管理您的系统
Element Software

NetApp
November 12, 2025

目录

管理您的系统

管理您的系统

您可以在 Element 用户界面中管理系统。这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。

- "启用多重身份验证"
- "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"

了解更多信息

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

启用多重身份验证

设置多重身份验证

多因素身份验证 (MFA) 使用第三方身份提供商 (IdP) 通过安全断言标记语言 (SAML) 来管理用户会话。 MFA 允许管理员根据需要配置其他身份验证因素，例如密码和短信，以及密码和电子邮件。

您可以使用 Element API 的以下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： "元素 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商 (IdP) 配置：`CreateIdpConfiguration`

   从第三方身份提供商 (IdP) 检索纯文本格式的身份提供商元数据。需要验证此元数据，以确保其 JSON 格式正确。有很多 JSON 格式化应用程序可供使用，例如： https://freeformatter.com/json-escape.html.

2. 通过 spMetadataUrl 检索集群元数据，并通过调用以下 API 方法将其复制到第三方身份提供商：`ListIdpConfigurations`

   spMetadataUrl 是一个 URL，用于从集群中检索身份提供商 (IdP) 的元数据，以便建立信任关系。

3. 在第三方身份提供商 (IdP) 上配置 SAML 断言，使其包含“`NameID`”属性，以便唯一标识用户进行审计日志记录，并使单点注销功能正常运行。
4. 通过调用以下 API 方法，创建一个或多个由第三方身份提供商 (IdP) 进行身份验证的集群管理员用户帐户：`AddIdpClusterAdmin`

为了达到预期效果，IdP 集群管理员的用户名应与 SAML 属性名称/值映射相匹配，如下例所示：

- email=bob@company.com — 其中 IdP 配置为在 SAML 属性中发布电子邮件地址。
- group=cluster-administrator - 其中 IdP 配置为释放一个组属性，所有用户都应该有权访问该组属性。请注意，出于安全考虑，SAML 属性名称/值对区分大小写。

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

查找更多信息

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

多因素身份验证的补充信息

关于多因素身份验证，您应该注意以下注意事项。

- 要刷新不再有效的身份提供商 (IdP) 证书，您需要使用非身份提供商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，集群上会创建一个 2048 位 SSL 证书。调用 API 方法时，应避免设置较小的证书： `SetSSLCertificate`

如果集群在升级前使用的证书小于 2048 位，则升级到 Element 12.0 或更高版本后，必须将集群证书更新为 2048 位或更高版本的证书。

- IdP 管理员用户不能直接用于进行 API 调用（例如，通过 SDK 或 Postman），也不能用于其他集成（例如，OpenStack Cinder 或 vCenter 插件）。如果需要创建具有这些权限的用户，请添加 LDAP 集群管理员用户或本地集群管理员用户。

查找更多信息

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

配置集群设置

启用和禁用集群的静态数据加密

使用SolidFire集群，您可以加密存储在集群驱动器上的所有静态数据。您可以使用以下任一方式启用对自加密驱动器 (SED) 的集群级保护"静态数据采用硬件或软件加密"。

您可以使用 Element UI 或 API 启用静态硬件加密。启用静态数据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 启用静态软件加密。

在集群创建期间，默认情况下不会启用基于硬件的静态加密，可以通过 Element UI 启用和禁用。

对于SolidFire全闪存存储集群，必须在创建集群期间启用静态软件加密，并且集群创建后不能禁用。

你需要什么

- 您拥有集群管理员权限，可以启用或更改加密设置。
- 对于基于硬件的静态加密，在更改加密设置之前，您已确保集群处于健康状态。
- 如果要禁用加密，则必须有两个节点参与集群才能访问密钥以禁用驱动器上的加密。

检查静态加密状态

要查看集群上静态加密和/或静态软件加密的当前状态，请使用以下方法："获取集群信息"方法。你可以使用"获取静态软件加密信息"获取集群用于加密静态数据的信息的方法。

Element软件用户界面仪表板 `https://<MVIP>/`目前仅显示基于硬件的加密的静态加密状态。

选项

- [启用基于硬件的静态数据加密]
- [启用静态数据软件加密]
- [禁用静态数据的硬件加密]

启用基于硬件的静态数据加密

要使用外部密钥管理配置启用静态加密，您必须通过以下方式启用静态加密："API" 。启用使用现有 Element UI 按钮后，将恢复使用内部生成的密钥。

1. 从元素用户界面中，选择“集群”>“设置”。
2. 选择“启用静态数据加密”。

启用静态数据软件加密

软件静态加密在集群上启用后无法禁用。

1. 在集群创建期间，运行"创建集群方法"和 `enableSoftwareEncryptionAtRest`设置为 `true`。

禁用静态数据的硬件加密

1. 从元素用户界面中，选择“集群”>“设置”。
2. 选择“禁用静态数据加密”。

查找更多信息

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

设置集群满阈值

您可以使用以下步骤更改系统生成块簇已满警告的级别。此外，您可以使用 ModifyClusterFullThreshold API 方法来更改系统生成块或元数据警告的级别。

你需要什么

您必须拥有集群管理员权限。

步骤

1. 点击“集群”>“设置”。
2. 在集群完全设置部分，输入一个百分比，表示在 Helix 无法从节点故障中恢复之前剩余容量为 _% 时发出警告警报。
3. 点击“保存更改”。

查找更多信息

"元素的块空间阈值是如何计算的"

启用和禁用卷负载均衡

从 Element 12.8 开始，您可以使用卷负载均衡，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 启用和禁用卷负载均衡（默认情况下处于禁用状态）。

步骤

1. 选择“集群”>“设置”。
2. 在“集群特定”部分，更改卷负载均衡的状态：

   启用卷负载均衡

   选择“启用基于实际 IOPS 的负载均衡”，并确认您的选择。

   禁用卷负载均衡：

   选择“禁用基于实际 IOPS 的负载均衡”，并确认您的选择。

3. （可选）选择“报告”>“概览”以确认“实际 IOPS 余额”的状态更改。您可能需要向下滚动集群健康信息才能查看状态。

查找更多信息

- "使用 API 启用卷负载均衡"
- "使用 API 禁用卷负载均衡"
- "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权限，以便临时允许NetApp支持人员通过 SSH 访问存储节点进行故障排除。

您必须拥有集群管理员权限才能更改支持访问权限。

1. 点击“集群”>“设置”。
2. 在“启用/禁用支持访问权限”部分，输入您希望允许支持人员访问的持续时间（以小时为单位）。
3. 点击“启用支持访问权限”。
4. *可选：*要禁用支持访问权限，请单击“禁用支持访问权限”。

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“使用条款”横幅，该横幅会在用户登录 Element UI 时显示。当用户点击横幅时，会出现一个文本对话框，其中包含您为集群配置的消息。横幅可以随时关闭。

您必须拥有集群管理员权限才能启用使用条款功能。

1. 点击“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

您可以编辑用户选择“使用条款”登录横幅时看到的文本。

你需要什么

- 您必须拥有集群管理员权限才能配置使用条款。
- 请确保已启用“使用条款”功能。

步骤

1. 点击“用户”>“使用条款”。
2. 在“使用条款”对话框中，编辑您想要显示的文本。

   请勿超过 4096 个字符。

3. 点击“保存更改”。

禁用“使用条款”横幅

您可以关闭“使用条款”横幅。禁用横幅后，用户在使用 Element UI 时不再需要接受使用条款。

你需要什么

- 您必须拥有集群管理员权限才能配置使用条款。
- 请确保已启用“使用条款”。

步骤

1. 点击“用户”>“使用条款”。
2. 单击“禁用”。

设置网络时间协议

配置集群要查询的网络时间协议服务器

您可以指示集群中的每个节点向网络时间协议 (NTP) 服务器查询更新。集群仅联系已配置的服务器，并向这些服务器请求 NTP 信息。

NTP用于通过网络同步时钟。连接到内部或外部 NTP 服务器应该是集群初始设置的一部分。

在集群上配置 NTP，使其指向本地 NTP 服务器。您可以使用 IP 地址或 FQDN 主机名。创建集群时默认的 NTP 服务器设置为 us.pool.ntp.org；但是，根据SolidFire集群的物理位置，有时可能无法连接到此站点。

使用 FQDN 取决于各个存储节点的 DNS 设置是否已就位并正常运行。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。

你可以同时使用 IPv4 地址和 IPv6 地址。

你需要什么

您必须拥有集群管理员权限才能配置此设置。

步骤

1. 在服务器设置中配置 IP 地址和/或 FQDN 列表。
2. 确保节点上的 DNS 设置正确。
3. 点击“集群”>“设置”。
4. 在“网络时间协议设置”下，选择“否”，即使用标准 NTP 配置。
5. 点击“保存更改”。

查找更多信息

- "配置集群监听 NTP 广播。"

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

配置集群监听 **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监听来自特定服务器的网络时间协议 (NTP) 广播消息。

NTP用于通过网络同步时钟。连接到内部或外部 NTP 服务器应该是集群初始设置的一部分。

你需要什么

- 您必须拥有集群管理员权限才能配置此设置。
- 您必须在网络上将 NTP 服务器配置为广播服务器。

步骤

1. 点击“集群”>“设置”。
2. 将使用广播模式的 NTP 服务器添加到服务器列表中。
3. 在网络时间协议设置中，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. 点击“保存更改”。

查找更多信息

- "配置集群要查询的网络时间协议服务器"
- "SolidFire和 Element 软件文档"
- "NetApp Element vCenter Server 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 (SNMP)。

您可以选择 SNMP 请求者、选择要使用的 SNMP 版本、识别 SNMP 基于用户的安全模型 (USM) 用户，并配置陷阱来监控SolidFire集群。您还可以查看和访问管理信息库文件。

你可以同时使用 IPv4 地址和 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**

  您可以查看或下载的 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，您可以添加请求者；如果使用版本 3，您可以设置 USM 用户。

- **SNMP**陷阱设置

  您可以确定要捕获哪些陷阱。您可以为每个陷阱接收者设置主机、端口和团体字符串。

配置 **SNMP** 请求器

启用 SNMP 版本 2 后，您可以启用或禁用请求者，并配置请求者以接收授权的 SNMP 请求。

1. 点击菜单：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 2”。
4. 在“请求者”部分，输入“社区字符串”和“网络”信息。

   默认情况下，团体字符串为 public，网络为 localhost。您可以更改这些默认设置。

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

查找更多信息

- 配置SNMP陷阱
- 使用管理信息库文件查看托管对象数据

配置 **SNMP USM** 用户

启用 SNMP 版本 3 时，需要配置一个 USM 用户来接收授权的 SNMP 请求。

1. 点击“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** 用户”部分，输入用户名、密码和密码短语。
5. *可选：*要添加另一个 USM 用户，请点击*添加 USM 用户*并输入名称、密码和密码短语。
6. 点击“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）来监控SolidFire集群的运行状况。

启用 SNMP 陷阱后， SolidFire集群会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

要选择要生成的陷阱并确定陷阱信息的接收者。默认情况下，不会生成任何陷阱。

1. 点击“集群”>“SNMP”。
2. 在“SNMP陷阱设置”部分，选择系统应生成的一种或多种陷阱类型：
   - 簇故障陷阱
   - 集群已解决的故障陷阱
   - 集群事件陷阱
3. 在“**Trap Recipients**”部分，输入接收者的主机、端口和团体字符串信息。
4. 可选：要添加另一个陷阱接收者，请单击*添加陷阱接收者*并输入主机、端口和团体字符串信息。
5. 点击“保存更改”。

使用管理信息库文件查看托管对象数据

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系统活动：

- 聚类统计
- 成交量统计
- 按账户统计的交易量
- 节点统计信息
- 其他数据，例如报告、错误和系统事件

该系统还支持访问包含 SF 系列产品上层访问点 (OID) 的 MIB 文件。

步骤

1. 点击“集群”>“SNMP”。
2. 在“SNMP MIB”下，单击要下载的 MIB 文件。
3. 在弹出的下载窗口中，打开或保存 MIB 文件。

管理驱动器

每个节点包含一个或多个物理驱动器，用于存储集群的一部分数据。将硬盘成功添加到集群后，集群即可利用硬盘的容量和性能。您可以使用 Element UI 来管理驱动器。

驱动细节

“集群”选项卡上的“驱动器”页面提供了集群中活动驱动器的列表。您可以通过选择“活动”、“可用”、“移除”、“擦除”和“失败”选项卡来筛选页面。

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且列在“可用”选项卡中的驱动器。

活动驱动器列表中包含以下元素。

- 驱动器 **ID**

  分配给硬盘的顺序编号。

- 节点 **ID**

  节点添加到集群时分配的节点编号。

- 节点名称

  存放驱动器的节点的名称。

- 投币口

  硬盘实际所在的插槽编号。

- 容量

  硬盘容量，单位为 GB。

- 序列号

  硬盘的序列号。

- 剩余磨损量

  磨损程度指示器。

  存储系统会报告每个固态硬盘 (SSD) 可用于写入和擦除数据的大致磨损量。硬盘使用完其设计写入和擦除周期的 5% 后，报告剩余磨损量为 95%。系统不会自动刷新硬盘磨损信息；您可以刷新或关闭并重新加载页面来刷新信息。

- 类型

  驱动类型。类型可以是块或元数据。

了解更多信息

- "SolidFire和 Element 软件文档"
- "NetApp Element vCenter Server 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集群总容量的 50% 以上，则该节点的部分容量将被禁用（“闲置”），以使其符合容量规则。在增加更多存储空间之前，这种情况将一直持续下去。如果添加一个非常大的节点，并且该节点也违反容量

规则，则先前被困的节点将不再被困，而新添加的节点将变为被困。为避免这种情况发生，容量应该始终成对添加。当节点发生孤立状态时，会抛出相应的集群故障。

查找更多信息

向集群添加节点

向集群添加节点

当需要更多存储空间时，或者在创建集群之后，您可以向集群添加节点。节点首次上电时需要进行初始配置。节点配置完成后，它将出现在待处理节点列表中，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。向集群添加节点时，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容量的节点，以满足容量增长的需求。向包含较小节点的集群中添加较大节点时，必须成对添加。这样就为 Double Helix 留出了足够的空间，以便在较大的节点之一发生故障时能够转移数据。您可以向较大的节点集群中添加较小的节点容量，以提高性能。

如果新添加的节点占集群总容量的 50% 以上，则该节点的部分容量将被禁用（“闲置”），以使其符合容量规则。在增加更多存储空间之前，这种情况将一直持续下去。如果添加一个非常大的节点，并且该节点也违反容量规则，则先前被困的节点将不再被困，而新添加的节点将变为被困。为避免这种情况发生，容量应该始终成对添加。当节点发生故障时，会抛出 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. 点击“待处理”查看待处理节点列表。

   添加节点的过程完成后，它们将出现在“活动节点”列表中。在此之前，待处理节点会出现在待处理活动列表中。

   当您将节点添加到集群时， SolidFire会在待添加节点上安装集群的 Element 软件版本。这可能需要几分钟。

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旁边的“操作”图标。
   - 要添加多个节点，请选中要添加的节点的复选框，然后选择“批量操作”。 *注意：*如果您添加的节点的 Element 软件版本与集群上运行的版本不同，则集群会异步地将该节点更新为集群主节点上运行的 Element 软件版本。节点更新后，会自动添加到集群中。在此异步过程中，节点将处于 pendingActive 状态。
4. 单击“添加”。

   该节点出现在活动节点列表中。

查找更多信息

Node 版本控制和兼容性

Node 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，Element 软件存储集群会自动将节点镜像到集群上的 Element 软件版本。

以下列表描述了构成 Element 软件版本号的软件版本重要性级别：

- 主要的

  第一个数字表示软件版本。不能将具有一个主要版本号的节点添加到具有其他主要修补版本号的节点组成的集群中，也不能使用具有不同主要版本号的节点创建一个集群。

- 次要的

  第二个数字表示添加到主要版本中的较小软件功能或对现有软件功能的增强。该组件在主版本组件内递增，表示此增量版本与任何其他具有不同次组件的 Element 软件增量版本都不兼容。例如，11.0 与 11.1 不兼容，11.1 与 11.2 也不兼容。

- 微

  第三个数字表示与主版本号.次版本号所代表的 Element 软件版本兼容的补丁（增量版本）。例如，11.0.1 与 11.0.2 兼容，11.0.2 与 11.0.3 兼容。

主版本号和次版本号必须匹配才能兼容。微型计算机的编号不必完全匹配即可兼容。

混合节点环境下的集群容量

集群中可以混合使用不同类型的节点。 SF系列2405、3010、4805、6010、9605、9010、19210、38410和H系列可以在集群中共存。

H 系列包括 H610S-1、H610S-2、H610S-4 和 H410S 节点。这些节点同时支持 10GbE 和 25GbE。

最好不要将未加密节点和加密节点混用。在混合节点集群中，任何节点的容量都不能超过集群总容量的 33%。例如，在一个包含四个 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。集群容量阈值是根据此情况下最大节点可能发生的损失来计算的。

根据您的 Element 软件版本，以下 SF 系列存储节点不受支持：

从……开始	不支持存储节点…
元素 12.8	• SF4805 • SF9605 • SF19210 • SF38410

从……开始	不支持存储节点…
元素 12.7	• SF2405 • SF9608
元素 12.0	• SF3010 • SF6010 • SF9010

如果您尝试将这些节点之一升级到不受支持的 Element 版本，您将看到一条错误消息，指出 Element 12.x 不支持该节点。

查看节点详情

您可以查看各个节点的详细信息，例如服务标签、驱动器详细信息以及利用率和驱动器统计信息的图形。集群选项卡的“节点”页面提供了“版本”列，您可以在其中查看每个节点的软件版本。

步骤

1. 点击“集群”>“节点”。
2. 要查看特定节点的详细信息，请单击节点的“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**：系统生成的节点 ID。
   - 节点名称：节点的主机名。
   - 节点角色：节点在集群中所扮演的角色。可能值：
     - 集群主节点：执行集群范围管理任务的节点，包含 MVIP 和 SVIP。
     - 集成节点：参与集群的节点。根据集群大小，集成节点的数量为 3 个或 5 个。
     - 光纤通道：集群中的一个节点。
   - 节点类型：节点的模型类型。
   - 活动硬盘：节点中活动硬盘的数量。
   - 节点利用率：基于节点热度的节点利用率百分比。显示的值是 recentPrimaryTotalHeat 的百分比。从 Element 12.8 版本开始可用。
   - 管理 **IP**：分配给节点的用于 1GbE 或 10GbE 网络管理任务的管理 IP (MIP) 地址。
   - 集群 **IP**：分配给节点的集群 IP (CIP) 地址，用于同一集群中节点之间的通信。
   - 存储 **IP**：分配给节点的存储 IP (SIP) 地址，用于 iSCSI 网络发现和所有数据网络流量。
   - 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编号。
- 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情

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。

查看连接到集群的光纤通道端口的相关信息。

步骤

1. 点击“集群”>“FC端口”。
2. 要筛选此页面上的信息，请点击“筛选”。
3. 请查看详细信息：
   - 节点 **ID**：承载连接会话的节点。
   - 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** 端口：光纤通道主机总线适配器 (HBA) 上的物理端口。
   - **WWNN**：全球节点名称。
   - **WWPN**：目标全球端口名称。
   - 交换机 **WWN**：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**：光纤通道架构上的节点端口 ID。
   - 速度：协商的光纤通道速度。可能的值如下：
     - 4Gbps
     - 8Gbps
     - 16Gbps

查找更多信息

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

管理虚拟网络

管理虚拟网络

SolidFire存储中的虚拟网络允许将位于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。使用 VLAN 标记可以在网络堆栈中隔离与集群的连接。

查找更多信息

- 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

您可以向集群配置中添加新的虚拟网络，以启用多租户环境连接到运行 Element 软件的集群。

你需要什么

- 确定将分配给集群节点上虚拟网络的 IP 地址块。
- 确定一个存储网络 IP (SVIP) 地址，该地址将用作所有NetApp Element存储流量的端点。

对于此配置，您必须考虑以下标准：

- 未启用 VRF 的 VLAN 要求发起方与 SVIP 位于同一子网中。
- 启用 VRF 的 VLAN 不需要发起方与 SVIP 位于同一子网中，并且支持路由。
- 默认的 SVIP 不要求发起方与 SVIP 位于同一子网中，并且支持路由。

添加虚拟网络时，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。虚拟网络地址会自动由各个节点批量配置并分配给这些节点。您无需手动为集群中的节点分配虚拟网络地址。

步骤

1. 点击“集群”>“网络”。
2. 点击“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**标签
    - **SVIP**
    - **Netmask**
    - （可选）描述
4. 输入 **IP** 地址块 中 IP 地址范围的 起始 **IP** 地址。
5. 输入 IP 地址范围的*大小*，即要包含在地址块中的 IP 地址数量。
6. 点击“添加块”为该 VLAN 添加一个非连续的 IP 地址块。
7. 点击“创建VLAN”。

查看虚拟网络详情

步骤

1. 点击“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：VLAN 网络的唯一用户指定名称。
   - **VLAN** 标签：创建虚拟网络时分配的 VLAN 标签。
   - **SVIP**：分配给虚拟网络的存储虚拟 IP 地址。
   - 子网掩码：此虚拟网络的子网掩码。
   - 网关：虚拟网络网关的唯一IP地址。必须启用 VRF。
   - **VRF** 已启用：指示虚拟路由和转发是否已启用。
   - 使用的**IP**地址：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)，它允许路由器中存在多个路由表实例并同时工作。此功能仅适用于存储网络。

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

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

查找更多信息

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、子网掩码和 IP 地址块大小。 VLAN 的 VLAN 标签和 SVIP 不能修改。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。

管理 VLAN IP 地址范围大小时，应注意以下限制：

- 您只能从创建 VLAN 时分配的初始 IP 地址范围内删除 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 地址块的大小。

- 当您尝试从初始 IP 地址范围或 IP 地址块中删除集群中节点正在使用的 IP 地址时，操作可能会失败。
- 您无法将特定正在使用的 IP 地址重新分配给集群中的其他节点。

您可以使用以下步骤添加 IP 地址块：

1. 选择“集群”>“网络”。
2. 选择要编辑的 VLAN 的“操作”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”为虚拟网络添加非连续的 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，以获取有关管理 VLAN IP 地址范围的故障排除帮助。

- "在 Element 集群的 VLAN 中添加存储节点后出现重复 IP 警告"
- "如何在 Element 中确定哪些 VLAN IP 地址正在使用以及这些 IP 地址分配给了哪些节点"

编辑 **VRF VLAN**

您可以更改 VRF VLAN 属性，例如 VLAN 名称、子网掩码、网关和 IP 地址块。

1. 点击“集群”>“网络”。
2. 单击要编辑的 VLAN 的“操作”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. 点击“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，必须先将地址块添加到另一个虚拟网络。

1. 点击“集群”>“网络”。
2. 单击要删除的 VLAN 旁边的“操作”图标。
3. 单击“删除”。
4. 确认消息。

查找更多信息

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，安全性对于解决方案的部署变得越来越重要。联邦信息处理标准（FIPS）是计算机安全和互操作性标准。符合 FIPS 140-2 标准的静态数据加密是整体安全解决方案的一个组成部分。

为了启用 FIPS 驱动器功能，您应该避免将一些节点支持 FIPS 驱动器功能而另一些节点不支持。

集群被视为符合 FIPS 标准的驱动器，需满足以下条件：

- 所有硬盘均通过了FIPS认证。
- 所有节点均为FIPS驱动节点。
- 已启用静态数据加密 (EAR)。
- FIPS驱动功能已启用。所有驱动器和节点都必须具备 FIPS 功能，并且必须启用静态加密才能启用 FIPS 驱动器功能。

启用静态数据加密

您可以启用和禁用集群范围内的静态数据加密。默认情况下不会启用此功能。要支持 FIPS 驱动器，必须启用静态加密。

1. 在NetApp Element软件用户界面中，单击“集群”>“设置”。
2. 点击“启用静态数据加密”。

查找更多信息

- 启用和禁用集群加密
- "SolidFire和 Element 软件文档"
- "NetApp Element vCenter Server 插件"

确定节点是否已准备好使用 FIPS 驱动器功能

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

生成的报告显示以下状态之一：

- 无：节点不支持 FIPS 驱动器功能。
- 部分：节点具备 FIPS 功能，但并非所有驱动器都是 FIPS 驱动器。
- 就绪：节点具备 FIPS 功能，所有驱动器均为 FIPS 驱动器，或者没有驱动器。

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，注意任何未显示“就绪”状态的节点。
3. 对于任何未显示“就绪”状态的节点，请检查驱动器是否支持 FIPS 驱动器功能：
   - 使用 Element API，输入： `GetHardwareList`
   - 请注意 **DriveEncryptionCapabilityType** 的值。如果是“fips”，则硬件可以支持FIPS驱动器功能。

     查看详情 `GetFipsReport` 或者 `ListDriveHardware` 在 "元素 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）。

查找更多信息

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

启用 **FIPS** 驱动器功能

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

集群上必须启用静态数据加密，并且所有节点和驱动器都必须具备 FIPS 功能，当 GetFipsReport 对所有节点显示“就绪”状态时，即可表明这一点。

步骤

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

```
EnableFeature params: FipsDrives
```

查找更多信息

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

检查 **FIPS** 驱动器状态

您可以使用NetApp Element软件检查集群上是否启用了 FIPS 驱动器功能。 `GetFeatureStatus` API 方法，用于显示 FIPS 驱动器启用状态是真还是假。

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

```
GetFeatureStatus
```

2. 回顾结果 `GetFeatureStatus`API调用。如果 FIPS 驱动器启用值为 True，则启用 FIPS 驱动器功能。

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

查找更多信息

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

排查 FIPS 驱动器功能故障

使用NetApp Element软件用户界面，您可以查看与 FIPS 驱动器功能相关的系统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驱动程序不匹配
   - FIPS 导致不合规
3. 有关解决方法建议，请参阅集群故障代码信息。

查找更多信息

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

建立安全通信

在您的集群上启用 HTTPS 的 FIPS 140-2 标准

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

使用NetApp Element软件，您可以选择在集群上启用联邦信息处理标准 (FIPS) 140-2 操作模式。启用此模式将激活NetApp加密安全模块 (NCSM)，并利用 FIPS 140-2 1 级认证加密，通过 HTTPS 对所有与NetApp Element UI 和 API 的通信进行加密。

启用 FIPS 140-2 模式后，无法禁用。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连接和存储连接中断。您应该仔细规划，只有当您的环境需要它提供的加密机制时才启用此模式。

更多信息请参阅 Element API 信息。

以下是启用 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 通信均使用 FIPS 140-2 批准的密码。

查找更多信息

- SSL密码
- "使用 Element API 管理存储"
- "SolidFire和 Element 软件文档"
- "NetApp Element vCenter Server 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，启用 FIPS 140-2 模式时还支持非标准密码。

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

- **FIPS 140-2** 已禁用

  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**标准

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

在您的集群上启用 HTTPS 的 FIPS 140-2 标准

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 (EKM) 结合集群外外部密钥服务器 (EKS) 提供安全的身份验证密钥 (AK) 管理。 AK 用于在需要时锁定和解锁自加密驱动器 (SED)。"静态加密"已在集群上启用。 EKS 提供 AK 的安全生成和存储。该集群利用密钥管理互操作协议 (KMIP)（OASIS 定义的标准协议）与 EKS 通信。

- "建立外部管理"
- "重新密钥软件加密静态主密钥"
- "恢复无法访问或无效的身份验证密钥"
- "外部密钥管理 API 命令"

查找更多信息

- "CreateCluster API 可用于启用静态软件加密。"
- "SolidFire和 Element 软件文档"
- "NetApp SolidFire和 Element 产品早期版本的文档"

设置外部密钥管理

您可以按照这些步骤，并使用列出的 Element API 方法来设置您的外部密钥管理功能。

你需要什么

- 如果您正在设置外部密钥管理并结合静态软件加密，则您已使用以下方式启用静态软件加密：："CreateCluster"在不包含卷的新集群上执行此方法。

步骤

1. 与外部密钥服务器（EKS）建立信任关系。
   a. 为 Element 集群创建公钥/私钥对，通过调用以下 API 方法与密钥服务器建立信任关系："创建公钥/私钥对"
   b. 获取证书颁发机构需要签署的证书签名请求（CSR）。 CSR 使密钥服务器能够验证将要访问密钥的 Element 集群是否已通过 Element 集群的身份验证。调用以下 API 方法："获取客户端证书签名请求"

c. 使用 EKS/证书颁发机构对检索到的 CSR 进行签名。更多信息请参阅第三方文档。

2. 在集群上创建服务器和提供程序，以便与 EKS 通信。密钥提供者定义密钥的获取地点，服务器定义要与之通信的 EKS 的具体属性。

   a. 通过调用以下 API 方法创建密钥提供程序，密钥服务器详细信息将存放于此："创建密钥提供程序Kmip"

   b. 通过调用以下 API 方法，创建提供证书颁发机构的签名证书和公钥证书的密钥服务器："创建密钥服务器Kmip" "测试密钥服务器Kmip"

      如果测试失败，请检查服务器连接和配置。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" "测试密钥提供程序Kmip"

      如果测试失败，请检查服务器连接和配置。然后重复测试。

3. 接下来，请执行以下操作之一，以实现静态数据加密：

   a. （用于静态数据硬件加密）启用"静态硬件加密"通过调用以下方法提供包含用于存储密钥的密钥服务器的密钥提供程序的 ID："启用静态加密" API 方法。

      > 您必须通过以下方式启用静态加密："API" 。使用现有的 Element UI 按钮启用静态加密将导致该功能恢复为使用内部生成的密钥。

   b. （针对静态软件加密）为了"静态软件加密"要使用新创建的密钥提供程序，请将密钥提供程序 ID 传递给"重新密钥软件静态加密主密钥"API 方法。

查找更多信息

- "启用和禁用集群加密"
- "SolidFire和 Element 软件文档"
- "NetApp SolidFire和 Element 产品早期版本的文档"

重新密钥软件加密静态主密钥

您可以使用 Element API 重新生成现有密钥。此过程会为您的外部密钥管理服务器创建一个新的替换主密钥。主钥匙总是用新的主钥匙替换，绝不会复制或覆盖。

您可能需要在以下某个过程中重新输入密码：

- 作为从内部密钥管理变更为外部密钥管理的一部分，创建新密钥。
- 为应对或防范安全事件而创建新密钥。

> 该过程是异步的，会在重新密钥操作完成之前返回响应。你可以使用"获取异步结果"用于轮询系统以查看进程何时完成的方法。

你需要什么

- 您已启用静态软件加密。"CreateCluster"在不包含卷且没有 I/O 的新集群上执行此方法。使用链接：../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`确认该州是 `enabled`在继续之前。

- 你有"建立了信任关系"SolidFire集群与外部密钥服务器 (EKS) 之间。运行"测试密钥提供程序Kmip"验证与密钥提供程序的连接是否已建立的方法。

步骤

1. 运行"ListKeyProvidersKmip"命令并复制密钥提供程序 ID(`keyProviderID`）。
2. 运行"重新密钥软件静态加密主密钥"和 `keyManagementType`参数为 `external`和 `keyProviderID`作为上一步中密钥提供者的 ID 号：

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

3. 复制 `asyncHandle`来自 `RekeySoftwareEncryptionAtRestMasterKey`命令响应。
4. 运行"获取异步结果"使用命令 `asyncHandle`使用上一步的值来确认配置更改。从命令响应中可以看到，旧的主密钥配置已更新为新的密钥信息。复制新的密钥提供程序 ID，以便在后续步骤中使用。

```
{
   "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. 运行 `GetSoftwareEncryptionatRestInfo`命令确认新的关键细节，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 管理存储"
- "SolidFire和 Element 软件文档"
- "NetApp SolidFire和 Element 产品早期版本的文档"

恢复无法访问或无效的身份验证密钥

偶尔会出现需要用户干预的错误。如果发生错误，将会生成集群故障（称为集群故障代码）。这里描述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。

当集群首次启动且密钥服务器无法访问或所需密钥不可用时，可能会发生这种情况。

1. 请按照集群故障代码（如有）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被标记为故障并置于“可用”状态。

清除步骤：

1. 再次添加驱动器。
2. 3到4分钟后，检查一下 `sliceServiceUnhealthy`故障已排除。

看"集群故障代码"了解更多信息。

外部密钥管理 API 命令

EKM管理和配置可用API列表。

用于在集群和外部客户拥有的服务器之间建立信任关系：

- 创建公钥/私钥对
- 获取客户端证书签名请求

用于定义外部客户自有服务器的具体细节：

- 创建密钥服务器Kmip
- 修改密钥服务器Kmip
- 删除密钥服务器Kmip
- GetKeyServerKmip
- ListKeyServersKmip
- 测试密钥服务器Kmip

用于创建和维护管理外部密钥服务器的密钥提供程序：

- 创建密钥提供程序Kmip
- 删除密钥提供程序Kmip
- AddKeyServerToProviderKmip
- 从提供程序中移除密钥服务器Kmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- 重新密钥软件静态加密主密钥
- 测试密钥提供程序Kmip

有关 API 方法的信息，请参阅 "API 参考信息"。