管理您的系統
Element Software

NetApp
November 19, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/element-software-123/storage/task_system_manage_mfa_set_up_multi_factor_authentication.html on November 19, 2025. Always check docs.netapp.com for the latest.

目錄

管理您的系統 1
以取得更多資訊 1
啟用多因素驗證 1
設定多因素驗證 1
多因素驗證的其他資訊 2
設定叢集設定 2
如需詳細資訊、請參閱 3
啟用及停用叢集的靜止加密 3
設定叢集完整臨界值 4
啟用和停用支援存取 5
管理使用條款橫幅 5
設定網路時間傳輸協定 6
管理SNMP 7
管理磁碟機 9
管理節點 10
檢視Fibre Channel連接埠詳細資料 13
管理虛擬網路 14
建立支援FIPS磁碟機的叢集 17
避免混用FIPS磁碟機的節點 17
在靜止狀態下啟用加密 18
識別節點是否已準備好使用FIPS磁碟機功能 18
啟用FIPS磁碟機功能 19
檢查FIPS磁碟機狀態 19
疑難排解FIPS磁碟機功能 19
在叢集上啟用FIPS 140-2 for HTTPS 20
如需詳細資訊、請參閱 20
SSL密碼 21
開始使用外部金鑰管理 22
設定外部金鑰管理 23
在REST主要金鑰重新輸入軟體加密 24
恢復無法存取或無效的驗證金鑰 26
外部金鑰管理API命令 26

管理您的系統

您可以在Element UI中管理系統。這包括啟用多因素驗證、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。

- "啟用多因素驗證"
- "設定叢集設定"
- "建立支援FIPS磁碟機的叢集"
- "開始使用外部金鑰管理"

以取得更多資訊

- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

啟用多因素驗證

多因素驗證（MFA）透過安全聲明標記語言（SAML）使用第三方身分識別供應商（IDP）來管理使用者工作階段。MFA可讓系統管理員視需要設定其他驗證因素、例如密碼和文字訊息、密碼和電子郵件訊息。

設定多因素驗證

您可以透過Element API使用這些基本步驟、將叢集設定為使用多因素驗證。

如需每種API方法的詳細資料、請參閱 "Element API參考"。

1. 透過呼叫下列API方法並以Json格式傳遞IDP中繼資料、為叢集建立新的協力廠商身分識別供應商（IDP）組態：「Create IdpConfiguration」（建立IdpConfiguration）

   IDP中繼資料以純文字格式從第三方IDP擷取。此中繼資料必須經過驗證、以確保其在Json中正確格式化。您可以使用許多Json格式化板應用程式、例如：https://freeformatter.com/json-escape.html。

2. 透過spmetadata Url擷取叢集中繼資料、以呼叫下列API方法複製到第三方IDP：「ListIdpConfigurations」

   SpMetadataUrl是一個URL、用於從叢集擷取IDP的服務供應商中繼資料、以建立信任關係。

3. 在協力廠商IDP上設定SAML斷言、以納入「NameID」屬性、以唯一識別使用者進行稽核記錄、並讓「單一登出」正常運作。
4. 建立一或多個由協力廠商IDP驗證的叢集管理員使用者帳戶、以取得授權、方法是呼叫下列API方法：「AddIdpClusterAdmin」

   IDP叢集管理員的使用者名稱應與SAML屬性名稱/值對應相符、以取得所需的效果、如下列範例所示：

- email=bob@company.com -其中IDP已設定為在SAML屬性中釋出電子郵件地址。
- Group=cluster系統管理員：其中IDP設定為釋放所有使用者應有存取權的群組內容。請注意、為了安全起見、SAML屬性名稱/值配對區分大小寫。

5. 若要為叢集啟用MFA、請呼叫下列API方法：「EnablIdpAuthentication」

如需詳細資訊、請參閱

- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

多因素驗證的其他資訊

您應該瞭解下列有關多因素驗證的注意事項。

- 若要重新整理不再有效的IDP憑證、您必須使用非IDP管理使用者來呼叫下列API方法：「更新IdpConfiguration」
- MFA與長度小於2048位元的憑證不相容。根據預設、會在叢集上建立一個2048位元SSL憑證。在呼叫API方法「etSSLCertificate」時、您應該避免設定較小的憑證

> 如果叢集使用的憑證在升級前低於2048位元、則叢集憑證必須在升級至Element 12或更新版本之後、以2048位元或更高的憑證進行更新。

- IDP管理使用者無法直接（例如透過SDK或Postman）撥打API呼叫、也無法用於其他整合（例如OpenStack Cinder或vCenter外掛程式）。如果您需要建立具有這些功能的使用者、請新增LDAP叢集管理使用者或本機叢集管理使用者。

如需詳細資訊、請參閱

- "使用Element API管理儲存設備"
- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

設定叢集設定

您可以從元素UI的「叢集」索引標籤檢視及變更整個叢集的設定、並執行叢集特定的工作。

您可以設定叢集完整度臨界值、支援存取、閒置加密、虛擬磁碟區、SnapMirror、 和NTP廣播用戶端。

選項

- 使用虛擬磁碟區
- 在元素ONTAP 叢集和叢集之間使用SnapMirror複寫
- 設定叢集完整臨界值
- 啟用和停用支援存取

- "如何計算元素的區塊空間臨界值"
- 啟用及停用叢集的加密
- 管理使用條款橫幅
- 設定叢集要查詢的網路時間傳輸協定伺服器
- 管理SNMP
- 管理磁碟機
- 管理節點
- 管理虛擬網路
- 檢視Fibre Channel連接埠詳細資料

如需詳細資訊、請參閱

- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

啟用及停用叢集的靜止加密

利用叢集、您可以加密儲存在叢集磁碟機上的所有閒置資料。SolidFire您可以使用任一種方法、啟用全叢集範圍的自我加密磁碟機（SED）保護 "硬體或軟體式加密"。

您可以使用Element UI或API在靜止時啟用硬體加密。啟用閒置時的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在閒置時啟用軟體加密。

在建立叢集期間、預設不會啟用閒置時的硬體加密、而且可以從元素UI啟用和停用。

> 對於支援所有Flash的儲存叢集、在建立叢集期間必須啟用閒置軟體加密功能、而且在建立叢集後無法停用。SolidFire

您需要的產品

- 您有叢集管理員權限可啟用或變更加密設定。
- 對於閒置的硬體加密、您在變更加密設定之前、已確保叢集處於正常狀態。
- 如果您停用加密、則必須有兩個節點參與叢集、才能存取金鑰來停用磁碟機上的加密。

檢查加密的靜止狀態

若要查看叢集上閒置加密和/或軟體加密的目前狀態、請使用 "GetClusterInfo" 方法。您可以使用 "GetSoftwareEncryptionAt恢復 資訊" 取得叢集用來加密閒置資料的資訊方法。

> 位於https://<MVIP>/`的Element軟體UI儀表板目前僅顯示硬體加密的靜止狀態加密。

選項

- [在靜止狀態下啟用硬體式加密]
- [在靜止狀態下啟用軟體式加密]

- [停用靜止時的硬體加密]

在靜止狀態下啟用硬體式加密

> 若要使用外部金鑰管理組態在閒置時啟用加密、您必須透過啟用加密功能 "API"。使用現有元素UI按鈕啟用時、會回復為使用內部產生的金鑰。

1. 在Element UI中、選取*叢集*>*設定*。
2. 選取*「Enable Encryption at REST （在**REST**啟用加密）」。

在靜止狀態下啟用軟體式加密

> 閒置的軟體加密無法在叢集上啟用之後停用。

1. 在建立叢集期間、執行 "建立叢集方法" 將「enableSoftwareEncryptionAtRest」設為「true」。

停用靜止時的硬體加密

1. 在Element UI中、選取*叢集*>*設定*。
2. 選擇*停用REST加密*。

如需詳細資訊、請參閱

- "零件與元件軟體文件SolidFire"
- "先前版本的NetApp SolidFire 產品及元素產品文件"

設定叢集完整臨界值

您可以使用下列步驟變更系統產生區塊叢集完整度警告的層級。此外、您也可以使用ModifyClusterFullThreshold API方法來變更系統產生區塊或中繼資料警告的層級。

您需要的產品

您必須擁有叢集管理員權限。

步驟

1. 按一下*叢集*>*設定*。
2. 在「叢集完整設定」區段中、輸入*當Helix無法從節點故障中恢復*之前、仍有_%容量保留時發出警告警示的百分比。
3. 按一下*儲存變更*。

如需詳細資訊、請參閱

"如何計算元素的區塊空間臨界值"

啟用和停用支援存取

您可以啟用支援存取功能、暫時允許NetApp支援人員透過SSH存取儲存節點進行疑難排解。

您必須擁有叢集管理權限、才能變更支援存取權限。

1. 按一下*叢集*>*設定*。
2. 在「啟用/停用支援存取」區段中、輸入您要允許支援人員存取的持續時間（以小時為單位）。
3. 按一下「啟用支援存取」。
4. 選用：*若要停用支援存取、請按一下*停用支援存取。

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

您可以啟用使用者登入Element UI時出現的「使用條款」橫幅。當使用者按一下橫幅時、會出現一個文字對話方塊、其中包含您為叢集設定的訊息。橫幅可隨時關閉。

您必須擁有叢集管理員權限、才能啟用「使用條款」功能。

1. 按一下「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。

   不得超過4096個字元。

3. 按一下「啟用」。

編輯使用條款橫幅

您可以編輯使用者在選取「使用條款」登入橫幅時看到的文字。

您需要的產品

- 您必須擁有叢集管理員權限、才能設定使用條款。
- 確認已啟用「使用條款」功能。

步驟

1. 按一下「使用者>*使用條款*」。
2. 在*使用條款*對話方塊中、編輯您要顯示的文字。

   不得超過4096個字元。

3. 按一下*儲存變更*。

停用使用條款橫幅

您可以停用「使用條款」橫幅。停用橫幅時、使用者不再需要接受元素UI的使用條款。

您需要的產品

- 您必須擁有叢集管理員權限、才能設定使用條款。
- 確認已啟用使用條款。

步驟

1. 按一下「使用者>*使用條款*」。
2. 按一下*停用*。

設定網路時間傳輸協定

設定網路時間傳輸協定（NTP）的方法有兩種：指示叢集中的每個節點聆聽廣播、或指示每個節點查詢NTP伺服器以取得更新。

NTP用於透過網路同步時鐘。連線至內部或外部NTP伺服器應是初始叢集設定的一部分。

設定叢集要查詢的網路時間傳輸協定伺服器

您可以指示叢集中的每個節點查詢網路時間傳輸協定（NTP）伺服器以取得更新。叢集只會連絡已設定的伺服器、並向其要求NTP資訊。

在叢集上設定NTP、以指向本機NTP伺服器。您可以使用IP位址或FQDN主機名稱。叢集建立時的預設NTP伺服器設為us.pool.ntp.org、但無法一律連線至此站台、視SolidFire 乎此叢集的實體位置而定。

使用FQDN取決於個別儲存節點的DNS設定是否已就緒且可正常運作。若要這麼做、請在每個儲存節點上設定DNS伺服器、並檢閱「網路連接埠需求」頁面、確保連接埠已開啟。

最多可輸入五個不同的NTP伺服器。

您可以同時使用IPv4和IPv6位址。

您需要的產品

您必須擁有叢集管理員權限才能設定此設定。

步驟

1. 在伺服器設定中設定IP和/或FQDN清單。
2. 請確定已在節點上正確設定DNS。
3. 按一下*叢集*>*設定*。
4. 在「Network Time Protocol Settings（網路時間傳輸協定設定）」下、選取「* No*（否*）」、這會使用標準NTP組態。
5. 按一下*儲存變更*。

如需詳細資訊、請參閱

- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

設定叢集以偵聽**NTP**廣播

透過廣播模式、您可以指示叢集中的每個節點在網路上聆聽來自特定伺服器的網路時間傳輸協定（NTP）廣播訊息。

您需要的產品

- 您必須擁有叢集管理員權限才能設定此設定。
- 您必須將網路上的NTP伺服器設定為廣播伺服器。

步驟

1. 按一下*叢集*>*設定*。
2. 將使用廣播模式的NTP伺服器輸入伺服器清單。
3. 在網路時間傳輸協定設定下、選取*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、輸入您在廣播模式中設定的NTP伺服器。
5. 按一下*儲存變更*。

如需詳細資訊、請參閱

- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

管理**SNMP**

您可以在叢集中設定簡單網路管理傳輸協定（SNMP）。

您可以選取SNMP申請者、選取要使用的SNMP版本、識別SNMP使用者型安全模式（USM）使用者、並設定設陷以監控SolidFire 叢集。您也可以檢視及存取管理資訊基礎檔案。

您可以同時使用IPv4和IPv6位址。

SNMP詳細資料

在「叢集」索引標籤的「SNMP」頁面上、您可以檢視下列資訊。

- * SNMP MIBS*

  您可以檢視或下載的mib檔案。

- 一般**SNMP**設定

  您可以啟用或停用SNMP。啟用SNMP之後、您可以選擇要使用的版本。如果使用版本2、您可以新增申請者、如果使用版本3、您可以設定USM使用者。

- * SNMP設陷設定*

  您可以識別要擷取的陷阱。您可以為每個陷阱收件者設定主機、連接埠和社群字串。

設定**SNMP**申請者

啟用SNMP版本2時、您可以啟用或停用申請者、並設定申請者接收授權的SNMP要求。

1. 按一下功能表：叢集[SNMP]。
2. 在「一般**SNMP**設定」下、按一下「是」以啟用SNMP。
3. 從*版本*清單中、選取*版本2 *。
4. 在*申請者*區段中、輸入*社群字串*和*網路*資訊。

   根據預設、社群字串為公用、網路為localhost。您可以變更這些預設設定。

5. 選用：*若要新增其他申請者、請按一下*新增申請者、然後輸入*社群字串*和*網路*資訊。
6. 按一下*儲存變更*。

如需詳細資訊、請參閱

- 設定SNMP設陷
- 使用管理資訊基礎檔案檢視託管物件資料

設定**SNMP USM**使用者

啟用SNMP版本3時、您需要設定USM使用者以接收授權的SNMP要求。

1. 按一下*叢集*>* SNMP *。
2. 在「一般**SNMP**設定」下、按一下「是」以啟用SNMP。
3. 從*版本*清單中、選取*版本3*。
4. 在「* USM使用者*」區段中、輸入名稱、密碼和通關密碼。
5. 選用：*若要新增另一個**USM**使用者、請按一下*新增**USM**使用者、然後輸入名稱、密碼和通關密碼。
6. 按一下*儲存變更*。

設定**SNMP**設陷

系統管理員可使用SNMP設陷（也稱為通知）來監控SolidFire 整個叢集的健全狀況。

啟用SNMP設陷時SolidFire 、Sing叢集會產生與事件記錄項目和系統警示相關的設陷。若要接收SNMP通知、您需要選擇應產生的陷阱、並識別陷阱資訊的收件者。根據預設、不會產生任何設陷。

1. 按一下*叢集*>* SNMP *。
2. 在系統應產生的「* SNMP設陷設定*」區段中、選取一或多種設陷類型：
   - 叢集故障設陷

- 叢集已解決的故障設陷
- 叢集事件設陷

3. 在「設陷收件者」區段中、輸入收件者的主機、連接埠和社群字串資訊。
4. 選用：若要新增其他設陷收件者、請按一下*「新增設陷收件者」*、然後輸入主機、連接埠和社群字串資訊。
5. 按一下*儲存變更*。

使用管理資訊基礎檔案檢視託管物件資料

您可以檢視及下載用於定義每個受管理物件的管理資訊庫（MIB）檔案。SNMP功能支援唯讀存取SolidFire-StorageCluster-mib中定義的物件。

在mib中提供的統計資料顯示下列系統活動：

- 叢集統計資料
- Volume統計資料
- 磁碟區（依帳戶統計資料）
- 節點統計資料
- 其他資料、例如報告、錯誤和系統事件

系統也支援存取包含SF系列產品上層存取點（OID）的mib檔案。

步驟

1. 按一下*叢集*>* SNMP *。
2. 在「* SNMP MIBs*」下、按一下您要下載的mib檔案。
3. 在產生的下載視窗中、開啟或儲存mib檔案。

管理磁碟機

每個節點都包含一或多個實體磁碟機、用於儲存叢集的部分資料。叢集會在磁碟機成功新增至叢集後、利用磁碟機的容量和效能。您可以使用Element UI來管理磁碟機。

以取得更多資訊

- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

磁碟機詳細資料

「叢集」索引標籤上的「磁碟機」頁面提供叢集中作用中磁碟機的清單。您可以從「作用中」、「可用」、「移除」、「清除」和「失敗」索引標籤中選取、以篩選頁面。

初次初始化叢集時、作用中磁碟機清單為空。您可以在SolidFire 建立新的叢集後、新增未指派給叢集的磁碟機、並在「可用」索引標籤中列出。

下列元素會出現在作用中磁碟機清單中。

- 磁碟機**ID**

  指派給磁碟機的連續編號。

- 節點**ID**

  節點新增至叢集時指派的節點編號。

- 節點名稱

  存放磁碟機的節點名稱。

- 插槽

  磁碟機實體所在的插槽編號。

- 容量

  磁碟機大小（單位：GB）。

- 序列

  磁碟機的序號。

- 剩餘磨損

  磨損程度指示燈。

  儲存系統會報告每個固態硬碟（SSD）可用於寫入和清除資料的大約可用損耗量。耗用其設計寫入和清除週期5%的磁碟機、報告剩餘的耗損率為95%。系統不會自動重新整理磁碟機耗損資訊、您可以重新整理或關閉頁面、然後重新載入頁面以重新整理資訊。

- 類型

  磁碟機類型。類型可以是區塊或中繼資料。

管理節點

您可以SolidFire 從「叢集」索引標籤的「節點」頁面管理功能區的儲存和光纖通道節點。

如果新增的節點佔叢集總容量的50%以上、則此節點的部分容量將無法使用（「閒置」）、因此符合容量規則。在新增更多儲存設備之前、情況仍會如此。如果新增的大型節點也不遵守容量規則、則先前閒置的節點將不再處於閒置狀態、而新新增的節點則會陷入閒置狀態。容量應一律成對新增、以避免這種情況發生。當節點變成閒置狀態時、會拋出適當的叢集故障。

如需詳細資訊、請參閱

新增節點至叢集

新增節點至叢集

您可以在需要更多儲存設備或建立叢集之後、將節點新增至叢集。節點第一次開機時、需要初始組態。節點設定完成後、就會顯示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。當您將節點新增至叢集時、叢集NetApp Element 會視需要在新節點上安裝叢集版本的資訊軟體。

您可以將容量較小或較大的節點新增至現有叢集。您可以將較大的節點容量新增至叢集、以利容量成長。必須成對新增較大的節點至具有較小節點的叢集。如此一來、如果其中一個較大的節點發生故障、就能有足夠的空間讓雙Helix移動資料。您可以將較小的節點容量新增至較大的節點叢集、以改善效能。

> 如果新增的節點佔叢集總容量的50%以上、則此節點的部分容量將無法使用（「閒置」）、因此符合容量規則。在新增更多儲存設備之前、情況仍會如此。如果新增的大型節點也不遵守容量規則、則先前閒置的節點將不再處於閒置狀態、而新新增的節點則會陷入閒置狀態。容量應一律成對新增、以避免這種情況發生。當節點變成閒置狀態時、會拋出strandedCapacity叢集故障。

"NetApp影片：根據您的需求擴充：擴充SolidFire 功能"

您可以將節點新增至NetApp HCI 各個不相同的應用裝置。

步驟

1. 選擇*叢集*>*節點*。
2. 按一下*「Pending」（待處理）*以檢視待處理節點的清單。

   新增節點的程序完成後、會顯示在「作用中節點」清單中。在此之前、擱置中的節點會出現在「Pending Active」（擱置中的作用中）清單中。

   將叢集新增至叢集時、可在暫掛節點上安裝叢集的元素軟體版本SolidFire 。這可能需要幾分鐘的時間。

3. 執行下列其中一項：
   - 若要新增個別節點、請按一下您要新增之節點的*「Actions」（動作）*圖示。
   - 若要新增多個節點、請選取要新增之節點的核取方塊、然後選取*大量動作*。*附註：*如果您要新增的節點的Element軟體版本與叢集上執行的版本不同、叢集會非同步地將節點更新為叢集主機上執行的Element軟體版本。節點更新後、會自動將自己新增至叢集。在此非同步程序期間、節點將處於「待處理作用中」狀態。
4. 按一下「 * 新增 * 」。

   節點會出現在作用中節點清單中。

如需詳細資訊、請參閱

節點版本管理與相容性

節點版本管理與相容性

節點相容性是根據安裝在節點上的Element軟體版本而定。如果節點和叢集不是相容版本、Element軟體型儲存叢集會自動將節點映像至叢集上的Element軟體版本。

下列清單說明組成元素軟體版本編號的軟體版本重要性層級：

- 重大

  第一個數字代表軟體版本。具有一個主要元件編號的節點無法新增至包含不同主要修補程式編號節點的叢集、也無法使用混合主要版本的節點來建立叢集。

- 次要

  第二個數字代表已新增至主要版本之現有軟體功能的較小軟體功能或增強功能。此元件會在主要版本元件內遞增、表示此遞增版本與其他含有不同次要元件的元件軟體遞增版本不相容。例如、11.0與11.1不相容、11.1與11.2不相容。

- 微

  第三個數字代表與Major.Minor元件所代表的Element軟體版本相容的修補程式（遞增版本）。例如、11.0.1與11.0.2相容、11.0.2與11.0.3相容。

相容性的主要和次要版本號碼必須相符。相容性不需要與微數字相符。

混合式節點環境中的叢集容量

您可以在叢集中混合不同類型的節點。SF系列2405、3010、4805、6010、9605、9010、19210、38410和H系列可共存於叢集內。

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

最好不要混用未加密和加密的節點。在混合式節點叢集中、任何節點都不能大於叢集總容量的33%。例如、在具有四個SF系列4805節點的叢集中、唯一可新增的最大節點是SF系列9605。叢集容量臨界值是根據這種情況下最大節點可能遺失的情況來計算。

從元件12開始、不支援下列SF系列儲存節點：

- SF3010
- SF6010
- SF9010

如果您將其中一個儲存節點升級至元件12、您將會看到錯誤訊息、指出元素12．0不支援此節點。

檢視節點詳細資料

您可以檢視個別節點的詳細資料、例如服務標籤、磁碟機詳細資料、以及使用率和磁碟機統計資料的圖形。「叢集」索引標籤的「節點」頁面會提供「版本」欄、您可以在其中檢視每個節點的軟體版本。

步驟

1. 按一下*叢集*>*節點*。
2. 若要檢視特定節點的詳細資料、請按一下節點的*「Actions」（動作）*圖示。
3. 按一下*檢視詳細資料*。

4. 檢閱節點詳細資料：
    - 節點**ID**：系統產生的節點ID。
    - 節點名稱：節點的主機名稱。
    - 可用的**4K IOP**：為節點設定的IOPS。
    - 節點角色：節點在叢集中的角色。可能值：
        - 叢集主機：執行叢集範圍管理工作、並包含MVIP和SVIP的節點。
        - 集合節點：參與叢集的節點。視叢集大小而定、共有3或5個頻道群節點。
        - Fibre Channel：叢集中的節點。
    - 節點類型：節點的模型類型。
    - 作用中磁碟機：節點中作用中磁碟機的數量。
    - 管理**IP**：指派給節點的管理IP（MIP）位址、用於1GbE或10GbE網路管理工作。
    - 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**：指派給用於iSCSI網路探索及所有資料網路流量之節點的儲存IP（Sip）位址。
    - 管理**VLAN ID**：管理區域網路的虛擬ID。
    - 儲存**VLAN ID**：儲存區域網路的虛擬ID。
    - 版本：每個節點上執行的軟體版本。
    - 複寫連接埠：節點上用於遠端複寫的連接埠。
    - 服務標籤：指派給節點的唯一服務標籤號碼。

檢視**Fibre Channel**連接埠詳細資料

您可以從「FC連接埠」頁面檢視光纖通道連接埠的詳細資料、例如其狀態、名稱和連接埠位址。

檢視連接至叢集的光纖通道連接埠相關資訊。

步驟

1. 按一下「叢集>* FC連接埠*」。
2. 若要篩選此頁面上的資訊、請按一下*篩選*。
3. 檢閱詳細資料：
    - 節點**ID**：裝載連線工作階段的節點。
    - 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介面卡（HBA）上的實體連接埠。
    - * WWNN*：全球節點名稱。
    - * WWPN*：全球目標連接埠名稱。
    - 交換器**WWW**：光纖通道交換器的全球名稱。

- 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：議定的光纖通道速度。可能的值如下：
  - 4Gbps
  - 8Gbps
  - 16Gbps

如需詳細資訊、請參閱

- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

管理虛擬網路

利用支援虛擬網路SolidFire 功能的虛擬網路功能、可將位於不同邏輯網路上的多個用戶端之間的流量連線至一個叢集。透過使用VLAN標記、將與叢集的連線隔離在網路堆疊中。

如需詳細資訊、請參閱

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

新增虛擬網路

您可以將新的虛擬網路新增至叢集組態、以啟用多租戶環境連線至執行Element軟體的叢集。

您需要的產品

- 識別將指派給叢集節點上虛擬網路的IP位址區塊。
- 識別儲存網路IP（SVIP）位址、做為所有NetApp Element 資訊儲存流量的端點。

> 您必須針對此組態考量下列條件：

- 未啟用VRF的VLAN要求啟動器與SVIP位於同一子網路中。
- 啟用VRF的VLAN不需要啟動器與SVIP位於相同的子網路、而且支援路由。
- 預設的SVIP不要求啟動器與SVIP位於同一子網路、而且支援路由傳送。

新增虛擬網路時、會為每個節點建立一個介面、每個節點都需要一個虛擬網路IP位址。您在建立新虛擬網路時指定的IP位址數目、必須等於或大於叢集中的節點數。虛擬網路位址會由個別節點自行大量配置及指派給個別節點。您不需要手動指派虛擬網路位址給叢集中的節點。

步驟

1. 按一下*叢集*>*網路*。
2. 單擊* Create vlan-*。
3. 在「建立新的**VLAN**」對話方塊中、於下列欄位中輸入值：
   - * VLAN名稱*
   - * VLAN標記*
   - * SVIP*
   - 網路遮罩
   - （選用）說明
4. 在「* IP位址區塊*」中輸入IP位址範圍的*起始IP位址。
5. 輸入IP範圍的*大小*作為區塊中要包含的IP位址數目。
6. 按一下「新增區塊」、為此VLAN新增不連續的IP位址區塊。
7. 單擊* Create vlan-*。

檢視虛擬網路詳細資料

步驟

1. 按一下*叢集*>*網路*。
2. 檢閱詳細資料。
   - * ID*：系統指派的VLAN網路唯一ID。
   - 名稱：使用者指派給VLAN網路的唯一名稱。
   - * VLAN Tag*：建立虛擬網路時指派的VLAN標記。
   - * SVIP*：指派給虛擬網路的儲存虛擬IP位址。
   - * Netmask*：此虛擬網路的網路遮罩。
   - 閘道：虛擬網路閘道的唯一IP位址。必須啟用VRF。
   - *已啟用VRF *：指示是否已啟用虛擬路由和轉送。
   - *使用的IP *：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）、讓路由器中存在多個路由表執行個體、並同時運作。此功能僅適用於儲存網路。

您只能在建立VLAN時啟用VRF。若要切換回非VRF、您必須刪除並重新建立VLAN。

1. 按一下*叢集*>*網路*。
2. 若要在新的VLAN上啟用VRF、請選取*建立VLAN*。
   a. 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*核取方塊。

c. 選用：輸入閘道。

3. 單擊* Create vlan-*。

如需詳細資訊、請參閱

新增虛擬網路

編輯虛擬網路

您可以變更VLAN屬性、例如VLAN名稱、網路遮罩和IP位址區塊大小。無法修改VLAN的VLAN標記和SVIP。閘道屬性不是非VRF VLAN的有效參數。

如果存在任何iSCSI、遠端複寫或其他網路工作階段、則修改可能會失敗。

管理VLAN IP位址範圍的大小時、請注意下列限制：

- 您只能從建立VLAN時指派的初始IP位址範圍中移除IP位址。
- 您可以移除在初始IP位址範圍之後新增的IP位址區塊、但無法移除IP位址來調整IP區塊的大小。
- 當您嘗試從初始IP位址範圍或IP區塊中移除叢集中節點正在使用的IP位址時、作業可能會失敗。
- 您無法將特定的使用中IP位址重新指派給叢集中的其他節點。

您可以使用下列程序新增IP位址區塊：

1. 選擇*叢集*>*網路*。
2. 選取您要編輯之VLAN的「動作」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. 選取*新增區塊*、為虛擬網路新增不連續的IP位址區塊。
6. 選取*儲存變更*。

疑難排解知識庫文章的連結

連結至知識庫文章、以協助疑難排解管理VLAN IP位址範圍的問題。

- "在元素叢集的VLAN中新增儲存節點後、出現重複的IP警告"
- "如何判斷哪些VLAN IP正在使用中、以及哪些節點已指派給元素中的IP"

編輯**VRF VLAN**

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

1. 按一下*叢集*>*網路*。
2. 按一下您要編輯之VLAN的「動作」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. 按一下*儲存變更*。

刪除虛擬網路

您可以移除虛擬網路物件。在移除虛擬網路之前、您必須先將位址區塊新增至其他虛擬網路。

1. 按一下*叢集*>*網路*。
2. 按一下您要刪除之VLAN的「動作」圖示。
3. 按一下*刪除*。
4. 確認訊息。

如需詳細資訊、請參閱

編輯虛擬網路

建立支援FIPS磁碟機的叢集

在許多客戶環境中部署解決方案、安全性變得越來越重要。聯邦資訊處理標準（FIPS）是電腦安全性與互通性的標準。FIPS 140-2認證的靜止資料加密是整體安全解決方案的一項元件。

- "避免混用FIPS磁碟機的節點"
- "在靜止狀態下啟用加密"
- "識別節點是否已準備好使用FIPS磁碟機功能"
- "啟用FIPS磁碟機功能"
- "檢查FIPS磁碟機狀態"
- "疑難排解FIPS磁碟機功能"

避免混用FIPS磁碟機的節點

為了準備啟用FIPS磁碟機功能、您應該避免在某些節點具有FIPS磁碟機功能、有些節點則不具備FIPS磁碟機功能時混用節點。

根據下列條件、叢集被視為符合FIPS磁碟機標準：

- 所有磁碟機均通過FIPS磁碟機認證。
- 所有節點均為FIPS磁碟機節點。
- 加密閒置（Ear）已啟用。
- FIPS磁碟機功能已啟用。所有磁碟機和節點都必須具備FIPS功能、且必須啟用靜止加密功能、才能啟用FIPS磁碟機功能。

在靜止狀態下啟用加密

您可以在閒置時啟用和停用全叢集加密。此功能預設為未啟用。若要支援FIPS磁碟機、您必須在閒置時啟用加密。

1. 在這個軟件UI中、按一下NetApp Element 叢集>*設定*。
2. 按一下「在**REST**啟用加密」。

如需詳細資訊、請參閱

- 啟用及停用叢集的加密
- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

識別節點是否已準備好使用**FIPS**磁碟機功能

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

產生的報告會顯示下列其中一種狀態：

- 無：節點無法支援FIPS磁碟機功能。
- 部分：節點支援FIPS、但並非所有磁碟機都是FIPS磁碟機。
- 就緒：節點支援FIPS、所有磁碟機均為FIPS磁碟機、或沒有磁碟機。

步驟

1. 使用Element API、輸入下列命令、檢查儲存叢集中的節點和磁碟機是否能夠使用FIPS磁碟機：

   《GetFipsReport》（《GetFipsReport》）

2. 檢閱結果、並記下任何未顯示「Ready（就緒）」狀態的節點。
3. 對於未顯示「Ready（就緒）」狀態的任何節點、請檢查磁碟機是否能夠支援FIPS磁碟機功能：
   - 使用元素API、輸入：「GetHardwareList」
   - 請注意* DriveEncryptionCapabilityType *的值。如果是「FIPS」、硬體就能支援FIPS磁碟機功能。

     請參閱中的「GetFipsReport」或「ListDriveHardware」詳細資料 "Element API參考"。

4. 如果磁碟機無法支援FIPS磁碟機功能、請以FIPS硬體（節點或磁碟機）更換硬體。

如需詳細資訊、請參閱

- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

啟用**FIPS**磁碟機功能

您可以使用NetApp Element 「啟用功能」API方法來啟用FIPS磁碟機功能。

必須在叢集上啟用靜止加密、且所有節點和磁碟機都必須具備FIPS功能、如GetFipsReport顯示所有節點的就緒狀態所示。

步驟

1. 使用Element API、輸入下列命令、在所有磁碟機上啟用FIPS：

   「EnablFeature參數：FipsDrives」

如需詳細資訊、請參閱

- "使用Element API管理儲存設備"
- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

檢查**FIPS**磁碟機狀態

您可以使用NetApp Element 支援FIPS磁碟機的API方法來檢查叢集上是否啟用FIPS磁碟機功能、此方法可顯示FIPS磁碟機啟用狀態為真或假。

1. 使用Element API、輸入下列命令、檢查叢集上的FIPS磁碟機功能：

   「GetFeatureStatus」

2. 檢閱「GetFeatureStatus」API呼叫的結果。如果FIPS磁碟機啟用值為True、則會啟用FIPS磁碟機功能。

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

如需詳細資訊、請參閱

- "使用Element API管理儲存設備"
- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

疑難排解**FIPS**磁碟機功能

您可以使用NetApp Element 這個解決方法來檢視有關叢集故障或系統中與FIPS磁碟機功能相關之錯誤的警示。

1. 使用元素UI、選取*報告*>*警示*。

2. 尋找叢集故障、包括：
    - FIPS磁碟機不相符
    - FIPS導致違反法規
3. 如需解決建議、請參閱叢集故障代碼資訊。

如需詳細資訊、請參閱

- 叢集故障代碼
- "使用Element API管理儲存設備"
- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

在叢集上啟用FIPS 140-2 for HTTPS

您可以使用啟用功能API方法、啟用FIPS 140-2操作模式進行HTTPS通訊。

有了支援的軟體、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。NetApp Element啟用此模式會啟動NetApp密碼編譯安全模組（NCSM）、並將FIPS 140-2 Level 1認證加密用於透過HTTPS傳輸至NetApp Element 整套UI和API的所有通訊。

> 啟用FIPS 140-2模式之後、就無法停用。啟用FIPS 140-2模式時、叢集中的每個節點都會重新開機並執行自我測試、以確保NCSM已正確啟用、並以FIPS 140-2認證模式運作。這會中斷叢集上的管理和儲存連線。您應該仔細規劃、而且只有在環境需要它提供的加密機制時才啟用此模式。

如需詳細資訊、請參閱Element API資訊。

以下是啟用FIPS的API要求範例：

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

啟用此操作模式之後、所有HTTPS通訊都會使用FIPS 140-2核准的密碼。

如需詳細資訊、請參閱

- SSL密碼
- "使用Element API管理儲存設備"
- "零件與元件軟體文件SolidFire"

- "vCenter Server的VMware vCenter外掛程式NetApp Element"

SSL密碼

SSL密碼是主機用來建立安全通訊的加密演算法。啟用FIPS 140-2模式時、元素軟體支援的標準密碼和非標準密碼。

下列清單提供元素軟體支援的標準安全通訊端層（SSL）密碼、以及啟用FIPS 140-2模式時支援的SSL密碼：

- * FIPS 140-2已停用*

  TLS_DHE_RSA_with _AES-122_CBC_SHA256（DH2048）- A

  TLS_DHE_RSA_with _AES-122_GCM_SHA256（DH2048）- A

  TLS_DHE_RSA_AT_AES-256_CBC_SHA256（DH2048）- A

  TLS_DHE_RSA_AT_AES-256_GCM_SHA384（DH2048）- A

  TLS_ECDHE_RSA_with _AES-122_CBC_SHA256（secp256r1）- A

  TLS_ECDHE_RSA_with _AES-122_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_AT_3DE_EDE_CBC_SHA（RSA 2048）- C

  TLS_RSA_AT_AES-122_CBC_SHA（RSA 2048）- A

  TLS_RSA_AT_AES-122_CBC_SHA256（RSA 2048）- A

  TLS_RSA_AT_AES-122_GCM_SHA256（RSA 2048）- A

  TLS_RSA_AT_AES-256_CBC_SHA（RSA 2048）- A

  TLS_RSA_AT_AES-256_CBC_SHA256（RSA 2048）- A

  TLS_RSA_AT_AES-256_GCM_SHA384（RSA 2048）- A

  TLS_RSA_with _Camella_128_CBC_SHA（RSA 2048）- A

  TLS_RSA_with _Camella_256_CBC_SHA（RSA 2048）- A

  TLS_RSA_AT_ID_CBC_SHA（RSA 2048）- A

  TLS_RSA_AT_RC4_122_MD5（RSA 2048）- C

  TLS_RSA_AT_RC4_128_SHa（RSA 2048）- C

  TLS_RSA_AT_SEIN_CBC_SHA（RSA 2048）- A

- * FIPS 140-2已啟用*

  TLS_DHE_RSA_with _AES-122_CBC_SHA256（DH2048）- A

  TLS_DHE_RSA_with _AES-122_GCM_SHA256（DH2048）- A

  TLS_DHE_RSA_AT_AES-256_CBC_SHA256（DH2048）- A

  TLS_DHE_RSA_AT_AES-256_GCM_SHA384（DH2048）- A

  TLS_ECDHE_RSA_with _AES-122_CBC_SHA256（第571r1節）- A

  TLS_ECDHE_RSA_with _AES-122_CBC_SHA256（secp256r1）- A

  TLS_ECDHE_RSA_with _AES-122_GCM_SHA256（secp256r1）- A

  TLS_ECDHE_RSA_with _AES-122_GCM_SHA256（第571r1節）- A

  TLS_ECDHE_RSA_with _AES-256_CBC_SHA384（第571r1節）- 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（第571r1節）- A

  TLS_RSA_AT_3DE_EDE_CBC_SHA（RSA 2048）- C

  TLS_RSA_AT_AES-122_CBC_SHA（RSA 2048）- A

  TLS_RSA_AT_AES-122_CBC_SHA256（RSA 2048）- A

  TLS_RSA_AT_AES-122_GCM_SHA256（RSA 2048）- A

  TLS_RSA_AT_AES-256_CBC_SHA（RSA 2048）- A

  TLS_RSA_AT_AES-256_CBC_SHA256（RSA 2048）- A

  TLS_RSA_AT_AES-256_GCM_SHA384（RSA 2048）- A

如需詳細資訊、請參閱

在叢集上啟用FIPS 140-2 for HTTPS

開始使用外部金鑰管理

外部金鑰管理（EKM）可搭配叢集外的外部金鑰伺服器（EKS）、提供安全驗證金鑰（AK）管理。當自動加密磁碟機（SED）處於鎖定和解除鎖定狀態時、即會使用這些AKs "加密閒置" 已在叢集上啟用。EKS提供安全的AKs世代與儲存設備。叢集利用金鑰管理互通性傳輸協定（KMIP）（OASIS定義的標準傳輸協定）與EKS通訊。

- "設定外部管理"
- "在REST主要金鑰重新輸入軟體加密"
- "恢復無法存取或無效的驗證金鑰"
- "外部金鑰管理API命令"

如需詳細資訊、請參閱

- "可用來在閒置時啟用軟體加密的叢集API"
- "零件與元件軟體文件SolidFire"
- "先前版本的NetApp SolidFire 產品及元素產品文件"

設定外部金鑰管理

您可以遵循下列步驟、並使用列出的Element API方法來設定外部金鑰管理功能。

您需要的產品

- 如果您要設定外部金鑰管理、並在閒置時搭配軟體加密、則已使用啟用軟體加密功能 "建立叢集" 不含磁碟區的新叢集方法。

步驟

1. 與外部金鑰伺服器（EKS）建立信任關係。
   a. 針對元素叢集建立公開/私密金鑰配對、以呼叫下列API方法來建立與金鑰伺服器的信任關係： "建立PublicPrivate KeyPair"
   b. 取得認證機構需要簽署的認證簽名要求（CSR）。CSR可讓金鑰伺服器驗證要存取金鑰的元素叢集是否已驗證為元素叢集。請撥打下列API方法： "GetClientCertificateSignRequest"
   c. 使用EKS/Certificate Authority簽署擷取的CSR。如需詳細資訊、請參閱第三方文件。
2. 在叢集上建立伺服器和供應商、以便與EKS通訊。金鑰供應商會定義金鑰的取得位置、而伺服器則會定義要與之通訊的EKS特定屬性。
   a. 透過呼叫下列API方法、建立主要伺服器詳細資料所在的主要供應商： "CreeKeyProviderKmip"
   b. 透過呼叫下列API方法來建立金鑰伺服器、以提供已簽署的憑證和憑證授權單位的公開金鑰憑證： "CreKeyServerKmip" "TestKeyServerKmip"

      如果測試失敗、請確認您的伺服器連線能力和組態。然後重複測試。

   c. 透過呼叫下列API方法、將金鑰伺服器新增至金鑰提供者容器："AddKeyServerToProviderKmip" "TestKeyProviderKmip"

      如果測試失敗、請確認您的伺服器連線能力和組態。然後重複測試。

3. 請執行下列其中一項、做為靜止加密的下一步：
   a. （用於靜止時的硬體加密）啟用 "硬體加密功能" 提供金鑰提供者的ID、其中包含用來透過呼叫來儲存金鑰的金鑰伺服器 "啟用EncryptionAtRest" API方法。

您必須透過啟用加密功能 "API"。使用現有元素UI按鈕啟用靜止加密、將會導致功能回復為使用內部產生的金鑰。

b. （用於閒置時的軟體加密） "軟體加密功能" 若要使用新建立的金鑰提供者、請將金鑰提供者ID傳送至 "RekeySoftwareEncryptionAt恢復 主金鑰" API方法。

如需詳細資訊、請參閱

- "啟用及停用叢集的加密"
- "零件與元件軟體文件SolidFire"
- "先前版本的NetApp SolidFire 產品及元素產品文件"

在REST主要金鑰重新輸入軟體加密

您可以使用Element API重新輸入現有的金鑰。此程序會為您的外部金鑰管理伺服器建立新的替代主金鑰。主金鑰一律由新的主金鑰取代、永遠不會複製或覆寫。

您可能需要重新輸入以下程序的一部分：

- 在從內部金鑰管理變更為外部金鑰管理的過程中、建立新的金鑰。
- 建立新的金鑰、做為對安全性相關事件的回應或保護。

此程序是非同步的、會在重新輸入作業完成之前傳回回應。您可以使用 "Get非 同步結果" 輪詢系統以查看程序何時完成的方法。

您需要的產品

- 您已使用啟用軟體加密功能 "建立叢集" 不含磁碟區且沒有I/O的新叢集上的方法使用 "9510c8e68784d05acbae2e947dde3cd8" 確認狀態為「已啟用」、然後再繼續。
- 您有 "建立信任關係" 在整個叢集與外部金鑰伺服器SolidFire （EKS）之間。執行 "TestKeyProviderKmip" 驗證是否已建立與金鑰提供者的連線的方法。

步驟

1. 執行 "listKeyProvidersKmip" 命令並複製金鑰提供者ID（「keyProviderID」）。
2. 執行 "RekeySoftwareEncryptionAt恢復 主金鑰" 將「keyManagementType」參數設為「external」、「keyProviderID」作為上一步金鑰提供者的ID號碼：

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

3. 從「RekeySoftwareEncryptionAt恢復 金鑰」命令回應中複製「asyncdyle」值。

4. 執行 "Get非 同步結果" 以上一個步驟的「asyncdyle」值來確認組態變更的命令。從命令回應中、您應該會看到舊版主金鑰組態已更新為新的金鑰資訊。複製新的金鑰提供者ID以供後續步驟使用。

```
{
   "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. 執行「GetSoftwareEncryptionatRestInfo」命令、確認已更新新的金鑰詳細資料、包括「keyProviderID」。

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

如需詳細資訊、請參閱

- "使用Element API管理儲存設備"
- "零件與元件軟體文件SolidFire"
- "先前版本的NetApp SolidFire 產品及元素產品文件"

恢復無法存取或無效的驗證金鑰

偶爾會發生需要使用者介入的錯誤。發生錯誤時、會產生叢集故障（稱為叢集故障代碼）。此處說明兩種最可能的案例。

由於**KmipServerFault**叢集故障、叢集無法解除鎖定磁碟機。

當叢集第一次開機且金鑰伺服器無法存取或所需的金鑰無法使用時、就會發生這種情況。

1. 請遵循叢集故障代碼（若有）中的還原步驟。

可能會設定交叉分析**eServiceUnhealthy**故障、因為中繼資料磁碟機已標示為故障、並置於「可用」狀態。

清除步驟：

1. 再次新增磁碟機。
2. 3到4分鐘後、請檢查「交叉服務不健全」故障是否已清除。

請參閱 "叢集故障代碼" 以取得更多資訊。

外部金鑰管理**API**命令

可用於管理及設定EKM的所有API清單。

用於建立叢集與外部客戶擁有伺服器之間的信任關係：

- 建立PublicPrivate KeyPair
- GetClientCertificateSignRequest

用於定義外部客戶擁有伺服器的特定詳細資料：

- CreKeyServerKmip
- ModifyKeyServerKmip
- 刪除KeyServerKmip
- GetKeyServerKmip
- listKeyServersKmip
- TestKeyServerKmip

用於建立及維護管理外部金鑰伺服器的主要供應商：

- CreeKeyProviderKmip

- 刪除KeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- listKeyProvidersKmip
- RekeySoftwareEncryptionAt恢復 主金鑰
- TestKeyProviderKmip

如需API方法的相關資訊、請參閱 "API參考資訊"。

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。