"
- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

檢查 **FIPS** 驅動器狀態

您可以使用NetApp Element軟體檢查叢集上是否啟用了 FIPS 磁碟機功能。 `GetFeatureStatus` API 方法，用於顯示 FIPS 磁碟機啟用狀態是真還是假。

1. 使用 Element API，透過輸入以下命令檢查叢集上的 FIPS 磁碟機功能：

```
GetFeatureStatus
```

2. 回顧結果 `GetFeatureStatus`API呼叫。如果 FIPS 磁碟機啟用值為 True，則啟用 FIPS 磁碟機功能。

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

查找更多信息

- "使用 Element API 管理存儲"
- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

排查 **FIPS** 驅動器功能故障

使用NetApp Element軟體使用者介面，您可以查看與 FIPS 驅動器功能相關的系統叢集故障或錯誤訊息的警報。

1. 使用 Element UI，選擇“報告”>“警報”。
2. 尋找集群故障，包括：
   - FIPS驅動程式不符
   - FIPS 導致不合規
3. 有關解決方法建議，請參閱群集故障碼資訊。

查找更多信息

- 叢集故障碼
- "使用 Element API 管理存儲"
- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

建立安全通信

在您的叢集上啟用 **HTTPS** 的 **FIPS 140-2** 標準

您可以使用 EnableFeature API 方法為 HTTPS 通訊啟用 FIPS 140-2 操作模式。

使用NetApp Element軟體，您可以選擇在叢集上啟用聯邦資訊處理標準 (FIPS) 140-2 操作模式。啟用此模式將啟動NetApp加密安全模組 (NCSM)，並利用 FIPS 140-2 1 級認證加密，透過 HTTPS 對所有與NetApp Element UI 和 API 的通訊進行加密。

啟用 FIPS 140-2 模式後，無法停用。啟用 FIPS 140-2 模式後，叢集中的每個節點都會重新啟動並執行自檢，以確保 NCSM 已正確啟用並在 FIPS 140-2 認證模式下運作。這會導致叢集上的管理連線和儲存連線中斷。您應該仔細規劃，只有當您的環境需要它提供的加密機制時才啟用此模式。

更多資訊請參閱 Element API 資訊。

以下是啟用 FIPS 的 API 請求範例：

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

啟用此操作模式後，所有 HTTPS 通訊均使用 FIPS 140-2 核准的密碼。

查找更多信息

- SSL密碼
- "使用 Element API 管理存儲"
- "SolidFire和 Element 軟體文檔"
- "NetApp Element vCenter Server 插件"

SSL密碼

SSL 密碼是主機用來建立安全通訊的加密演算法。 Element 軟體支援標準密碼，啟用 FIPS 140-2 模式時也支援非標準密碼。

以下列表提供了 Element 軟體支援的標準安全通訊端層 (SSL) 密碼套件，以及啟用 FIPS 140-2 模式時支援的 SSL 密碼套件：

- **FIPS 140-2** 已停用

  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

- 符合**FIPS 140-2**標準

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

查找更多信息

在您的叢集上啟用 HTTPS 的 FIPS 140-2 標準

開始使用外部密鑰管理

開始使用外部密鑰管理

外部金鑰管理 (EKM) 結合叢集外外部金鑰伺服器 (EKS) 提供安全的驗證金鑰 (AK) 管理。AK 用於在需要時鎖定和解鎖自加密磁碟機 (SED)。"靜態加密"已在叢集上啟用。 EKS 提供 AK 的安全產生和儲存。此叢集利用金鑰管理互通協定 (KMIP)（OASIS 定義的標準協定）與 EKS 通訊。

- "建立外部管理"
- "重新金鑰軟體加密靜態主金鑰"
- "恢復無法存取或無效的身份驗證金鑰"
- "外部金鑰管理 API 指令"

查找更多信息

- "CreateCluster API 可用於啟用靜態軟體加密。"
- "SolidFire和 Element 軟體文檔"
- "NetApp SolidFire和 Element 產品早期版本的文檔"

設定外部密鑰管理

您可以按照這些步驟，並使用列出的 Element API 方法來設定您的外部金鑰管理功能。

你需要什麼

- 如果您正在設定外部金鑰管理並結合靜態軟體加密，則您已使用以下方式啟用靜態軟體加密："建立集群"在不包含磁碟區的新叢集上執行此方法。

步驟

1. 與外部密鑰伺服器（EKS）建立信任關係。
   a. 為 Element 叢集建立公鑰/私鑰對，透過呼叫以下 API 方法與金鑰伺服器建立信任關係："創建公鑰/私鑰對"
   b. 取得憑證授權單位需要簽署的憑證簽署請求（CSR）。 CSR 讓金鑰伺服器能夠驗證將要存取金鑰的 Element 叢集是否已通過 Element 叢集的驗證。呼叫以下 API 方法："取得用戶端憑證簽署請求"

c. 使用 EKS/憑證授權單位對檢索到的 CSR 進行簽署。更多資訊請參閱第三方文件。

2. 在叢集上建立伺服器和提供程序，以便與 EKS 通訊。金鑰提供者定義金鑰的取得地點，伺服器定義要與之通訊的 EKS 的特定屬性。

   a. 透過呼叫以下 API 方法建立金鑰提供程序，金鑰伺服器詳細資訊將存放於此："建立金鑰提供者Kmip"

   b. 透過呼叫以下 API 方法，建立提供憑證授權單位的簽署憑證和公鑰憑證的金鑰伺服器："建立金鑰伺服器Kmip" "測試金鑰伺服器Kmip"

      如果測試失敗，請檢查伺服器連線和設定。然後重複測試。

   c. 透過呼叫以下 API 方法將金鑰伺服器新增至金鑰提供者容器："AddKeyServerToProviderKmip" "測試密鑰提供者Kmip"

      如果測試失敗，請檢查伺服器連線和設定。然後重複測試。

3. 接下來，請執行以下操作之一，以實現靜態資料加密：

   a. （用於靜態資料硬體加密）啟用"靜態硬體加密"透過呼叫以下方法提供包含用於儲存金鑰的金鑰伺服器的金鑰提供者的 ID："啟用靜態加密" API 方法。

      > ⓘ 您必須透過以下方式啟用靜態加密："API" 。使用現有的 Element UI 按鈕啟用靜態加密將導致該功能恢復為使用內部產生的金鑰。

   b. （針對靜態軟體加密）為了"靜態軟體加密"若要使用新建立的密鑰提供程序，請將密鑰提供者 ID 傳遞給"重新金鑰軟體靜態加密主金鑰"API 方法。

查找更多信息

- "啟用和停用叢集加密"
- "SolidFire和 Element 軟體文檔"
- "NetApp SolidFire和 Element 產品早期版本的文檔"

重新金鑰軟體加密靜態主金鑰

您可以使用 Element API 重新產生現有金鑰。此過程會為您的外部金鑰管理伺服器建立一個新的替換主密鑰。主鑰匙總是用新的主鑰匙替換，絕不會複製或覆蓋。

您可能需要在執行下列任一操作時重新輸入密碼：

- 作為從內部金鑰管理變更為外部金鑰管理的一部分，建立新金鑰。
- 為因應或防範安全事件而建立新金鑰。

> ⓘ 該過程是異步的，會在重新密鑰操作完成之前返回回應。你可以使用"取得非同步結果"用於輪詢系統以查看進程何時完成的方法。

你需要什麼

- 您已啟用靜態軟體加密。"建立集群"在不包含磁碟區且沒有 I/O 的新叢集上執行此方法。使用連結：../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`確認該州是 `enabled`在繼續之前。

- 你有"建立了信任關係"SolidFire叢集與外部金鑰伺服器 (EKS) 之間。運行"測試密鑰提供者Kmip"驗證與金鑰提供者的連線是否已建立的方法。

步驟

1. 運行"ListKeyProvidersKmip"命令並複製密鑰提供者 ID(`keyProviderID`）。
2. 運行"重新金鑰軟體靜態加密主金鑰"和 `keyManagementType`參數為 `external`和 `keyProviderID`作為上一步中密鑰提供者的 ID 號碼：

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

3. 複製 `asyncHandle`來自 `RekeySoftwareEncryptionAtRestMasterKey`命令響應。
4. 運行"取得非同步結果"使用命令 `asyncHandle`使用上一步的值來確認設定變更。從命令回應中可以看到，舊的主密鑰配置已更新為新的密鑰資訊。複製新的密鑰提供者 ID，以便在後續步驟中使用。

```
{
   "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. 運行 `GetSoftwareEncryptionatRestInfo`命令確認新的關鍵細節，包括 `keyProviderID`已更新。

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

查找更多信息

- "使用 Element API 管理存儲"
- "SolidFire和 Element 軟體文檔"
- "NetApp SolidFire和 Element 產品早期版本的文檔"

恢復無法存取或無效的身份驗證金鑰

偶爾會出現需要使用者介入的錯誤。如果發生錯誤，將會產生叢集故障（稱為叢集故障碼）。這裡描述了兩種最有可能的情況。

由於 **KmipServerFault** 叢集故障，叢集無法解鎖磁碟機。

當叢集首次啟動且密鑰伺服器無法存取或所需密鑰不可用時，可能會發生這種情況。

1. 請依照叢集故障碼（如有）中的復原步驟進行操作。

可能會設定 **sliceServiceUnhealthy** 故障，因為元資料磁碟機已被標記為故障並置於「可用」狀態。

清除步驟：

1. 再次新增驅動器。
2. 3到4分鐘後，檢查一下 `sliceServiceUnhealthy`故障已排除。

看"叢集故障碼"了解更多。

外部金鑰管理 API 指令

EKM管理和設定可用API清單。

用於在叢集和外部客戶擁有的伺服器之間建立信任關係：

- 創建公鑰/私鑰對
- 取得用戶端憑證簽署請求

用於定義外部客戶自有伺服器的具體細節：

- 建立金鑰伺服器Kmip
- 修改金鑰伺服器Kmip
- 刪除金鑰伺服器Kmip
- GetKeyServerKmip
- ListKeyServersKmip
- 測試金鑰伺服器Kmip

用於建立和維護管理外部密鑰伺服器的密鑰提供者：

- 建立金鑰提供者Kmip
- 刪除金鑰提供者Kmip
- AddKeyServerToProviderKmip
- 從提供者中移除金鑰伺服器Kmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- 重新金鑰軟體靜態加密主金鑰
- 測試密鑰提供者Kmip

有關 API 方法的信息，請參閱 "API 參考資訊"。