管理您的系统
Element Software

NetApp
November 12, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/element-software/storage/concept_system_manage_system_management.html on November 12, 2025. Always check docs.netapp.com for the latest.

目录

管理您的系统 1
- 管理您的系统 1
  - 有关详细信息 ... 1
- 启用多因素身份验证 1
  - 设置多因素身份验证 1
  - 用于多因素身份验证的追加信息 2
- 配置集群设置 2
  - 为集群启用和禁用空闲加密 2
  - 设置集群全满阈值 4
  - 启用和禁用卷负载平衡 4
  - 启用和禁用支持访问 5
  - 管理使用条款横幅 5
  - 设置网络时间协议 6
  - 管理 SNMP 7
  - 管理驱动器 9
  - 管理节点 10
  - 查看光纤通道端口详细信息 14
  - 管理虚拟网络 14
- 创建支持 FIPS 驱动器的集群 18
  - 为 FIPS 驱动器功能准备元素集群 18
  - 启用空闲加密 18
  - 确定节点是否已准备好使用 FIPS 驱动器功能 18
  - 启用 FIPS 驱动器功能 19
  - 检查 FIPS 驱动器状态 19
  - 对 FIPS 驱动器功能进行故障排除 20
- 建立安全通信 20
  - 在集群上为 HTTPS 启用 FIPS 140-2 20
  - SSL 密码 21
- 开始使用外部密钥管理 23
  - 开始使用外部密钥管理 23
  - 设置外部密钥管理 23
  - 重新设置 REST 主密钥的软件加密密钥 24
  - 恢复不可访问或无效的身份验证密钥 27
  - 外部密钥管理 API 命令 27

管理您的系统

管理您的系统

您可以在 Element UI 中管理系统。其中包括启用多因素身份验证，管理集群设置，支持联邦信息处理标准（ FIPS ）以及使用外部密钥管理。

- "启用多因素身份验证"
- "配置集群设置"
- "创建支持 FIPS 驱动器的集群"
- "开始使用外部密钥管理"

有关详细信息 ...

- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

启用多因素身份验证

设置多因素身份验证

多因素身份验证（ MFA ）通过安全断言标记语言（ Security Assertion Markup Language ， SAML ）使用第三方身份提供程序（ IdP ）来管理用户会话。通过 MFA ，管理员可以根据需要配置其他身份验证因素，例如密码和文本消息以及密码和电子邮件消息。

您可以通过 Element API 使用这些基本步骤来设置集群以使用多因素身份验证。

每个 API 方法的详细信息可以在以下位置找到： "Element API 参考"。

1. 通过调用以下 API 方法并以 JSON 格式传递 IdP 元数据，为集群创建新的第三方身份提供程序（ IdP ）配置： `CreateIdpConfiguration`

   从第三方 IdP 检索纯文本格式的 IdP 元数据。需要验证此元数据，以确保其在 JSON 中格式正确。您可以使用多种 JSON 格式化程序应用程序，例如： https://freeformatter.com/json-escape.html 。

2. 通过 spMetadataUrl 检索集群元数据，通过调用以下 API 方法复制到第三方 IdP ： `ListIdpConfigurations`

   spMetadataUrl 是一个 URL ，用于从集群中为 IdP 检索服务提供商元数据，以便建立信任关系。

3. 在第三方 IdP 上配置 SAML 断言，使其包含 "`NameID` " 属性，以便为审核日志记录和单点注销正确识别用户。
4. 通过调用以下 API 方法创建一个或多个经过第三方 IdP 身份验证的集群管理员用户帐户以进行授权 ： `AddIdpClusterAdmin`

IdP 集群管理员的用户名应与 SAML 属性名称 / 值映射匹配以获得所需效果，如以下示例所示：

- email=bob@company.com —其中 IdP 配置为释放 SAML 属性中的电子邮件地址。
- group=cluster-administrator —其中 IdP 配置为释放所有用户都应具有访问权限的组属性。请注意，出于安全考虑， SAML 属性名称 / 值配对区分大小写。

5. 通过调用以下 API 方法为集群启用 MFA： `EnableIdpAuthentication`

了解更多信息

- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

用于多因素身份验证的追加信息

您应了解以下与多因素身份验证相关的注意事项。

- 要刷新不再有效的 IdP 证书，您需要使用非 IdP 管理员用户调用以下 API 方法：`UpdateIdpConfiguration`
- MFA 与长度小于 2048 位的证书不兼容。默认情况下，系统会在集群上创建 2048 位 SSL 证书。调用 API 方法时，应避免设置较小的证书： `setSSLCertificate`

如果集群使用的证书在升级前小于 2048 位，则在升级到 Element 12.0 或更高版本后，必须使用 2048 位或更高版本的证书更新集群证书。

- IdP 管理员用户不能用于直接调用 API （例如通过 SDK 或 Postman ）或用于其他集成（例如 OpenStack Cinder 或 vCenter 插件）。如果需要创建具有这些功能的用户，请添加 LDAP 集群管理员用户或本地集群管理员用户。

了解更多信息

- "使用 Element API 管理存储"
- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

配置集群设置

为集群启用和禁用空闲加密

使用 SolidFire 集群，您可以对存储在集群驱动器上的所有空闲数据进行加密。您可以使用任一方法在集群范围内对自加密驱动器（ SED ）启用保护 "基于硬件或软件的空闲加密"。

您可以使用 Element UI 或 API 启用空闲硬件加密。启用空闲硬件加密功能不会影响集群的性能或效率。您只能使用 Element API 启用空闲软件加密。

默认情况下，在创建集群期间不会启用基于硬件的空闲加密，您可以从 Element UI 中启用和禁用此加密。

对于 SolidFire 全闪存存储集群，必须在创建集群期间启用空闲软件加密，并且在创建集群后无法禁用该加密。

您需要的内容

- 您拥有启用或更改加密设置的集群管理员权限。
- 对于基于硬件的空闲加密，在更改加密设置之前，您已确保集群处于运行状况良好的状态。
- 如果要禁用加密，则集群中必须有两个节点，才能访问密钥以禁用驱动器上的加密。

检查空闲时加密状态

要查看集群上的空闲加密和 / 或空闲软件加密的当前状态，请使用 "GetClusterInfo" 方法您可以使用 "GetSoftwareEncryptionAtRestInfo" 获取集群用于对空闲数据进行加密的信息的方法。

`https://<MVIP>/` 上的 Element 软件 UI 信息板当前仅显示基于硬件的加密的空闲加密状态。

选项

- [启用基于硬件的空闲加密]
- [启用基于软件的空闲加密]
- [禁用基于硬件的空闲加密]

启用基于硬件的空闲加密

要使用外部密钥管理配置启用空闲加密，必须通过启用空闲加密 "API"。使用现有 Element UI 按钮启用将还原为使用内部生成的密钥。

1. 从 Element UI 中，选择 * 集群 * > * 设置 * 。
2. 选择 * 启用空闲加密 * 。

启用基于软件的空闲加密

在集群上启用空闲软件加密后，无法禁用此功能。

1. 在创建集群期间，运行 "创建集群方法" 使用 `enableSoftwareEncryptionAtRest` 设置为 `true` 。

禁用基于硬件的空闲加密

1. 从 Element UI 中，选择 * 集群 * > * 设置 * 。
2. 选择 * 禁用空闲加密 * 。

了解更多信息

- "SolidFire 和 Element 软件文档"
- "早期版本的 NetApp SolidFire 和 Element 产品的文档"

设置集群全满阈值

您可以使用以下步骤更改系统生成块集群填充度警告的级别。此外，您还可以使用 ModifyClusterFullThreshold API 方法更改系统生成块或元数据警告的级别。

您需要的内容

您必须具有集群管理员权限。

步骤

1. 单击 * 集群 * > * 设置 * 。
2. 在 Cluster Full Settings 部分的 * 当 Helix 无法从节点故障中恢复之前剩余 _% 容量时发出警告警报 * 中输入一个百分比。
3. 单击 * 保存更改 * 。

了解更多信息

"如何计算 Element 的块空间阈值"

启用和禁用卷负载平衡

从Element 128开始、您可以使用卷负载平衡根据每个卷的实际IOPS (而不是QoS策略中配置的最小IOPS)在节点之间平衡卷。您可以使用Element UI或API启用和禁用卷负载平衡、此功能默认处于禁用状态。

步骤

1. 选择*集群*>*设置*。
2. 在集群专用部分中、更改卷负载平衡的状态：

   启用卷负载平衡

   选择*启用实际IOPs*上的负载平衡，然后确认您的选择。

   禁用卷负载平衡：

   选择*禁用实际IOPs*上的负载平衡，然后确认您的选择。

3. (可选)选择*Reporting"(报告)>*Overview*以确认实际IOPS平衡状态更改。您可能需要向下滚动集群运行状况信息才能查看状态。

了解更多信息

- "使用API启用卷负载平衡"
- "使用API禁用卷负载平衡"
- "创建和管理卷 QoS 策略"

启用和禁用支持访问

您可以启用支持访问，以便临时允许 NetApp 支持人员通过 SSH 访问存储节点以进行故障排除。

要更改支持访问权限，您必须具有集群管理员权限。

1. 单击 * 集群 * > * 设置 * 。
2. 在启用 / 禁用支持访问部分中，输入要允许支持人员访问的持续时间（以小时为单位）。
3. 单击 * 启用支持访问 * 。
4. * 可选： * 要禁用支持访问，请单击 * 禁用支持访问 * 。

管理使用条款横幅

您可以启用，编辑或配置包含用户消息的横幅。

选项

[启用使用条款横幅] [编辑使用条款横幅] [禁用使用条款横幅]

启用使用条款横幅

您可以启用在用户登录到 Element UI 时显示的 " 使用条款 " 横幅。当用户单击此横幅时，将显示一个文本对话框，其中包含您为集群配置的消息。可以随时取消此横幅。

要启用使用条款功能，您必须具有集群管理员权限。

1. 单击 * 用户 * > * 使用条款 * 。
2. 在 * 使用条款 * 表单中，输入要在使用条款对话框中显示的文本。

   请勿超过 4096 个字符。

3. 单击 * 启用 * 。

编辑使用条款横幅

您可以编辑用户在选择使用条款登录横幅时看到的文本。

您需要的内容

- 要配置使用条款，您必须具有集群管理员权限。
- 确保已启用使用条款功能。

步骤

1. 单击 * 用户 * > * 使用条款 * 。
2. 在 * 使用条款 * 对话框中，编辑要显示的文本。

   请勿超过 4096 个字符。

3. 单击 * 保存更改 * 。

禁用使用条款横幅

您可以禁用使用条款横幅。禁用此横幅后，用户在使用 Element UI 时不再需要接受使用条款。

您需要的内容

- 要配置使用条款，您必须具有集群管理员权限。
- 确保已启用使用条款。

步骤

1. 单击 * 用户 * > * 使用条款 * 。
2. 单击 * 禁用 * 。

设置网络时间协议

配置要查询的集群的网络时间协议服务器

您可以指示集群中的每个节点查询网络时间协议（ NTP ）服务器以获取更新。集群仅会联系已配置的服务器并从这些服务器请求 NTP 信息。

NTP 用于通过网络同步时钟。在初始集群设置过程中，应连接到内部或外部 NTP 服务器。

在集群上配置 NTP 以指向本地 NTP 服务器。您可以使用 IP 地址或 FQDN 主机名。创建集群时的默认 NTP 服务器设置为 us.pool.ntp.org ；但是，根据 SolidFire 集群的物理位置，无法始终与此站点建立连接。

使用 FQDN 取决于单个存储节点的 DNS 设置是否已设置且正常运行。为此，请在每个存储节点上配置 DNS 服务器，并通过查看网络端口要求页面确保端口已打开。

您最多可以输入五个不同的 NTP 服务器。

您可以同时使用 IPv4 和 IPv6 地址。

您需要的内容

要配置此设置，您必须具有集群管理员权限。

步骤

1. 在服务器设置中配置 IP 和 / 或 FQDN 列表。
2. 确保已在节点上正确设置 DNS 。
3. 单击 * 集群 * > * 设置 * 。
4. 在网络时间协议设置下，选择 * 否 * ，它使用标准 NTP 配置。
5. 单击 * 保存更改 * 。

了解更多信息

- "配置集群以侦听 NTP 广播"

- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

配置集群以侦听 NTP 广播

通过使用广播模式，您可以指示集群中的每个节点在网络上侦听特定服务器发出的网络时间协议（ Network Time Protocol ， NTP ）广播消息。

NTP 用于通过网络同步时钟。在初始集群设置过程中，应连接到内部或外部 NTP 服务器。

您需要的内容

- 要配置此设置，您必须具有集群管理员权限。
- 您必须将网络上的 NTP 服务器配置为广播服务器。

步骤

1. 单击 * 集群 * > * 设置 * 。
2. 在服务器列表中输入正在使用广播模式的一个或多个 NTP 服务器。
3. 在网络时间协议设置下，选择 * 是 * 以使用广播客户端。
4. 要设置广播客户端，请在 * 服务器 * 字段中输入您在广播模式下配置的 NTP 服务器。
5. 单击 * 保存更改 * 。

了解更多信息

- "配置要查询的集群的网络时间协议服务器"
- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

管理 SNMP

了解 SNMP

您可以在集群中配置简单网络管理协议（ Simple Network Management Protocol ， SNMP ）。

您可以选择 SNMP 请求程序，选择要使用的 SNMP 版本，确定 SNMP 基于用户的安全模型（ User-Based Security Model ， USM ）用户并配置陷阱以监控 SolidFire 集群。您还可以查看和访问管理信息库文件。

您可以同时使用 IPv4 和 IPv6 地址。

SNMP 详细信息

在集群选项卡的 SNMP 页面上，您可以查看以下信息。

- * SNMP MIB *

  可供查看或下载的 MIB 文件。

- * 常规 SNMP 设置 *

  您可以启用或禁用 SNMP 。启用 SNMP 后，您可以选择要使用的版本。如果使用版本 2 ，则可以添加请求程序；如果使用版本 3 ，则可以设置 USM 用户。

- * SNMP 陷阱设置 *

  您可以确定要捕获的陷阱。您可以为每个陷阱接收方设置主机，端口和社区字符串。

配置 **SNMP** 请求程序

启用 SNMP 版本 2 后，您可以启用或禁用请求程序，并将请求程序配置为接收授权的 SNMP 请求。

1. 单击菜单： Cluster[SNMP] 。
2. 在 * 常规 SNMP 设置 * 下，单击 * 是 * 以启用 SNMP 。
3. 从 * 版本 * 列表中，选择 * 版本 2* 。
4. 在 * 请求程序 * 部分中，输入 * 社区字符串 * 和 * 网络 * 信息。

   默认情况下，社区字符串为公有，网络为 localhost 。您可以更改这些默认设置。

5. * 可选： * 要添加另一个请求程序，请单击 * 添加请求程序 * 并输入 * 社区字符串 * 和 * 网络 * 信息。
6. 单击 * 保存更改 * 。

了解更多信息

- 配置 SNMP 陷阱
- 使用管理信息库文件查看受管对象数据

配置 **SNMP USM** 用户

启用 SNMP 版本 3 时，需要配置 USM 用户以接收授权的 SNMP 请求。

1. 单击 * 集群 * > * SNMP * 。
2. 在 * 常规 SNMP 设置 * 下，单击 * 是 * 以启用 SNMP 。
3. 从 * 版本 * 列表中，选择 * 版本 3* 。
4. 在 * USM Users* 部分中，输入名称，密码和密码短语。
5. * 可选： * 要添加另一个 USM 用户，请单击 * 添加 USM 用户 * 并输入名称，密码和密码短语。
6. 单击 * 保存更改 * 。

配置 **SNMP** 陷阱

系统管理员可以使用 SNMP 陷阱（也称为通知）监控 SolidFire 集群的运行状况。

启用 SNMP 陷阱后， SolidFire 集群将生成与事件日志条目和系统警报关联的陷阱。要接收 SNMP 通知，您需

要选择应生成的陷阱，并确定陷阱信息的收件人。默认情况下，不会生成任何陷阱。

1. 单击 * 集群 * > * SNMP * 。
2. 在 * SNMP 陷阱设置 * 部分中选择系统应生成的一种或多种类型的陷阱：
   - 集群故障陷阱
   - 集群已解决故障陷阱
   - 集群事件陷阱
3. 在 * 陷阱收件人 * 部分中，输入收件人的主机，端口和社区字符串信息。
4. * 可选 * ：要添加另一个陷阱接收方，请单击 * 添加陷阱接收方 * 并输入主机，端口和社区字符串信息。
5. 单击 * 保存更改 * 。

使用管理信息库文件查看受管对象数据

您可以查看和下载用于定义每个受管对象的管理信息库（ MIB ）文件。SNMP 功能支持对 SolidFire-StorageCluster-MIB 中定义的对象进行只读访问。

MIB 中提供的统计数据显示了以下各项的系统活动：

- 集群统计信息
- 卷统计信息
- 按帐户统计信息显示卷
- 节点统计信息
- 其他数据，例如报告，错误和系统事件

此外，系统还支持访问包含 SF 系列产品的上一级访问点（ OID ）的 MIB 文件。

步骤

1. 单击 * 集群 * > * SNMP * 。
2. 在 * SNMP MIBS* 下，单击要下载的 MIB 文件。
3. 在显示的下载窗口中，打开或保存 MIB 文件。

管理驱动器

每个节点都包含一个或多个物理驱动器，用于存储集群的部分数据。成功将驱动器添加到集群后，集群将利用驱动器的容量和性能。您可以使用 Element UI 管理驱动器。

驱动器详细信息

"Cluster" 选项卡上的 "Drives" 页面提供了集群中活动驱动器的列表。您可以通过从 "Active" ， "Available" ， "Removing" ， "Erasing" 和 "Failed" 选项卡中选择来筛选页面。

首次初始化集群时，活动驱动器列表为空。创建新的 SolidFire 集群后，您可以添加未分配给集群并在 " 可用 " 选项卡中列出的驱动器。

以下元素将显示在活动驱动器列表中。

- * 驱动器 ID*

  分配给驱动器的序列号。

- * 节点 ID*

  将节点添加到集群时分配的节点编号。

- * 节点名称 *

  托管驱动器的节点的名称。

- * 插槽 *

  驱动器实际所在的插槽编号。

- * 容量 *

  驱动器的大小，以 GB 为单位。

- * 串行 *

  驱动器的序列号。

- * 剩余耗损 *

  损耗级别指示器。

  存储系统会报告每个固态驱动器（ SSD ）上可用于写入和擦除数据的近似耗损量。如果某个驱动器消耗了 5% 的设计写入和擦除周期，则会报告剩余耗损率为 95% 。系统不会自动刷新驱动器损耗信息；您可以刷新或关闭并重新加载此页面以刷新此信息。

- * 类型 *

  驱动器的类型。类型可以是块或元数据。

有关详细信息 ...

- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

管理节点

管理节点

您可以从集群选项卡的节点页面管理 SolidFire 存储和光纤通道节点。

如果新添加的节点占用的集群总容量超过 50% ，则此节点的某些容量将变为不可用（ " 孤立 " ），以使其符合容量规则。在添加更多存储之前，情况始终如此。如果添加的节点非常大，并且也不遵守容量规则，则先前的孤

立节点将不再处于孤立状态，而新添加的节点将变为孤立状态。应始终成对添加容量，以避免发生这种情况。当节点变为孤立时，会引发相应的集群故障。

了解更多信息

将节点添加到集群

将节点添加到集群

您可以在需要更多存储时或在创建集群后向集群添加节点。首次打开电源时，节点需要进行初始配置。配置节点后，它将显示在待定节点列表中，您可以将其添加到集群中。

集群中每个节点上的软件版本必须兼容。将节点添加到集群时，集群会根据需要在新节点上安装集群版本的 NetApp Element 软件。

您可以向现有集群添加容量较小或较大的节点。您可以向集群添加更大的节点容量，以支持容量增长。必须成对向节点较小的集群添加较大的节点。这样，如果一个较大的节点发生故障，双 Helix 就可以有足够的空间来移动数据。您可以将较小的节点容量添加到较大的节点集群以提高性能。

> 如果新添加的节点占用的集群总容量超过 50% ，则此节点的某些容量将变为不可用（ " 孤立 " ），以使其符合容量规则。在添加更多存储之前，情况始终如此。如果添加的节点非常大，并且也不遵守容量规则，则先前的孤立节点将不再处于孤立状态，而新添加的节点将变为孤立状态。应始终成对添加容量，以避免发生这种情况。当节点变为孤立时，将引发 strandedCapacity 集群故障。

"NetApp 视频：按需扩展：扩展 SolidFire 集群"

您可以向NetApp HCI 设备添加节点。

步骤

1. 选择 * 集群 * > * 节点 * 。
2. 单击 * 待定 * 以查看待定节点列表。

   添加节点的过程完成后、这些节点将显示在"Active nodes"列表中。在此之前，待定节点将显示在 "Pending Active" 列表中。

   将待定节点添加到集群时、SolidFire 会在这些节点上安装集群的Element软件版本。这可能需要几分钟时间。

3. 执行以下操作之一：
   - 要添加单个节点，请单击要添加的节点对应的 * 操作 * 图标。
   - 要添加多个节点，请选中要添加的节点对应的复选框，然后选中 * 批量操作 * 。* 注： * 如果要添加的节点的 Element 软件版本与集群上运行的版本不同，则集群会异步将此节点更新为集群主节点上运行的 Element 软件版本。更新节点后，它会自动将自己添加到集群中。在此异步过程中，节点将处于 pendingActive 状态。
4. 单击 * 添加 * 。

   此节点将显示在活动节点列表中。

了解更多信息

节点版本控制和兼容性

节点版本控制和兼容性

节点兼容性取决于节点上安装的 Element 软件版本。如果节点和集群的版本不兼容，则基于 Element 软件的存储集群会根据集群上的 Element 软件版本自动创建节点映像。

以下列表介绍了构成 Element 软件版本号的软件版本重要性级别：

- * 主要 *

  第一个数字用于指定软件版本。不能将具有一个主要组件编号的节点添加到包含具有不同主要修补程序编号的节点的集群中，也不能使用具有混合主要版本的节点创建集群。

- * 次要 *

  第二个数字用于指定已添加到主要版本的现有软件功能的较小软件功能或增强功能。此组件会在主要版本组件中递增，以表示此增量版本与具有其他次要组件的任何其他 Element 软件增量版本不兼容。例如， 11.0 与 11.1 不兼容， 11.1 与 11.2 不兼容。

- * 微 *

  第三个数字用于指定与主 .minor 组件表示的 Element 软件版本兼容的修补程序（增量版本）。例如， 11.0.1 与 11.0.2 兼容， 11.0.2 与 11.0.3 兼容。

主要版本号和次要版本号必须匹配才能兼容。微型数字不必匹配即可实现兼容性。

混合节点环境中的集群容量

您可以在一个集群中混用不同类型的节点。SF 系列 2405 ， 3010 ， 4805 ， 6010 ， 9605 ， 9010 ， 19210 ， 38410 和 H 系列可以同时位于一个集群中。

H 系列由 H610S-1 ， H610S-2 ， H610S-4 和 H410S 节点组成。这些节点支持 10GbE 和 25GbE 。

最好不要混用非加密节点和加密节点。在混合节点集群中，任何节点都不能超过集群总容量的 33% 。例如，在具有四个 SF 系列 4805 节点的集群中，可以单独添加的最大节点是 SF 系列 9605 。在这种情况下，集群容量阈值是根据最大节点的潜在损失计算的。

根据您的Element软件版本、不支持以下SF系列存储节点：

开头为 ...	不支持存储节点...
Element 12.8	• SF4805 • SF9605 • SF19210 • SF38410

开头为 ...	不支持存储节点...
要素12.7.	• SF2405 • SF9608
Element 12.0	• SF3010 • SF6010 • SF9010

如果您尝试将其中一个节点升级到不受支持的Element版本、则会看到一条错误消息、指出Element 12.x不支持此节点

查看节点详细信息

您可以查看单个节点的详细信息，例如服务标签，驱动器详细信息以及利用率图形和驱动器统计信息。"Cluster" 选项卡的 "Nodes" 页面提供了 "Version" 列，您可以在此列中查看每个节点的软件版本。

步骤

1. 单击 * 集群 * > * 节点 * 。
2. 要查看特定节点的详细信息，请单击某个节点的 * 操作 * 图标。
3. 单击 * 查看详细信息 * 。
4. 查看节点详细信息：
   - * 节点 ID* ： 系统为节点生成的 ID 。
   - * 节点名称 * ： 节点的主机名。
   - * 节点角色 * ： 节点在集群中的角色。可能值：
     - Cluster Master ： 执行集群范围管理任务并包含 MVIP 和 SVIP 的节点。
     - 集合节点：加入集群的节点。根据集群大小，有 3 个或 5 个集合节点。
     - Fibre Channel ： 集群中的节点。
   - * 节点类型 * ： 节点的型号类型。
   - * 活动驱动器 * ： 节点中活动驱动器的数量。
   - 节点利用率：基于节点利用率的节点利用率百分比。显示的值以百分比形式显示为recentMaryTotalHeat。从Element 12.8开始提供。
   - * 管理 IP* ： 为执行 1GbE 或 10GbE 网络管理任务而分配给节点的管理 IP （ MIP ）地址。
   - * 集群 IP* ： 分配给节点的集群 IP （ CIP ）地址，用于在同一集群中的节点之间进行通信。
   - * 存储 IP* ： 分配给用于 iSCSI 网络发现和所有数据网络流量的节点的存储 IP （ SIP ）地址。
   - * 管理 VLAN ID* ： 管理局域网的虚拟 ID 。
   - * 存储 VLAN ID* ： 存储局域网的虚拟 ID 。
   - * 版本 * ： 每个节点上运行的软件版本。

- * 复制端口 *： 节点上用于远程复制的端口。
- * 服务标签 *： 分配给节点的唯一服务标签号。
- 自定义保护域：分配给节点的自定义保护域。

查看光纤通道端口详细信息

您可以从 FC 端口页面查看光纤通道端口的详细信息，例如其状态，名称和端口地址。

查看有关连接到集群的光纤通道端口的信息。

步骤

1. 单击 * 集群 * > * FC 端口 * 。
2. 要筛选此页面上的信息，请单击 * 筛选器 * 。
3. 查看详细信息：
   - * 节点 ID*： 托管连接会话的节点。
   - * 节点名称 *： 系统生成的节点名称。
   - * 插槽 *： 光纤通道端口所在的插槽编号。
   - * HBA Port*： 光纤通道主机总线适配器（ HBA ）上的物理端口。
   - * WWN*： 全球通用节点名称。
   - * WWPN *： 目标全球通用端口名称。
   - * 交换机 WWW*： 光纤通道交换机的全球通用名称。
   - * 端口状态 *： 端口的当前状态。
   - **nPort ID**： 光纤通道网络结构上的节点端口 ID 。
   - * 速度 *： 协商的光纤通道速度。可能值如下：
     - 4 Gbps
     - 8 Gbps
     - 16 Gbps

了解更多信息

- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

管理虚拟网络

管理虚拟网络

通过 SolidFire 存储中的虚拟网络，可以将不同逻辑网络上的多个客户端之间的流量连接到一个集群。通过使用 VLAN 标记在网络堆栈中隔离与集群的连接。

了解更多信息

- 添加虚拟网络
- 启用虚拟路由和转发
- 编辑虚拟网络
- 编辑 VRF VLAN
- 删除虚拟网络

添加虚拟网络

您可以将新的虚拟网络添加到集群配置中，以使多租户环境能够连接到运行 Element 软件的集群。

您需要的内容

- 确定要分配给集群节点上虚拟网络的 IP 地址块。
- 确定要用作所有 NetApp Element 存储流量的端点的存储网络 IP （ SVIP ）地址。

对于此配置，必须考虑以下条件：

- 未启用 VRF 的 VLAN 要求启动程序与 SVIP 位于同一子网中。
- 启用了 VRF 的 VLAN 不要求启动程序与 SVIP 位于同一子网中，并且支持路由。
- 默认 SVIP 不要求启动程序与 SVIP 位于同一子网中，并且支持路由。

添加虚拟网络时，系统会为每个节点创建一个接口，每个接口都需要一个虚拟网络 IP 地址。创建新虚拟网络时指定的 IP 地址数量必须等于或大于集群中的节点数量。虚拟网络地址由各个节点批量配置并自动分配给这些节点。您无需手动为集群中的节点分配虚拟网络地址。

步骤

1. 单击 * 集群 * > * 网络 * 。
2. 单击 * 创建 VLAN* 。
3. 在 * 创建新 VLAN* 对话框中，在以下字段中输入值：
    - * VLAN 名称 *
    - * VLAN 标记 *
    - * SVIP*
    - * 网络掩码 *
    - （可选） * 问题描述 *
4. 在 * IP 地址块 * 中输入 IP 地址范围的 * 起始 IP* 地址。
5. 输入 IP 范围的 * 大小 * 作为要包含在块中的 IP 地址数。
6. 单击 * 添加块 * 为此 VLAN 添加非连续 IP 地址块。
7. 单击 * 创建 VLAN* 。

查看虚拟网络详细信息

步骤

1. 单击 * 集群 * > * 网络 * 。
2. 查看详细信息。
   - * ID * ： VLAN 网络的唯一 ID ，由系统分配。
   - * 名称 * ： 用户为 VLAN 网络分配的唯一名称。
   - * VLAN 标记 * ： 创建虚拟网络时分配的 VLAN 标记。
   - * 。 svip* ： 分配给虚拟网络的存储虚拟 IP 地址。
   - * 网络掩码 * ： 此虚拟网络的网络掩码。
   - * 网关 * ： 虚拟网络网关的唯一 IP 地址。必须启用 VRF 。
   - * 已启用 VRF * ： 指示是否已启用虚拟路由和转发。
   - * 已用 IP * ： 用于虚拟网络的虚拟网络 IP 地址范围。

启用虚拟路由和转发

您可以启用虚拟路由和转发（ VRF ），从而允许一个路由器中存在多个路由表实例并同时运行。此功能仅适用于存储网络。

您只能在创建 VLAN 时启用 VRF 。如果要切换回非 VRF ，必须删除并重新创建 VLAN 。

1. 单击 * 集群 * > * 网络 * 。
2. 要在新 VLAN 上启用 VRF ，请选择 * 创建 VLAN* 。
   a. 输入新 VRF/VLAN 的相关信息。请参见添加虚拟网络。
   b. 选中 * 启用 VRF* 复选框。
   c. * 可选 * ： 输入网关。
3. 单击 * 创建 VLAN* 。

了解更多信息

添加虚拟网络

编辑虚拟网络

您可以更改 VLAN 属性，例如 VLAN 名称，网络掩码和 IP 地址块大小。无法修改 VLAN 的 VLAN 标记和 SVIP 。对于非 VRF VLAN ，网关属性不是有效参数。

如果存在任何 iSCSI ，远程复制或其他网络会话，则修改可能会失败。

在管理 VLAN IP 地址范围的大小时，应注意以下限制：

- 您只能从创建 VLAN 时分配的初始 IP 地址范围中删除 IP 地址。
- 您可以删除在初始 IP 地址范围之后添加的 IP 地址块，但不能通过删除 IP 地址来调整 IP 块的大小。

- 当您尝试从初始 IP 地址范围或 IP 块中删除集群中节点正在使用的 IP 地址时，此操作可能会失败。
- 您不能将特定的已用 IP 地址重新分配给集群中的其他节点。

您可以使用以下操作步骤添加 IP 地址块：

1. 选择 * 集群 * > * 网络 * 。
2. 选择要编辑的 VLAN 对应的 "Actions" 图标。
3. 选择 * 编辑 * 。
4. 在 * 编辑 VLAN* 对话框中，输入 VLAN 的新属性。
5. 选择 * 添加块 * 可为虚拟网络添加非连续 IP 地址块。
6. 选择 * 保存更改 * 。

故障排除知识库文章链接

链接到知识库文章，以帮助您解决管理 VLAN IP 地址范围的问题。

- "在 Element 集群上的 VLAN 中添加存储节点后出现重复 IP 警告"
- "如何在 Element 中确定正在使用的 VLAN IP 以及将这些 IP 分配给哪些节点"

编辑 **VRF VLAN**

您可以更改 VRF VLAN 属性，例如 VLAN 名称，网络掩码，网关和 IP 地址块。

1. 单击 * 集群 * > * 网络 * 。
2. 单击要编辑的 VLAN 对应的 "Actions" 图标。
3. 单击 * 编辑 * 。
4. 在 * 编辑 VLAN* 对话框中输入 VRF VLAN 的新属性。
5. 单击 * 保存更改 * 。

删除虚拟网络

您可以删除虚拟网络对象。在删除虚拟网络之前，必须将地址块添加到另一个虚拟网络。

1. 单击 * 集群 * > * 网络 * 。
2. 单击要删除的 VLAN 对应的 "Actions" 图标。
3. 单击 * 删除 * 。
4. 确认消息。

了解更多信息

编辑虚拟网络

创建支持 FIPS 驱动器的集群

为 FIPS 驱动器功能准备元素集群

在许多客户环境中部署解决方案时，安全性变得越来越重要。联邦信息处理标准（ FIPS ）是计算机安全和互操作性的标准。经 FIPS 140-2 认证的空闲数据加密是整体安全解决方案的一个组成部分。

要准备启用 FIPS 驱动器功能，您应避免混用某些支持 FIPS 驱动器而另一些不支持 FIPS 驱动器的节点。

根据以下条件，集群被视为符合 FIPS 驱动器：

- 所有驱动器均已认证为 FIPS 驱动器。
- 所有节点均为 FIPS 驱动器节点。
- 已启用空闲加密（ EAR ）。
- 已启用 FIPS 驱动器功能。所有驱动器和节点都必须支持 FIPS ，并且必须启用空闲加密才能启用 FIPS 驱动器功能。

启用空闲加密

您可以启用和禁用集群范围的空闲加密。默认情况下，不会启用此功能。要支持 FIPS 驱动器，必须启用空闲加密。

1. 在 NetApp Element 软件 UI 中，单击 * 集群 * > * 设置 * 。
2. 单击 * 启用空闲加密 * 。

了解更多信息

- 为集群启用和禁用加密
- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

确定节点是否已准备好使用 FIPS 驱动器功能

您应使用 NetApp Element 软件 GetFipsReport API 方法检查存储集群中的所有节点是否均已准备好支持 FIPS 驱动器。

生成的报告将显示以下状态之一：

- None ： 节点不支持 FIPS 驱动器功能。
- Partial ： 节点支持 FIPS ，但并非所有驱动器都是 FIPS 驱动器。
- Ready ： 节点支持 FIPS ，并且所有驱动器均为 FIPS 驱动器或不存在任何驱动器。

步骤

1. 使用 Element API 输入以下命令，检查存储集群中的节点和驱动器是否支持 FIPS 驱动器：

`GetFipsReport`

2. 查看结果，记下未显示 Ready 状态的任何节点。
3. 对于未显示 Ready 状态的任何节点，请检查此驱动器是否支持 FIPS 驱动器功能：
   - 使用 Element API 输入： `GetHardwareList`
   - 请注意 * 驱动器加密容量类型 * 的值。如果为 FIPS ，则硬件可以支持 FIPS 驱动器功能。

     查看详情 `GetFipsReport` 或者 `ListDriveHardware` 在 "Element API 参考"。
4. 如果驱动器不支持 FIPS 驱动器功能，请将硬件更换为 FIPS 硬件（节点或驱动器）。

了解更多信息

- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

启用 FIPS 驱动器功能

您可以使用 NetApp Element 软件 `EnableFeature` API 方法启用 FIPS 驱动器功能。

必须在集群上启用空闲加密，并且所有节点和驱动器都必须支持 FIPS ，如 GetFipsReport 为所有节点显示 Ready 状态时所示。

步骤

1. 使用 Element API 输入以下命令，在所有驱动器上启用 FIPS ：

   `EnableFeature` 参数： `FipsDrives`

了解更多信息

- "使用 Element API 管理存储"
- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

检查 FIPS 驱动器状态

您可以使用 NetApp Element 软件 `GetFeatureStatus` API 方法检查集群上是否启用了 FIPS 驱动器功能，该方法显示了 FIPS 驱动器已启用状态是 true 还是 false 。

1. 使用 Element API ，输入以下命令检查集群上的 FIPS 驱动器功能：

   `GetFeatureStatus`

2. 查看 `GetFeatureStatus` API 调用的结果。如果 FIPS 驱动器启用值为 True ，则会启用 FIPS 驱动器功能。

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

了解更多信息

- "使用 Element API 管理存储"
- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

对 **FIPS** 驱动器功能进行故障排除

使用 NetApp Element 软件 UI ，您可以查看有关系统中与 FIPS 驱动器功能相关的集群故障或错误信息的警报。

1. 使用 Element UI ，选择 * 报告 * > * 警报 * 。
2. 查找集群故障，包括：
    - FIPS 驱动器不匹配
    - FIPS 驱动器不合规
3. 有关解决方案建议，请参见集群故障代码信息。

了解更多信息

- 集群故障代码
- "使用 Element API 管理存储"
- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

建立安全通信

在集群上为 **HTTPS** 启用 **FIPS 140-2**

您可以使用 EnableFeature API 方法为 HTTPS 通信启用 FIPS 140-2 操作模式。

借助 NetApp Element 软件，您可以选择在集群上启用联邦信息处理标准（ Federal Information Processing Standards ， FIPS ） 140-2 操作模式。启用此模式将激活NetApp加密安全模块(NetApp Cryptographic Security Module、NCSM)、并对通过HTTPS与NetApp Element UI和API进行的所有通信使用FIPS 140-2 1级认证加密。

启用 FIPS 140-2 模式后，无法将其禁用。启用 FIPS 140-2 模式后，集群中的每个节点都会重新启动并运行自检，以确保 NCSM 已正确启用并在 FIPS 140-2 认证模式下运行。这会导致集群上的管理和存储连接中断。您应仔细规划，并且只有在您的环境需要此模式提供的加密机制时才启用此模式。

有关详细信息，请参见 Element API 信息。

以下是用于启用 FIPS 的 API 请求示例：

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

启用此操作模式后，所有 HTTPS 通信都将使用 FIPS 140-2 批准的密码。

了解更多信息

- SSL 密码
- "使用 Element API 管理存储"
- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

SSL 密码

SSL 密码是主机用来建立安全通信的加密算法。Element 软件支持标准密码，而启用 FIPS 140-2 模式时则支持非标准密码。

以下列表提供了 Element 软件支持的标准安全套接字层（ SSL ）密码以及启用 FIPS 140-2 模式时支持的 SSL 密码：

- 已禁用 * FIPS 140-2 *

  tls_DHE_RSA_WIT_AES_128_CBC_SHA256 （ DH 2048 ） - A

  tls_DHE_RSA_WIT_AES_128_GCM_SHA256 （ DH 2048 ） - A

  tls_DHE_RSA_WIT_AES_256_CBC_SHA256 （ DH 2048 ） - A

  tls_DHE_RSA_WIT_AES_256_GCM_SHA384 （ DH 2048 ）— A

  tls_ECDHE_RSA_WIT_AES_128_CBC_SHA256 （ secp256r1 ）— A

  tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256 （ secp256r1 ）— A

tls_ECDHE_RSA_WITE_AES_256_CBC_SHA384 （ secp256r1 ） — A

tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384 （ secp256r1 ） — A

tls_rsa_and_3DES_EDE_CBC_SHA （ RSA 2048 ） - C

tls_rsa_and_aes_128_cbc_sha （ RSA 2048 ） — A

tls_rsa_and_aes_128_cbc_SHA256 （ RSA 2048 ） - A

tls_rsa_and_aes_128_gcm_SHA256 （ RSA 2048 ） — A

tls_rsa_and_aes_256_cbc_sha （ RSA 2048 ） — A

tls_rsa_and_aes_256_cbc_SHA256 （ RSA 2048 ） - A

tls_rsa_and_aes_256_gcm_SHA384 （ RSA 2048 ） — A

tls_rsa_and_Camellia_128_CBC_SHA （ RSA 2048 ） — A

tls_rsa_and_Camellia_256_CBC_SHA （ RSA 2048 ） — A

tls_rsa_and_ide_cbc_sha （ RSA 2048 ） — A

tls_rsa_and_rc4_128_md5 （ RSA 2048 ） - C

tls_rsa_and_rc4_128_sha （ RSA 2048 ） - C

tls_rsa_and_seed_cbc_sha （ RSA 2048 ） — A

- 已启用 * FIPS 140-2

tls_DHE_RSA_WIT_AES_128_CBC_SHA256 （ DH 2048 ） - A

tls_DHE_RSA_WIT_AES_128_GCM_SHA256 （ DH 2048 ） - A

tls_DHE_RSA_WIT_AES_256_CBC_SHA256 （ DH 2048 ） - A

tls_DHE_RSA_WIT_AES_256_GCM_SHA384 （ DH 2048 ） — A

tls_ECDHE_RSA_WITE_AES_128_CBC_SHA256 （ sect571r1 ） — A

tls_ECDHE_RSA_WIT_AES_128_CBC_SHA256 （ secp256r1 ） — A

tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256 （ secp256r1 ） — A

tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256 （ sect571r1 ） — A

tls_ECDHE_RSA_WITE_AES_256_CBC_SHA384 （ sect571r1 ） — A

tls_ECDHE_RSA_WITE_AES_256_CBC_SHA384 （ secp256r1 ） — A

tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384 （ secp256r1 ） — A

tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384 （ sect571r1 ）— A

tls_rsa_and_3DES_EDE_CBC_SHA （ RSA 2048 ） - C

tls_rsa_and_aes_128_cbc_sha （ RSA 2048 ）— A

tls_rsa_and_aes_128_cbc_SHA256 （ RSA 2048 ） - A

tls_rsa_and_aes_128_gcm_SHA256 （ RSA 2048 ）— A

tls_rsa_and_aes_256_cbc_sha （ RSA 2048 ）— A

tls_rsa_and_aes_256_cbc_SHA256 （ RSA 2048 ） - A

tls_rsa_and_aes_256_gcm_SHA384 （ RSA 2048 ）— A

了解更多信息

在集群上为 HTTPS 启用 FIPS 140-2

开始使用外部密钥管理

开始使用外部密钥管理

外部密钥管理（ External Key Management ， EKM ）可与集群外外部密钥服务器（ External Key Server ， EKS ）结合使用，提供安全身份验证密钥（ Authentication Key ， AK ）管理。在这种情况下，可以使用这些 AK 锁定和解锁自加密驱动器（ SED ） "空闲加密" 已在集群上启用。EKS 可以安全地生成和存储 AK 。集群利用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）（ OASIS 定义的标准协议）与 EKS 进行通信。

- "设置外部管理"
- "重新设置 REST 主密钥的软件加密密钥"
- "恢复不可访问或无效的身份验证密钥"
- "外部密钥管理 API 命令"

了解更多信息

- "CreateCluster API ，可用于启用空闲软件加密"
- "SolidFire 和 Element 软件文档"
- "早期版本的 NetApp SolidFire 和 Element 产品的文档"

设置外部密钥管理

您可以按照以下步骤操作，并使用列出的 Element API 方法设置外部密钥管理功能。

您需要的内容

- 如果要将外部密钥管理与空闲软件加密结合使用，则已使用启用空闲软件加密 "CreateCluster" 方法。

步骤

1. 与外部密钥服务器（ EKS ）建立信任关系。
   a. 通过调用以下 API 方法，为 Element 集群创建一个公共 / 专用密钥对，用于与密钥服务器建立信任关系： "CreatePublicPrivateKeyPair"
   b. 获取证书颁发机构需要签名的证书签名请求（ CSR ）。通过 CSR ，密钥服务器可以验证要访问密钥的 Element 集群是否已作为 Element 集群进行身份验证。调用以下 API 方法： "GetClientCertificateSignRequest"
   c. 使用 EKS/ 证书颁发机构对检索到的 CSR 进行签名。有关详细信息，请参见第三方文档。
2. 在集群上创建服务器和提供程序以与 EKS 进行通信。密钥提供程序用于定义应从何处获取密钥，服务器用于定义要与之通信的 EKS 的特定属性。
   a. 通过调用以下 API 方法创建密钥服务器详细信息所在的密钥提供程序： "CreateKeyProviderKmip"
   b. 通过调用以下 API 方法，创建一个提供证书颁发机构的签名证书和公有密钥证书的密钥服务器： "CreateKeyServerKmip" "TestKeyServerKmip"

      如果测试失败，请验证您的服务器连接和配置。然后重复测试。

   c. 通过调用以下 API 方法将密钥服务器添加到密钥提供程序容器中："AddKeyServerToProviderKmip" "TestKeyProviderKmip"

      如果测试失败，请验证您的服务器连接和配置。然后重复测试。

3. 执行以下操作之一作为空闲加密的下一步：
   a. （用于空闲硬件加密）启用 "空闲硬件加密" 通过调用来提供用于存储密钥的密钥服务器所在的密钥提供程序的 ID "EnableEncryptionAtRest" API 方法。

      > 您必须通过启用空闲加密 "API"。使用现有 Element UI 按钮启用空闲加密将使用内部生成的密钥对功能进行发生原因还原。

   b. （用于空闲软件加密） "空闲软件加密" 要使用新创建的密钥提供程序，请将密钥提供程序 ID 传递到 "RekeySoftwareEncryptionAtRestMasterKey" API 方法。

了解更多信息

- "为集群启用和禁用加密"
- "SolidFire 和 Element 软件文档"
- "早期版本的 NetApp SolidFire 和 Element 产品的文档"

重新设置 **REST** 主密钥的软件加密密钥

您可以使用 Element API 重新设置现有密钥的密钥。此过程将为外部密钥管理服务器创建一个新的替换主密钥。主密钥始终会替换为新的主密钥，并且不会复制或覆盖。

您可能需要在以下过程之一中重新设置密钥：

- 在从内部密钥管理到外部密钥管理的变更过程中创建新密钥。
- 创建一个新密钥，作为对安全相关事件的响应或保护。

> 此过程是异步的，在重新设置密钥操作完成之前返回响应。您可以使用 "GetAsyncResult" 对系统进行轮询以查看进程何时完成的方法。

您需要的内容

- 您已使用启用空闲软件加密 "CreateCluster" 方法，用于新集群，该集群不包含卷，也不具有 I/O使用 … "9510c8e68784d05acbae2e947dde3cd8" 在继续操作之前，确认状态为 `enabled` 。
- 您已拥有 "建立信任关系" 在 SolidFire 集群和外部密钥服务器（ EKS ）之间。运行 "TestKeyProviderKmip" 用于验证是否已建立与密钥提供程序的连接的方法。

步骤

1. 运行 "ListKeyProvidersKmip" 命令并复制密钥提供程序 ID （`keyProviderID`）。
2. 运行 "RekeySoftwareEncryptionAtRestMasterKey" 将 `keyManagementType` 参数设置为 `external` ，并将 `keyProviderID` 作为上一步中密钥提供程序的 ID 编号：

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

3. 从 `RekeySoftwareEncryptionAtRestMasterKey` 命令响应中复制 `asyncHandle` 值。
4. 运行 "GetAsyncResult" 包含上一步中的 `asyncHandle` 值的命令，用于确认配置更改。在命令响应中，您应看到旧主密钥配置已使用新密钥信息进行更新。复制新密钥提供程序 ID ，以供稍后使用。

```
{
   "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. 运行 `GetSoftwareEncryptionatRestInfo` 命令以确认新密钥详细信息（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
   },
}
```

了解更多信息

- "使用 Element API 管理存储"
- "SolidFire 和 Element 软件文档"
- "早期版本的 NetApp SolidFire 和 Element 产品的文档"

恢复不可访问或无效的身份验证密钥

有时，可能会发生需要用户干预的错误。如果发生错误，将生成集群故障（称为集群故障代码）。下面介绍了两种最可能的情况。

由于 **KmipServerFault** 集群故障，集群无法解锁驱动器。

当集群首次启动，密钥服务器不可访问或所需密钥不可用时，可能会发生这种情况。

1. 按照集群故障代码（如果有）中的恢复步骤进行操作。

可能会设置 **sliceServiceUnhealthy** 故障，因为元数据驱动器已标记为 **Failed** 并置于 **"available"** 状态。

清除步骤：

1. 重新添加驱动器。
2. 3 到 4 分钟后，检查 `sliceServiceUnhealthy` 故障是否已清除。

请参见 "集群故障代码" 有关详细信息 …

外部密钥管理 **API** 命令

列出可用于管理和配置 EKM 的所有 API 。

用于在集群与客户拥有的外部服务器之间建立信任关系：

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

用于定义客户拥有的外部服务器的特定详细信息：

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

用于创建和维护用于管理外部密钥服务器的密钥提供程序：

- CreateKeyProviderKmip
- DeleteKeyProviderKmip

- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

有关 API 方法的信息，请参阅 "API 参考信息"。

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。