使用 **Element** 软件管理存储

Element Software

NetApp
November 12, 2025

目录

使用 Element 软件管理存储

使用 Element 软件管理存储

使用 Element 软件设置 SolidFire 存储，监控集群容量和性能以及管理多租户基础架构中的存储活动。

Element 是 SolidFire 集群的核心存储操作系统。Element 软件可在集群中的所有节点上独立运行，并可使集群节点将资源组合在一起，并作为一个存储系统提供给外部客户端。Element 软件负责整个系统的所有集群协调，扩展和管理工作。

软件界面基于 Element API 构建。

- "访问 Element 软件用户界面"
- "在部署后配置 SolidFire 系统选项"
- "升级存储系统组件"
- "使用 Element 软件 UI 中的基本选项"
- "管理帐户"
- "管理您的系统"
- "管理卷和虚拟卷"
- "保护您的数据"
- "对系统进行故障排除"

了解更多信息

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

访问 Element 软件用户界面

您可以使用主集群节点的管理虚拟 IP （ MVIP ）地址访问 Element UI 。

您必须确保在浏览器中禁用弹出窗口阻止程序和 NoScript 设置。

根据集群创建期间的配置，您可以使用 IPv4 或 IPv6 地址访问此 UI 。

1. 选择以下选项之一：
   - IPv6 ： 输入 https://[IPv6 MVIP address] ，例如：

     ```
     https://[fd20:8b1e:b256:45a::1234]/
     ```

   - IPv4 ： 输入 https://[IPv4 MVIP address] ，例如：

```
https://10.123.456.789/
```

2. 对于 DNS ，输入主机名。
3. 单击任何身份验证证书消息。

了解更多信息

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

在部署后配置 SolidFire 系统选项

在部署后配置 SolidFire 系统选项

设置 SolidFire 系统后，您可能需要执行一些可选任务。

如果更改系统中的凭据，您可能希望了解对其他组件的影响。

此外，您还可以配置多因素身份验证，外部密钥管理和联邦信息处理标准（ FIPS ）安全性的设置。您还应根据需要查看更新密码。

了解更多信息

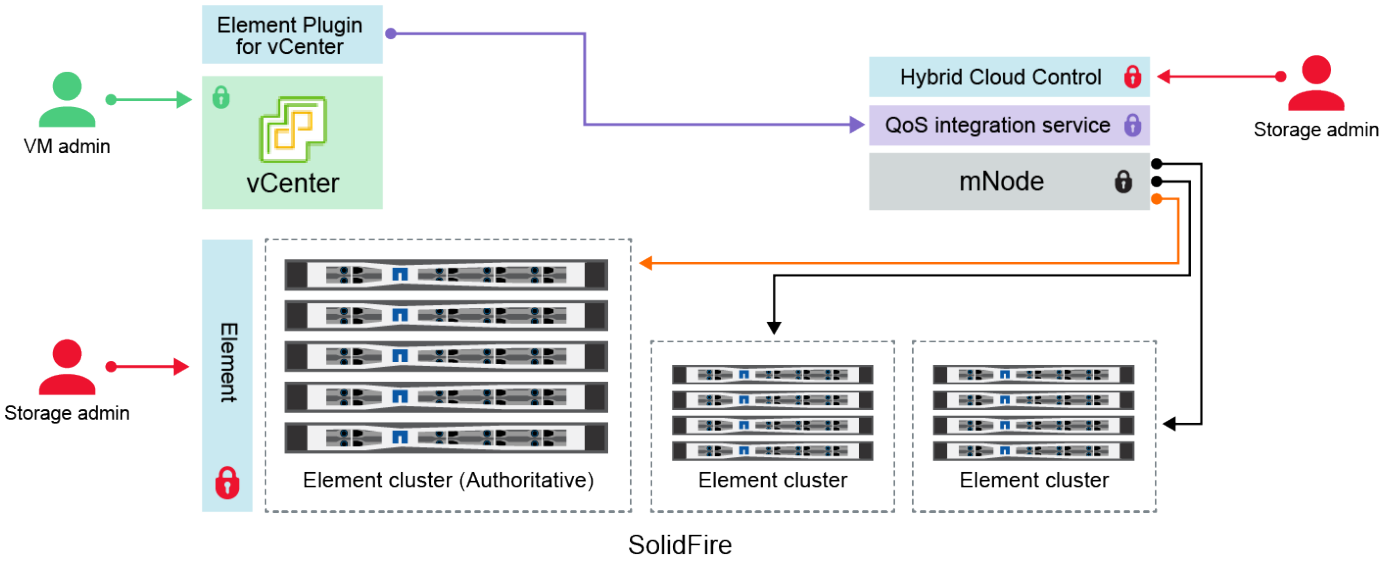
- "在 NetApp HCI 和 NetApp SolidFire 中更改凭据"
- "更改 Element 软件的默认 SSL 证书"
- "更改节点的 IPMI 密码"
- "启用多因素身份验证"
- "开始使用外部密钥管理"
- "创建支持 FIPS 驱动器的集群"

在 NetApp HCI 和 NetApp SolidFire 中更改凭据

根据部署 NetApp HCI 或 NetApp SolidFire 的组织中的安全策略，更改凭据或密码通常是安全实践的一部分。在更改密码之前，您应了解此部署对其他软件组件的影响。

如果您更改了 NetApp HCI 或 NetApp SolidFire 部署中某个组件的凭据，下表将提供有关对其他组件的影响的指导。

NetApp SolidFire 组件交互
：



凭据类型和图标	管理员使用情况	请参见以下说明
Element 凭据	• 适用场景 *： NetApp HCI 和 SolidFire 管理员可以使用这些凭据登录到： • Element 存储集群上的 Element 用户界面 • 管理节点（ mnode ）上的混合云控制 当 Hybrid Cloud Control 管理多个存储集群时，它仅接受存储集群的管理员凭据，即最初为 mnode 设置的 *authoritative cluster* 。对于稍后添加到 Hybrid Cloud Control 的存储集群， mnode 会安全地存储管理员凭据。如果更改了随后添加的存储集群的凭据，则还必须使用 mnode API 在 mnode 中更新这些凭据。	• "更新存储集群管理员密码。" • 使用更新 mnode 中的存储集群管理员凭据 "modifyclusteradmin API"。
vSphere 单点登录凭据	• 适用场景 *：仅限 NetApp HCI 管理员可以使用这些凭据登录到 VMware vSphere Client 。如果 vCenter 是 NetApp HCI 安装的一部分，则凭据会在 NetApp 部署引擎中配置如下： • 使用指定密码 username@vsphere.local ，和 • 使用指定密码 administrator@vsphere.local 。使用现有 vCenter 部署 NetApp HCI 时， vSphere 单点登录凭据由 IT VMware 管理员管理。	"更新 vCenter 和 ESXi 凭据"。

凭据类型和图标	管理员使用情况	请参见以下说明
基板管理控制器（BMC）凭据 	• 适用场景 *： 仅限 NetApp HCI 管理员可以使用这些凭据登录到 NetApp HCI 部署中 NetApp 计算节点的 BMC 。BMC 可提供基本的硬件监控和虚拟控制台功能。 每个 NetApp 计算节点的 BMC （有时称为 *ipmi* ）凭据都安全地存储在 NetApp HCI 部署中的 mnode 上。在计算节点固件升级期间， NetApp Hybrid Cloud Control 使用服务帐户容量中的 BMC 凭据与计算节点中的 BMC 进行通信。 更改 BMC 凭据后，还必须在 mnode 上更新相应计算节点的凭据，以保留所有 Hybrid Cloud Control 功能。	• "为 NetApp HCI 上的每个节点配置 IPMI"。 • 对于 H410C ， H610C 和 H615C 节点， "更改默认 IPMI 密码"。 • 对于 H410S 和 H610S 节点， "更改默认 IPM 密码"。 • "更改管理节点上的 BMC 凭据"。
ESXi 凭据 	• 适用场景 *： 仅限 NetApp HCI 管理员可以使用 SSH 或本地 DCUI 使用本地 root 帐户登录到 ESXi 主机。在 NetApp HCI 部署中，用户名为 "root" ，密码是在 NetApp 部署引擎中首次安装该计算节点期间指定的。 每个 NetApp 计算节点的 ESXi 根凭据都安全地存储在 NetApp HCI 部署中的 mnode 上。在计算节点固件升级和运行状况检查期间， NetApp Hybrid Cloud Control 使用服务帐户容量中的凭据直接与 ESXi 主机进行通信。 如果 VMware 管理员更改了 ESXi 根凭据，则必须在 mnode 上更新相应计算节点的凭据，才能保留 Hybrid Cloud Control 功能。	"更新 vCenter 和 ESXi 主机的凭据"。
QoS 集成密码 	• 适用场景 *： NetApp HCI ，在 SolidFire 中可选 不用于管理员交互式登录。 VMware vSphere 与 Element 软件之间的 QoS 集成可通过以下方式实现： • 适用于 vCenter Server 的 Element 插件，和 • mnode 上的 QoS 服务。 对于身份验证， QoS 服务使用在此上下文中专用的密码。QoS 密码是在首次安装适用于 vCenter Server 的 Element 插件期间指定的，或者在 NetApp HCI 部署期间自动生成的。 不会对其他组件造成影响。	"在适用于 vCenter Server 的 NetApp Element 插件中更新 QoSSIOC 凭据"。 适用于vCenter Server SIOC的NetApp Element 插件密码也称为_QoSSIOC密码_。 查看 {url-peak} [适用于vCenter Server的Element插件知识库文章^。

凭据类型和图标	管理员使用情况	请参见以下说明
vCenter Service Appliance 凭据 	• NetApp 部署引擎 *：仅在 NetApp HCI 部署引擎设置的情况下才支持适用场景 管理员可以登录到 vCenter Server 设备虚拟机。在 NetApp HCI 部署中，用户名为 "root" ，密码是在 NetApp 部署引擎中首次安装该计算节点期间指定的。根据部署的 VMware vSphere 版本，vSphere Single Sign-On 域中的某些管理员也可以登录到设备。 不会对其他组件造成影响。	无需更改。
NetApp 管理节点管理员凭据 	• 适用场景 *： NetApp HCI ，在 SolidFire 中可选 管理员可以登录到 NetApp 管理节点虚拟机进行高级配置和故障排除。根据部署的管理节点版本，默认情况下不会启用通过 SSH 登录。 在 NetApp HCI 部署中，用户在 NetApp 部署引擎中首次安装该计算节点期间指定了用户名和密码。 不会对其他组件造成影响。	无需更改。

了解更多信息

- "更改 Element 软件的默认 SSL 证书"
- "更改节点的 IPMI 密码"
- "启用多因素身份验证"
- "开始使用外部密钥管理"
- "创建支持 FIPS 驱动器的集群"

更改 **Element** 软件的默认 **SSL** 证书

您可以使用 NetApp Element API 更改集群中存储节点的默认 SSL 证书和专用密钥。

创建 NetApp Element 软件集群时，集群会创建一个唯一的自签名安全套接字层（ SSL ）证书和专用密钥，用于通过 Element UI ，每节点 UI 或 API 进行所有 HTTPS 通信。Element 软件支持自签名证书以及由可信证书颁发机构（ CA ）颁发和验证的证书。

您可以使用以下 API 方法获取有关默认 SSL 证书的详细信息并进行更改。

- * GetSSLCertificate *

  您可以使用 "GetSSLCertificate方法" 检索有关当前安装的SSL证书的信息、包括所有证书详细信息。

- * 设置 SSLCertificate *

  您可以使用 "SetSSLCertificate方法" 将集群和每节点SSL证书设置为您提供的证书和专用密钥。系统会验证

证书和专用密钥，以防止应用无效证书。

- * 删除 SSLCertificer*

  。 "RemoveSSLCertificate方法" 删除当前安装的SSL证书和专用密钥。然后，集群将生成新的自签名证书和专用密钥。

> 集群 SSL 证书会自动应用于添加到集群中的所有新节点。从集群中删除的任何节点都会还原为自签名证书，并且所有用户定义的证书和密钥信息都会从该节点中删除。

了解更多信息

- "更改管理节点的默认SSL证书"
- "在Element Software中设置自定义SSL证书有哪些要求？"
- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

更改节点的默认 **IPMI** 密码

您可以在对节点具有远程 IPMI 访问权限后立即更改默认的智能平台管理接口（ Intelligent Platform Management Interface ， IPMI ）管理员密码。如果存在任何安装更新，您可能需要执行此操作。

有关为节点配置 IPM 访问的详细信息，请参见 "为每个节点配置 IPMI"。

您可以更改以下节点的 IPM 密码：

- H410S 节点
- H610S 节点

更改 **H410S** 节点的默认 **IPMI** 密码

配置 IPMI 网络端口后，应尽快更改每个存储节点上 IPMI 管理员帐户的默认密码。

您需要的内容

您应该已为每个存储节点配置 IPMI IP 地址。

步骤

1. 在可以访问 IPMI 网络的计算机上打开 Web 浏览器，然后浏览到此节点的 IPMI IP 地址。
2. 在登录提示符处输入用户名 `admin` 和密码 `admin` 。
3. 登录后，单击 * 配置 * 选项卡。
4. 单击 * 用户 * 。
5. 选择 `admin` user ，然后单击 * 修改用户 * 。
6. 选中 * 更改密码 * 复选框。

7. 在 * 密码 * 和 * 确认密码 * 字段中输入新密码。
8. 单击 * 修改 * ，然后单击 * 确定 * 。
9. 对具有默认 IPMI 密码的任何其他 H410S 节点重复此操作步骤。

更改 **H610S** 节点的默认 **IPMI** 密码

配置 IPMI 网络端口后，应尽快更改每个存储节点上 IPMI 管理员帐户的默认密码。

您需要的内容

您应该已为每个存储节点配置 IPMI IP 地址。

步骤

1. 在可以访问 IPMI 网络的计算机上打开 Web 浏览器，然后浏览到此节点的 IPMI IP 地址。
2. 在登录提示符处输入用户名 `root` 和密码 `calvin` 。
3. 登录后，单击页面左上角的菜单导航图标以打开边栏抽屉。
4. 单击 * 设置 * 。
5. 单击 * 用户管理 * 。
6. 从列表中选择 * 管理员 * 用户。
7. 启用 * 更改密码 * 复选框。
8. 在 * 密码 * 和 * 确认密码 * 字段中输入新的强密码。
9. 单击页面底部的 * 保存 * 。
10. 对具有默认 IPMI 密码的任何其他 H610S 节点重复此操作步骤。

了解更多信息

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

使用 **Element** 软件 **UI** 中的基本选项

使用 **Element** 软件 **UI** 中的基本选项

您可以通过 NetApp Element 软件 Web 用户界面（ Element UI ）监控 SolidFire 系统并在其上执行常见任务。

基本选项包括查看由 UI 活动激活的 API 命令以及提供反馈。

- "查看 API 活动"
- "Element 界面中的图标"
- "提供反馈"

有关详细信息 ...

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

API活动

查看 **API** 活动

Element 系统使用 NetApp Element API 作为其特性和功能的基础。使用 Element UI ，您可以在使用界面时查看系统上各种类型的实时 API 活动。通过 API 日志，您可以查看用户发起的后台系统 API 活动，以及在当前查看的页面上进行的 API 调用。

您可以使用 API 日志确定用于某些任务的 API 方法，并了解如何使用 API 方法和对象构建自定义应用程序。

有关每种方法的详细信息，请参见 "Element 软件 API 参考"。

1. 在 Element UI 导航栏中，单击 * API Log* 。
2. 要修改 API 日志窗口中显示的 API 活动类型，请执行以下步骤：
   a. 选择 * 请求 * 以显示 API 请求流量。
   b. 选择 * 响应 * 可显示 API 响应流量。
   c. 通过选择以下选项之一筛选 API 流量的类型：
      - * 用户已启动 * ： 此 Web UI 会话期间您的活动生成的 API 流量。
      - * 后台轮询 * ： 后台系统活动生成的 API 流量。
      - * 当前页面 * ： 当前正在查看的页面上的任务生成的 API 流量。

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"

接口刷新率受集群负载影响

根据 API 响应时间，集群可能会自动调整您正在查看的 NetApp Element 软件页面的某些部分的数据刷新间隔。

在浏览器中重新加载页面时，刷新间隔将重置为默认值。您可以通过单击页面右上角的集群名称来查看当前刷新间隔。请注意，此间隔控制发出 API 请求的频率，而不是数据从服务器返回的速度。

当集群负载过重时，它可能会对来自 Element UI 的 API 请求进行排队。在极少数情况下，如果系统响应明显延迟，例如网络连接速度较慢加上集群繁忙，则如果系统不能足够快地响应已排队的 API 请求，您可能会从 Element UI 中注销。如果重定向到注销屏幕，则可以在忽略任何初始浏览器身份验证提示后重新登录。返回概述页面后，如果浏览器未保存集群凭据，系统可能会提示您输入这些凭据。

Element 界面中的图标

NetApp Element 软件界面会显示一些图标，表示您可以对系统资源执行的操作。

下表提供了快速参考：

图标。	Description
	操作
	备份到
	克隆或复制
	删除或清除
	编辑
	筛选器
	配对
	刷新
	还原
	还原自
	回滚
	Snapshot

提供反馈

您可以使用反馈表帮助改进 Element 软件 Web 用户界面并解决任何 UI 问题，此反馈表可

通过整个 UI 访问。

1. 在 Element UI 的任何页面中，单击 * 反馈 * 按钮。
2. 在摘要和问题描述字段中输入相关信息。
3. 附加任何有用的屏幕截图。
4. 输入名称和电子邮件地址。
5. 选中此复选框可包含有关当前环境的数据。
6. 单击 * 提交 * 。

了解更多信息

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

管理帐户

管理帐户

在SolidFire 存储系统中、租户可以使用帐户使客户端能够连接到集群上的卷。创建卷时、卷会分配给特定帐户。您还可以管理 SolidFire 存储系统的集群管理员帐户。

- "使用CHAP处理帐户"
- "管理集群管理员用户帐户"

有关详细信息 ...

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

使用**CHAP**处理帐户

在SolidFire 存储系统中、租户可以使用帐户使客户端能够连接到集群上的卷。帐户包含访问分配给它的卷所需的质询握手身份验证协议(Challenge-Handshake Authentication Protocol、CHAP)身份验证。创建卷时、卷会分配给特定帐户。

一个帐户最多可以分配 2 ， 000 个卷，但一个卷只能属于一个帐户。

CHAP算法

从Element 12.7开始、支持符合FIPS的安全CHAP算法SHA1、SHA-256和SHA3-256。当主机iSCSI启动程序创建与Element iSCSI目标的iSCSI会话时、它会请求要使用的CHAP算法列表。Element iSCSI目标会从主机iSCSI启动程序请求的列表中选择它支持的第一个算法。要确认Element iSCSI目标选择的是最安全的算法、您必须将主机iSCSI启动程序配置为发送从最安全位置(例如SHA3-256)到最不安全位置(例如 SHA1或MD5。如果主机iSCSI启动程序未请求SHA算法、则Element iSCSI目标会选择MD5、前提是主机中的建议算法列表包含MD5。您可能需要更新主机iSCSI启动程序配置、以支持安全算法。

在Element 12.7或更高版本升级期间、如果已更新主机iSCSI启动程序配置以发送包含SHA算法列表的会话请求、则在存储节点重新启动时、新的安全算法将激活、并使用最安全的协议建立新的或重新连接的iSCSI会话。在升级期间、所有现有iSCSI会话都会从MD5过渡到SHA。如果不更新主机iSCSI启动程序配置以请求SHA、则现有iSCSI会话将继续使用MD5。稍后、在更新主机iSCSI启动程序CHAP算法后、iSCSI会话应根据导致iSCSI会话重新连接的维护活动逐渐从MD5过渡到SHA。

例如、Red Hat Enterprise Linux (RHEL) 8.3中的默认主机iSCSI启动程序的`node.session.auth.chap_algs = SHA3-256、SHA256、SHA1、MD5`设置已注释、这会导致iSCSI启动程序仅使用MD5。在主机上取消此设置的注释并重新启动iSCSI启动程序会触发来自该主机的iSCSI会话、以便开始使用SHA3-256。

如果需要、您可以使用 "ListISCSISessions" API方法、用于查看每个会话所使用的CHAP算法。

创建帐户

您可以创建帐户以允许访问卷。

系统中的每个帐户名称都必须是唯一的。

1. 选择 * 管理 * > * 帐户 * 。
2. 单击 * 创建帐户 * 。
3. 输入 * 用户名 * 。
4. 在 * CHAP Settings* 部分中，输入以下信息：

   将凭据字段留空可自动生成任一密码。

   - 用于 CHAP 节点会话身份验证的 * 启动程序机密 * 。
   - 用于 CHAP 节点会话身份验证的 * 目标机密 * 。
5. 单击 * 创建帐户 * 。

查看帐户详细信息

您可以通过图形格式查看各个帐户的性能活动。

图形信息提供帐户的 I/O 和吞吐量信息。平均和峰值活动级别以 10 秒报告周期为增量进行显示。这些统计信息包括分配给帐户的所有卷的活动。

1. 选择 * 管理 * > * 帐户 * 。
2. 单击帐户对应的 "Actions" 图标。
3. 单击 * 查看详细信息 * 。

下面是一些详细信息：

- * 状态 * ： 帐户的状态。可能值：
  - Active ： 处于活动状态的帐户。
  - locked ： 已锁定的帐户。
  - removed ： 已删除并清除的帐户。

- * 活动卷 *： 分配给帐户的活动卷数。
- * 压缩 *： 分配给帐户的卷的压缩效率得分。
- * 重复数据删除 *： 分配给帐户的卷的重复数据删除效率得分。
- * 精简配置 *： 分配给帐户的卷的精简配置效率得分。
- * 整体效率 *： 分配给帐户的卷的整体效率得分。

编辑帐户

您可以编辑帐户以更改状态，更改 CHAP 密码或修改帐户名称。

修改帐户中的 CHAP 设置或从访问组中删除启动程序或卷可能会使发生原因启动程序意外丢失对卷的访问权限。要验证卷访问不会意外丢失，请始终注销将受帐户或访问组更改影响的 iSCSI 会话，并验证启动程序是否可以在完成启动程序设置和集群设置的任何更改后重新连接到卷。

> 与管理服务关联的永久性卷将分配给在安装或升级期间创建的新帐户。如果您使用的是永久性卷，请勿修改或删除其关联帐户。

1. 选择 * 管理 * > * 帐户 * 。
2. 单击帐户对应的 "Actions" 图标。
3. 在显示的菜单中，选择 * 编辑 * 。
4. * 可选： * 编辑 * 用户名 * 。
5. * 可选： * 单击 * 状态 * 下拉列表并选择其他状态。

> 将状态更改为 * 已锁定 * 将终止与帐户的所有 iSCSI 连接，并且无法再访问此帐户。与帐户关联的卷会保留下来，但这些卷不能通过 iSCSI 发现。

6. * 可选： * 在 * CHAP Settings* 下，编辑用于节点会话身份验证的 * 启动程序机密 * 和 * 目标机密 * 凭据。

> 如果不更改 * CHAP Settings* 凭据，它们将保持不变。如果将凭据字段留空，系统将生成新密码。

7. 单击 * 保存更改 * 。

删除帐户

您可以删除不再需要的帐户。

删除帐户之前，请删除并清除与帐户关联的所有卷。

> 与管理服务关联的永久性卷将分配给在安装或升级期间创建的新帐户。如果您使用的是永久性卷，请勿修改或删除其关联帐户。

1. 选择 * 管理 * > * 帐户 * 。
2. 单击要删除的帐户对应的 "Actions" 图标。
3. 在显示的菜单中，选择 * 删除 * 。

4. 确认操作。

了解更多信息

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

管理集群管理员用户帐户

您可以通过创建，删除和编辑集群管理员帐户，更改集群管理员密码以及配置 LDAP 设置来管理用户的系统访问来管理 SolidFire 存储系统的集群管理员帐户。

存储集群管理员帐户类型

运行 NetApp Element 软件的存储集群中可以存在两种类型的管理员帐户：主集群管理员帐户和集群管理员帐户。

- * 主集群管理员帐户 *

  此管理员帐户是在创建集群时创建的。此帐户是对集群具有最高访问级别的主管理帐户。此帐户类似于 Linux 系统中的 root 用户。您可以更改此管理员帐户的密码。

- * 集群管理员帐户 *

  您可以为集群管理员帐户授予有限的管理访问权限，以便在集群中执行特定任务。分配给每个集群管理员帐户的凭据用于对存储系统中的 API 和 Element UI 请求进行身份验证。

> 要通过每节点 UI 访问集群中的活动节点，需要使用本地（非 LDAP ）集群管理员帐户。访问尚未加入集群的节点不需要帐户凭据。

查看集群管理员详细信息

1. 要创建集群范围（非 LDAP ）的集群管理员帐户，请执行以下操作：
   a. 单击 * 用户 * > * 集群管理员 * 。
2. 在用户选项卡的集群管理员页面上，您可以查看以下信息。
   - * ID * ： 分配给集群管理员帐户的序列号。
   - * 用户名 * ： 创建集群管理员帐户时为其指定的名称。
   - * 访问 * ： 分配给用户帐户的用户权限。可能值：
     - 读取
     - 报告
     - nodes
     - 驱动器
     - volumes
     - —帐户

- clusterAdmins
- 管理员
- 支持管理员

> 所有权限均可用于管理员访问类型。
>
> 通过API提供的某些访问类型在Element UI中不可用。

+

- * 类型 * ： 集群管理员的类型。可能值：
  - 集群
  - ldap
- * 属性 * ： 如果集群管理员帐户是使用 Element API 创建的，则此列将显示使用该方法设置的任何名称 - 值对。

  看"《 NetApp Element 软件 API 参考》"。

创建集群管理员帐户

您可以创建具有允许或限制对存储系统特定区域的访问权限的新集群管理员帐户。设置集群管理员帐户权限时，系统会为您未分配给集群管理员的任何权限授予只读权限。

如果要创建 LDAP 集群管理员帐户，请确保在开始之前已在集群上配置 LDAP 。

"使用 Element 用户界面启用 LDAP 身份验证"

您可以稍后更改报告，节点，驱动器，卷，帐户的集群管理员帐户权限。 和集群级别访问。启用某个权限后，系统会为此级别分配写入访问权限。系统会为管理员用户授予对您未选择的级别的只读访问权限。

您也可以稍后删除系统管理员创建的任何集群管理员用户帐户。您不能删除在创建集群时创建的主集群管理员帐户。

1. 要创建集群范围（非 LDAP ）的集群管理员帐户，请执行以下操作：
   a. 单击 * 用户 * > * 集群管理员 * 。
   b. 单击 * 创建集群管理员 * 。
   c. 选择 * 集群 * 用户类型。
   d. 输入帐户的用户名和密码并确认密码。
   e. 选择要应用于帐户的用户权限。
   f. 选中此复选框以同意最终用户许可协议。
   g. 单击 * 创建集群管理员 * 。
2. 要在 LDAP 目录中创建集群管理员帐户，请执行以下操作：
   a. 单击 * 集群 * > * LDAP * 。
   b. 确保已启用 LDAP 身份验证。

c. 单击 * 测试用户身份验证 * ，然后复制为用户或用户所属组之一显示的可分辨名称，以便您可以稍后粘贴。
d. 单击 * 用户 * > * 集群管理员 * 。
e. 单击 * 创建集群管理员 * 。
f. 选择 LDAP 用户类型。
g. 在 Distinguished Name 字段中，按照文本框中的示例输入用户或组的完整可分辨名称。或者，也可以从先前复制的可分辨名称中粘贴该名称。

   如果可分辨名称属于某个组，则 LDAP 服务器上属于该组的任何用户都将拥有此管理员帐户的权限。

要添加 LDAP 集群管理员用户或组，用户名的常规格式为 "`ldap： < 完整可分辨名称 >` " 。

a. 选择要应用于帐户的用户权限。
b. 选中此复选框以同意最终用户许可协议。
c. 单击 * 创建集群管理员 * 。

编辑集群管理员权限

您可以更改报告，节点，驱动器，卷，帐户的集群管理员帐户权限， 和集群级别访问。启用某个权限后，系统会为此级别分配写入访问权限。系统会为管理员用户授予对您未选择的级别的只读访问权限。

1. 单击 * 用户 * > * 集群管理员 * 。
2. 单击要编辑的集群管理员对应的 "Actions" 图标。
3. 单击 * 编辑 * 。
4. 选择要应用于帐户的用户权限。
5. 单击 * 保存更改 * 。

更改集群管理员帐户的密码

您可以使用 Element UI 更改集群管理员密码。

1. 单击 * 用户 * > * 集群管理员 * 。
2. 单击要编辑的集群管理员对应的 "Actions" 图标。
3. 单击 * 编辑 * 。
4. 在更改密码字段中，输入新密码并进行确认。
5. 单击 * 保存更改 * 。

相关信息

- "了解可用于Element API的访问类型"
- "使用 Element 用户界面启用 LDAP 身份验证"
- "禁用 LDAP"
- "适用于 vCenter Server 的 NetApp Element 插件"

管理 LDAP

您可以设置轻型目录访问协议（ Lightweight Directory Access Protocol ， LDAP ），以便为 SolidFire 存储启用基于目录的安全登录功能。您可以在集群级别配置 LDAP 并授权 LDAP 用户和组。

管理 LDAP 涉及使用现有 Microsoft Active Directory 环境为 SolidFire 集群设置 LDAP 身份验证并测试配置。

您可以同时使用 IPv4 和 IPv6 地址。

启用 LDAP 涉及以下高级步骤，详细说明如下：

1. * 完成 LDAP 支持的预配置步骤 * 。验证您是否具有配置 LDAP 身份验证所需的所有详细信息。
2. * 启用 LDAP 身份验证 * 。使用 Element UI 或 Element API 。
3. * 验证 LDAP 配置 * 。或者，也可以通过运行 GetLdapConfiguration API 方法或使用 Element UI 检查 LCAP 配置来检查集群是否配置了正确的值。
4. * 测试 LDAP 身份验证 * （使用 `readonly` 用户）。通过运行 TestLdapAuthentication API 方法或使用 Element UI 测试 LDAP 配置是否正确。在此初始测试中，请使用 `readonly` 用户的用户名 `sAMAccountName` 。这将验证您的集群是否已正确配置 LDAP 身份验证，并验证 `readonly` 凭据和访问是否正确。如果此步骤失败，请重复步骤 1 到 3 。
5. * 测试 LDAP 身份验证 * （使用要添加的用户帐户）。使用要添加为 Element 集群管理员的用户帐户重复 setp 4 。复制 `d`**名称** （ DN ）或用户（或组）。此 DN 将在步骤 6 中使用。
6. * 添加 LDAP 集群管理 * （复制并粘贴测试 LDAP 身份验证步骤中的 DN ）。使用 Element UI 或 AddLdapClusterAdmin API 方法，创建具有适当访问级别的新集群管理员用户。对于用户名，请粘贴您在步骤 5 中复制的完整 DN 。这样可以确保 DN 格式正确。
7. * 测试集群管理员访问权限 * 。使用新创建的 LDAP 集群管理员用户登录到集群。如果添加了 LDAP 组，则可以以该组中的任何用户身份登录。

完成 **LDAP** 支持的预配置步骤

在 Element 中启用 LDAP 支持之前，您应先设置 Windows Active Directory 服务器并执行其他预配置任务。

步骤

1. 设置 Windows Active Directory 服务器。
2. * 可选： * 启用 LDAPS 支持。
3. 创建用户和组。
4. 创建一个只读服务帐户（例如 `sfreadonly` ），用于搜索 LDAP 目录。

使用 **Element** 用户界面启用 **LDAP** 身份验证

您可以配置存储系统与现有 LDAP 服务器的集成。这样， LDAP 管理员就可以集中管理用户的存储系统访问权限。

您可以使用 Element 用户界面或 Element API 配置 LDAP 。此操作步骤介绍了如何使用 Element UI 配置 LDAP 。

此示例显示了如何在 SolidFire 上配置 LDAP 身份验证，并使用 `SearchAndBind` 作为身份验证类型。此示例使用一个 Windows Server 2012 R2 Active Directory 服务器。

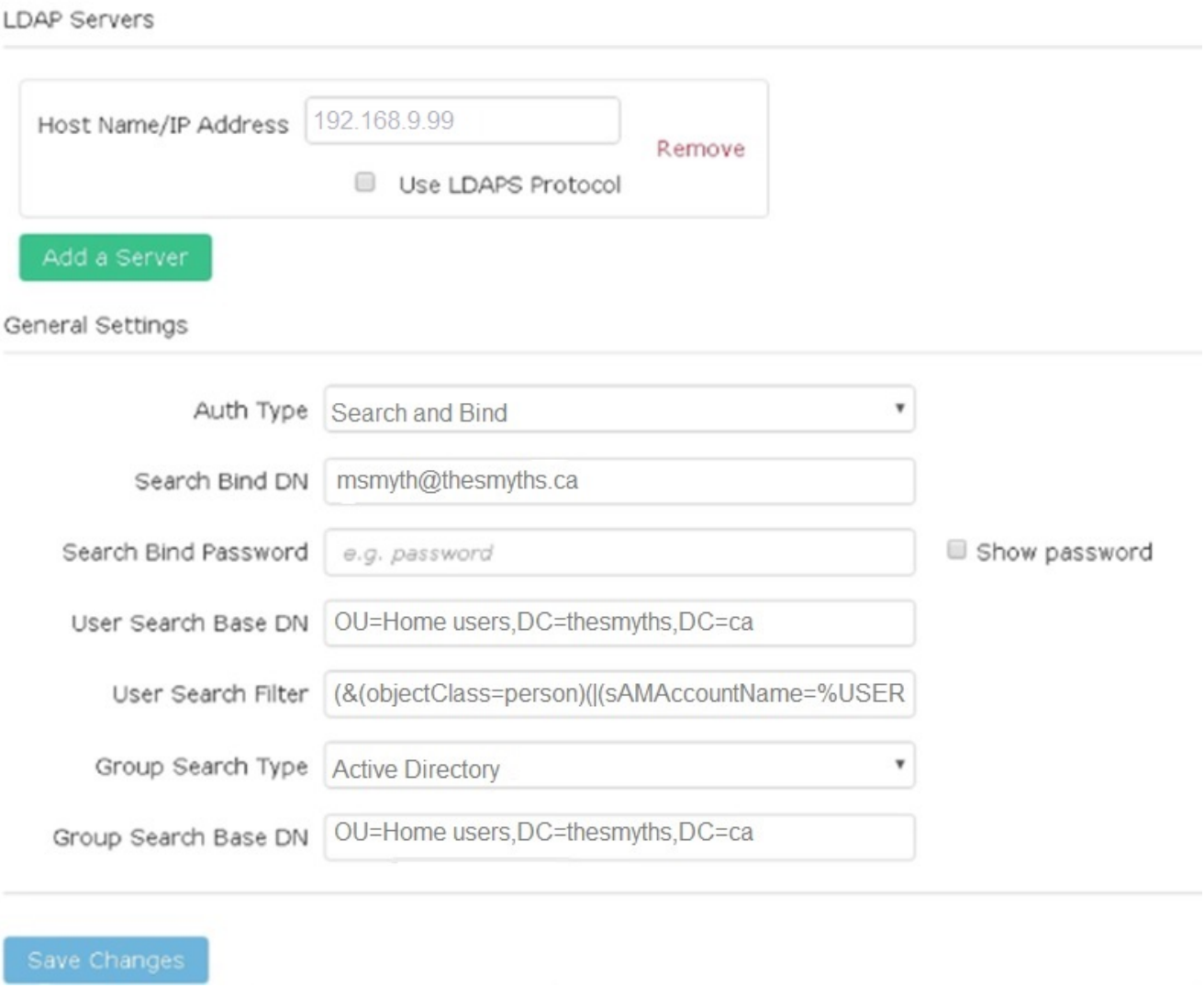
步骤

1. 单击 * 集群 * > * LDAP * 。
2. 单击 * 是 * 以启用 LDAP 身份验证。
3. 单击 * 添加服务器 * 。
4. 输入 * 主机名 /IP 地址 * 。

   也可以输入可选的自定义端口号。

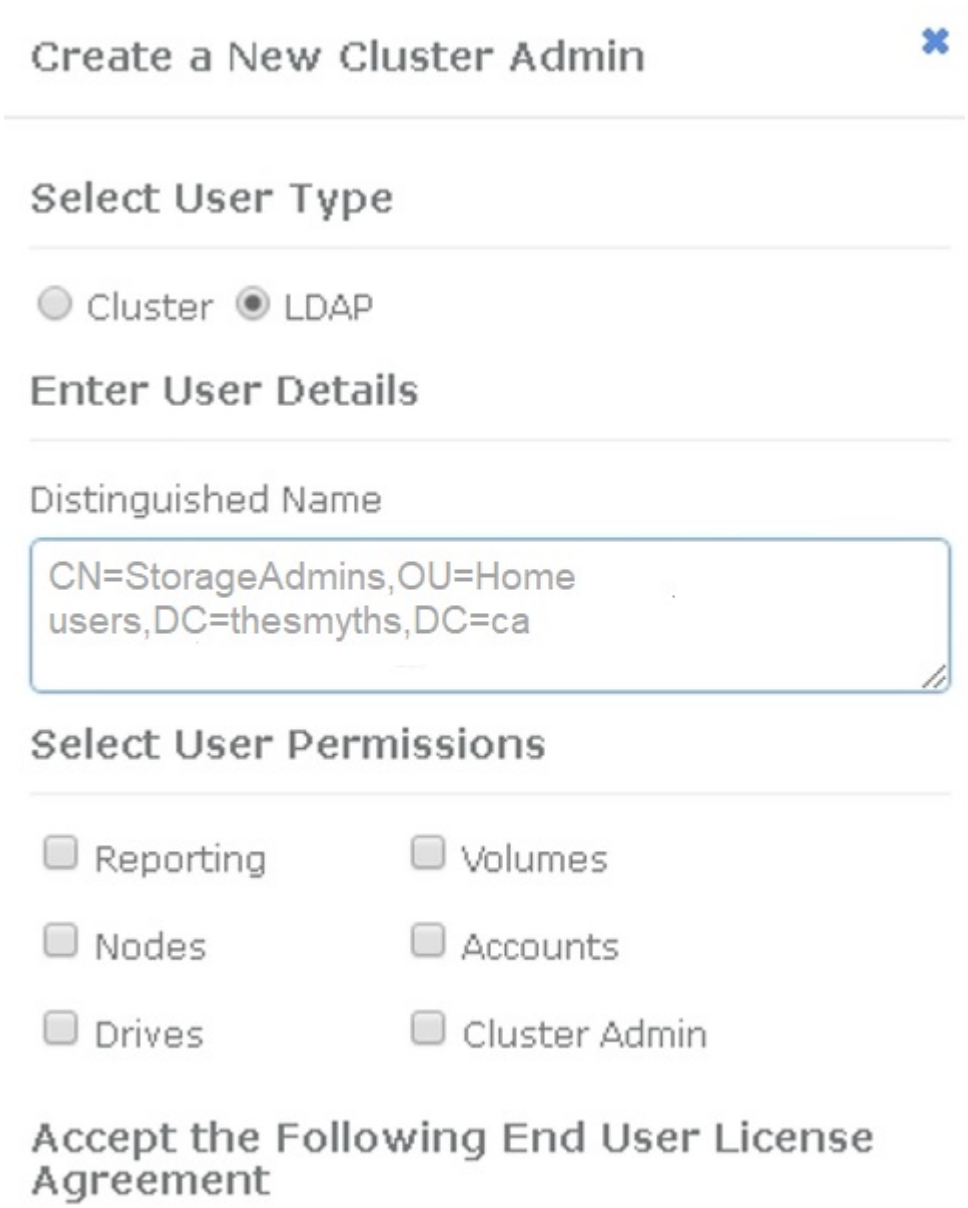
   例如，要添加自定义端口号，请输入 < 主机名或 IP 地址 > ： < 端口号 >

5. * 可选： * 选择 * 使用 LDAPS 协议 * 。
6. 在 * 常规设置 * 中输入所需信息。



7. 单击 * 启用 LDAP* 。
8. 如果要测试用户的服务器访问权限，请单击 * 测试用户身份验证 * 。

9. 复制显示的可分辨名称和用户组信息，以供日后创建集群管理员时使用。
10. 单击 * 保存更改 * 以保存任何新设置。
11. 要在此组中创建用户以便任何人都可以登录，请完成以下操作：
    a. 单击 * 用户 * > * 查看 * 。



    b. 对于新用户，单击 "User Type" （用户类型）中的 "* ldap* " ，然后将您复制的组粘贴到 "Distinguished Name" （可分辨名称）字段中。
    c. 选择权限，通常为所有权限。
    d. 向下滚动到最终用户许可协议，然后单击 * 我接受 * 。
    e. 单击 * 创建集群管理员 * 。

       现在，您的用户具有 Active Directory 组的值。

要对此进行测试，请从 Element UI 中注销，然后以该组中的用户身份重新登录。

使用 **Element API** 启用 **LDAP** 身份验证

您可以配置存储系统与现有 LDAP 服务器的集成。这样， LDAP 管理员就可以集中管理用户的存储系统访问权限。

您可以使用 Element 用户界面或 Element API 配置 LDAP 。此操作步骤介绍了如何使用 Element API 配置 LDAP 。

要在 SolidFire 集群上利用 LDAP 身份验证，请首先使用 `EnableLdapAuthentication` API 方法在集群上启用 LDAP 身份验证。

步骤

1. 首先使用 `EnableLdapAuthentication` API 方法在集群上启用 LDAP 身份验证。
2. 输入所需信息。

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. 更改以下参数的值：

使用的参数	**Description**
AuthType： SearchAndBind	指示集群将使用只读服务帐户首先搜索要进行身份验证的用户，然后在发现并经过身份验证后绑定该用户。
groupSearchBaseDN： DC=prodtest ，dc=solidfire ， dc=net	指定 LDAP 树中开始搜索组的位置。在本示例中，我们使用了树的根。如果 LDAP 树非常大，您可能需要将其设置为更精细的子树以减少搜索时间。

使用的参数	Description
userSearchBaseDN： DC=prodtest， dc=solidfire， dc=net	指定 LDAP 树中开始搜索用户的位置。在本示例中，我们使用了树的根。如果 LDAP 树非常大，您可能需要将其设置为更精细的子树以减少搜索时间。
groupSearchType： ActiveDirectory	使用 Windows Active Directory 服务器作为 LDAP 服务器。

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
要使用 userPrincipalName （用于登录的电子邮件地址），您可以将 userSearchFilter 更改为：
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
或者，要同时搜索 userPrincipalName 和 sAMAccountName ，您可以使用以下 userSearchFilter：
 	
`"(&(objectClass=person)(`
	（ sAMAccountName=%USERNAME% ）（ userPrincipalName=%USERNAME% ））" ——

利用 sAMAccountName 作为我们登录到 SolidFire 集群的用户名。这些设置会指示 LDAP 在 sAMAccountName 属性中搜索登录期间指定的用户名，并将搜索限制为在 objectClass 属性中使用 "`person` " 作为值的条目。	searchBindDN
这是将用于搜索 LDAP 目录的只读用户的可分辨名称。对于 Active Directory ，通常最容易为用户使用 userPrincipalName （电子邮件地址格式）。	searchBindPassword

要对此进行测试，请从 Element UI 中注销，然后以该组中的用户身份重新登录。

查看 **LDAP** 详细信息

在 "Cluster" 选项卡上的 "LDAP" 页面上查看 LDAP 信息。

要查看这些 LDAP 配置设置，必须启用 LDAP 。

1. 要使用 Element UI 查看 LDAP 详细信息，请单击 * 集群 * > * LDAP * 。
   - * 主机名 /IP 地址 * ： LDAP 或 LDAPS 目录服务器的地址。
   - * 身份验证类型 * ： 用户身份验证方法。可能值：
     - 直接绑定
     - 搜索并绑定
   - * 搜索绑定 DN* ： 用于登录以对用户执行 LDAP 搜索的完全限定 DN （需要对 LDAP 目录具有绑定级别访问权限）。
   - * 搜索绑定密码 * ： 用于对 LDAP 服务器访问进行身份验证的密码。
   - * 用户搜索基础 DN* ： 用于开始用户搜索的树的基础 DN 。系统将从指定位置搜索子树。
   - * 用户搜索筛选器 * ： 使用您的域名输入以下内容：

     `（ & （ objectClass=person ）（ = （ sAMAccountName=%USERNAME% ）（ userPrincipalName=%USERNAME% ））`
   - * 组搜索类型 * ： 用于控制使用的默认组搜索筛选器的搜索类型。可能值：
     - Active Directory ： 用户的所有 LDAP 组的嵌套成员资格。
     - 无组：无组支持。
     - Member DN ： 成员 DN 样式的组（单层）。
   - * 组搜索基础 DN* ： 用于开始组搜索的树的基础 DN 。系统将从指定位置搜索子树。
   - * 测试用户身份验证 * ： 配置 LDAP 后，使用此选项测试 LDAP 服务器的用户名和密码身份验证。输入已存在的帐户以测试此问题。此时将显示可分辨名称和用户组信息，您可以复制这些信息以供日后创建集群管理员时使用。

测试 **LDAP** 配置

配置 LDAP 后，您应使用 Element UI 或 Element API `TestLdapAuthentication` 方法对其进行测试。

步骤

1. 要使用 Element UI 测试 LDAP 配置，请执行以下操作：
   a. 单击 * 集群 * > * LDAP * 。
   b. 单击 * 测试 LDAP 身份验证 * 。
   c. 使用下表中的信息解决任何问题：

错误消息	Description
`xLDAPUserNotFound`	• 在已配置的 `userSearchBaseDN` 子树中未找到要测试的用户。 • `userSearchFilter` 配置不正确。

错误消息	Description
`xLDAPBindFailed (Error: Invalid credentials)`	• 要测试的用户名是有效的 LDAP 用户，但提供的密码不正确。 • 要测试的用户名是有效的 LDAP 用户，但此帐户当前已禁用。
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	LDAP 服务器 URI 不正确。
`xLDAPSearchBindFailed (Error: Invalid credentials)`	只读用户名或密码配置不正确。
`xLDAPSearchFailed (Error: No such object)`	`userSearchBaseDN` 不是 LDAP 树中的有效位置。
`xLDAPSearchFailed (Error: Referral)`	• `userSearchBaseDN` 不是 LDAP 树中的有效位置。 • `userSearchBaseDN` 和 `groupSearchBaseDN` 位于嵌套的 OU 中。这可能会引发发生原因权限问题。临时解决策将在用户和组基本 DN 条目中包含 OU （例如：`ou=storage ， cn=company ， cn=com` ）

2. 要使用 Element API 测试 LDAP 配置，请执行以下操作：
   a. 调用 TestLdapAuthentication 方法。

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

   b. 查看结果。如果 API 调用成功，结果将包括指定用户的可分辨名称以及用户所属的组列表。

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

禁用 **LDAP**

您可以使用 Element UI 禁用 LDAP 集成。

开始之前，您应记下所有配置设置，因为禁用 LDAP 会擦除所有设置。

步骤

1. 单击 * 集群 * > * LDAP * 。
2. 单击 * 否 * 。
3. 单击 * 禁用 LDAP* 。

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
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"。

管理卷和虚拟卷

了解如何管理卷和虚拟卷

您可以从 Element UI 中的 Management 选项卡管理运行 Element 软件的集群中的数据。可用的集群管理功能包括创建和管理数据卷，卷访问组，启动程序和服务质量（ QoS ）策略。

使用卷

SolidFire 系统使用卷配置存储。卷是 iSCSI 或光纤通道客户端通过网络访问的块设备。从 "Management" 选项卡上的 "Volumes" 页面中，您可以在节点上创建，修改，克隆和删除卷。您还可以查看有关卷带宽和 I/O 使用情况的统计信息。

"了解如何处理卷"

使用虚拟卷

您可以使用 Element UI 查看虚拟卷及其关联存储容器，协议端点，绑定和主机的信息并执行相关任务。

NetApp Element 软件存储系统在出厂时已禁用虚拟卷（ VVol ）功能。您必须执行一次性任务，通过 Element

UI 手动启用 vSphere VVol 功能。

启用 VVol 功能后，用户界面中将显示 VVol 选项卡，其中提供了与 VVol 相关的监控和有限管理选项。此外，一个称为 VASA Provider 的存储端软件组件可充当 vSphere 的存储感知服务。大多数 VVOL 命令（例如 VVOL 创建，克隆和编辑）都由 vCenter Server 或 ESXi 主机启动，并由 VASA Provider 转换为 Element 软件存储系统的 Element API 。可以使用 Element UI 启动用于创建，删除和管理存储容器以及删除虚拟卷的命令。

在 Element 软件存储系统中使用虚拟卷功能所需的大多数配置均在 vSphere 中进行。要在 vCenter 中注册 VASA Provider ，创建和管理 VVOL 数据存储库以及根据策略管理存储，请参见 _VMware vSphere 适用于 SolidFire 存储的虚拟卷配置指南。

对于Element 12.5及更早版本、请勿将多个NetApp Element VASA Provider注册到一个vCenter实例中。如果添加了另一个 NetApp Element VASA 提供程序，则会使所有 VVOL 数据存储库无法访问。

如果您已在 vCenter 中注册了 VASA Provider ，则可通过升级修补程序为多个 vCenter 提供 VASA 支持。要安装，请从下载 VASA39 .tar.gz 文件 "NetApp 软件下载" 并按照清单中的说明进行操作。NetApp Element VASA 提供程序使用 NetApp 证书。使用此修补程序时， vCenter 会未经修改地使用此证书来支持多个 vCenter 以供 VASA 和 VVol 使用。请勿修改证书。VASA 不支持自定义 SSL 证书。

"了解如何使用虚拟卷"

使用卷访问组和启动程序

您可以使用 iSCSI 启动程序或光纤通道启动程序访问卷访问组中定义的卷。

您可以通过在一组卷中映射 iSCSI 启动程序 IQN 或光纤通道 WWPN 来创建访问组。添加到访问组的每个 IQN 都可以访问组中的每个卷，而无需 CHAP 身份验证。

CHAP 身份验证方法有两种：

- 帐户级别的 CHAP 身份验证：您可以为帐户分配 CHAP 身份验证。
- 启动程序级别的 CHAP 身份验证：您可以为特定启动程序分配唯一的 CHAP 目标和密钥，而无需在单个帐户中绑定到单个 CHAP 。此启动程序级别的 CHAP 身份验证将取代帐户级别的凭据。

您也可以选择使用按启动程序 CHAP 强制执行启动程序授权和按启动程序 CHAP 身份验证。这些选项可以按启动程序定义，访问组可以包含具有不同选项的混合启动程序。

添加到访问组的每个 WWPN 都允许通过光纤通道网络访问此访问组中的卷。

卷访问组具有以下限制：

- 一个访问组最多允许 64 个 IQN 或 WWPN 。
- 一个访问组最多可由 2000 个卷组成。
- IQN 或 WWPN 只能属于一个访问组。
- 一个卷最多可属于四个访问组。

"了解如何与批量访问组和发起者合作"

有关详细信息 ...

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

使用卷

管理服务质量策略

通过服务质量（ QoS ）策略，您可以创建和保存可应用于多个卷的标准化服务质量设置。您可以从 "Management" 选项卡上的 "QoS Policies" 页面创建，编辑和删除 QoS 策略。

如果使用的是 QoS 策略，请勿对卷使用自定义 QoS 。自定义 QoS 将覆盖和调整卷 QoS 设置的 QoS 策略值。

"NetApp 视频： SolidFire 服务质量策略"

请参见 "性能和服务质量"。

- 创建 QoS 策略
- 编辑 QoS 策略
- 删除 QoS 策略

创建 **QoS** 策略

您可以创建 QoS 策略并在创建卷时应用它们。

1. 选择 * 管理 * > * QoS 策略 * 。
2. 单击 * 创建 QoS 策略 * 。
3. 输入 * 策略名称 * 。
4. 输入最小 IOPS* ，最大 IOPS* 和突发 IOPS* 值。
5. 单击 * 创建 QoS 策略 * 。

编辑 **QoS** 策略

您可以更改现有 QoS 策略的名称或编辑与该策略关联的值。更改 QoS 策略会影响与此策略关联的所有卷。

1. 选择 * 管理 * > * QoS 策略 * 。
2. 单击要编辑的 QoS 策略对应的 "Actions" 图标。
3. 在显示的菜单中，选择 "* 编辑 " 。
4. 在 * 编辑 QoS 策略 * 对话框中，根据需要修改以下属性：
    - Policy name
    - 最小 IOPS
    - 最大 IOPS

- 突发 IOPS

5. 单击 * 保存更改 * 。

删除 QoS 策略

您可以删除不再需要的 QoS 策略。删除 QoS 策略时，与该策略关联的所有卷都会保留 QoS 设置，但不会与某个策略关联。

如果您尝试取消卷与 QoS 策略的关联，则可以将该卷的 QoS 设置更改为自定义。

1. 选择 * 管理 * > * QoS 策略 * 。
2. 单击要删除的 QoS 策略对应的 "Actions" 图标。
3. 在显示的菜单中，选择 * 删除 * 。
4. 确认操作。

了解更多信息

- "删除卷的 QoS 策略关联"
- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

管理卷

SolidFire 系统使用卷配置存储。卷是 iSCSI 或光纤通道客户端通过网络访问的块设备。

从 "Management" 选项卡上的 "Volumes" 页面中，您可以在节点上创建，修改，克隆和删除卷。

创建卷

您可以创建一个卷并将该卷与给定帐户相关联。每个卷都必须与一个帐户相关联。通过此关联，帐户可以使用 CHAP 凭据通过 iSCSI 启动程序访问卷。

您可以在创建卷期间为卷指定 QoS 设置。

1. 选择 * 管理 * > * 卷 * 。
2. 单击 * 创建卷 * 。
3. 在 * 创建新卷 * 对话框中，输入 * 卷名称 * 。
4. 输入卷的总大小。

默认卷大小选择以 GB 为单位。您可以使用以 GB 或 GiB 为单位的大小创建卷：

- 1 GB = 1 000 000 000 字节
- 1GiB = 1 073 741 824 字节

5. 为卷选择 * 块大小 * 。
6. 单击 * 帐户 * 下拉列表，然后选择应有权访问卷的帐户。

如果帐户不存在，请单击 * 创建帐户 * 链接，输入新帐户名称，然后单击 * 创建 * 。此时将创建帐户并将其与新卷关联。

如果帐户数超过 50 个，则不会显示此列表。开始键入，自动完成功能将显示可能的值供您选择。

7. 要设置 * 服务质量 * ，请执行以下操作之一：
   a. 在 * 策略 * 下，您可以选择现有 QoS 策略（如果可用）。
   b. 在 * 自定义设置 * 下，为 IOPS 设置自定义的最小值，最大值和突发值，或者使用默认 QoS 值。

      最大或突发 IOPS 值大于 20 ， 000 IOPS 的卷可能需要较高的队列深度或多个会话，才能在单个卷上实现此级别的 IOPS 。
8. 单击 * 创建卷 * 。

查看卷详细信息

1. 选择 * 管理 * > * 卷 * 。
2. 查看详细信息。
   - * ID * ： 系统为卷生成的 ID 。
   - * 名称 * ： 创建卷时为卷指定的名称。
   - * 帐户 * ： 分配给卷的帐户的名称。
   - * 访问组 * ： 卷所属的一个或多个卷访问组的名称。
   - * 访问 * ： 创建卷时分配给卷的访问类型。可能值：
     - Read / Write ： 接受所有读取和写入。
     - Read Only ： 允许所有读取活动；不允许写入。
     - Locked ： 仅允许管理员访问。
     - ReplicationTarget ： 指定为复制卷对中的目标卷。
   - * 已用 * ： 卷中已用空间的百分比。
   - * 大小 * ： 卷的总大小（以 GB 为单位）。
   - 主节点**ID**：此卷的主节点。
   - 二级节点**ID**：此卷的二级节点列表。在过渡状态期间可以是多个值、例如二级节点更改、但通常只有一个值。
   - * QoS限制*：确定卷是否因主存储节点上的高负载而受到限制。
   - * QoS 策略 * ： 用户定义的 QoS 策略的名称和链接。
   - * 最小 IOPS* ： 卷保证的最小 IOPS 数。
   - * 最大 IOPS* ： 卷允许的最大 IOPS 数。
   - * 突发 IOPS* ： 卷在短时间内允许的最大 IOPS 数。默认值为 15 ， 000 。
   - * 快照 * ： 为卷创建的快照数量。
   - * 属性 * ： 已通过 API 方法以密钥 / 值对的形式分配给卷的属性。

- * 。 512e* ：指示卷上是否启用了 512e 。可能值：
  - 是的。
  - 否
- * 创建时间 * ：卷的创建日期和时间。

查看单个卷详细信息

您可以查看单个卷的性能统计信息。

1. 选择 * 报告 * > * 卷性能 * 。
2. 在卷列表中，单击某个卷对应的 "Actions" 图标。
3. 单击 * 查看详细信息 * 。

   页面底部将显示一个托盘，其中包含有关卷的常规信息。

4. 要查看有关卷的更多详细信息，请单击 * 查看更多详细信息 * 。

   系统将显示卷的详细信息以及性能图形。

编辑活动卷

您可以修改卷属性，例如 QoS 值，卷大小以及计算字节值时使用的度量单位。您还可以修改帐户访问权限以使用复制或限制对卷的访问。

在以下情况下，如果集群上有足够的空间，则可以调整卷大小：

- 正常运行条件。
- 正在报告卷错误或故障。
- 正在克隆此卷。
- 正在重新同步此卷。

步骤

1. 选择 * 管理 * > * 卷 * 。
2. 在 * 活动 * 窗口中，单击要编辑的卷对应的 "Actions" 图标。
3. 单击 * 编辑 * 。
4. * 可选： * 更改卷的总大小。
   - 您可以增加卷的大小，但不能减小卷的大小。一次调整大小操作只能调整一个卷的大小。垃圾收集操作和软件升级不会中断调整大小操作。
   - 如果要调整用于复制的卷大小，则应首先增加分配为复制目标的卷的大小。然后，您可以调整源卷的大小。目标卷可以大于或等于源卷，但不能小于源卷。

     默认卷大小选择以 GB 为单位。您可以使用以 GB 或 GiB 为单位的大小创建卷：

   - 1 GB = 1 000 000 000 字节

- 1GiB = 1 073 741 824 字节

5. * 可选： * 选择不同的帐户访问级别，如下所示：
   - 只读
   - 读 / 写
   - 已锁定
   - 复制目标
6. * 可选： * 选择应有权访问卷的帐户。

   如果帐户不存在，请单击 * 创建帐户 * 链接，输入新帐户名称，然后单击 * 创建 * 。此时将创建帐户并将其与卷关联。

   如果帐户数超过 50 个，则不会显示此列表。开始键入，自动完成功能将显示可能的值供您选择。

7. * 可选： * 要更改 * 服务质量 * 中的选择，请执行以下操作之一：
   a. 在 * 策略 * 下，您可以选择现有 QoS 策略（如果可用）。
   b. 在 * 自定义设置 * 下，为 IOPS 设置自定义的最小值，最大值和突发值，或者使用默认 QoS 值。

   如果要在卷上使用 QoS 策略，则可以设置自定义 QoS 以删除与卷的 QoS 策略关联。自定义 QoS 将覆盖和调整卷 QoS 设置的 QoS 策略值。

   更改 IOPS 值时，应以十或百为单位递增。输入值需要有效的整数。

   为卷配置极高的突发值。这样，系统就可以更快地处理偶尔出现的大型块顺序工作负载，同时仍会限制卷的持续 IOPS 。

8. 单击 * 保存更改 * 。

删除卷

您可以从 Element 存储集群中删除一个或多个卷。

系统不会立即清除已删除的卷；此卷在大约八小时内保持可用。如果在系统清除卷之前还原该卷，则该卷将恢复联机并还原 iSCSI 连接。

如果删除用于创建快照的卷，则其关联快照将变为非活动状态。清除已删除的源卷后，关联的非活动快照也会从系统中删除。

与管理服务关联的永久性卷会在安装或升级期间创建并分配给新帐户。如果您使用的是永久性卷，请勿修改或删除这些卷或其关联帐户。

步骤

1. 选择 * 管理 * > * 卷 * 。
2. 要删除单个卷，请执行以下步骤：

a. 单击要删除的卷对应的 "Actions" 图标。
b. 在显示的菜单中，单击 * 删除 * 。
c. 确认操作。

系统会将卷移动到 * 卷 * 页面上的 * 已删除 * 区域。

3. 要删除多个卷，请执行以下步骤：
   a. 在卷列表中，选中要删除的任何卷旁边的框。
   b. 单击 * 批量操作 * 。
   c. 在显示的菜单中，单击 * 删除 * 。
   d. 确认操作。

      系统会将这些卷移动到 * 卷 * 页面上的 * 已删除 * 区域。

还原已删除的卷

如果某个卷已被删除但尚未清除，您可以还原系统中的卷。系统会在删除卷后大约八小时自动清除该卷。如果系统已清除卷，则无法还原它。

1. 选择 * 管理 * > * 卷 * 。
2. 单击 * 已删除 * 选项卡可查看已删除卷的列表。
3. 单击要还原的卷对应的 "Actions" 图标。
4. 在显示的菜单中，单击 * 还原 * 。
5. 确认操作。

   此卷将放置在 * 活动 * 卷列表中，并恢复与此卷的 iSCSI 连接。

清除卷

清除卷后，该卷将从系统中永久删除。卷中的所有数据都将丢失。

系统会在删除后八小时自动清除已删除的卷。但是，如果要在计划的时间之前清除卷，则可以执行此操作。

1. 选择 * 管理 * > * 卷 * 。
2. 单击 * 已删除 * 按钮。
3. 执行以下步骤以清除单个或多个卷。

选项	步骤
清除单个卷	a. 单击要清除的卷对应的 "Actions" 图标。 b. 单击 * 清除 * 。 c. 确认操作。

选项	步骤
清除多个卷	a. 选择要清除的卷。 b. 单击 * 批量操作 * 。 c. 在显示的菜单中，选择 * 清除 * 。 d. 确认操作。

克隆卷

您可以为单个卷或多个卷创建克隆，以便为数据创建时间点副本。克隆卷时，系统会创建卷的快照，然后为该快照引用的数据创建一份副本。这是一个异步过程，此过程所需的时间量取决于要克隆的卷大小和当前集群负载。

集群一次最多支持每个卷运行两个克隆请求，一次最多支持八个活动卷克隆操作。超过这些限制的请求将排队等待稍后处理。

操作系统在处理克隆卷方面有所不同。VMware ESXi 会将克隆的卷视为卷副本或快照卷。此卷将成为可用于创建新数据存储库的设备。有关挂载克隆卷和处理快照 LUN 的详细信息，请参见上的 VMware 文档 "挂载 VMFS 数据存储库副本" 和 "管理重复的 VMFS 数据存储库"。

在通过克隆到较小的大小截断克隆的卷之前，请确保准备好分区，使其适合较小的卷。

步骤

1. 选择 * 管理 * > * 卷 * 。
2. 要克隆单个卷，请执行以下步骤：
   a. 在 * 活动 * 页面上的卷列表中，单击要克隆的卷对应的 "Actions" 图标。
   b. 在显示的菜单中，单击 * 克隆 * 。
   c. 在 * 克隆卷 * 窗口中，输入新克隆的卷的卷名称。
   d. 使用 * 卷大小 * 自旋框和列表为卷选择一个大小和度量单位。

      默认卷大小选择以 GB 为单位。您可以使用以 GB 或 GiB 为单位的大小创建卷：

      - 1 GB = 1 000 000 000 字节
      - 1GiB = 1 073 741 824 字节

   e. 选择新克隆卷的访问类型。
   f. 从 * 帐户 * 列表中选择要与新克隆的卷关联的帐户。

      如果您单击 * 创建帐户 * 链接，输入帐户名称并单击 * 创建 * ，则可以在此步骤中创建帐户。创建帐户后，系统会自动将其添加到 * 帐户 * 列表中。

3. 要克隆多个卷，请执行以下步骤：
   a. 在 * 活动 * 页面上的卷列表中，选中要克隆的任何卷旁边的框。
   b. 单击 * 批量操作 * 。

c. 在显示的菜单中，选择 * 克隆 * 。

d. 在 * 克隆多个卷 * 对话框的 * 新卷名称前缀 * 字段中，输入克隆卷的前缀。

e. 从 * 帐户 * 列表中选择要与克隆卷关联的帐户。

f. 选择克隆卷的访问类型。

4. 单击 * 开始克隆 * 。

增加克隆的卷大小会导致新卷在卷末尾具有额外的可用空间。根据卷的使用方式，您可能需要在可用空间中扩展分区或创建新分区来利用它。

有关详细信息 ...

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

将 **LUN** 分配给光纤通道卷

您可以更改卷访问组中光纤通道卷的 LUN 分配。您还可以在创建卷访问组时分配光纤通道卷 LUN 。

分配新的光纤通道 LUN 是一项高级功能，可能会对连接的主机产生未知后果。例如，可能不会在主机上自动发现新的 LUN ID ，并且主机可能需要重新扫描才能发现新的 LUN ID 。

1. 选择 * 管理 * > * 访问组 * 。
2. 单击要编辑的访问组对应的 "Actions" 图标。
3. 在显示的菜单中，选择 "* 编辑 " 。
4. 在 * 编辑卷访问组 * 对话框的 * 分配 LUN ID* 下，单击 * LUN 分配 * 列表上的箭头。
5. 对于列表中要将 LUN 分配给的每个卷，请在相应的 * LUN * 字段中输入一个新值。
6. 单击 * 保存更改 * 。

将 **QoS** 策略应用于卷

您可以将现有 QoS 策略批量应用于一个或多个卷。

要批量应用的 QoS 策略必须存在。

1. 选择 * 管理 * > * 卷 * 。
2. 在卷列表中，选中要应用 QoS 策略的任何卷旁边的框。
3. 单击 * 批量操作 * 。
4. 在显示的菜单中，单击 * 应用 QoS 策略 * 。
5. 从下拉列表中选择 QoS 策略。
6. 单击 * 应用 * 。

了解更多信息

服务质量策略

删除卷的 **QoS** 策略关联

您可以通过选择自定义 QoS 设置从卷中删除 QoS 策略关联。

要修改的卷应与 QoS 策略关联。

1. 选择 * 管理 * > * 卷 * 。
2. 单击包含要修改的 QoS 策略的卷的 "Actions" 图标。
3. 单击 * 编辑 * 。
4. 在显示的菜单中的 * 服务质量 * 下，单击 * 自定义设置 * 。
5. 修改 * 最小 IOPS* ， * 最大 IOPS* 和 * 突发 IOPS* ，或者保留默认设置。
6. 单击 * 保存更改 * 。

了解更多信息

删除 QoS 策略

使用虚拟卷

启用虚拟卷

您必须通过 NetApp Element 软件手动启用 vSphere 虚拟卷（ VVol ）功能。默认情况下， Element 软件系统随附的 VVol 功能处于禁用状态，它不会在新安装或升级过程中自动启用。启用 VVol 功能是一次性配置任务。

您需要的内容

- 集群必须运行 Element 9.0 或更高版本。
- 集群必须连接到与 VVol 兼容的 ESXi 6.0 或更高版本环境。
- 如果您使用的是 Element 11.3 或更高版本，则集群必须连接到 ESXi 6.0 Update 3 或更高版本的环境。

> 启用 vSphere 虚拟卷功能会永久更改 Element 软件配置。只有当集群连接到与 VMware ESXi VVol 兼容的环境时，才应启用 VVol 功能。您只能通过将集群恢复为出厂映像来禁用 VVol 功能并还原默认设置，此映像将删除系统上的所有数据。

步骤

1. 选择 * 集群 * > * 设置 * 。
2. 查找虚拟卷的集群专用设置。
3. 单击 * 启用虚拟卷 * 。
4. 单击 * 是 * 确认虚拟卷配置更改。

   Element UI 中将显示 * VVols* 选项卡。

启用 VVol 功能后， SolidFire 集群将启动 VASA Provider ，为 VASA 流量打开端口 8444 ，并创建可由 vCenter 和所有 ESXi 主机发现的协议端点。

5. 从 * 集群 * > * 设置 * 中的虚拟卷（ VVol ）设置复制 VASA Provider URL 。您将使用此 URL 在 vCenter 中注册 VASA Provider 。
6. 在 * VVols* > * 存储容器 * 中创建存储容器。

您必须至少创建一个存储容器，才能将 VM 配置到 VVol 数据存储库。

7. 选择 * VVols* > * 协议端点 * 。
8. 验证是否已为集群中的每个节点创建协议端点。

vSphere 中还需要执行其他配置任务。要在 vCenter 中注册 VASA Provider ，创建和管理 VVOL 数据存储库以及根据策略管理存储，请参见 _VMware vSphere 适用于 SolidFire 存储的虚拟卷配置指南。

了解更多信息

"《适用于 SolidFire 存储的 VMware vSphere 虚拟卷配置指南》"

查看虚拟卷详细信息

您可以在 Element UI 中查看集群上所有活动虚拟卷的虚拟卷信息。您还可以查看每个虚拟卷的性能活动，包括输入，输出，吞吐量，延迟， 队列深度和卷信息。

您需要的内容

- 您应已在 Element UI 中为集群启用 VVol 功能。
- 您应已创建关联的存储容器。
- 您应已将 vSphere 集群配置为使用 Element 软件 VVol 功能。
- 您应已在 vSphere 中至少创建一个虚拟机。

步骤

1. 单击 * VVols* > * 虚拟卷 * 。

   此时将显示所有活动虚拟卷的信息。

2. 单击要查看的虚拟卷的 * 操作 * 图标。
3. 在显示的菜单中，选择 * 查看详细信息 * 。

详细信息

"VVols" 选项卡的 "Virtual Volumes" 页面提供了有关集群上每个活动虚拟卷的信息，例如卷 ID ，快照 ID ，父虚拟卷 ID 和虚拟卷 ID 。

- * 卷 ID* ： 底层卷的 ID 。

- * 快照 ID*： 底层卷快照的 ID 。如果虚拟卷不表示 SolidFire 快照，则此值为 0 。
- * 父虚拟卷 ID*： 父虚拟卷的虚拟卷 ID 。如果 ID 全部为零，则虚拟卷是独立的，不会链接到父卷。
- * 虚拟卷 ID*： 虚拟卷的 UUID 。
- * 名称 *： 分配给虚拟卷的名称。
- * 存储容器 *： 拥有虚拟卷的存储容器。
- * 子操作系统类型 *： 与虚拟卷关联的操作系统。
- * 虚拟卷类型 *： 虚拟卷类型：配置，数据，内存，交换或其他。
- * 访问 *： 分配给虚拟卷的读写权限。
- * 大小 *： 虚拟卷的大小，以 GB 或 GiB 为单位。
- * 快照 *： 关联快照的数量。单击此数字可链接到快照详细信息。
- * 最小 IOPS*： 虚拟卷的最小 IOPS QoS 设置。
- * 最大 IOPS*： 虚拟卷的最大 IOPS QoS 设置。
- * 突发 IOPS*： 虚拟卷的最大突发 QoS 设置。
- * VMW_vmid*： 以 "VMW_" 开头的字段中的信息由 VMware 定义。
- * 创建时间 *： 完成虚拟卷创建任务的时间。

单个虚拟卷详细信息

在选择单个虚拟卷并查看其详细信息时， "VVols" 选项卡上的 "Virtual Volumes" 页面将提供以下虚拟卷信息。

- * VMW_XXX*： 以 "VMW_" 开头的字段中的信息由 VMware 定义。
- * 父虚拟卷 ID*： 父虚拟卷的虚拟卷 ID 。如果 ID 全部为零，则虚拟卷是独立的，不会链接到父卷。
- * 虚拟卷 ID*： 虚拟卷的 UUID 。
- * 虚拟卷类型 *： 虚拟卷类型：配置，数据，内存，交换或其他。
- * 卷 ID*： 底层卷的 ID 。
- * 访问 *： 分配给虚拟卷的读写权限。
- * 帐户名称 *： 包含卷的帐户的名称。
- * 访问组 *： 关联的卷访问组。
- * 总卷大小 *： 总配置容量（以字节为单位）。
- * 非零块 *： 上次垃圾回收操作完成后包含数据的 4KiB 块总数。
- * 零块 *： 完成最后一轮垃圾回收操作后不含数据的 4KiB 块的总数。
- * 快照 *： 关联快照的数量。单击此数字可链接到快照详细信息。
- * 最小 IOPS*： 虚拟卷的最小 IOPS QoS 设置。
- * 最大 IOPS*： 虚拟卷的最大 IOPS QoS 设置。
- * 突发 IOPS*： 虚拟卷的最大突发 QoS 设置。
- * 启用 512*： 由于虚拟卷始终使用 512 字节块大小模拟，因此值始终为 yes 。

- * 卷已配对 *： 指示卷是否已配对。
- * 创建时间 *： 完成虚拟卷创建任务的时间。
- * 块大小 *： 卷上块的大小。
- * 未对齐写入 *： 对于 512e 卷，不在 4k 扇区边界上的写入操作数。未对齐写入次数较多可能表示分区对齐不正确。
- * 未对齐读取 *： 对于 512e 卷，不在 4k 扇区边界上的读取操作数。未对齐读取次数较多可能表示分区对齐不正确。
- * SCSI EUI 设备 ID*： 卷的全局唯一 SCSI 设备标识符，采用基于 EUI-64 的 16 字节格式。
- * scsiNAADeviceID*： NAA IEEE 注册扩展格式的卷的全局唯一 SCSI 设备标识符。
- * 属性 *： JSON 对象格式的名称 - 值对列表。

删除虚拟卷

尽管应始终从 VMware 管理层删除虚拟卷，但您可以从 Element UI 中删除虚拟卷。只有在绝对必要时，才应从 Element UI 中删除虚拟卷，例如 vSphere 无法清理 SolidFire 存储上的虚拟卷时。

1. 选择 * VVols* > * 虚拟卷 * 。
2. 单击要删除的虚拟卷对应的 "Actions" 图标。
3. 在显示的菜单中，选择 * 删除 * 。

> 您应从 VMware 管理层删除虚拟卷，以确保在删除之前正确解除虚拟卷的绑定。只有在绝对必要时，才应从 Element UI 中删除虚拟卷，例如 vSphere 无法清理 SolidFire 存储上的虚拟卷时。如果从 Element UI 中删除虚拟卷，则此卷将立即清除。

4. 确认操作。
5. 刷新虚拟卷列表以确认虚拟卷已被删除。
6. * 可选 *： 选择 * 报告 * > * 事件日志 * 以确认清除已成功。

管理存储容器

存储容器是在运行 Element 软件的集群上创建的 vSphere 数据存储库表示形式。

此时将创建存储容器并将其绑定到 NetApp Element 帐户。在 Element 存储上创建的存储容器在 vCenter 和 ESXi 中显示为 vSphere 数据存储库。存储容器不会在 Element 存储上分配任何空间。它们仅用于从逻辑上关联虚拟卷。

每个集群最多支持四个存储容器。要启用 VVol 功能，至少需要一个存储容器。

创建存储容器

您可以在 Element UI 中创建存储容器，并在 vCenter 中发现它们。您必须至少创建一个存储容器，才能开始配置 VVol 支持的虚拟机。

开始之前，请在 Element UI 中为集群启用 VVol 功能。

步骤

1. 选择 * VVols* > * 存储容器 * 。
2. 单击 * 创建存储容器 * 按钮。
3. 在 * 创建新存储容器 * 对话框中输入存储容器信息：
   a. 输入存储容器的名称。
   b. 配置 CHAP 的启动程序和目标密钥。

      将 "CHAP Settings" 字段留空可自动生成密钥。

   c. 单击 * 创建存储容器 * 按钮。
4. 验证新存储容器是否显示在 * 存储容器 * 子选项卡的列表中。

   由于 NetApp Element 帐户 ID 会自动创建并分配给存储容器，因此无需手动创建帐户。

查看存储容器详细信息

在 "VVols" 选项卡的 "Storage Containers" 页面上，您可以查看集群上所有活动存储容器的信息。

- * 帐户 ID* ： 与存储容器关联的 NetApp Element 帐户的 ID 。
- * 名称 * ： 存储容器的名称。
- * 状态 * ： 存储容器的状态。可能值：
  - Active ： 存储容器正在使用中。
  - locked ： 存储容器已锁定。
- * PE Type* ： 协议端点类型（ SCSI 是 Element 软件唯一可用的协议）。
- * 存储容器 ID* ： 虚拟卷存储容器的 UUID 。
- * 活动虚拟卷 * ： 与存储容器关联的活动虚拟卷的数量。

查看单个存储容器详细信息

您可以通过从 "VVols" 选项卡上的 "Storage Containers" 页面中选择单个存储容器来查看其存储容器信息。

- * 帐户 ID* ： 与存储容器关联的 NetApp Element 帐户的 ID 。
- * 名称 * ： 存储容器的名称。
- * 状态 * ： 存储容器的状态。可能值：
  - Active ： 存储容器正在使用中。
  - locked ： 存储容器已锁定。
- * CHAP Initiator Secret* ： 启动程序的唯一 CHAP 密钥。
- * CHAP Target Secret* ： 目标的唯一 CHAP 密钥。
- * 存储容器 ID* ： 虚拟卷存储容器的 UUID 。
- * 协议端点类型 * ： 表示协议端点类型（ SCSI 是唯一可用的协议）。

编辑存储容器

您可以在 Element UI 中修改存储容器 CHAP 身份验证。

1. 选择 * VVols* > * 存储容器 * 。
2. 单击要编辑的存储容器的 * 操作 * 图标。
3. 在显示的菜单中，选择 * 编辑 * 。
4. 在 CHAP Settings 下，编辑用于身份验证的 Initiator Secret 和 Target Secret 凭据。

   如果不更改 CHAP 设置凭据，它们将保持不变。如果您将凭据字段留空，系统将自动生成新密码。

5. 单击 * 保存更改 * 。

删除存储容器

您可以从 Element UI 中删除存储容器。

您需要的内容

确保已从 VVol 数据存储库中删除所有虚拟机。

步骤

1. 选择 * VVols* > * 存储容器 * 。
2. 单击要删除的存储容器的 * 操作 * 图标。
3. 在显示的菜单中，选择 * 删除 * 。
4. 确认操作。
5. 刷新 * 存储容器 * 子选项卡中的存储容器列表，以确认此存储容器已被删除。

协议端点

了解协议端点

协议端点是指主机用来对运行 NetApp Element 软件的集群上的存储进行寻址的访问点。协议端点不能由用户删除或修改，不与帐户关联，也不能添加到卷访问组。

运行 Element 软件的集群会自动为集群中的每个存储节点创建一个协议端点。例如，一个六节点存储集群具有六个协议端点，这些协议端点映射到每个 ESXi 主机。协议端点由 Element 软件动态管理，并可根据需要创建，移动或删除，而无需任何干预。协议端点是多路径的目标，并充当附属 LUN 的 I/O 代理。每个协议端点都使用一个可用的 SCSI 地址，就像标准 iSCSI 目标一样。协议端点在 vSphere 客户端中显示为单块（ 512 字节）存储设备，但此存储设备不可格式化或用作存储。

iSCSI 是唯一受支持的协议。不支持光纤通道协议。

协议端点详细信息

"VVols" 选项卡上的 "Protocol Endpoints" 页面提供了协议端点信息。

- * 主提供程序 ID*

  主协议端点提供程序的 ID 。

- * 二级提供程序 ID*

  二级协议端点提供程序的 ID 。

- * 协议端点 ID*

  协议端点的 UUID 。

- * 协议端点状态 *

  协议端点的状态。可能值如下：

  - Active ： 协议端点正在使用中。
  - start ： 协议端点正在启动。
  - failover ： 协议端点已进行故障转移。
  - Reserved ： 已保留协议端点。

- * 提供程序类型 *

  协议端点提供程序的类型。可能值如下：

  - 主卷
  - 二级

- * SCSI NAA 设备 ID*

  NAA IEEE 注册扩展格式中协议端点的全局唯一 SCSI 设备标识符。

绑定

了解装订

要对虚拟卷执行 I/O 操作， ESXi 主机必须先绑定虚拟卷。

SolidFire 集群会选择最佳协议端点，创建将 ESXi 主机和虚拟卷与协议端点关联的绑定，并将此绑定返回到 ESXi 主机。绑定后， ESXi 主机可以对绑定的虚拟卷执行 I/O 操作。

绑定详细信息

"VVols" 选项卡上的 "Bindings" 页面提供了有关每个虚拟卷的绑定信息。

此时将显示以下信息：

- * 主机 ID*

  托管虚拟卷且为集群所知的 ESXi 主机的 UUID 。

- * 协议端点 ID*

  与 SolidFire 集群中的每个节点对应的协议端点 ID 。

- * 带内协议端点 ID*

  协议端点的 SCSI NAA 设备 ID 。

- * 协议端点类型 *

  协议端点类型。

- * VVol 绑定 ID*

  虚拟卷的绑定 UUID 。

- * VVol ID*

  虚拟卷的通用唯一标识符（ UUID ）。

- * VVol 二级 ID*

  虚拟卷的二级 ID ，即 SCSI 二级 LUN ID 。

主机详细信息

"VVols" 选项卡上的 "Hosts" 页面提供了有关托管虚拟卷的 VMware ESXi 主机的信息。

此时将显示以下信息：

- * 主机 ID*

  托管虚拟卷且为集群所知的 ESXi 主机的 UUID 。

- * 主机地址 *

  ESXi 主机的 IP 地址或 DNS 名称。

- * 绑定 *

  ESXi 主机绑定的所有虚拟卷的绑定 ID 。

- * ESX 集群 ID*

  vSphere 主机集群 ID 或 vCenter GUID 。

- * 启动程序 IQN*

  虚拟卷主机的启动程序 IQN 。

- * SolidFire 协议端点 ID*

当前对 ESXi 主机可见的协议端点。

使用卷访问组和启动程序

创建卷访问组

您可以通过将启动程序映射到一组卷来创建卷访问组，以实现安全访问。然后，您可以使用帐户 CHAP 启动程序密钥和目标密钥授予对组中卷的访问权限。

如果使用基于启动程序的 CHAP ，则可以为卷访问组中的单个启动程序添加 CHAP 凭据，从而提高安全性。这样，您就可以将此选项应用于已存在的卷访问组。

步骤

1. 单击 * 管理 * > * 访问组 * 。
2. 单击 * 创建访问组 * 。
3. 在 * 名称 * 字段中输入卷访问组的名称。
4. 通过以下方式之一将启动程序添加到卷访问组：

选项	Description
添加光纤通道启动程序	a. 在 "Add Initiators" 下，从 "Unbound Fibre Channel Initiators" 列表中选择一个现有光纤通道启动程序。 b. 单击 * 添加 FC 启动程序 * 。 如果单击 * 创建启动程序 * 链接，输入启动程序名称并单击 * 创建 * ，则可以在此步骤中创建启动程序。创建启动程序后，系统会自动将其添加到启动程序列表中。 格式示例如下： `5f:47:ac:c0:5c:74:d4:02`

选项	Description
添加 iSCSI 启动程序	在 "Add Initiators" 下，从 "Initiators" 列表中选择一个现有启动程序。* 注： * 如果单击 * 创建启动程序 * 链接，输入启动程序名称并单击 * 创建 * ，则可以在此步骤中创建启动程序。创建启动程序后，系统会自动将其添加到启动程序列表中。 格式示例如下： `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` 您可以通过在 * 管理 * > * 卷 * > * 活动 * 列表中选择卷的操作菜单中的 * 查看详细信息 * 来找到每个卷的启动程序 IQN 。 修改启动程序时，可以将 requiredCHAP 属性切换为 True ，从而可以设置目标启动程序密钥。有关详细信息，请参见有关 ModifyInitiator API 方法的 API 信息。 "使用 Element API 管理存储"

5. * 可选： * 根据需要添加更多启动程序。
6. 在添加卷下，从 * 卷 * 列表中选择一个卷。

   此卷将显示在 * 已连接卷 * 列表中。
7. * 可选： * 根据需要添加更多卷。
8. 单击 * 创建访问组 * 。

了解更多信息

将卷添加到访问组

查看单个访问组详细信息

您可以通过图形格式查看单个访问组的详细信息，例如连接的卷和启动程序。

1. 单击 * 管理 * > * 访问组 * 。
2. 单击访问组对应的 "Actions" 图标。
3. 单击 * 查看详细信息 * 。

卷访问组详细信息

" 管理 " 选项卡上的 " 访问组 " 页面提供了有关卷访问组的信息。

此时将显示以下信息：

- * ID * ：系统为访问组生成的 ID 。

- * 名称 *： 创建访问组时为其指定的名称。
- * 活动卷 *： 访问组中活动卷的数量。
- * 压缩 *： 访问组的压缩效率得分。
- * 重复数据删除 *： 访问组的重复数据删除效率得分。
- * 精简配置 *： 访问组的精简配置效率得分。
- * 整体效率 *： 访问组的整体效率得分。
- * 启动程序 *： 连接到访问组的启动程序数量。

将卷添加到访问组

您可以将卷添加到卷访问组。每个卷可以属于多个卷访问组；您可以在 * 活动 * 卷页面上查看每个卷所属的组。

您也可以使用此操作步骤向光纤通道卷访问组添加卷。

1. 单击 * 管理 * > * 访问组 * 。
2. 单击要将卷添加到的访问组对应的 "Actions" 图标。
3. 单击 * 编辑 * 按钮。
4. 在添加卷下，从 * 卷 * 列表中选择一个卷。

   您可以重复此步骤来添加更多卷。

5. 单击 * 保存更改 * 。

从访问组中删除卷

从访问组中删除卷后，该组将无法再访问该卷。

修改帐户中的 CHAP 设置或从访问组中删除启动程序或卷可能会使发生原因启动程序意外丢失对卷的访问权限。要验证卷访问不会意外丢失，请始终注销将受帐户或访问组更改影响的 iSCSI 会话，并验证启动程序是否可以在完成启动程序设置和集群设置的任何更改后重新连接到卷。

1. 单击 * 管理 * > * 访问组 * 。
2. 单击要从中删除卷的访问组对应的 "Actions" 图标。
3. 单击 * 编辑 * 。
4. 在 * 编辑卷访问组 * 对话框的添加卷下，单击 * 附加卷 * 列表上的箭头。
5. 从列表中选择要删除的卷，然后单击 * x * 图标从列表中删除该卷。

   您可以重复执行此步骤来删除更多卷。

6. 单击 * 保存更改 * 。

创建启动程序

您可以创建 iSCSI 或光纤通道启动程序，也可以为其分配别名。

此外，您还可以使用 API 调用来分配基于启动程序的 CHAP 属性。要为每个启动程序添加 CHAP 帐户名称和凭据，必须使用 `CreateInitiator` API 调用删除和添加 CHAP 访问和属性。通过 `CreateInitiators` 和 `ModfyInitiators` API 调用指定一个或多个 virtualNetworkID ，可以将启动程序访问限制为一个或多个 VLAN 。如果未指定虚拟网络，则启动程序可以访问所有网络。

详情请参阅 API 参考信息。 "使用 Element API 管理存储"

步骤

1. 单击 * 管理 * > * 启动程序 * 。
2. 单击 * 创建启动程序 * 。
3. 执行以下步骤以创建一个或多个启动程序：

选项	步骤
创建一个启动程序	a. 单击 * 创建单个启动程序 * 。 b. 在 * IQN/WWPN* 字段中输入启动程序的 IQN 或 WWPN 。 c. 在 * 别名 * 字段中输入启动程序的友好名称。 d. 单击 * 创建启动程序 * 。
创建多个启动程序	a. 单击 * 批量创建启动程序 * 。 b. 在文本框中输入 IQN 或 WWPN 列表。 c. 单击 * 添加启动程序 * 。 d. 从生成的列表中选择一个启动程序，然后单击 * 别名 * 列中对应的添加图标，为启动程序添加别名。 e. 单击复选标记以确认新别名。 f. 单击 * 创建启动程序 * 。

编辑启动程序

您可以更改现有启动程序的别名，也可以添加别名（如果尚不存在）。

要为每个启动程序添加 CHAP 帐户名称和凭据，您必须使用 `ModfyInitiator` API 调用来删除和添加 CHAP 访问和属性。

看"使用 Element API 管理存储"。

步骤

1. 单击 * 管理 * > * 启动程序 * 。
2. 单击要编辑的启动程序对应的 "Actions" 图标。

3. 单击 * 编辑 * 。
4. 在 * 别名 * 字段中输入启动程序的新别名。
5. 单击 * 保存更改 * 。

将单个启动程序添加到卷访问组

您可以将启动程序添加到现有卷访问组。

将启动程序添加到卷访问组时，启动程序可以访问该卷访问组中的所有卷。

您可以通过单击 "Actions" 图标并在活动卷列表中为卷选择 * 查看详细信息 * 来查找每个卷的启动程序。

如果使用基于启动程序的 CHAP ，则可以为卷访问组中的单个启动程序添加 CHAP 凭据，从而提高安全性。这样，您就可以将此选项应用于已存在的卷访问组。

步骤

1. 单击 * 管理 * > * 访问组 * 。
2. 单击要编辑的访问组的 * 操作 * 图标。
3. 单击 * 编辑 * 。
4. 要将光纤通道启动程序添加到卷访问组，请执行以下步骤：
   a. 在添加启动程序下，从 * 未绑定光纤通道启动程序 * 列表中选择一个现有光纤通道启动程序。
   b. 单击 * 添加 FC 启动程序 * 。

      如果单击 * 创建启动程序 * 链接，输入启动程序名称并单击 * 创建 * ，则可以在此步骤中创建启动程序。创建启动程序后，系统会自动将其添加到 * 启动程序 * 列表中。

      格式示例如下：

```
5f:47:ac:c0:5c:74:d4:02
```

5. 要将 iSCSI 启动程序添加到卷访问组，请在添加启动程序下，从 * 启动程序 * 列表中选择一个现有启动程序。

   如果单击 * 创建启动程序 * 链接，输入启动程序名称并单击 * 创建 * ，则可以在此步骤中创建启动程序。创建启动程序后，系统会自动将其添加到 * 启动程序 * 列表中。

   可接受的启动程序 IQN 格式如下： iqn.yyyy-mm ，其中 y 和 m 是数字，后跟文本，文本必须仅包含数字，小写字母字符，句点（ . ），冒号（： ）或短划线（ - ）。

   格式示例如下：

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

您可以在 * 管理 * > * 卷 * 活动卷页面中找到每个卷的启动程序 IQN ，方法是单击操作图标，然后选择卷的 * 查看详细信息 * 。

6. 单击 * 保存更改 * 。

将多个启动程序添加到卷访问组

您可以向现有卷访问组添加多个启动程序，以允许访问卷访问组中的卷，无论是否需要 CHAP 身份验证。

将启动程序添加到卷访问组时，启动程序可以访问该卷访问组中的所有卷。

您可以通过单击操作图标并单击活动卷列表中卷的 * 查看详细信息 * 来查找每个卷的启动程序。

您可以将多个启动程序添加到现有卷访问组中，以便能够访问卷，并为该卷访问组中的每个启动程序分配唯一的 CHAP 凭据。这样，您就可以将此选项应用于已存在的卷访问组。

您可以使用 API 调用来分配基于启动程序的 CHAP 属性。要为每个启动程序添加 CHAP 帐户名称和凭据，必须使用 ModifyInitiator API 调用删除和添加 CHAP 访问和属性。

有关详细信息，请参阅"使用 Element API 管理存储"。

步骤

1. 单击 * 管理 * > * 启动程序 * 。
2. 选择要添加到访问组的启动程序。
3. 单击 * 批量操作 * 按钮。
4. 单击 * 添加到卷访问组 * 。
5. 在添加到卷访问组对话框中，从 * 卷访问组 * 列表中选择一个访问组。
6. 单击 * 添加 * 。

从访问组中删除启动程序

从访问组中删除启动程序后，它将无法再访问该卷访问组中的卷。对卷的正常帐户访问不会中断。

修改帐户中的 CHAP 设置或从访问组中删除启动程序或卷可能会使发生原因启动程序意外丢失对卷的访问权限。要验证卷访问不会意外丢失，请始终注销将受帐户或访问组更改影响的 iSCSI 会话，并验证启动程序是否可以在完成启动程序设置和集群设置的任何更改后重新连接到卷。

步骤

1. 单击 * 管理 * > * 访问组 * 。
2. 单击要删除的访问组的 * 操作 * 图标。
3. 在显示的菜单中，选择 * 编辑 * 。
4. 在 * 编辑卷访问组 * 对话框的添加启动程序下，单击 * 启动程序 * 列表上的箭头。
5. 为要从访问组中删除的每个启动程序选择 x 图标。

6. 单击 * 保存更改 * 。

删除访问组

您可以删除不再需要的访问组。在删除卷访问组之前，您无需从该组中删除启动程序 ID 和卷 ID 。删除访问组后，对卷的组访问将中断。

1. 单击 * 管理 * > * 访问组 * 。
2. 单击要删除的访问组的 * 操作 * 图标。
3. 在显示的菜单中，单击 * 删除 * 。
4. 要同时删除与此访问组关联的启动程序，请选中 * 删除此访问组中的启动程序 * 复选框。
5. 确认操作。

删除启动程序

您可以在不再需要启动程序后将其删除。删除启动程序时，系统会将其从任何关联的卷访问组中删除。在重置连接之前，使用启动程序的所有连接都将保持有效。

步骤

1. 单击 * 管理 * > * 启动程序 * 。
2. 执行以下步骤以删除一个或多个启动程序：

选项	步骤
删除单个启动程序	a. 单击要删除的启动程序的 * 操作 * 图标。 b. 单击 * 删除 * 。 c. 确认操作。
删除多个启动程序	a. 选中要删除的启动程序旁边的复选框。 b. 单击 * 批量操作 * 按钮。 c. 在显示的菜单中，选择 * 删除 * 。 d. 确认操作。

保护您的数据

保护您的数据

通过 NetApp Element 软件，您可以通过多种方式保护数据，例如为单个卷或一组卷创建快照，在 Element 上运行的集群和卷之间进行复制以及复制到 ONTAP 系统。

- * 快照 *

仅快照数据保护功能可将特定时间点发生更改的数据复制到远程集群。仅复制在源集群上创建的快照。而源卷的活动写入则不是。

使用卷快照进行数据保护

- * 在 Element 上运行的集群和卷之间进行远程复制 *

  您可以从运行在 Element 上的集群对中的任一集群同步或异步复制卷数据，以实现故障转移和故障恢复。

  在运行 NetApp Element 软件的集群之间执行远程复制

- * 使用 SnapMirror 技术在 Element 和 ONTAP 集群之间进行复制 *

  借助 NetApp SnapMirror 技术，您可以将使用 Element 创建的快照复制到 ONTAP 以实现灾难恢复。在 SnapMirror 关系中， Element 是一个端点，而 ONTAP 是另一个端点。

  在 Element 和 ONTAP 集群之间使用 SnapMirror 复制

- * 从 SolidFire ， S3 或 Swift 对象存储备份和还原卷 *

  您可以将卷备份和还原到其他 SolidFire 存储以及与 Amazon S3 或 OpenStack Swift 兼容的二级对象存储。

  将卷备份和还原到 SolidFire ， S3 或 Swift 对象存储

有关详细信息 ...

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

使用卷快照进行数据保护

使用卷快照进行数据保护

卷快照是卷的时间点副本。如果需要将卷回滚到创建快照时的状态，您可以为卷创建快照并稍后使用该快照。

快照与卷克隆类似。但是，快照只是卷元数据的副本，因此您无法挂载或向其写入数据。创建卷快照也只需少量系统资源和空间，因此创建快照的速度比克隆快。

您可以为单个卷或一组卷创建快照。

也可以将快照复制到远程集群并将其用作卷的备份副本。这样，您就可以使用复制的快照将卷回滚到特定时间点。或者，您也可以从复制的快照创建卷的克隆。

了解更多信息

- 使用单个卷快照进行数据保护
- 使用组快照执行数据保护任务
- 计划快照

使用单个卷快照进行数据保护

卷快照是卷的时间点副本。您可以使用单个卷，而不是一组卷来创建快照。

了解更多信息

- 创建卷快照
- 编辑快照保留
- 删除快照
- 从快照克隆卷
- 将卷回滚到快照
- 将卷快照备份到 Amazon S3 对象存储
- 将卷快照备份到 OpenStack Swift 对象存储
- 将卷快照备份到 SolidFire 集群

创建卷快照

您可以为活动卷创建快照，以便在任意时间点保留卷映像。一个卷最多可以创建 32 个快照。

1. 单击 * 管理 * > * 卷 * 。
2. 单击要用于快照的卷的 * 操作 * 图标。
3. 在显示的菜单中，选择 * 快照 * 。
4. 在 * 创建卷的快照 * 对话框中，输入新的快照名称。
5. * 可选： * 选中 * 配对时在复制中包含快照 * 复选框，以确保配对父卷时在复制中捕获快照。
6. 要设置快照的保留，请选择以下选项之一：
   - 单击 * 永久保留 * 可在系统上无限期保留快照。
   - 单击 * 设置保留期限 * ，然后使用日期调整框选择系统保留快照的时间长度。
7. 要创建单个即时快照，请执行以下步骤：
   a. 单击 * 立即创建快照 * 。
   b. 单击 "* 创建 Snapshot" 。
8. 要计划在未来某个时间运行快照，请执行以下步骤：
   a. 单击 * 创建 Snapshot 计划 * 。
   b. 输入 * 新计划名称 * 。
   c. 从列表中选择一个 * 计划类型 * 。
   d. * 可选： * 选中 * 重复计划 * 复选框可定期重复计划的快照。
   e. 单击 * 创建计划 * 。

了解更多信息

计划快照

编辑快照保留

您可以更改快照的保留期限，以控制系统何时删除快照或是否删除快照。您指定的保留期限从输入新间隔开始。设置保留期限时，您可以选择从当前时间开始的期限（保留期限不会从快照创建时间开始计算）。您可以以分钟，小时和天为单位指定间隔。

步骤

1. 单击 * 数据保护 * > * 快照 * 。
2. 单击要编辑的快照对应的 * 操作 * 图标。
3. 在显示的菜单中，单击 * 编辑 * 。
4. * 可选： * 选中 "* 配对时在复制中包含 Snapshot" 复选框，以确保在配对父卷时在复制中捕获快照。
5. * 可选： * 选择快照的保留选项：
   - 单击 * 永久保留 * 可在系统上无限期保留快照。
   - 单击 * 设置保留期限 * ，然后使用日期调整框选择系统保留快照的时间长度。
6. 单击 * 保存更改 * 。

删除快照

您可以从运行 Element 软件的存储集群中删除卷快照。删除快照时，系统会立即将其删除。

您可以删除正在从源集群复制的快照。如果删除快照时快照正在同步到目标集群，则同步复制将完成，快照将从源集群中删除。快照不会从目标集群中删除。

您还可以从目标集群中删除已复制到目标的快照。已删除的快照将保留在目标上已删除的快照列表中，直到系统检测到您已删除源集群上的快照为止。当目标检测到您已删除源快照时，目标将停止复制该快照。

从源集群中删除快照时，目标集群快照不受影响（反之亦然）。

1. 单击 * 数据保护 * > * 快照 * 。
2. 单击要删除的快照对应的 * 操作 * 图标。
3. 在显示的菜单中，选择 * 删除 * 。
4. 确认操作。

从快照克隆卷

您可以从卷的快照创建新卷。执行此操作时，系统会使用创建快照时卷上包含的数据使用快照信息克隆新卷。此过程会在新创建的卷中存储有关卷的其他快照的信息。

1. 单击 * 数据保护 * > * 快照 * 。
2. 单击要用于卷克隆的快照的 * 操作 * 图标。

3. 在显示的菜单中，单击 * 从 Snapshot 克隆卷 * 。
4. 在 * 从 Snapshot 克隆卷 * 对话框中输入 * 卷名称 * 。
5. 为新卷选择 * 总大小 * 和大小单位。
6. 为卷选择 * 访问 * 类型。
7. 从列表中选择一个 * 帐户 * 以与新卷关联。
8. 单击 * 开始克隆 * 。

将卷回滚到快照

您可以随时将卷回滚到上一个快照。此操作将还原自创建快照以来对卷所做的任何更改。

步骤

1. 单击 * 数据保护 * > * 快照 * 。
2. 单击要用于卷回滚的快照的 * 操作 * 图标。
3. 在显示的菜单中，选择 * 将卷回滚到 Snapshot* 。
4. * 可选： * 要在回滚到快照之前保存卷的当前状态，请执行以下操作：
   a. 在 * 回滚到 Snapshot* 对话框中，选择 * 将卷的当前状态另存为 Snapshot* 。
   b. 输入新快照的名称。
5. 单击 * 回滚 Snapshot* 。

备份卷快照

备份卷快照

您可以使用集成备份功能备份卷快照。您可以将快照从 SolidFire 集群备份到外部对象存储或另一个 SolidFire 集群。将快照备份到外部对象存储时，必须与允许读 / 写操作的对象存储建立连接。

- "将卷快照备份到 Amazon S3 对象存储"
- "将卷快照备份到 OpenStack Swift 对象存储"
- "将卷快照备份到 SolidFire 集群"

将卷快照备份到 **Amazon S3** 对象存储

您可以将 SolidFire 快照备份到与 Amazon S3 兼容的外部对象存储。

1. 单击 "* 数据保护 ">> * 快照 * 。
2. 单击要备份的快照对应的 * 操作 * 图标。
3. 在显示的菜单中，单击 * 备份至 * 。
4. 在 * 集成备份 * 对话框的 * 备份至 * 下，选择 * S3* 。
5. 在 * 数据格式 * 下选择一个选项：

- * 原生 *： 只有 SolidFire 存储系统可以读取的压缩格式。
- * 未压缩 *： 与其他系统兼容的未压缩格式。

6. 在 * 主机名 * 字段中输入用于访问对象存储的主机名。
7. 在 * 访问密钥 ID* 字段中输入帐户的访问密钥 ID 。
8. 在 * 机密访问密钥 * 字段中输入帐户的机密访问密钥。
9. 在 * S3 Bucket* 字段中输入用于存储备份的 S3 存储分段。
10. * 可选 *： 在 * 名称标记 * 字段中输入要附加到前缀的名称标记。
11. 单击 * 开始读取 * 。

将卷快照备份到 **OpenStack Swift** 对象存储

您可以将 SolidFire 快照备份到与 OpenStack Swift 兼容的二级对象存储。

1. 单击 * 数据保护 * > * 快照 * 。
2. 单击要备份的快照对应的 * 操作 * 图标。
3. 在显示的菜单中，单击 * 备份至 * 。
4. 在 * 集成备份 * 对话框的 * 备份到 * 下，选择 * Swift* 。
5. 在 * 数据格式 * 下选择一个选项：
   - * 原生 *： 只有 SolidFire 存储系统可以读取的压缩格式。
   - * 未压缩 *： 与其他系统兼容的未压缩格式。
6. 输入用于访问对象存储的 * URL * 。
7. 为帐户输入 * 用户名 * 。
8. 输入帐户的 * 身份验证密钥 * 。
9. 输入用于存储备份的 * 容器 * 。
10. * 可选 *： 输入 * 名称标记 * 。
11. 单击 * 开始读取 * 。

将卷快照备份到 **SolidFire** 集群

您可以将驻留在 SolidFire 集群上的卷快照备份到远程 SolidFire 集群。

确保源集群和目标集群已配对。

在将一个集群备份或还原到另一个集群时，系统会生成一个密钥，用于在集群之间进行身份验证。此批量卷写入密钥允许源集群向目标集群进行身份验证，从而在写入目标卷时提供一定的安全性。在备份或还原过程中，您需要先从目标卷生成批量卷写入密钥，然后再开始此操作。

1. 在目标集群上，单击 * 管理 * > * 卷 * 。
2. 单击目标卷的 * 操作 * 图标。
3. 在显示的菜单中，单击 * 从 * 还原。

4. 在 * 集成还原 * 对话框中的 * 从 * 还原下，选择 * SolidFire * 。
5. 在 * 数据格式 * 下选择一种数据格式：
   - * 原生 * ： 只有 SolidFire 存储系统可以读取的压缩格式。
   - * 未压缩 * ： 与其他系统兼容的未压缩格式。
6. 单击 * 生成密钥 * 。
7. 将密钥从 * 批量卷写入密钥 * 框复制到剪贴板。
8. 在源集群上，单击 * 数据保护 * > * 快照 * 。
9. 单击要用于备份的快照对应的 "Actions" 图标。
10. 在显示的菜单中，单击 * 备份至 * 。
11. 在 "* 备份至 * " 下的 "* 集成备份 "* 对话框中，选择 * SolidFire * 。
12. 在 * 数据格式 * 字段中选择先前选择的相同数据格式。
13. 在 * 远程集群 MVIP* 字段中输入目标卷集群的管理虚拟 IP 地址。
14. 在 * 远程集群用户名 * 字段中输入远程集群用户名。
15. 在 * 远程集群密码 * 字段中输入远程集群密码。
16. 在 * 批量卷写入密钥 * 字段中，粘贴您先前在目标集群上生成的密钥。
17. 单击 * 开始读取 * 。

使用组快照进行数据保护

使用组快照执行数据保护任务

您可以为一组相关卷创建组快照，以便为每个卷保留元数据的时间点副本。您可以将来使用组快照作为备份或回滚，将卷组的状态还原到先前的状态。

了解更多信息

- 创建组快照
- 编辑组快照
- 编辑组快照的成员
- 删除组快照
- 将卷回滚到组快照
- 克隆多个卷
- 从组快照克隆多个卷

组快照详细信息

" 数据保护 " 选项卡上的 " 组快照 " 页面提供了有关组快照的信息。

- * ID *

系统为组快照生成的 ID 。

- * UUID *

  组快照的唯一 ID 。

- * 名称 *

  用户定义的组快照名称。

- * 创建时间 *

  创建组快照的时间。

- * 状态 *

  快照的当前状态。可能值：

  - Preparing ： 正在准备快照以供使用，该快照尚不可写入。
  - Done ： 此快照已完成准备，现在可供使用。
  - Active ： 快照是活动分支。

- * 卷数 *

  组中的卷数。

- * 保留至 *

  删除快照的日期和时间。

- * 远程复制 *

  指示是否已启用快照以复制到远程 SolidFire 集群。可能值：

  - Enabled ： 已为快照启用远程复制。
  - Disabled ： 未为快照启用远程复制。

创建组快照

您可以为一组卷创建快照，也可以创建组快照计划以自动执行组快照。一个组快照一次可以一致地创建多达 32 个卷的快照。

步骤

1. 单击 * 管理 * > * 卷 * 。
2. 使用复选框为一组卷选择多个卷。
3. 单击 * 批量操作 * 。
4. 单击 * 组 Snapshot* 。
5. 在创建卷的组快照对话框中输入新的组快照名称。

6. * 可选： * 选中 * 配对时将每个组快照成员包括在复制中 * 复选框，以确保在配对父卷时在复制中捕获每个快照。
7. 为组快照选择一个保留选项：
   - 单击 * 永久保留 * 可在系统上无限期保留快照。
   - 单击 * 设置保留期限 * ，然后使用日期调整框选择系统保留快照的时间长度。
8. 要创建单个即时快照，请执行以下步骤：
   a. 单击 * 立即创建组快照 * 。
   b. 单击 * 创建组快照 * 。
9. 要计划在未来某个时间运行快照，请执行以下步骤：
   a. 单击 * 创建组快照计划 * 。
   b. 输入 * 新计划名称 * 。
   c. 从列表中选择 * 计划类型 * 。
   d. * 可选： * 选中 * 重复计划 * 复选框可定期重复计划的快照。
   e. 单击 * 创建计划 * 。

编辑组快照

您可以编辑现有组快照的复制和保留设置。

1. 单击 * 数据保护 * > * 组快照 * 。
2. 单击要编辑的组快照对应的 "Actions" 图标。
3. 在显示的菜单中，选择 * 编辑 * 。
4. * 可选： * 要更改组快照的复制设置，请执行以下操作：
   a. 单击 * 当前复制 * 旁边的 * 编辑 * 。
   b. 选中 * 配对时将每个组快照成员包括在复制中 * 复选框，以确保配对父卷时在复制中捕获每个快照。
5. * 可选： * 要更改组快照的保留设置，请从以下选项中进行选择：
   a. 单击 * 当前保留 * 旁边的 * 编辑 * 。
   b. 为组快照选择一个保留选项：
      - 单击 * 永久保留 * 可在系统上无限期保留快照。
      - 单击 * 设置保留期限 * ，然后使用日期调整框选择系统保留快照的时间长度。
6. 单击 * 保存更改 * 。

删除组快照

您可以从系统中删除组快照。删除组快照时，您可以选择是删除与组关联的所有快照，还是将其保留为单个快照。

如果删除属于组快照的卷或快照，则无法再回滚到组快照。但是，您可以单独回滚每个卷。

1. 单击 * 数据保护 * > * 组快照 * 。
2. 单击要删除的快照对应的 "Actions" 图标。
3. 在显示的菜单中，单击 * 删除 * 。
4. 在确认对话框中选择以下选项之一：
   - 单击 * 删除组快照和所有组快照成员 * 以删除组快照和所有成员快照。
   - 单击 * 将组快照成员保留为单个快照 * 可删除组快照，但保留所有成员快照。
5. 确认操作。

将卷回滚到组快照

您可以随时将一组卷回滚到组快照。

回滚一组卷时，组中的所有卷都将还原到创建组快照时的状态。回滚还会将卷大小还原为原始快照中记录的大小。如果系统已清除某个卷，则在清除时也会删除该卷的所有快照；系统不会还原任何已删除的卷快照。

1. 单击 * 数据保护 * > * 组快照 * 。
2. 单击要用于卷回滚的组快照对应的 "Actions" 图标。
3. 在显示的菜单中，选择 * 将卷回滚到组 Snapshot* 。
4. * 可选 * ： 要在回滚到快照之前保存卷的当前状态，请执行以下操作：
   a. 在 * 回滚到 Snapshot* 对话框中，选择 * 将卷的当前状态另存为组快照 * 。
   b. 输入新快照的名称。
5. 单击 * 回滚组 Snapshot* 。

编辑组快照的成员

您可以编辑现有组快照的成员的保留设置。

1. 单击 * 数据保护 * > * 快照 * 。
2. 单击 * 成员 * 选项卡。
3. 单击要编辑的组快照成员对应的 "Actions" 图标。
4. 在显示的菜单中，选择 * 编辑 * 。
5. 要更改快照的复制设置，请选择以下选项：
   - 单击 * 永久保留 * 可在系统上无限期保留快照。
   - 单击 * 设置保留期限 * ，然后使用日期调整框选择系统保留快照的时间长度。
6. 单击 * 保存更改 * 。

克隆多个卷

您可以通过单个操作创建多个卷克隆，以便为一组卷上的数据创建时间点副本。

克隆卷时，系统会创建卷的快照，然后使用快照中的数据创建新卷。您可以挂载新卷克隆并向其写入数据。克隆多个卷是一个异步过程，所需时间会有所不同，具体取决于要克隆的卷的大小和数量。

卷大小和当前集群负载会影响完成克隆操作所需的时间。

步骤

1. 单击 * 管理 * > * 卷 * 。
2. 单击 * 活动 * 选项卡。
3. 使用复选框选择多个卷，创建一组卷。
4. 单击 * 批量操作 * 。
5. 单击显示的菜单中的 * 克隆 * 。
6. 在 * 克隆多个卷 * 对话框中输入 * 新卷名称前缀 * 。

   前缀将应用于组中的所有卷。

7. * 可选： * 选择克隆所属的其他帐户。

   如果不选择帐户，系统会将新卷分配给当前卷帐户。

8. * 可选： * 为克隆中的卷选择不同的访问方法。

   如果不选择访问方法，系统将使用当前卷访问。

9. 单击 * 开始克隆 * 。

从组快照克隆多个卷

您可以从时间点组快照克隆一组卷。此操作要求卷的组快照已存在，因为组快照用作创建卷的基础。创建卷后，您可以像系统中的任何其他卷一样使用这些卷。

卷大小和当前集群负载会影响完成克隆操作所需的时间。

1. 单击 * 数据保护 * > * 组快照 * 。
2. 单击要用于卷克隆的组快照对应的 "Actions" 图标。
3. 在显示的菜单中，选择 * 从组 Snapshot 克隆卷 * 。
4. 在 * 从组 Snapshot 克隆卷 * 对话框中输入 * 新卷名称前缀 * 。

   前缀将应用于从组快照创建的所有卷。

5. * 可选： * 选择克隆所属的其他帐户。

   如果不选择帐户，系统会将新卷分配给当前卷帐户。

6. * 可选： * 为克隆中的卷选择不同的访问方法。

   如果不选择访问方法，系统将使用当前卷访问。

7. 单击 * 开始克隆 * 。

计划快照

计划快照

您可以通过计划按指定间隔执行卷快照来保护卷或一组卷上的数据。您可以计划自动运行单个卷快照或组快照。

在配置快照计划时，您可以从基于一周中某天或一个月中某天的时间间隔中进行选择。您还可以指定下一个快照发生前的天数，小时数和分钟数。如果要复制卷，您可以将生成的快照存储在远程存储系统上。

了解更多信息

- 创建快照计划
- 编辑快照计划
- 删除快照计划
- 复制快照计划

Snapshot 计划详细信息

在 "Data Protection">"Schedules" 页面上，您可以在快照计划列表中查看以下信息。

- * ID *

  系统为快照生成的 ID 。

- * 类型 *

  计划的类型。Snapshot 是当前唯一支持的类型。

- * 名称 *

  创建计划时为计划指定的名称。Snapshot 计划名称的长度最多可以包含 223 个字符，并且包含 a-z ， 0-9 和短划线（ - ）字符。

- * 频率 *

  运行计划的频率。频率可以设置为小时和分钟，周或月。

- * 重复 *

  指示计划是仅运行一次还是定期运行。

- * 手动暂停 *

  指示是否已手动暂停计划。

- * 卷 ID*

  运行计划时计划要使用的卷的 ID 。

- * 上次运行 *

上次运行计划的时间。

- * 上次运行状态 *

  上次执行计划的结果。可能值：

  - success
  - 失败

创建快照计划

您可以计划按指定间隔自动创建一个或多个卷的快照。

在配置快照计划时，您可以从基于一周中某天或一个月中某天的时间间隔中进行选择。您还可以创建重复计划，并指定下一个快照发生前的天数，小时数和分钟数。

如果计划在不可被 5 分钟整除的时间段运行快照，则快照将在下一个可被 5 分钟整除的时间段运行。例如，如果计划在 12： 42： 00 UTC 运行快照，则快照将在 12： 45： 00 UTC 运行。您不能计划以少于 5 分钟的间隔运行快照。

从Element 12.5开始、您可以启用串行创建、并从UI中选择以先出(First-in-First-Out、FIFO)为基础保留快照。

- *启用串行创建*选项指定一次仅复制一个快照。如果先前的快照复制仍在进行中、则创建新快照将失败。如果未选中此复选框、则在另一个快照复制仍在进行中时、允许创建快照。
- 通过* FIFO *选项、可以保留一致数量的最新快照。选中此复选框后、快照将按FIFO保留。当FIFO快照队列达到其最大深度后、插入新的FIFO快照时、最旧的FIFO快照将被丢弃。

步骤

1. 选择*数据保护*>*计划*。
2. 选择 * 创建计划 * 。
3. 在 * 卷 ID CSV* 字段中，输入要包含在快照操作中的单个卷 ID 或逗号分隔的卷 ID 列表。
4. 输入新计划名称。
5. 选择计划类型，然后从提供的选项中设置计划。
6. * 可选： * 选择 * 重复计划 * 可无限期重复执行快照计划。
7. * 可选： * 在 * 新快照名称 * 字段中输入新快照的名称。

   如果将此字段留空，则系统将使用创建快照的时间和日期作为名称。

8. * 可选： * 选中 * 配对时在复制中包含快照 * 复选框，以确保配对父卷时在复制中捕获快照。
9. *可选：*选中*启用串行创建*复选框以确保一次仅复制一个快照。
10. 要设置快照的保留，请选择以下选项：
    - *可选：*选中*先出先出*复选框以保留一致数量的最新快照。
    - 选择*永久保留*可在系统上无限期保留快照。
    - 选择*设置保留期限*、然后使用日期调整框选择系统保留快照的时间长度。
11. 选择 * 创建计划 * 。

编辑快照计划

您可以修改现有快照计划。修改后，计划下次运行时，将使用更新后的属性。原始计划创建的所有快照都将保留在存储系统上。

步骤

1. 单击 * 数据保护 * > * 计划 * 。
2. 单击要更改的计划对应的 * 操作 * 图标。
3. 在显示的菜单中，单击 * 编辑 * 。
4. 在 * 卷 ID CSV* 字段中，修改当前包含在快照操作中的单个卷 ID 或逗号分隔的卷 ID 列表。
5. 要暂停或恢复计划，请选择以下选项：
   - 要暂停活动计划，请从 * 手动暂停计划 * 列表中选择 * 是 * 。
   - 要恢复已暂停的计划，请从 * 手动暂停计划 * 列表中选择 * 否 * 。
6. 如果需要，在 * 新计划名称 * 字段中为计划输入其他名称。
7. 要将计划更改为在一周或一个月的不同日期运行，请选择 * 计划类型 * 并使用提供的选项更改计划。
8. * 可选： * 选择 * 重复计划 * 可无限期重复执行快照计划。
9. * 可选： * 在 * 新快照名称 * 字段中输入或修改新快照的名称。

   如果将此字段留空，则系统将使用创建快照的时间和日期作为名称。

10. * 可选： * 选中 * 配对时在复制中包含快照 * 复选框，以确保配对父卷时在复制中捕获快照。
11. 要更改保留设置，请选择以下选项：
    - 单击 * 永久保留 * 可在系统上无限期保留快照。
    - 单击 * 设置保留期限 * ，然后使用日期调整框选择系统保留快照的时间长度。
12. 单击 * 保存更改 * 。

复制快照计划

您可以复制计划并维护其当前属性。

1. 单击 * 数据保护 * > * 计划 * 。
2. 单击要复制的计划对应的 "Actions" 图标。
3. 在显示的菜单中，单击 * 创建副本 * 。

   此时将显示 * 创建计划 * 对话框，其中填充了计划的当前属性。

4. * 可选： * 输入新计划的名称和更新属性。
5. 单击 * 创建计划 * 。

删除快照计划

您可以删除快照计划。删除此计划后，它将不会运行任何将来计划的快照。计划创建的所

有快照都将保留在存储系统上。

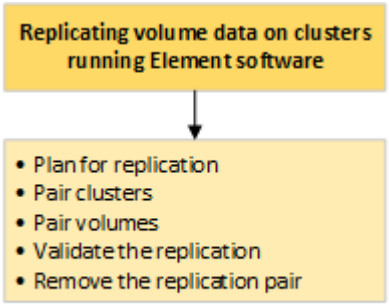
1. 单击 * 数据保护 * > * 计划 * 。
2. 单击要删除的计划对应的 * 操作 * 图标。
3. 在显示的菜单中，单击 * 删除 * 。
4. 确认操作。

在运行 NetApp Element 软件的集群之间执行远程复制

在运行 **NetApp Element** 软件的集群之间执行远程复制

对于运行 Element 软件的集群，通过实时复制可以快速创建卷数据的远程副本。您可以将一个存储集群与最多四个其他存储集群配对。您可以从集群对中的任一集群同步或异步复制卷数据，以实现故障转移和故障恢复。

复制过程包括以下步骤：



- "规划集群和卷配对以实现实时复制"
- "对集群进行配对以进行复制"
- "对卷配对"
- "验证卷复制"
- "复制后删除卷关系"
- "管理卷关系"

规划集群和卷配对以实现实时复制

实时远程复制要求您对运行 Element 软件的两个存储集群配对，对每个集群上的卷配对并验证复制。复制完成后，应删除卷关系。

您需要的内容

- 您必须对要配对的一个或两个集群拥有集群管理员权限。
- 配对集群的管理网络和存储网络上的所有节点 IP 地址将相互路由。
- 所有配对节点的 MTU 必须相同，并且在集群之间端到端都支持 MTU 。

- 两个存储集群都应具有唯一的集群名称， MVIP ， SVIP 和所有节点 IP 地址。
- 集群上的 Element 软件版本之间的差异不超过一个主要版本。如果差异较大，则必须升级其中一个集群才能执行数据复制。

> WAN 加速器设备尚未获得 NetApp 认证，无法在复制数据时使用。如果部署在复制数据的两个集群之间，则这些设备可能会干扰数据压缩和重复数据删除。在生产环境中部署任何 WAN 加速器设备之前，请务必对其影响进行全面的评估。

了解更多信息

- 对集群进行配对以进行复制
- 对卷配对
- 为配对卷分配复制源和目标

对集群进行配对以进行复制

对集群进行配对以进行复制

要使用实时复制功能，您必须首先将两个集群配对。将两个集群配对并连接后，您可以将一个集群上的活动卷配置为持续复制到另一个集群，从而提供持续数据保护（ CDP ）。

您需要的内容

- 您必须对要配对的一个或两个集群拥有集群管理员权限。
- 所有节点 MIP 和 SIP 将相互路由。
- 集群之间的往返延迟低于 2000 毫秒。
- 两个存储集群都应具有唯一的集群名称， MVIP ， SVIP 和所有节点 IP 地址。
- 集群上的 Element 软件版本之间的差异不超过一个主要版本。如果差异较大，则必须升级其中一个集群才能执行数据复制。

> 集群配对要求管理网络上的节点之间具有完全连接。复制需要在存储集群网络上的各个节点之间建立连接。

您可以将一个集群与最多四个其他集群配对以复制卷。您还可以将集群组中的集群彼此配对。

使用 **MVIP** 或配对密钥对集群配对

如果对源集群和目标集群都具有集群管理员访问权限，则可以使用目标集群的 MVIP 对这两个集群进行配对。如果集群管理员只能访问集群对中的一个集群，则可以在目标集群上使用配对密钥来完成集群配对。

1. 选择以下方法之一对集群配对：
   - "使用 MVIP 对集群配对"如果两个集群都有集群管理员访问权限，则使用此方法。该方法利用远程集群的 MVIP 来配对两个集群。
   - "使用配对密钥对集群配对"如果集群管理员只能访问其中一个集群，则可以使用此方法。该方法生成一个配对密钥，该密钥可用于目标集群以完成集群配对。

了解更多信息

网络端口要求

使用 **MVIP** 对集群配对

您可以使用一个集群的 MVIP 与另一个集群建立连接，从而将两个集群配对以实现实时复制。要使用此方法，需要对两个集群都具有集群管理员访问权限。集群管理员用户名和密码用于在集群配对之前对集群访问进行身份验证。

1. 在本地集群上，选择 * 数据保护 * > * 集群对 * 。
2. 单击 * 配对集群 * 。
3. 单击 * 开始配对 * ，然后单击 * 是 * 以指示您有权访问远程集群。
4. 输入远程集群 MVIP 地址。
5. 单击 * 在远程集群上完成配对 * 。

   在 * 需要身份验证 * 窗口中，输入远程集群的集群管理员用户名和密码。
6. 在远程集群上，选择 * 数据保护 * > * 集群对 * 。
7. 单击 * 配对集群 * 。
8. 单击 * 完成配对 * 。
9. 单击 * 完成配对 * 按钮。

了解更多信息

- 使用配对密钥对集群配对
- "使用 MVIP 对集群配对（视频）"

使用配对密钥对集群配对

如果您对本地集群拥有集群管理员访问权限，但对远程集群没有访问权限，则可以使用配对密钥对这些集群进行配对。配对密钥会在本地集群上生成，然后安全地发送给远程站点的集群管理员，以建立连接并完成集群配对以实现实时复制。

1. 在本地集群上，选择 * 数据保护 * > * 集群对 * 。
2. 单击 * 配对集群 * 。
3. 单击 * 开始配对 * 并单击 * 否 * 以指示您无权访问远程集群。
4. 单击 * 生成密钥 * 。

   此操作将生成用于配对的文本密钥，并在本地集群上创建未配置的集群对。如果您未完成操作步骤，则需要手动删除集群对。
5. 将集群配对密钥复制到剪贴板。
6. 使配对密钥可供远程集群站点的集群管理员访问。

集群配对密钥包含一个版本的 MVIP ，用户名，密码和数据库信息，以允许通过卷连接进行远程复制。此密钥应以安全的方式处理，而不是以允许意外或不安全地访问用户名或密码的方式存储。

请勿修改配对密钥中的任何字符。如果修改此密钥，则此密钥将无效。

7. 在远程集群上，选择 * 数据保护 * > * 集群对 * 。
8. 单击 * 配对集群 * 。
9. 单击 * 完成配对 * ，然后在 * 配对密钥 * 字段中输入配对密钥（建议使用粘贴方法）。
10. 单击 * 完成配对 * 。

了解更多信息

- 使用 MVIP 对集群配对
- "使用集群配对密钥对集群配对（视频）"

验证集群对连接

完成集群配对后，您可能需要验证集群对连接以确保复制成功。

1. 在本地集群上，选择 * 数据保护 * > * 集群对 * 。
2. 在 * 集群对 * 窗口中，验证集群对是否已连接。
3. * 可选： * 导航回本地集群和 * 集群对 * 窗口，并验证集群对是否已连接。

对卷配对

对卷配对

在集群对中的集群之间建立连接后，您可以将一个集群上的卷与该集群对中另一个集群上的卷配对。建立卷配对关系后，您必须确定哪个卷是复制目标。

您可以将两个卷配对，以实现实时复制，这些卷存储在已连接集群对中的不同存储集群上。将两个集群配对后，您可以将一个集群上的活动卷配置为持续复制到另一个集群，从而提供持续数据保护（ CDP ）。您也可以将任一卷分配为复制的源卷或目标卷。

卷配对始终是一对一的。在某个卷与另一个集群上的卷配对后，您将无法再将其与任何其他卷配对。

您需要的内容

- 您已在集群对中的集群之间建立连接。
- 您对要配对的一个或两个集群拥有集群管理员权限。

步骤

1. 创建具有读取或写入访问权限的目标卷
2. 使用卷 ID 或配对密钥对卷配对
3. 为配对卷分配复制源和目标

复制过程涉及两个端点：源卷和目标卷。创建目标卷时，卷会自动设置为读 / 写模式，以便在复制期间接受数据。

1. 选择 * 管理 * > * 卷 * 。
2. 单击 * 创建卷 * 。
3. 在创建新卷对话框中，输入卷名称。
4. 输入卷的总大小，选择卷的块大小，然后选择应有权访问该卷的帐户。
5. 单击 * 创建卷 * 。
6. 在 "Active" 窗口中，单击卷对应的 "Actions" 图标。
7. 单击 * 编辑 * 。
8. 将帐户访问级别更改为 Replication Target 。
9. 单击 * 保存更改 * 。

使用卷 **ID** 或配对密钥对卷配对

使用卷 **ID** 对卷配对

如果您拥有对要配对的卷所在的两个集群的集群管理员访问权限，则可以将一个卷与远程集群上的另一个卷配对。此方法使用远程集群上卷的卷 ID 来发起连接。

您需要的内容

- 确保包含卷的集群已配对。
- 在远程集群上创建新卷。

> 您可以在配对过程完成后分配复制源和目标。复制源或目标可以是卷对中的任一卷。您应创建一个目标卷，该卷不包含任何数据，并且与源卷具有完全相同的特征，例如大小，卷的块大小设置（ 512e 或 4k ）以及 QoS 配置。如果您将现有卷分配为复制目标，则该卷上的数据将被覆盖。目标卷可以大于或等于源卷，但不能小于源卷。

- 了解目标卷 ID 。

步骤

1. 选择 * 管理 * > * 卷 * 。
2. 单击要配对的卷对应的 * 操作 * 图标。
3. 单击 * 配对 * 。
4. 在 * 配对卷 * 对话框中，选择 * 开始配对 * 。
5. 选择 * 我做 * 表示您有权访问远程集群。
6. 从列表中选择 * 复制模式 * ：
   - * 实时（异步） * ：在源集群上提交写入后，将向客户端确认这些写入。
   - * 实时（同步） * ：在源集群和目标集群上提交写入后，将向客户端确认写入。

◦ * 仅限 Snapshot * ： 仅复制在源集群上创建的快照。不会复制源卷中的活动写入。

7. 从列表中选择一个远程集群。
8. 选择远程卷 ID 。
9. 单击 * 开始配对 * 。

   系统将打开一个 Web 浏览器选项卡，此选项卡会连接到远程集群的 Element UI 。您可能需要使用集群管理员凭据登录到远程集群。

10. 在远程集群的 Element UI 中，选择 * 完成配对 * 。
11. 确认 * 确认卷配对 * 中的详细信息。
12. 单击 * 完成配对 * 。

    确认配对后，两个集群将开始连接要配对的卷。在配对过程中，您可以在 * 卷对 * 窗口的 * 卷状态 * 列中看到消息。卷对将显示 `PausedMisconfigured` ，直到分配了卷对的源和目标为止。

    成功完成配对后，建议您刷新 Volumes 表以从配对卷的 * 操作 * 列表中删除 * 配对 * 选项。如果不刷新表，则 * 配对 * 选项仍可供选择。如果您再次选择 * 配对 * 选项，则会打开一个新选项卡，并且由于卷已配对，系统会在` Element UI 页面的 * 配对卷 * 窗口中报告一条 `STartVolumePairing Failed ： xVolumeAlreadyPaired" 错误消息。

了解更多信息

- 卷配对消息
- 卷配对警告
- 为配对卷分配复制源和目标

使用配对密钥对卷配对

如果您只有源集群的集群管理员权限（您没有远程集群的集群管理员凭据），则可以使用配对密钥将一个卷与远程集群上的另一个卷配对。

您需要的内容

- 确保包含卷的集群已配对。
- 确保远程集群上有一个要用于配对的卷。

> 您可以在配对过程完成后分配复制源和目标。复制源或目标可以是卷对中的任一卷。您应创建一个目标卷，该卷不包含任何数据，并且与源卷具有完全相同的特征，例如大小，卷的块大小设置（ 512e 或 4k ）以及 QoS 配置。如果您将现有卷分配为复制目标，则该卷上的数据将被覆盖。目标卷可以大于或等于源卷，但不能小于源卷。

步骤

1. 选择 * 管理 * > * 卷 * 。
2. 单击要配对的卷的 * 操作 * 图标。
3. 单击 * 配对 * 。

4. 在 * 配对卷 * 对话框中，选择 * 开始配对 * 。
5. 选择 * 我不 * 表示您无权访问远程集群。
6. 从列表中选择 * 复制模式 * ：
   - * 实时（异步） * ：在源集群上提交写入后，将向客户端确认这些写入。
   - * 实时（同步） * ：在源集群和目标集群上提交写入后，将向客户端确认写入。
   - * 仅限 Snapshot * ：仅复制在源集群上创建的快照。不会复制源卷中的活动写入。
7. 单击 * 生成密钥 * 。

   此操作将生成一个用于配对的文本密钥，并在本地集群上创建一个未配置的卷对。如果您未完成操作步骤，则需要手动删除卷对。

8. 将配对密钥复制到计算机的剪贴板。
9. 使配对密钥可供远程集群站点的集群管理员访问。

   应以安全的方式对待卷配对密钥，使用时不应允许意外或不安全的访问。

   请勿修改配对密钥中的任何字符。如果修改此密钥，则此密钥将无效。

10. 在远程集群 Element UI 中，选择 * 管理 * > * 卷 * 。
11. 单击要配对的卷对应的 "Actions" 图标。
12. 单击 * 配对 * 。
13. 在 * 配对卷 * 对话框中，选择 * 完成配对 * 。
14. 将配对密钥从另一个集群粘贴到 * 配对密钥 * 框中。
15. 单击 * 完成配对 * 。

    确认配对后，两个集群将开始连接要配对的卷。在配对过程中，您可以在 * 卷对 * 窗口的 * 卷状态 * 列中看到消息。卷对将显示 `PausedMisconfigured` ，直到分配了卷对的源和目标为止。

    成功完成配对后，建议您刷新 Volumes 表以从配对卷的 * 操作 * 列表中删除 * 配对 * 选项。如果不刷新表，则 * 配对 * 选项仍可供选择。如果您再次选择 * 配对 * 选项，则会打开一个新选项卡，并且由于卷已配对，系统会在` Element UI 页面的 * 配对卷 * 窗口中报告一条 `STartVolumePairing Failed ： xVolumeAlreadyPaired" 错误消息。

了解更多信息

- 卷配对消息
- 卷配对警告
- 为配对卷分配复制源和目标

为配对卷分配复制源和目标

卷配对后，您必须分配源卷及其复制目标卷。复制源或目标可以是卷对中的任一卷。如果

源卷不可用，您也可以使用此操作步骤将发送到源卷的数据重定向到远程目标卷。

您需要的内容

您可以访问包含源卷和目标卷的集群。

步骤

1. 准备源卷：
   a. 从包含要分配为源的卷的集群中，选择 * 管理 * > * 卷 * 。
   b. 单击要分配为源的卷的 * 操作 * 图标，然后单击 * 编辑 * 。
   c. 在 * 访问 * 下拉列表中，选择 * 读取 / 写入 * 。

   > 如果要反转源分配和目标分配，此操作将对卷对执行发生原因操作以显示以下消息，直到分配了新的复制目标： `PausedMisconfigured`

   更改访问权限会暂停卷复制并导致数据传输停止。请确保您已在两个站点协调这些更改。

   a. 单击 * 保存更改 * 。
2. 准备目标卷：
   a. 从包含要分配为目标的卷的集群中，选择 * 管理 * > * 卷 * 。
   b. 单击要分配为目标的卷对应的 "Actions" 图标，然后单击 * 编辑 * 。
   c. 在 * 访问 * 下拉列表中，选择 * 复制目标 * 。

   > 如果您将现有卷分配为复制目标，则该卷上的数据将被覆盖。您应使用不包含任何数据且与源卷具有完全相同特征的新目标卷，例如大小， 512e 设置和 QoS 配置。目标卷可以大于或等于源卷，但不能小于源卷。

   d. 单击 * 保存更改 * 。

了解更多信息

- 使用卷 ID 对卷配对
- 使用配对密钥对卷配对

验证卷复制

复制卷后，您应确保源卷和目标卷处于活动状态。处于活动状态时，卷将配对，数据将从源卷发送到目标卷，并且数据处于同步状态。

1. 从两个集群中，选择 * 数据保护 * > * 卷对 * 。
2. 验证卷状态是否为 "Active" 。

了解更多信息

卷配对警告

复制后删除卷关系

复制完成后，如果您不再需要此卷对关系，则可以删除此卷关系。

1. 选择 * 数据保护 * > * 卷对 * 。
2. 单击要删除的卷对对应的 * 操作 * 图标。
3. 单击 * 删除 * 。
4. 确认消息。

管理卷关系

暂停复制

如果需要在短时间内停止 I/O 处理，可以手动暂停复制。如果 I/O 处理量激增，而您希望降低处理负载，则可能需要暂停复制。

1. 选择 * 数据保护 * > * 卷对 * 。
2. 单击卷对对应的 "Actions" 图标。
3. 单击 * 编辑 * 。
4. 在 * 编辑卷对 * 窗格中，手动暂停复制过程。

   手动暂停或恢复卷复制会导致数据传输停止或恢复。请确保您已在两个站点协调这些更改。

5. 单击 * 保存更改 * 。

更改复制模式

您可以编辑卷对属性以更改卷对关系的复制模式。

1. 选择 * 数据保护 * > * 卷对 * 。
2. 单击卷对对应的 "Actions" 图标。
3. 单击 * 编辑 * 。
4. 在 * 编辑卷对 * 窗格中，选择新的复制模式：
   - * 实时（异步） * ：在源集群上提交写入后，将向客户端确认这些写入。
   - * 实时（同步） * ：在源集群和目标集群上提交写入后，将向客户端确认写入。
   - * 仅限 Snapshot * ：仅复制在源集群上创建的快照。不会复制源卷中的活动写入。* 注意： * 更改复制模式会立即更改此模式。请确保您已在两个站点协调这些更改。
5. 单击 * 保存更改 * 。

删除卷对

如果要删除两个卷之间的对关联，可以删除卷对。

1. 选择 * 数据保护 * > * 卷对 * 。

2. 单击要删除的卷对对应的 "Actions" 图标。
3. 单击 * 删除 * 。
4. 确认消息。

删除集群对

您可以从集群对中任一集群的 Element UI 中删除集群对。

1. 单击 * 数据保护 * > * 集群对 * 。
2. 单击集群对对应的 "Actions" 图标。
3. 在显示的菜单中，单击 * 删除 * 。
4. 确认操作。
5. 从集群配对中的第二个集群重新执行这些步骤。

集群对详细信息

"Data Protection" 选项卡上的 "Cluster Pairs" 页面提供了有关已配对或正在配对的集群的信息。系统将在状态列中显示配对和进度消息。

- * ID *

  系统为每个集群对生成的 ID 。

- * 远程集群名称 *

  对中另一个集群的名称。

- * 远程 MVIP*

  对中另一个集群的管理虚拟 IP 地址。

- * 状态 *

  远程集群的复制状态

- * 复制卷 *

  集群中已配对进行复制的卷数。

- * UUID *

  为对中的每个集群指定的唯一 ID 。

体积对

卷对详细信息

"Data Protection" 选项卡上的 "Volume Pairs" 页面提供了有关已配对或正在配对的卷的信

息。系统会在卷状态列中显示配对和进度消息。

- * ID *

  系统为卷生成的 ID 。

- * 名称 *

  创建卷时为卷指定的名称。卷名称最多可以包含 223 个字符，并且包含 a-z ， 0-9 和短划线（ - ）。

- * 帐户 *

  分配给卷的帐户的名称。

- * 卷状态 *

  卷的复制状态

- * 快照状态 *

  快照卷的状态。

- * 模式 *

  客户端写入复制方法。可能值如下：

  - 异步
  - 仅 Snapshot
  - 同步

- * 方向 *

  卷数据的方向：

  - 源卷图标（→）表示正在将数据写入集群外的目标。
  - 目标卷图标（←）表示正在从外部源向本地卷写入数据。

- * 异步延迟 *

  自卷上次与远程集群同步以来的时间长度。如果卷未配对，则此值为 null 。

- * 远程集群 *

  卷所在远程集群的名称。

- * 远程卷 ID*

  远程集群上卷的卷 ID 。

- * 远程卷名称 *

  创建远程卷时为其指定的名称。

卷配对消息

在初始配对过程中，您可以从 "Data Protection" 选项卡下的 "Volume Pairs" 页面查看卷配对消息。在复制卷列表视图中，此对的源端和目标端都可以显示这些消息。

- * 已禁用已断开连接 *

  源复制或同步 RPC 超时。与远程集群的连接已断开。检查与集群的网络连接。

- * 正在重新同步连接 *

  此时，远程复制同步处于活动状态。开始同步过程并等待数据。

- * 正在重新同步 RRSync*

  正在为配对集群创建卷元数据的单个 Helix 副本。

- * 正在重新同步 LocalSync*

  正在为配对集群创建卷元数据的双 Helix 副本。

- * 正在重新同步数据传输 *

  数据传输已恢复。

- * 活动 *

  卷已配对，正在将数据从源卷发送到目标卷，并且数据处于同步状态。

- * 闲置 *

  未发生复制活动。

卷配对警告

在对卷配对后， "Data Protection" 选项卡上的 "Volume Pairs" 页面将提供这些消息。这些消息可以在复制卷列表视图中显示在卷对的源端和目标端（除非另有说明）。

- * PausedClusterFull*

  由于目标集群已满，因此无法继续进行源复制和批量数据传输。此消息仅显示在对的源端。

- * PausedExceededMaxSnapshotCount*

  目标卷已具有最大快照数，无法复制其他快照。

- * PausedManual*

  本地卷已手动暂停。必须先取消暂停，然后复制才能恢复。

- * PausedManualRemote*

远程卷处于手动暂停模式。在复制恢复之前，需要手动干预以取消暂停远程卷。

- * PausedMisconfigure*

  正在等待活动源和目标。恢复复制需要手动干预。

- * PausedQoS"

  目标 QoS 无法维持传入 IO 。复制将自动恢复。此消息仅显示在对的源端。

- * PausedSlowLink*

  检测到链路速度较慢并停止复制。复制将自动恢复。此消息仅显示在对的源端。

- * PausedVolumeSizeMismatch*

  目标卷的大小与源卷不同。

- * PausedXCopy"

  正在对源卷发出 SCSI XCOPY 命令。必须先完成命令，然后才能恢复复制。此消息仅显示在对的源端。

- * StoppedMisconfigure*

  检测到永久配置错误。远程卷已清除或取消配对。无法执行更正操作；必须建立新的配对。

在Element和ONTAP集群之间使用SnapMirror复制(Element UI)

在Element和ONTAP集群之间使用SnapMirror复制(Element UI)

您可以从NetApp Element UI中的数据保护选项卡创建SnapMirror关系。要在用户界面中查看此信息，必须启用 SnapMirror 功能。

NetApp Element 软件和 ONTAP 集群之间的 SnapMirror 复制不支持 IPv6 。

"NetApp 视频：适用于 NetApp HCI 和 Element 软件的 SnapMirror"

运行 NetApp Element 软件的系统支持使用 SnapMirror 功能在 NetApp ONTAP 系统中复制和还原 Snapshot 副本。使用此技术的主要原因是将 NetApp HCI 灾难恢复到 ONTAP 。端点包括 ONTAP ， ONTAP Select 和 Cloud Volumes ONTAP 。请参见 TR-4641 NetApp HCI 数据保护。

"NetApp 技术报告 4641 ：《 NetApp HCI 数据保护》"

了解更多信息

- "使用 NetApp HCI ， ONTAP 和融合基础架构构建 Data Fabric"
- "NetApp Element软件和ONTAP之间的复制(ONTAP命令行界面)"

SnapMirror 概述

运行 NetApp Element 软件的系统支持 SnapMirror 功能，可使用 NetApp ONTAP 系统复

制和还原快照。

运行 Element 的系统可以直接与 ONTAP 系统 9.3 或更高版本上的 SnapMirror 进行通信。NetApp Element API 提供了在集群、卷和快照上启用SnapMirror功能的方法。此外， Element UI 还提供了管理 Element 软件和 ONTAP 系统之间的 SnapMirror 关系所需的所有功能。

您可以在特定使用情形下将 ONTAP 发起的卷复制到 Element 卷，但功能有限。有关详细信息，请参见 "在Element软件和ONTAP之间进行复制(ONTAP命令行界面)"。

在集群上启用 **SnapMirror**

您必须通过NetApp Element UI在集群级别手动启用SnapMirror功能。默认情况下，系统随附的 SnapMirror 功能处于禁用状态，并且在新安装或升级过程中不会自动启用此功能。启用 SnapMirror 功能是一次性配置任务。

只能为运行 Element 软件并与 NetApp ONTAP 系统上的卷结合使用的集群启用 SnapMirror 。只有当集群已连接并可与 NetApp ONTAP 卷结合使用时，才应启用 SnapMirror 功能。

您需要的内容

存储集群必须运行 NetApp Element 软件。

步骤

1. 单击 * 集群 * > * 设置 * 。
2. 查找 SnapMirror 的集群专用设置。
3. 单击 * 启用 SnapMirror* 。

   启用 SnapMirror 功能会永久更改 Element 软件配置。您只能通过将集群恢复为出厂映像来禁用 SnapMirror 功能并还原默认设置。

4. 单击 * 是 * 确认 SnapMirror 配置更改。

在卷上启用 **SnapMirror**

您必须在 Element UI 中对卷启用 SnapMirror 。这样可以将数据复制到指定的 ONTAP 卷。这是运行 NetApp Element 软件的集群管理员为 SnapMirror 提供的控制卷的权限。

您需要的内容

- 您已在 Element UI 中为集群启用 SnapMirror 。
- SnapMirror 端点可用。
- 卷的块大小必须为 512e 。
- 此卷不参与远程复制。
- 卷访问类型不是复制目标。

您也可以在创建或克隆卷时设置此属性。

步骤

1. 单击 * 管理 * > * 卷 * 。
2. 单击要为其启用 SnapMirror 的卷的 * 操作 * 图标。
3. 在显示的菜单中，选择 * 编辑 * 。
4. 在 * 编辑卷 * 对话框中，选中 * 启用 SnapMirror* 复选框。
5. 单击 * 保存更改 * 。

创建 **SnapMirror** 端点

您必须先在NetApp Element UI中创建SnapMirror端点、然后才能创建关系。

SnapMirror 端点是指用作运行 Element 软件的集群的复制目标的 ONTAP 集群。在创建 SnapMirror 关系之前，请先创建 SnapMirror 端点。

您最多可以在运行 Element 软件的存储集群上创建和管理四个 SnapMirror 端点。

如果现有端点最初是使用 API 创建的，但未保存凭据，则可以在 Element UI 中查看此端点并验证其是否存在，但无法使用 Element UI 对其进行管理。然后，只能使用 Element API 管理此端点。

有关 API 方法的详细信息，请参阅 "使用 Element API 管理存储"。

您需要的内容

- 您应已在 Element UI 中为存储集群启用 SnapMirror 。
- 您知道端点的 ONTAP 凭据。

步骤

1. 单击 * 数据保护 * > * SnapMirror 端点 * 。
2. 单击 * 创建端点 * 。
3. 在 * 创建新端点 * 对话框中，输入 ONTAP 系统的集群管理 IP 地址。
4. 输入与此端点关联的 ONTAP 管理员凭据。
5. 查看其他详细信息：
   - LIF ： 列出用于与 Element 通信的 ONTAP 集群间逻辑接口。
   - status ： 显示 SnapMirror 端点的当前状态。可能的值包括：已连接，已断开连接和非受管。
6. 单击 * 创建端点 * 。

创建 **SnapMirror** 关系

您必须在NetApp Element UI中创建SnapMirror关系。

如果某个卷尚未启用 SnapMirror ，而您选择从 Element UI 创建关系，则该卷会自动启用 SnapMirror 。

您需要的内容

已在卷上启用 SnapMirror 。

步骤

1. 单击 * 管理 * > * 卷 * 。
2. 单击要加入此关系的卷的 * 操作 * 图标。
3. 单击 * 创建 SnapMirror 关系 * 。
4. 在 * 创建 SnapMirror 关系 * 对话框中，从 * 端点 * 列表中选择一个端点。
5. 选择是使用新的 ONTAP 卷还是现有 ONTAP 卷创建关系。
6. 要在 Element UI 中创建新的 ONTAP 卷，请单击 * 创建新卷 * 。
   a. 为此关系选择 * Storage Virtual Machine* 。
   b. 从下拉列表中选择 * 聚合 * 。
   c. 在 * 卷名称后缀 * 字段中，输入后缀。

      系统会检测源卷名称并将其复制到 * 卷名称 * 字段。输入的后缀将附加名称。

   d. 单击 * 创建目标卷 * 。
7. 要使用现有 ONTAP 卷，请单击 * 使用现有卷 * 。
   a. 为此关系选择 * Storage Virtual Machine* 。
   b. 选择此新关系的目标卷。
8. 在 * 关系详细信息 * 部分中，选择一个策略。如果选定策略具有保留规则，则 " 规则 " 表将显示规则和关联标签。
9. * 可选 * ： 选择一个计划。

   这将确定此关系创建副本的频率。

10. * 可选 * ： 在 * 将带宽限制为 * 字段中，输入与此关系关联的数据传输可占用的最大带宽量。
11. 查看其他详细信息：
    - * 状态 * ： 目标卷的当前关系状态。可能值包括：
      - Uninitialized ： 目标卷尚未初始化。
      - snapmirrored ： 目标卷已初始化并准备好接收 SnapMirror 更新。
      - Broken-off ： 目标卷为读 / 写卷，并且存在快照。
    - * 状态 * ： 关系的当前状态。可能值包括 idle ， transferring ， checking ， quiescing ， quiesced ， 已排队，正在准备，正在完成，正在中止和正在中断。
    - * 滞后时间 * ： 目标系统滞后于源系统的时间量，以秒为单位。滞后时间不能超过传输计划间隔。
    - * 带宽限制 * ： 与此关系关联的数据传输可占用的最大带宽量。
    - * 上次传输 * ： 上次传输快照的时间戳。单击以了解更多信息。
    - * 策略名称 * ： 关系的 ONTAP SnapMirror 策略的名称。
    - * 策略类型 * ： 为关系选择的 ONTAP SnapMirror 策略的类型。可能值包括：

- 异步镜像
- mirror_vault

◦ * 计划名称 * ： 为此关系选择的 ONTAP 系统上原有计划的名称。

12. 要此时不初始化，请确保未选中 * 初始化 * 复选框。

> 初始化可能非常耗时。您可能希望在非高峰时段运行此操作。初始化会执行基线传输；它会创建源卷的快照副本，然后将该副本及其引用的所有数据块传输到目标卷。您可以手动初始化，也可以使用计划根据计划启动初始化过程（以及后续更新）。

13. 单击 * 创建关系 * 。
14. 单击 * 数据保护 * > * SnapMirror 关系 * 以查看此新的 SnapMirror 关系。

SnapMirror 关系操作

您可以从数据保护选项卡的 SnapMirror 关系页面配置关系。此处介绍了 "Actions" 图标中的选项。

- * 编辑 * ： 编辑关系使用的策略或计划。
- * 删除 * ： 删除 SnapMirror 关系。此功能不会删除目标卷。
- * 初始化 * ： 执行第一次初始基线数据传输以建立新关系。
- * 更新 * ： 对关系执行按需更新，将自上次更新以来包含的所有新数据和 Snapshot 副本复制到目标。
- * 暂停 * ： 阻止对关系进行任何进一步更新。
- * 恢复 * ： 恢复已暂停的关系。
- * 中断 * ： 将目标卷设为读写卷，并停止当前和未来的所有传输。确定客户端未使用原始源卷，因为反向重新同步操作会使原始源卷变为只读。
- * 重新同步 * ： 在中断发生之前按相同方向重新建立已中断的关系。
- * 反向重新同步 * ： 自动执行必要的步骤，以反向创建和初始化新关系。只有当现有关系处于断开状态时，才能执行此操作。此操作不会删除当前关系。原始源卷将还原为最新的通用 Snapshot 副本，并与目标重新同步。自上次成功更新 SnapMirror 以来对原始源卷所做的任何更改都将丢失。对当前目标卷所做的任何更改或写入当前目标卷的新数据将发送回原始源卷。
- * 中止 * ： 取消当前正在进行的传输。如果为已中止的关系发出 SnapMirror 更新，则此关系将从中止之前创建的最后一个重新启动检查点继续进行上次传输。

SnapMirror 标签

SnapMirror 标签

SnapMirror 标签用作根据关系的保留规则传输指定快照的标记。

对快照应用标签会将其标记为 SnapMirror 复制的目标。此关系的角色是，在数据传输时强制实施这些规则，方法是选择具有匹配标签的快照，将其复制到目标卷并确保保留正确数量的副本。它是指用于确定保留计数和保留期限的策略。此策略可以包含任意数量的规则，并且每个规则都有一个唯一标签。此标签用作快照与保留规则之间的链接。

SnapMirror 标签用于指示对选定快照，组快照或计划应用的规则。

向快照添加 **SnapMirror** 标签

SnapMirror 标签用于指定 SnapMirror 端点上的快照保留策略。您可以为快照和组快照添加标签。

您可以从现有 SnapMirror 关系对话框或 NetApp ONTAP 系统管理器中查看可用标签。

向组快照添加标签时，各个快照的任何现有标签将被覆盖。

您需要的内容

- 已在集群上启用 SnapMirror 。
- 要添加的标签已存在于 ONTAP 中。

步骤

1. 单击 * 数据保护 * > * 快照 * 或 * 组快照 * 页面。
2. 单击要添加 SnapMirror 标签的快照或组快照的 * 操作 * 图标。
3. 在 * 编辑 Snapshot* 对话框的 * SnapMirror 标签 * 字段中输入文本。此标签必须与应用于 SnapMirror 关系的策略中的规则标签匹配。
4. 单击 * 保存更改 * 。

将 **SnapMirror** 标签添加到快照计划中

您可以向快照计划添加 SnapMirror 标签，以确保应用 SnapMirror 策略。您可以从现有 SnapMirror 关系对话框或 NetAppONTAP System Manager 中查看可用标签。

您需要的内容

- 必须在集群级别启用 SnapMirror 。
- 要添加的标签已存在于 ONTAP 中。

步骤

1. 单击 * 数据保护 * > * 计划 * 。
2. 通过以下方式之一将 SnapMirror 标签添加到计划中：

选项	步骤
创建新计划	a. 选择 * 创建计划 * 。 b. 输入所有其他相关详细信息。 c. 选择 * 创建计划 * 。

选项	步骤
修改现有计划	a. 单击要添加标签的计划的 * 操作 * 图标，然后选择 * 编辑 * 。 b. 在显示的对话框中，在 * SnapMirror Label* 字段中输入文本。 c. 选择 * 保存更改 * 。

了解更多信息

创建快照计划

使用 **SnapMirror** 进行灾难恢复

使用 **SnapMirror** 进行灾难恢复

如果运行 NetApp Element 软件的卷或集群出现问题，请使用 SnapMirror 功能中断关系并故障转移到目标卷。

如果原始集群完全出现故障或不存在，请联系 NetApp 支持部门以获得进一步帮助。

从 **Element** 集群执行故障转移

您可以从 Element 集群执行故障转移，以使目标卷成为读 / 写卷，并可供目标端的主机访问。在从 Element 集群执行故障转移之前，必须中断 SnapMirror 关系。

使用 NetApp Element UI 执行故障转移。如果 Element UI 不可用，您也可以使用 ONTAP 系统管理器或 ONTAP 命令行界面对中断关系命令执行问题描述操作。

您需要的内容

- SnapMirror 关系已存在，并且目标卷上至少有一个有效快照。
- 由于主站点发生计划外中断或计划内事件，您需要故障转移到目标卷。

步骤

1. 在 Element UI 中，单击 * 数据保护 * > * SnapMirror 关系 * 。
2. 查找与要进行故障转移的源卷的关系。
3. 单击 * 操作 * 图标。
4. 单击 * 中断 * 。
5. 确认操作。

   现在，目标集群上的卷具有读写访问权限，可以挂载到应用程序主机以恢复生产工作负载。由于此操作，所有 SnapMirror 复制都将暂停。此关系将显示已断开状态。

对 **Element** 执行故障恢复

缓解主端的问题描述后，您必须重新同步原始源卷并故障恢复到 NetApp Element 软件。根据原始源卷是否仍然存在或是否需要故障恢复到新创建的卷，您执行的步骤会有所不同。

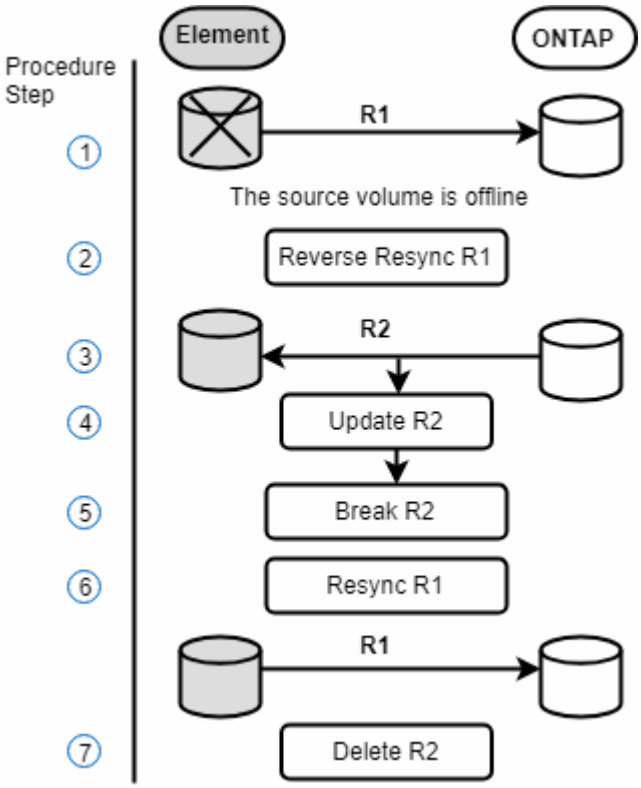
SnapMirror 故障恢复场景

SnapMirror 灾难恢复功能在两种故障恢复情形中进行了说明。假定原始关系已进行故障转移（已中断）。

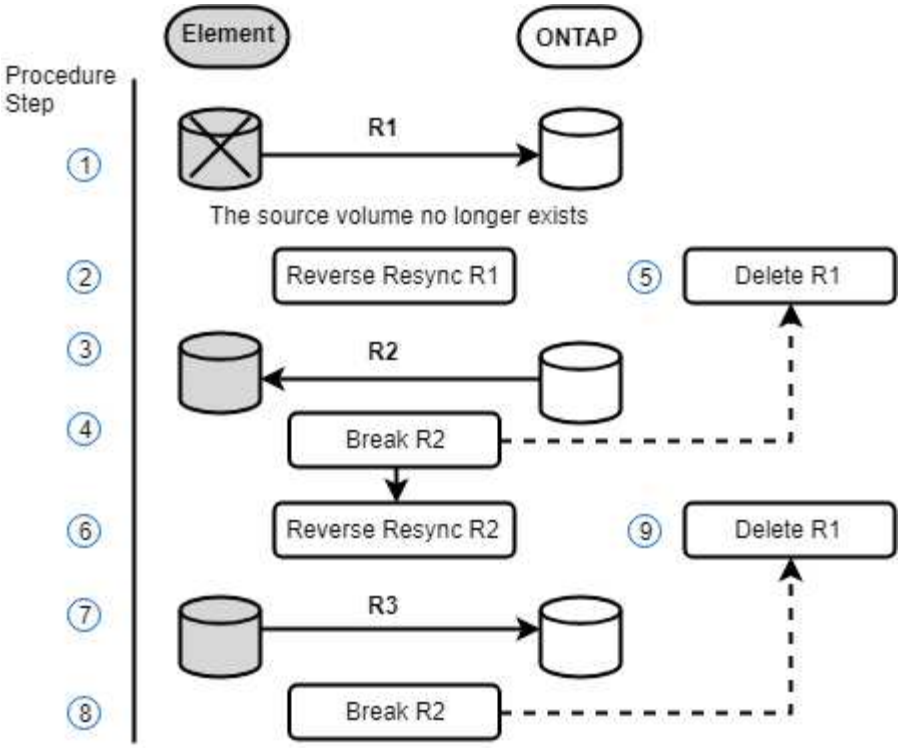
添加了相应过程中的步骤以供参考。

> 在此处的示例中， R1 表示原始关系，其中运行 NetApp Element 软件的集群是原始源卷（ Element ），而 ONTAP 是原始目标卷（ ONTAP ）。R2 和 R3 表示通过反向重新同步操作创建的反向关系。

下图显示了源卷仍存在时的故障恢复场景：



下图显示了源卷不再存在时的故障恢复场景：



了解更多信息

- 如果源卷仍存在，请执行故障恢复
- 源卷不再存在时执行故障恢复
- SnapMirror 故障恢复场景

如果源卷仍存在，请执行故障恢复

您可以使用NetApp Element UI重新同步原始源卷并执行故障恢复。此操作步骤适用场景情形下，原始源卷仍存在。

1. 在 Element UI 中，找到为执行故障转移而中断的关系。
2. 单击 "Actions" 图标，然后单击 * 反向重新同步 * 。
3. 确认操作。

> 反向重新同步操作会创建一个新关系，在此关系中，初始源卷和目标卷的角色将发生反转（这会导致两个关系，因为初始关系仍然存在）。在反向重新同步操作中，原始目标卷中的任何新数据都会传输到原始源卷。您可以继续访问目标端上的活动卷并向其写入数据，但在重定向回初始主卷之前，您需要断开与源卷连接的所有主机并执行 SnapMirror 更新。

4. 单击刚刚创建的反向关系的 "Actions" 图标，然后单击 * 更新 * 。

   现在，您已完成反向重新同步，并确保目标端上的卷未连接任何活动会话，并且最新数据位于原始主卷上，您可以执行以下步骤来完成故障恢复并重新激活原始主卷：

5. 单击反向关系的 "Actions" 图标，然后单击 * 中断 * 。

6. 单击原始关系的 "Actions" 图标，然后单击 * 重新同步 * 。

   现在，可以挂载原始主卷，以便在原始主卷上恢复生产工作负载。原始 SnapMirror 复制将根据为此关系配置的策略和计划恢复。

7. 确认原始关系状态为 `snapmirrored` 后，单击反向关系的 "Actions" 图标，然后单击 * 删除 * 。

了解更多信息

SnapMirror 故障恢复场景

源卷不再存在时执行故障恢复

您可以使用NetApp Element UI重新同步原始源卷并执行故障恢复。本节介绍了初始源卷已丢失但初始集群仍完好的适用场景情形。有关如何还原到新集群的说明，请参见 NetApp 支持站点上的文档。

您需要的内容

- Element 卷和 ONTAP 卷之间的复制关系已断开。
- Element 卷已丢失，无法恢复。
- 原始卷名称显示为未找到。

步骤

1. 在 Element UI 中，找到为执行故障转移而中断的关系。
   - 最佳实践： * 记下原始已断开关系的 SnapMirror 策略和计划详细信息。重新创建此关系时，需要此信息。
2. 单击 * 操作 * 图标，然后单击 * 反向重新同步 * 。
3. 确认操作。

   反向重新同步操作将创建一个新关系，在此关系中，初始源卷和目标卷的角色将发生反转（这会导致两个关系，因为初始关系仍然存在）。由于原始卷不再存在，系统将创建一个与原始源卷具有相同卷名称和卷大小的新 Element 卷。新卷将分配一个名为 sm-recovery 的默认 QoS 策略，并与名为 sm-recovery 的默认帐户关联。您需要手动编辑 SnapMirror 创建的所有卷的帐户和 QoS 策略，以替换已销毁的原始源卷。

   在反向重新同步操作中，最新快照中的数据将传输到新卷。您可以继续访问目标端上的活动卷并向其写入数据，但在稍后恢复初始主关系之前，您需要断开与活动卷连接的所有主机并执行 SnapMirror 更新。完成反向重新同步并确保目标端上的卷未连接任何活动会话且最新数据位于原始主卷上后，请继续执行以下步骤以完成故障恢复并重新激活原始主卷：

4. 单击反向重新同步操作期间创建的反向关系的 * 操作 * 图标，然后单击 * 中断 * 。
5. 单击源卷不存在的原始关系的 * 操作 * 图标，然后单击 * 删除 * 。
6. 单击步骤 4 中中断的反向关系的 * 操作 * 图标，然后单击 * 反向重新同步 * 。
7. 这样会反转源和目标，并导致与原始关系具有相同的卷源和卷目标关系。
8. 单击 * 操作 * 图标和 * 编辑 * 以使用您记下的原始 QoS 策略和计划设置更新此关系。

9. 现在，可以安全地删除步骤 6 中反向重新同步的反向关系。

了解更多信息

SnapMirror 故障恢复场景

执行从 **ONTAP** 到 **Element** 的传输或一次性迁移

通常，在使用 SnapMirror 从运行 NetApp Element 软件的 SolidFire 存储集群到 ONTAP 软件进行灾难恢复时， Element 是源，而 ONTAP 是目标。但是，在某些情况下，ONTAP 存储系统可以用作源，而 Element 可以用作目标。

- 存在两种情形：
  - 先前不存在灾难恢复关系。按照此操作步骤中的所有步骤进行操作。
  - 先前存在灾难恢复关系，但用于此缓解的卷之间不存在此关系。在这种情况下，请仅执行下面的步骤 3 和 4 。

您需要的内容

- Element 目标节点必须可供 ONTAP 访问。
- 必须已为 Element 卷启用 SnapMirror 复制。

您必须以 hostip： /lun/<id_number> 的形式指定 Element 目标路径，其中 lun 是实际字符串 "`lun` "，id_number 是 Element 卷的 ID 。

步骤

1. 使用 ONTAP 创建与 Element 集群的关系：

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name -type XDP -schedule schedule -policy
    policy
```

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

2. 使用 snapmirror show 命令验证是否已创建 ONTAP 关系。

   请参见 ONTAP 文档中有关创建复制关系的信息，有关完整的命令语法，请参见 ONTAP 手册页。

3. 使用 `ElementCreateVolume` API 创建目标卷并将目标卷访问模式设置为 SnapMirror：

   使用 Element API 创建 Element 卷

```
{
   "method": "CreateVolume",
   "params": {
         "name": "SMTargetVolumeTest2",
         "accountID": 1,
         "totalSize": 100000000000,
         "enable512e": true,
         "attributes": {},
         "qosPolicyID": 1,
         "enableSnapMirrorReplication": true,
         "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. 使用 ONTAP `snapmirror initialize` 命令初始化复制关系：

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

NetApp Element软件和ONTAP之间的复制(ONTAP命令行界面)

NetApp Element软件和ONTAP之间的复制概述(ONTAP命令行界面)

您可以使用SnapMirror将Element卷的Snapshot副本复制到ONTAP目标、从而确保Element系统上的业务连续性。如果 Element 站点发生灾难，您可以从 ONTAP 系统向客户端提供数据，然后在服务还原后重新激活 Element 系统。

从ONTAP 9。4开始、您可以将在ONTAP节点上创建的LUN的Snapshot副本复制回Element系统。您可能已在 Element 站点发生中断期间创建 LUN ，也可能正在使用 LUN 将数据从 ONTAP 迁移到 Element 软件。

如果符合以下条件，则应使用 Element 到 ONTAP 备份：

- 您希望使用最佳实践，而不是浏览每个可用选项。
- 您希望使用 ONTAP 命令行界面（ CLI ），而不是 System Manager 或自动化脚本编写工具。
- 您正在使用 iSCSI 向客户端提供数据。

如果需要其他SnapMirror配置或概念信息，请参见"数据保护概述"。

关于 Element 和 ONTAP 之间的复制

从ONTAP 9。3开始、您可以使用SnapMirror将Element卷的Snapshot副本复制到ONTAP目标。如果 Element 站点发生灾难，您可以从 ONTAP 系统向客户端提供数据，然后在服务还原后重新激活 Element 源卷。

从ONTAP 9。4开始、您可以将在ONTAP节点上创建的LUN的Snapshot副本复制回Element系统。您可能已在

Element 站点发生中断期间创建 LUN ，也可能正在使用 LUN 将数据从 ONTAP 迁移到 Element 软件。

数据保护关系的类型

SnapMirror 提供两种类型的数据保护关系。对于每种类型、SnapMirror都会在初始化或更新关系之前为Element源卷创建一个Snapshot副本：

- 在_Disaster Recovery (DR)_数据保护关系中、目标卷仅包含SnapMirror创建的Snapshot副本、当主站点发生灾难时、您可以继续从该副本提供数据。
- 在_long-term保留_数据保护关系中、目标卷包含由Element软件创建的时间点Snapshot副本以及由SnapMirror创建的Snapshot副本。例如、您可能希望保留在20年内创建的每月Snapshot副本。

默认策略

首次调用 SnapMirror 时，它会执行从源卷到目标卷的 *baseline transfer* 。*snapmirror policy* 用于定义基线内容以及任何更新。

您可以在创建数据保护关系时使用默认策略或自定义策略。policy type__用于确定要包含的Snapshot副本以及要保留的副本数。

下表显示了默认策略。使用 `MirrorLatest`策略创建传统灾难恢复关系。使用 `MirrorAndVault`或 `Unified7year`策略创建统一复制关系、在此关系中、在同一目标卷上配置灾难恢复和长期保留。

策略	策略类型	更新行为
MirrorLatest	异步镜像	传输SnapMirror创建的Snapshot副本。
MirrorAndVault	镜像存储	传输SnapMirror创建的Snapshot副本以及自上次更新以来创建的任何较不近期的Snapshot副本、前提是它们具有SnapMirror标签`daily`或"`Weekly`"。
Unified7year	镜像存储	传输SnapMirror创建的Snapshot副本以及自上次更新以来创建的任何较不近的Snapshot副本、但前提是它们具有SnapMirror标签`daily`、“Weekly `m或"`每月”。

有关SnapMirror策略的完整背景信息，包括要使用的策略的指导，请参见"数据保护概述"。

了解 **SnapMirror** 标签

策略类型为`mirrirr-vor`的每个策略都必须具有一条规则、用于指定要复制的Snapshot副本。例如、规则"`daily`"指示只应复制分配了SnapMirror标签"`daily`"的Snapshot副本。您可以在配置Element Snapshot副本时分配SnapMirror标签。

从 **Element** 源集群复制到 **ONTAP** 目标集群

您可以使用SnapMirror将Element卷的Snapshot副本复制到ONTAP目标系统。如果 Element 站点发生灾难，您可以从 ONTAP 系统向客户端提供数据，然后在服务还原后重新激活 Element 源卷。

Element 卷大致相当于 ONTAP LUN 。初始化 Element 软件和 ONTAP 之间的数据保护关系后， SnapMirror 将使用 Element 卷的名称创建一个 LUN 。如果 LUN 满足 Element 到 ONTAP 复制的要求， SnapMirror 会将数据

复制到现有 LUN 。

复制规则如下：

- ONTAP 卷只能包含一个 Element 卷中的数据。
- 您不能将数据从一个 ONTAP 卷复制到多个 Element 卷。

从 **ONTAP** 源集群复制到 **Element** 目标集群

从ONTAP 9。4开始、您可以将在ONTAP系统上创建的LUN的Snapshot副本复制回Element卷：

- 如果 Element 源和 ONTAP 目标之间已存在 SnapMirror 关系，则在从目标提供数据时创建的 LUN 会在重新激活源后自动复制。
- 否则，您必须在 ONTAP 源集群和 Element 目标集群之间创建和初始化 SnapMirror 关系。

复制规则如下：

- 复制关系的策略类型必须为 "`async-mirror` " 。

  不支持类型为 `mirror-vault` 的策略。

- 仅支持 iSCSI LUN 。
- 不能将多个 LUN 从 ONTAP 卷复制到 Element 卷。
- 您不能将 LUN 从 ONTAP 卷复制到多个 Element 卷。

前提条件

在 Element 和 ONTAP 之间配置数据保护关系之前，您必须已完成以下任务：

- Element 集群必须运行 NetApp Element 软件 10.1 或更高版本。
- ONTAP 集群必须运行 ONTAP 9.3 或更高版本。
- SnapMirror 必须已在 ONTAP 集群上获得许可。
- 您必须已在 Element 和 ONTAP 集群上配置足够大的卷以处理预期的数据传输。
- 如果您使用的是"`mirrirr-vault"`策略类型、则必须已为要复制的Element Snapshot副本配置SnapMirror标签。

  您只能在或中使用执行此任务"Element软件Web UI""API 方法"。

- 您必须确保端口 5010 可用。
- 如果您预计可能需要移动目标卷，则必须确保源卷和目标卷之间存在全网状连接。Element 源集群上的每个节点都必须能够与 ONTAP 目标集群上的每个节点进行通信。

支持详细信息

下表显示了 Element 到 ONTAP 备份的支持详细信息。

资源或功能	支持详细信息

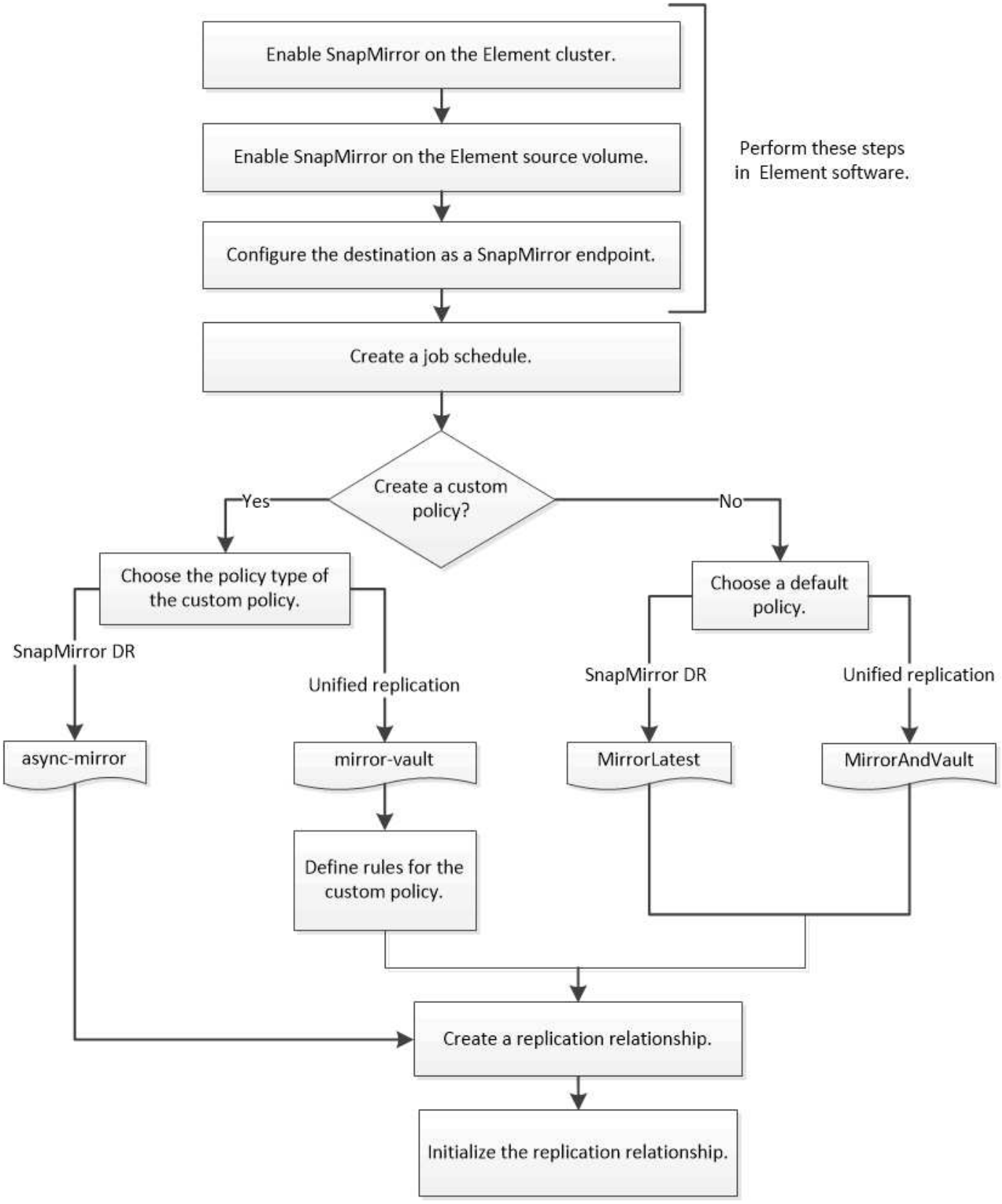
SnapMirror	• 不支持 SnapMirror 还原功能。 • `MirrorAllSnapshots`不支持和 `XDPDefault`策略。 • 不支持 "`vault` " 策略类型。 • 不支持系统定义的规则 "`all_source_snapshots` " 。 • 只有在从 Element 软件复制到 ONTAP 时，才支持使用 `mirror-vault` 策略类型。使用 "`async-mirror` " 从 ONTAP 复制到 Element 软件。 • `-schedule`不支持和 `-prefix`选项。 `snapmirror policy add-rule` • `-preserve`不支持和 `-quick-resync`选项。 `snapmirror resync` • 不会保留存储效率。 • 不支持扇出和级联数据保护部署。
ONTAP	• 从 ONTAP 9.4 和 Element 10.3 开始，支持 ONTAP Select 。 • 从 ONTAP 9.5 和 Element 11.0 开始，支持 Cloud Volumes ONTAP 。
Element	• 卷大小限制为 8 TiB 。 • 卷块大小必须为 512 字节。不支持 4 k 字节块大小。 • 卷大小必须是 1 MiB 的倍数。 • 不会保留卷属性。 • 要复制的最大Snapshot副本数为30。
网络	• 每次传输都允许使用一个 TCP 连接。 • 必须将 Element 节点指定为 IP 地址。不支持 DNS 主机名查找。 • 不支持 IP 空间。
SnapLock	不支持 SnapLock 卷。
FlexGroup	不支持 FlexGroup 卷。
SVM 灾难恢复	不支持 SVM DR 配置中的 ONTAP 卷。
MetroCluster	不支持 MetroCluster 配置中的 ONTAP 卷。

Element 和 **ONTAP** 之间的复制工作流

无论要将数据从 Element 复制到 ONTAP 还是从 ONTAP 复制到 Element ，都需要配置作业计划，指定策略以及创建和初始化关系。您可以使用默认策略或自定义策略。

此工作流假定您已完成中列出的必备任务"前提条件"。有关SnapMirror策略的完整背景信息，包括要使用的策略

的指导，请参见"数据保护概述"。



在 **Element** 软件中启用 **SnapMirror**

在 **Element** 集群上启用 **SnapMirror**

您必须先在 Element 集群上启用 SnapMirror ，然后才能创建复制关系。您只能在Element软件Web UI中或使用执行此任务"API 方法"。

开始之前

- Element 集群必须运行 NetApp Element 软件 10.1 或更高版本。
- 只能为与 NetApp ONTAP 卷一起使用的 Element 集群启用 SnapMirror 。

关于此任务

默认情况下， Element 系统附带的 SnapMirror 处于禁用状态。在新安装或升级过程中，不会自动启用 SnapMirror 。

> 启用后，无法禁用 SnapMirror 。只能通过将集群恢复为出厂映像来禁用 SnapMirror 功能并还原默认设置。

步骤

1. 单击 * 集群 * > * 设置 * 。
2. 查找 SnapMirror 的集群专用设置。
3. 单击 * 启用 SnapMirror* 。

在 **Element** 源卷上启用 **SnapMirror**

您必须先在 Element 源卷上启用 SnapMirror ，然后才能创建复制关系。您只能在Element软件Web UI中或使用和"ModifyVolumes"API方法执行此任务"ModifyVolume"。

开始之前

- 您必须已在 Element 集群上启用 SnapMirror 。
- 卷块大小必须为 512 字节。
- 卷不能参与 Element 远程复制。
- 卷访问类型不能为 "`Replication Target` " 。

关于此任务

以下操作步骤假定卷已存在。您也可以在创建或克隆卷时启用 SnapMirror 。

步骤

1. 选择 * 管理 * > * 卷 * 。
2. 选择卷对应的 按钮。
3. 在下拉菜单中，选择 * 编辑 * 。
4. 在 * 编辑卷 * 对话框中，选择 * 启用 SnapMirror* 。
5. 选择 * 保存更改 * 。

创建 **SnapMirror** 端点

必须先创建SnapMirror端点，然后才能创建复制关系。您只能在 Element 软件的 Web 用户界面中或使用以下方式执行此任务： "SnapMirror API 方法"。

开始之前

您必须已在 Element 集群上启用 SnapMirror 。

步骤

1. 单击 * 数据保护 * > * SnapMirror 端点 * 。
2. 单击 * 创建端点 * 。
3. 在 * 创建新端点 * 对话框中，输入 ONTAP 集群管理 IP 地址。
4. 输入 ONTAP 集群管理员的用户 ID 和密码。
5. 单击 * 创建端点 * 。

配置复制关系

创建复制作业计划

无论要将数据从 Element 复制到 ONTAP 还是从 ONTAP 复制到 Element ，都需要配置作业计划，指定策略以及创建和初始化关系。您可以使用默认策略或自定义策略。

您可以使用 `job schedule cron create`命令创建复制作业计划。作业计划用于确定SnapMirror何时自动更新分配了该计划的数据保护关系。

关于此任务

您可以在创建数据保护关系时分配作业计划。如果不分配作业计划，则必须手动更新此关系。

步骤

1. 创建作业计划：

   ```
   job schedule cron create -name job_name -month month -dayofweek day_of_week
   -day day_of_month -hour hour -minute minute
   ```

   对于 `-month`、 `-dayofweek`和 `-hour`，您可以指定 `all`分别在每月、每周的某一天和每小时运行作业。

   从 ONTAP 9.10.1 开始，您可以在作业计划中包含 Vserver ：

   ```
   job schedule cron create -name job_name -vserver Vserver_name -month month
   -dayofweek day_of_week -day day_of_month -hour hour -minute minute
   ```

   以下示例将创建一个名为的作业计划、该计划 `my_weekly`将在星期六凌晨3：00运行：

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

创建自定义复制策略

您可以在创建复制关系时使用默认策略或自定义策略。对于自定义统一复制策略、您必须定义一个或多个_RERUSE_、以确定初始化和更新期间传输的Snapshot副本。

如果关系的默认策略不适用，您可以创建自定义复制策略。例如、您可能希望在网络传输中压缩数据、或者修改SnapMirror尝试传输Snapshot副本的次数。

关于此任务

复制策略的 *policy type* 决定了它支持的关系类型。下表显示了可用的策略类型。

Policy type	关系类型
异步镜像	SnapMirror灾难恢复
镜像存储	统一复制

步骤

1. 创建自定义复制策略：

   ```
   snapmirror policy create -vserver SVM -policy policy -type async-
   mirror|mirror-vault -comment comment -tries transfer_tries -transfer-priority
   low|normal -is-network-compression-enabled true|false
   ```

   有关完整的命令语法，请参见手册页。

   从ONTAP 9。5开始、您可以使用参数指定为SnapMirror同步关系创建通用Snapshot副本计划的计划`-common-snapshot-schedule`。默认情况下、SnapMirror同步关系的通用Snapshot副本计划为一小时。您可以为SnapMirror同步关系的Snapshot副本计划指定一个介于30分钟到两小时之间的值。

   以下示例将为 SnapMirror 灾难恢复创建一个自定义复制策略，以便为数据传输启用网络压缩：

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_compressed -type async-mirror -comment “DR with network compression
   enabled” -is-network-compression-enabled true
   ```

   以下示例将为统一复制创建自定义复制策略：

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
   -type mirror-vault
   ```

完成后

对于"`mirrirr-vor`"策略类型、您必须定义规则来确定初始化和更新期间传输的Snapshot副本。

使用 `snapmirror policy show`命令验证是否已创建SnapMirror策略。有关完整的命令语法，请参见手册页。

为策略定义规则

对于`策略类型为"`mirrirr-vault"的自定义策略、您必须至少定义一个规则来确定初始化和更新期间传输的Snapshot副本。您还可以为 `mirror-vault` 策略类型的默认策略定义规则。

关于此任务

策略类型为`mirrirr-vor`的每个策略都必须具有一条规则、用于指定要复制的Snapshot副本。例如、规则"`bi-monthlyn`"指示只应复制分配了SnapMirror标签"`bi-monthlyn`"的Snapshot副本。您可以在配置Element Snapshot副本时分配SnapMirror标签。

每个策略类型都与一个或多个系统定义的规则相关联。指定策略类型时，系统会自动为策略分配这些规则。下表显示了系统定义的规则。

系统定义的规则	用于策略类型	结果
sm_created	异步镜像，镜像存储	SnapMirror创建的Snapshot副本会在初始化和更新时传输。
每天	镜像存储	初始化和更新时会传输源上SnapMirror标签为`daily`的新Snapshot副本。
每周	镜像存储	初始化和更新时会传输源上SnapMirror标签为"`Weekly`"的新Snapshot副本。
每月	镜像存储	初始化和更新时会传输源上SnapMirror标签为`m` onh 的新Snapshot副本。

您可以根据需要为默认策略或自定义策略指定其他规则。例如：

- 对于默认 `MirrorAndVault`策略、您可以创建一个名为"`bi-monthly"`的规则、以匹配源上具有"`bi-monthly"` SnapMirror标签的Snapshot副本。
- 对于策略类型为`mirrirr-vor`的自定义策略、您可以创建一个名为"`bi-Weekly`"的规则、以匹配源上具有"`bi-Weekly`" SnapMirror标签的Snapshot副本。

步骤

1. 为策略定义规则：

   ```
   snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
   -label snapmirror-label -keep retention_count
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将一个带有SnapMirror标签的规则添加 `bi-monthly`到默认策略中 `MirrorAndVault`：

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

以下示例将一个带有SnapMirror标签的规则添加 `bi-weekly`到自定义策略中 `my_snapvault`：

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

以下示例将一个带有SnapMirror标签的规则添加 `app_consistent`到自定义策略中 `Sync`：

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

然后、您可以从源集群复制与此SnapMirror标签匹配的Snapshot副本：

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

创建复制关系

创建从 **Element** 源到 **ONTAP** 目标的关系

主存储中的源卷与二级存储中的目标卷之间的关系称为 *data protection relationship* 。您可以使用 `snapmirror create`命令创建从Element源到ONTAP目标或从ONTAP源到Element目标的数据保护关系。

您可以使用SnapMirror将Element卷的Snapshot副本复制到ONTAP目标系统。如果 Element 站点发生灾难，您可以从 ONTAP 系统向客户端提供数据，然后在服务还原后重新激活 Element 源卷。

开始之前

- 包含要复制的卷的 Element 节点必须可供 ONTAP 访问。
- 必须已为 Element 卷启用 SnapMirror 复制。
- 如果您使用的是"`mirrirr-vault"`策略类型、则必须已为要复制的Element Snapshot副本配置SnapMirror标签。

> 您只能在或中使用执行此任务"Element软件Web UI""API 方法"。

关于此任务

您必须以的形式指定Element源路径 `<hostip:>/lun/<name>`，其中“`LUN`”是实际字符串“`LUN`”，是Element卷的名称。 `name`

Element 卷大致相当于 ONTAP LUN 。初始化 Element 软件和 ONTAP 之间的数据保护关系后， SnapMirror 将使用 Element 卷的名称创建一个 LUN 。如果 LUN 满足从 Element 软件复制到 ONTAP 的要求， SnapMirror 会将数据复制到现有 LUN 。

复制规则如下：

- ONTAP 卷只能包含一个 Element 卷中的数据。
- 您不能将数据从一个 ONTAP 卷复制到多个 Element 卷。

在ONTAP 9™3及更早版本中，目标卷最多可包含251个Snapshot副本。在ONTAP 9 4及更高版本中，目标卷最多可包含1019个Snapshot副本。

步骤

1. 从目标集群中，创建从 Element 源到 ONTAP 目标的复制关系：

   ```
   snapmirror create -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume> -type XDP -schedule schedule -policy
   <policy>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将使用默认策略创建SnapMirror灾难恢复关系 `MirrorLatest`：

   ```
   cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst -type XDP -schedule my_daily
   -policy MirrorLatest
   ```

   以下示例将使用默认策略创建统一复制关系 `MirrorAndVault`：

   ```
   cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst -type XDP -schedule my_daily
   -policy MirrorAndVault
   ```

   以下示例将使用策略创建统一复制关系 `Unified7year`：

   ```
   cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst -type XDP -schedule my_daily
   -policy Unified7year
   ```

   以下示例将使用自定义策略创建统一复制关系 `my_unified`：

   ```
   cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst -type XDP -schedule my_daily
   -policy my_unified
   ```

完成后

使用 `snapmirror show`命令验证是否已创建SnapMirror关系。有关完整的命令语法，请参见手册页。

创建从 **ONTAP** 源到 **Element** 目标的关系

从ONTAP 9。4开始、您可以使用SnapMirror将在ONTAP源上创建的LUN的Snapshot副本复制回Element目标。您可能正在使用 LUN 将数据从 ONTAP 迁移到 Element 软件。

开始之前

- Element 目标节点必须可供 ONTAP 访问。
- 必须已为 Element 卷启用 SnapMirror 复制。

关于此任务

您必须以的形式指定Element目标路径 `<hostip:>/lun/<name>`，其中“`LUN`”是实际字符串“`LUN`”，是Element卷的名称。 `name`

复制规则如下：

- 复制关系的策略类型必须为 "`async-mirror` " 。

  您可以使用默认策略或自定义策略。

- 仅支持 iSCSI LUN 。
- 不能将多个 LUN 从 ONTAP 卷复制到 Element 卷。
- 您不能将 LUN 从 ONTAP 卷复制到多个 Element 卷。

步骤

1. 创建从 ONTAP 源到 Element 目标的复制关系：

   ```
   snapmirror create -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -type XDP -schedule schedule -policy
   <policy>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将使用默认策略创建SnapMirror灾难恢复关系 `MirrorLatest`：

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy MirrorLatest
   ```

   以下示例将使用自定义策略创建SnapMirror灾难恢复关系 `my_mirror`：

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy my_mirror
```

完成后

使用 `snapmirror show`命令验证是否已创建SnapMirror关系。有关完整的命令语法，请参见手册页。

初始化复制关系

对于所有关系类型、初始化都会执行_baseline传输_：它会为源卷创建一个Snapshot副本、然后将该副本及其引用的所有数据块传输到目标卷。

开始之前

- 包含要复制的卷的 Element 节点必须可供 ONTAP 访问。
- 必须已为 Element 卷启用 SnapMirror 复制。
- 如果您使用的是"`mirrirr-vault"`策略类型、则必须已为要复制的Element Snapshot副本配置SnapMirror标签。

您只能在或中使用执行此任务"Element软件Web UI""API 方法"。

关于此任务

您必须以的形式指定Element源路径 `<hostip:>/lun/<name>`，其中“LUN”是实际字符串“LUN”，是Element卷的名称。 *name*

初始化可能非常耗时。您可能希望在非高峰时段运行基线传输。

如果由于任何原因从 ONTAP 源到 Element 目标的关系初始化失败，则即使您已更正此问题（例如，无效的 LUN 名称），初始化也将继续失败。临时解决策如下所示：

1. 删除此关系。
2. 删除 Element 目标卷。
3. 创建新的 Element 目标卷。
4. 创建并初始化从 ONTAP 源到 Element 目标卷的新关系。

步骤

1. 初始化复制关系：

   ```
   snapmirror initialize -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume|cluster://SVM/volume>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将初始化IP地址10.0.0.11处的源卷与上的目标卷 `volA_dst`之间的 `svm_backup`关系 `0005`：

```
cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

从 SnapMirror 灾难恢复目标卷提供数据

使目标卷可写

如果因发生灾难而禁用了 SnapMirror 灾难恢复关系中的主站点，则可以从目标卷提供数据，而不会造成任何中断。在主站点恢复服务后，您可以重新激活源卷。

您需要先使目标卷可写，然后才能将数据从该卷提供给客户端。您可以使用命令停止向目标进行的计划传输、使用命令停止正在进行的传输、 `snapmirror abort`并 `snapmirror break`使用 `snapmirror quiesce`命令将目标设为可写。

关于此任务

您必须以的形式指定Element源路径 `<hostip:>/lun/<name>`，其中“LUN”是实际字符串“LUN”，是Element卷的名称。 `name`

步骤

1. 停止向目标进行的计划传输：

   ```
   snapmirror quiesce -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将停止IP地址10.0.0.11处的源卷与上的目标卷 `volA_dst`之间的 `svm_backup`计划传输 `0005`：

   ```
   cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

2. 停止正在向目标传输的数据：

   ```
   snapmirror abort -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将停止IP地址10.0.0.11处的源卷与上的 `svm_backup`目标 `volA_dst`卷之间正在进行的传输 `0005`：

   ```
   cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

3. 中断 SnapMirror 灾难恢复关系：

   ```
   snapmirror break -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将中断IP地址10.0.0.11处的源卷与上的目标卷和 `volA_dst`上的 `svm_backup`目标卷 `volA_dst`之间的 `svm_backup`关系 `0005`：

   ```
   cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

配置用于数据访问的目标卷

在使目标卷可写后，您必须为该卷配置数据访问。在重新激活源卷之前， SAN 主机可以从目标卷访问数据。

1. 将 Element LUN 映射到相应的启动程序组。
2. 创建从 SAN 主机启动程序到 SAN LIF 的 iSCSI 会话。
3. 在 SAN 客户端上，执行存储重新扫描以检测已连接的 LUN 。

重新激活原始源卷

当您不再需要从目标提供数据时，可以在源卷和目标卷之间重新建立初始数据保护关系。

关于此任务

以下操作步骤假定原始源卷中的基线完好无损。如果基线不完好，则必须在执行操作步骤之前创建并初始化提供数据的卷与原始源卷之间的关系。

您必须以的形式指定Element源路径 `<hostip:>/lun/<name>`，其中“`LUN`”是实际字符串“`LUN`”，是Element卷的名称。 `name`

从ONTAP 9。4开始、重新激活Element源后、系统会自动复制在从ONTAP目标提供数据时创建的LUN的Snapshot副本。

复制规则如下：

- 仅支持 iSCSI LUN 。
- 不能将多个 LUN 从 ONTAP 卷复制到 Element 卷。
- 您不能将 LUN 从 ONTAP 卷复制到多个 Element 卷。

步骤

1. 删除原始数据保护关系：

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

有关完整的命令语法，请参见手册页。

以下示例将删除IP地址10.0.0.11处的初始源卷与上提供数据的卷 `volA_dst`之间的 `svm_backup`关系 `0005`：

```
cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

2. 反转原始数据保护关系：

```
snapmirror resync -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name> -policy <policy>
```

有关完整的命令语法，请参见手册页。

虽然重新同步不需要基线传输，但它可能非常耗时。您可能希望在非高峰时段运行重新同步。

以下示例将反转IP地址10.0.0.11处的初始源卷与上提供数据的卷 `volA_dst`之间的 `svm_backup`关系 `0005`：

```
cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

3. 更新已反转的关系：

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name>
```

有关完整的命令语法，请参见手册页。

> 如果源和目标上不存在通用Snapshot副本、则命令将失败。使用 `snapmirror initialize` 重新初始化此关系。

以下示例将更新上提供数据的卷与IP地址10.0.0.11处的 `svm_backup`初始源卷 `0005`之间的关系 `volA_dst`：

```
cluster_dst::> snapmirror update -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

4. 停止已反转关系的计划传输：

```
snapmirror quiesce -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name>
```

有关完整的命令语法，请参见手册页。

以下示例将停止上提供数据的卷与IP地址10.0.0.11处的 svm_backup`初始源卷 `0005`之间的计划传输 `volA_dst：

```
cluster_dst::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

5. 停止已反转关系的正在进行的传输：

   ```
   snapmirror abort -source-path <SVM:volume>|<cluster://SVM/volume> -destination
   -path <hostip:>/lun/<name>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将停止上提供数据的卷与IP地址10.0.0.11处的 svm_backup`初始源卷 `0005`之间正在进行的传输 `volA_dst：

   ```
   cluster_dst::> snapmirror abort -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005
   ```

6. 中断已反转的关系：

   ```
   snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume> -destination
   -path <hostip:>/lun/<name>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将中断上 svm_backup`提供数据的卷与IP地址10.0.0.11处的初始源卷 `0005`之间的关系 `volA_dst：

   ```
   cluster_dst::> snapmirror break -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005
   ```

7. 删除已反转的数据保护关系：

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将删除IP地址10.0.0.11处的初始源卷与上提供数据的卷 volA_dst`之间的 `svm_backup`已反转关系 `0005：

   ```
   cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
   ```

8. 重新建立原始数据保护关系：

   ```
   snapmirror resync -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将在IP地址10.0.0.11处的初始源卷和上的 `svm_backup`初始目标卷 `volA_dst`之间重新建立关系 `0005`：

   ```
   cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

完成后

使用 `snapmirror show`命令验证是否已创建SnapMirror关系。有关完整的命令语法，请参见手册页。

手动更新复制关系

如果更新因网络错误而失败，您可能需要手动更新复制关系。

关于此任务

您必须以的形式指定Element源路径 `<hostip:>/lun/<name>`，其中“LUN”是实际字符串“LUN”，是Element卷的名称。 `name`

步骤

1. 手动更新复制关系：

   ```
   snapmirror update -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   有关完整的命令语法，请参见手册页。

   > 如果源和目标上不存在通用Snapshot副本、则命令将失败。使用 `snapmirror initialize` 重新初始化此关系。

   以下示例将更新IP地址10.0.0.11处的源卷与上的目标 `volA_dst`卷之间的 `svm_backup`关系 `0005`：

   ```
   cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

重新同步复制关系

在将目标卷设为可写之后，在因源卷和目标卷上不存在通用 Snapshot 副本而导致更新失败之后，或者如果要更改此关系的复制策略，则需要重新同步复制关系。

关于此任务

虽然重新同步不需要基线传输，但它可能非常耗时。您可能希望在非高峰时段运行重新同步。

您必须以的形式指定Element源路径 `<hostip:>/lun/<name>`，其中“`LUN`”是实际字符串“`LUN`”，是Element卷的名称。 `name`

步骤

1. 重新同步源卷和目标卷：

   ```
   snapmirror resync -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume> -type XDP -policy <policy>
   ```

   有关完整的命令语法，请参见手册页。

   以下示例将重新同步IP地址10.0.0.11处的源卷与上的目标 `volA_dst`卷之间的 `svm_backup`关系 `0005`：

   ```
   cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
   -policy MirrorLatest -destination-path svm_backup:volA_dst
   ```

备份和还原卷

备份和还原卷

您可以将卷备份和还原到其他 SolidFire 存储以及与 Amazon S3 或 OpenStack Swift 兼容的二级对象存储。

从 OpenStack Swift 或 Amazon S3 还原卷时，您需要原始备份过程中的清单信息。如果要还原的卷是在 SolidFire 存储系统上备份的，则不需要清单信息。

了解更多信息

- 将卷备份到 Amazon S3 对象存储
- 将卷备份到 OpenStack Swift 对象存储
- 将卷备份到 SolidFire 存储集群
- 从 Amazon S3 对象存储上的备份还原卷
- 从 OpenStack Swift 对象存储上的备份还原卷
- 从 SolidFire 存储集群上的备份还原卷

将卷备份到 **Amazon S3** 对象存储

您可以将卷备份到与 Amazon S3 兼容的外部对象存储。

1. 单击 * 管理 * > * 卷 * 。
2. 单击要备份的卷对应的 "Actions" 图标。

3. 在显示的菜单中，单击 * 备份至 * 。
4. 在 * 集成备份 * 对话框的 * 备份至 * 下，选择 * S3* 。
5. 在 * 数据格式 * 下选择一个选项：
    - * 原生 * ： 只有 SolidFire 存储系统可以读取的压缩格式。
    - * 未压缩 * ： 与其他系统兼容的未压缩格式。
6. 在 * 主机名 * 字段中输入用于访问对象存储的主机名。
7. 在 * 访问密钥 ID* 字段中输入帐户的访问密钥 ID 。
8. 在 * 机密访问密钥 * 字段中输入帐户的机密访问密钥。
9. 在 * S3 Bucket* 字段中输入用于存储备份的 S3 存储分段。
10. 在 * 名称标记 * 字段中输入要附加到前缀的名称标记。
11. 单击 * 开始读取 * 。

将卷备份到 **OpenStack Swift** 对象存储

您可以将卷备份到与 OpenStack Swift 兼容的外部对象存储。

1. 单击 * 管理 * > * 卷 * 。
2. 单击要备份的卷对应的 "Actions" 图标。
3. 在显示的菜单中，单击 * 备份至 * 。
4. 在 * 集成备份 * 对话框的 * 备份至 * 下，选择 * Swift* 。
5. 在 * 数据格式 * 下选择一种数据格式：
    - * 原生 * ： 只有 SolidFire 存储系统可以读取的压缩格式。
    - * 未压缩 * ： 与其他系统兼容的未压缩格式。
6. 在 * URL * 字段中输入用于访问对象存储的 URL 。
7. 在 * 用户名 * 字段中输入帐户的用户名。
8. 在 * 身份验证密钥 * 字段中输入帐户的身份验证密钥。
9. 在 * 容器 * 字段中输入用于存储备份的容器。
10. * 可选 * ： 在 * 名称标记 * 字段中输入要附加到前缀的名称标记。
11. 单击 * 开始读取 * 。

将卷备份到 **SolidFire** 存储集群

对于运行 Element 软件的存储集群，您可以将集群上的卷备份到远程集群。

确保源集群和目标集群已配对。

请参见 "对集群进行配对以进行复制"。

在将一个集群备份或还原到另一个集群时，系统会生成一个密钥，用于在集群之间进行身份验证。此批量卷写入密钥允许源集群向目标集群进行身份验证，从而在写入目标卷时提供一定的安全性。在备份或还原过程中，您需

要先从目标卷生成批量卷写入密钥，然后再开始此操作。

1. 在目标集群上，选择 * 管理 * > * 卷 * 。
2. 单击目标卷对应的 "Actions" 图标。
3. 在显示的菜单中，单击 * 从 * 还原。
4. 在 * 集成还原 * 对话框的 * 从 * 还原下，选择 * SolidFire * 。
5. 在 * 数据格式 * 下选择一个选项：
   - * 原生 * ： 只有 SolidFire 存储系统可以读取的压缩格式。
   - * 未压缩 * ： 与其他系统兼容的未压缩格式。
6. 单击 * 生成密钥 * 。
7. 将密钥从 * 批量卷写入密钥 * 框复制到剪贴板。
8. 在源集群上，转到 * 管理 * > * 卷 * 。
9. 单击要备份的卷对应的 "Actions" 图标。
10. 在显示的菜单中，单击 * 备份至 * 。
11. 在 * 集成备份 * 对话框的 * 备份至 * 下，选择 * SolidFire * 。
12. 在 * 数据格式 * 字段中选择您先前选择的相同选项。
13. 在 * 远程集群 MVIP* 字段中输入目标卷集群的管理虚拟 IP 地址。
14. 在 * 远程集群用户名 * 字段中输入远程集群用户名。
15. 在 * 远程集群密码 * 字段中输入远程集群密码。
16. 在 * 批量卷写入密钥 * 字段中，粘贴您先前在目标集群上生成的密钥。
17. 单击 * 开始读取 * 。

从 **Amazon S3** 对象存储上的备份还原卷

您可以从 Amazon S3 对象存储上的备份还原卷。

1. 单击 * 报告 * > * 事件日志 * 。
2. 找到创建需要还原的备份的备份事件。
3. 在事件的 * 详细信息 * 列中，单击 * 显示详细信息 * 。
4. 将清单信息复制到剪贴板。
5. 单击 * 管理 * > * 卷 * 。
6. 单击要还原的卷对应的 "Actions" 图标。
7. 在显示的菜单中，单击 * 从 * 还原。
8. 在 * 集成还原 * 对话框中的 * 从 * 还原下，选择 * S3* 。
9. 在 * 数据格式 * 下选择与备份匹配的选项：
   - * 原生 * ： 只有 SolidFire 存储系统可以读取的压缩格式。
   - * 未压缩 * ： 与其他系统兼容的未压缩格式。

10. 在 * 主机名 * 字段中输入用于访问对象存储的主机名。
11. 在 * 访问密钥 ID* 字段中输入帐户的访问密钥 ID 。
12. 在 * 机密访问密钥 * 字段中输入帐户的机密访问密钥。
13. 在 * S3 Bucket* 字段中输入用于存储备份的 S3 存储分段。
14. 将清单信息粘贴到 * 清单 * 字段中。
15. 单击 * 开始写入 * 。

从 **OpenStack Swift** 对象存储上的备份还原卷

您可以从 OpenStack Swift 对象存储上的备份还原卷。

1. 单击 * 报告 * > * 事件日志 * 。
2. 找到创建需要还原的备份的备份事件。
3. 在事件的 * 详细信息 * 列中，单击 * 显示详细信息 * 。
4. 将清单信息复制到剪贴板。
5. 单击 * 管理 * > * 卷 * 。
6. 单击要还原的卷对应的 "Actions" 图标。
7. 在显示的菜单中，单击 * 从 * 还原。
8. 在 * 集成还原 * 对话框的 * 还原自 * 下，选择 * Swift* 。
9. 在 * 数据格式 * 下选择与备份匹配的选项：
    - * 原生 * ： 只有 SolidFire 存储系统可以读取的压缩格式。
    - * 未压缩 * ： 与其他系统兼容的未压缩格式。
10. 在 * URL * 字段中输入用于访问对象存储的 URL 。
11. 在 * 用户名 * 字段中输入帐户的用户名。
12. 在 * 身份验证密钥 * 字段中输入帐户的身份验证密钥。
13. 在 * 容器 * 字段中输入用于存储备份的容器的名称。
14. 将清单信息粘贴到 * 清单 * 字段中。
15. 单击 * 开始写入 * 。

从 **SolidFire** 存储集群上的备份还原卷

您可以从 SolidFire 存储集群上的备份还原卷。

在将一个集群备份或还原到另一个集群时，系统会生成一个密钥，用于在集群之间进行身份验证。此批量卷写入密钥允许源集群向目标集群进行身份验证，从而在写入目标卷时提供一定的安全性。在备份或还原过程中，您需要先从目标卷生成批量卷写入密钥，然后再开始此操作。

1. 在目标集群上，单击 * 管理 * > * 卷 * 。
2. 单击要还原的卷对应的 "Actions" 图标。

3. 在显示的菜单中，单击 * 从 * 还原。
4. 在 * 集成还原 * 对话框的 * 从 * 还原下，选择 * SolidFire * 。
5. 在 * 数据格式 * 下选择与备份匹配的选项：
   - * 原生 * ： 只有 SolidFire 存储系统可以读取的压缩格式。
   - * 未压缩 * ： 与其他系统兼容的未压缩格式。
6. 单击 * 生成密钥 * 。
7. 将 * 批量卷写入密钥 * 信息复制到剪贴板。
8. 在源集群上，单击 * 管理 * > * 卷 * 。
9. 单击要用于还原的卷对应的 "Actions" 图标。
10. 在显示的菜单中，单击 * 备份至 * 。
11. 在 * 集成备份 * 对话框中，选择 * 备份至 * 下的 * SolidFire * 。
12. 在 * 数据格式 * 下选择与备份匹配的选项。
13. 在 * 远程集群 MVIP* 字段中输入目标卷集群的管理虚拟 IP 地址。
14. 在 * 远程集群用户名 * 字段中输入远程集群用户名。
15. 在 * 远程集群密码 * 字段中输入远程集群密码。
16. 将密钥从剪贴板粘贴到 * 批量卷写入密钥 * 字段中。
17. 单击 * 开始读取 * 。

配置自定义保护域

对于包含两个以上存储节点的 Element 集群，您可以为每个节点配置自定义保护域。配置自定义保护域时，必须将集群中的所有节点分配给域。

分配保护域时，节点之间将开始数据同步，某些集群操作将不可用，直到数据同步完成为止。为集群配置自定义保护域后，在添加新存储节点时，您无法为新节点添加驱动器，除非为此节点分配一个保护域并允许完成数据同步。请访问 "保护域文档" 了解有关保护域的更多信息。

要使自定义保护域方案对集群有用，必须将每个机箱中的所有存储节点分配到同一个自定义保护域。为此，您需要根据需要创建尽可能多的自定义保护域（最小的自定义保护域方案为三个域）。最佳做法是，为每个域配置相同数量的节点，并尝试确保分配给特定域的每个节点的类型相同。

步骤

1. 单击 * 集群 * > * 节点 * 。
2. 单击 * 配置保护域 * 。

   在 * 配置自定义保护域 * 窗口中，您可以看到当前配置的保护域（如果有）以及各个节点的保护域分配。
3. 输入新自定义保护域的名称，然后单击 * 创建 * 。

   对需要创建的所有新保护域重复此步骤。

4. 对于 * 分配节点 * 列表中的每个节点，单击 * 保护域 * 列中的下拉列表，然后选择要分配给该节点的保护域。

> 在应用更改之前，请确保了解您的节点和机箱布局，您配置的自定义保护域方案以及该方案对数据保护的影响。如果您应用保护域方案并立即需要进行更改，则可能需要一段时间才能进行更改，因为应用配置后会发生数据同步。

5. 单击 * 配置保护域 * 。

结果

根据集群的大小，域之间的数据同步数据可能需要一段时间。数据同步完成后，您可以在 * 集群 * > * 节点 * 页面上查看自定义保护域分配， Element Web UI 信息板会在 * 自定义保护域运行状况 * 窗格中显示集群的保护状态。

可能的错误

应用自定义保护域配置后，您可能会看到以下错误：

error	Description	解决方法：
SetProtectionDomainLayout 失败：ProtectionDomainLayout 会使 nodeID ｛ 9 ｝ 不可用。默认名称和非默认名称不能同时使用。	节点未分配保护域。	为节点分配保护域。
SetProtectionDomainLayout 失败：保护域类型 " 自定义 " 拆分保护域类型 " 机箱 " 。	多节点机箱中的节点分配的保护域与机箱中的其他节点不同。	确保为机箱中的所有节点分配相同的保护域。

了解更多信息

- "自定义保护域"
- "使用 Element API 管理存储"

对系统进行故障排除

系统事件

查看有关系统事件的信息

您可以查看有关在系统中检测到的各种事件的信息。系统每 30 秒刷新一次事件消息。事件日志显示集群的关键事件。

1. 在 Element UI 中，选择 * 报告 * > * 事件日志 * 。

   对于每个事件，您都会看到以下信息：

项目	Description
ID	与每个事件关联的唯一 ID 。

事件类型	所记录的事件类型，例如 API 事件或克隆事件。
message	与事件关联的消息。
详细信息	有助于确定事件发生原因的信息。
服务 ID	报告事件的服务（如果适用）。
Node	报告事件的节点（如果适用）。
驱动器 ID	报告事件的驱动器（如果适用）。
事件时间	事件发生的时间。

了解更多信息

事件类型

事件类型

系统会报告多种类型的事件；每个事件都是系统已完成的一项操作。事件可以是例行事件，正常事件或需要管理员注意的事件。"Event Log" 页面上的 "Event Types" 列指示系统中发生事件的部分。

系统不会在事件日志中记录只读 API 命令。

以下列表介绍了事件日志中显示的事件类型：

- apiEvent*

  用户通过 API 或 Web UI 启动的事件，用于修改设置。

- * 二进制分配事件 *

  与数据箱分配相关的事件。箱本质上是保存数据的容器，并在整个集群中进行映射。

- **binSyncEvent**

  与在块服务之间重新分配数据相关的系统事件。

- * bsCheckEvent*

  与块服务检查相关的系统事件。

- * bsKillEvent*

  与块服务终止相关的系统事件。

- * bulkOpEvent*

  与对整个卷执行的操作相关的事件，例如备份，还原，快照或克隆。

- * cloneEvent*

  与卷克隆相关的事件。

- * clusterMasterEvent*

  集群初始化或集群配置更改时显示的事件，例如添加或删除节点。

- 【csum_event】* cSumEvent*

  与端到端校验和验证期间检测到校验和不匹配相关的事件。

  检测到校验和不匹配的服务会在生成此事件后自动停止且不重新启动。

- * 数据事件 *

  与读取和写入数据相关的事件。

- * dbEvent*

  与集群中的集合节点维护的全局数据库相关的事件。

- * 驱动器事件 *

  与驱动器操作相关的事件。

- * 加密 AtRestEvent*

  与集群上的加密过程相关的事件。

- * 信号群事件 *

  与增加或减少集合中的节点数相关的事件。

- * fibreChannelEvent*

  与节点配置和连接相关的事件。

- * gcEvent*

  与进程相关的事件每 60 分钟运行一次，用于回收块驱动器上的存储。此过程也称为垃圾收集。

- * ieEvent*

  内部系统错误。

- * 安装事件 *

  自动软件安装事件。正在待定节点上自动安装软件。

- * iSCSIEvent *

  与系统中的 iSCSI 问题相关的事件。

- * 限制事件 *

  与帐户或集群中接近允许的最大数量的卷或虚拟卷数相关的事件。

- * 维护模式事件 *

  与节点维护模式相关的事件，例如禁用节点。

- 【网络事件】网络事件

  与每个物理网络接口卡(NIC)接口的网络错误报告相关的事件。

  如果接口的任何错误计数在10分钟的监控间隔内超过默认阈值1000、则会触发这些事件。这些事件适用于网络错误、例如收到的未命中、循环冗余检查(CRC)错误、长度错误、溢出错误和帧错误。

- * platformHardwareEvent*

  与在硬件设备上检测到的问题相关的事件。

- * 远程集群事件 *

  与远程集群配对相关的事件。

- * 计划程序事件 *

  与计划快照相关的事件。

- * 服务事件 *

  与系统服务状态相关的事件。

- * sliceEvent*

  与分区服务器相关的事件，例如删除元数据驱动器或卷。

  有三种类型的分区重新分配事件，其中包括有关分配卷的服务的信息：

  - 翻转：将主服务更改为新的主服务

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - 移动：将二级服务更改为新的二级服务

    ```
    sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
    ```

  - 修剪：从一组服务中删除卷

```
sliceID {oldSecondaryServiceID(s)}
```

- * snmpTrapEvent*

  与 SNMP 陷阱相关的事件。

- * statEvent*

  与系统统计信息相关的事件。

- * tsEvent*

  与系统传输服务相关的事件。

- * 未预期异常 *

  与意外系统异常相关的事件。

- **ureEvent**

  与从存储设备读取时发生的不可恢复读取错误相关的事件。

- * vasaProviderEvent*

  与 VASA （ vSphere 存储感知 API ）提供程序相关的事件。

查看正在运行的任务的状态

您可以在 Web UI 中查看由 ListSyncJobs 和 ListBulkVolumeJobs API 方法报告的正在运行的任务的进度和完成状态。您可以从 Element UI 的 Reporting 选项卡访问 Running Tasks 页面。

如果任务数量很多，系统可能会将其排入队列并分批运行。"Running Tasks" 页面将显示当前正在同步的服务。任务完成后，它将被替换为下一个已排队的同步任务。同步任务可能会继续显示在 "Running Tasks" 页面上，直到没有其他任务可完成为止。

您可以在包含目标卷的集群的 "Running Tasks" 页面上查看正在进行复制的卷的复制同步数据。

系统警报

查看系统警报

您可以查看有关系统中集群故障或错误的信息的警报。警报可以是信息，警告或错误，可以很好地指示集群的运行状况。大多数错误都会自动自行解决。

您可以使用 ListClusterFaults API 方法自动监控警报。这样，您就可以收到有关发生的所有警报的通知。

1. 在 Element UI 中，选择 * 报告 * > * 警报 * 。

系统每 30 秒刷新一次页面上的警报。

对于每个事件，您都会看到以下信息：

项目	Description
ID	与集群警报关联的唯一 ID 。
severity	警报的重要性。可能值： • 警告：可能很快需要关注的次要问题描述。仍允许系统升级。 • 错误：可能会降低发生原因性能或丢失高可用性（ HA ）的故障。错误通常不会影响服务。 • 严重：影响服务的严重故障。系统无法提供 API 或客户端 I/O 请求。在此状态下运行可能会导致数据丢失。 • 最佳实践：未使用建议的系统配置最佳实践。
Type	故障影响的组件。可以是节点，驱动器，集群，服务或卷。
Node	此故障所引用节点的节点 ID 。对于节点和驱动器故障，会提供此参数，否则会设置为 - （短划线）。
驱动器 ID	此故障所引用的驱动器的驱动器 ID 。对于驱动器故障，会提供此参数，否则会设置为 - （短划线）。
错误代码	一个描述性代码，用于指示故障的原因。
详细信息	故障的问题描述以及其他详细信息。
Date	记录故障的日期和时间。

2. 单击某个警报的 * 显示详细信息 * 可查看有关该警报的信息。
3. 要查看页面上所有警报的详细信息，请单击详细信息列。

系统解决警报后，有关警报的所有信息（包括警报解决日期）将移至 "Resolved" （已解决）区域。

了解更多信息

- 集群故障代码
- "使用 Element API 管理存储"

系统会通过生成故障代码来报告可能需要关注的错误或状态，此故障代码会列在 "Alerts" 页面上。这些代码可帮助您确定系统中哪个组件出现警报以及生成警报的原因。

以下列表概述了不同类型的代码：

- * 身份验证服务故障 *

  一个或多个集群节点上的身份验证服务未按预期运行。

  请联系 NetApp 支持部门以获得帮助。

- * 可用 VirtualNetworkIPAddressLow*

  IP 地址块中的虚拟网络地址数量较少。

  要解决此故障，请向虚拟网络地址块添加更多 IP 地址。

- * 块集群完整 *

  没有足够的可用块存储空间来支持单节点丢失。有关集群填充度级别的详细信息，请参见 GetClusterFullThreshold API 方法。此集群故障指示以下情况之一：

  - stage3Low （ Warning ）：已超过用户定义的阈值。调整 "Cluster Full" 设置或添加更多节点。
  - stage4Critical （ Error ）：没有足够的空间从单节点故障中恢复。不允许创建卷，快照和克隆。
  - stage5CompletelyConsumed （严重） 1 ；不允许写入或新的 iSCSI 连接。将保持当前的 iSCSI 连接。写入将失败，直到向集群添加更多容量为止。

  要解决此故障，请清除或删除卷，或者向存储集群添加另一个存储节点。

- * 块已降级 *

  由于发生故障，块数据不再完全复制。

severity	Description
警告	只能访问块数据的两个完整副本。
error	只能访问块数据的一个完整副本。
严重	无法访问块数据的完整副本。

- 注： * 警告状态只能发生在三重 Helix 系统上。

  要解决此故障，请还原任何脱机节点或块服务，或者联系 NetApp 支持部门以获得帮助。

- * 块服务 TooFull*

  块服务正在使用过多空间。

要解决此故障，请添加更多已配置容量。

- * 块服务运行状况不正常 *

  检测到块服务运行状况不正常：

  - 严重性 = 警告：不执行任何操作。此警告期限将在 cTimeUntilBSisKiledMSec=330000 毫秒后过期。
  - 严重性 = 错误：系统正在自动停用数据并将其数据重新复制到其他运行状况良好的驱动器。
  - 严重性 = 严重：多个节点上的故障块服务大于或等于复制计数（双 Helix 为 2 ）。数据不可用，无法完成箱同步。

    检查网络连接问题和硬件错误。如果特定硬件组件出现故障，则会出现其他故障。当可访问块服务或已停用此服务时，此故障将得以清除。

- * BmcSelfTestFailed

  基板管理控制器(BMC)未通过自检。

  请联系NetApp支持部门以获得帮助。

  在升级到Element 12.5或更高版本期间、如果节点先前存在故障BMC、或者在升级期间节点的BMC出现故障、则不会生成`BmcSelfTestFailed`故障。如果在升级期间自检失败的BMC会在整个集群完成升级后出现问题描述 A `BmcSelfTestFailed`警告故障。

- * 时钟 SkewExceedsFaultThreshold *

  集群主节点与提供令牌的节点之间的时间偏差超过建议的阈值。存储集群无法自动更正节点之间的时间偏差。

  要解决此故障，请使用网络内部的 NTP 服务器，而不是使用安装默认值。如果您使用的是内部 NTP 服务器，请联系 NetApp 支持部门以获得帮助。

- * clusterCannotSync*

  出现空间不足的情况，脱机块存储驱动器上的数据无法同步到仍处于活动状态的驱动器。

  要解决此故障，请添加更多存储。

- * clusterFull *

  存储集群中没有更多可用存储空间。

  要解决此故障，请添加更多存储。

- * 集群 IOPSAreOverProvisioned *

  集群 IOPS 配置过度。所有最小 QoS IOPS 的总和大于集群的预期 IOPS 。无法同时为所有卷保持最低 QoS 。

  要解决此问题描述，请降低卷的最小 QoS IOPS 设置。

- * cpuTherMalEventThreshold *

一个或多个CPU上的CPU散热事件数超过配置的阈值。

如果在10分钟内未检测到新的CPU散热事件、则此警告将自行解决。

- * 禁用 DriveSecurityFailed

  集群未配置为启用驱动器安全性（空闲加密），但至少有一个驱动器启用了驱动器安全性，这意味着在这些驱动器上禁用驱动器安全性失败。此故障会记录为 "`Warning` " 严重性。

  要解决此故障，请查看故障详细信息以了解无法禁用驱动器安全保护的原因。可能的原因包括：

  - 无法获取加密密钥，请调查此密钥或外部密钥服务器的访问问题。
  - 对驱动器执行禁用操作失败，请确定是否可能获取了错误的密钥。

    如果这两种情况都不是导致故障的原因，则可能需要更换驱动器。

  您可以尝试恢复未成功禁用安全的驱动器，即使提供的身份验证密钥正确也是如此。要执行此操作，请将驱动器移至 "Available" （可用）以从系统中删除，对驱动器执行安全擦除并将其移回 "Active" （活动）。

- * 已断开 ClusterPair*

  集群对已断开连接或配置不正确。

  检查集群之间的网络连接。

- * 断开 RemoteNode*

  远程节点已断开连接或配置不正确。

  检查节点之间的网络连接。

- * 断开 SnapMirrorEndpoint*

  远程 SnapMirror 端点已断开连接或配置不正确。

  检查集群与远程 SnapMirrorEndpoint 之间的网络连接。

- * 可用驱动器 *

  集群中有一个或多个驱动器可用。通常，所有集群都应添加所有驱动器，而不应使任何驱动器处于可用状态。如果意外出现此故障，请联系 NetApp 支持部门。

  要解决此故障，请向存储集群添加任何可用驱动器。

- * 驱动器已启用 *

  当一个或多个驱动器发生故障时，集群将返回此故障，表示以下情况之一：

  - 驱动器管理器无法访问此驱动器。
  - 分区或块服务失败次数过多，可能是由于驱动器读取或写入失败，无法重新启动。
  - 驱动器缺失。

- 无法访问节点的主服务（此节点中的所有驱动器均视为缺失 / 故障）。
- 驱动器已锁定，无法获取驱动器的身份验证密钥。
- 驱动器已锁定，解锁操作失败。

  要解决此问题描述，请执行以下操作：

- 检查节点的网络连接。
- 更换驱动器。
- 确保身份验证密钥可用。

- * 驱动器运行状况故障 *

  驱动器未通过智能运行状况检查，因此驱动器的功能会降低。此故障具有严重严重性级别：

  - 插槽中序列号为 < 序列号 > 的驱动器： < 节点插槽 >< 驱动器插槽 > 未通过 SMART 整体运行状况检查。

  要解决此故障，请更换驱动器。

- * 驱动器 WearFault *

  驱动器的剩余寿命已降至阈值以下，但它仍在运行。此故障可能存在两个严重性级别：严重和警告：

  - 序列号为 < 序列号 > 的驱动器插槽： < 节点插槽 >< 驱动器插槽 > 具有严重的损耗级别。
  - 驱动器的插槽： <node slot><drive slot> 中的序列号为 <serial number> ，因此预留的损耗较低。

    要解决此故障，请尽快更换驱动器。

- * 双工 ClusterMasterCandidate*

  检测到多个存储集群候选主存储。

  请联系 NetApp 支持部门以获得帮助。

- * 启用 DriveSecurityFailed

  集群已配置为需要驱动器安全性（空闲加密），但至少一个驱动器无法启用驱动器安全性。此故障会记录为 "`Warning` " 严重性。

  要解决此故障，请查看故障详细信息以了解无法启用驱动器安全保护的原因。可能的原因包括：

  - 无法获取加密密钥，请调查此密钥或外部密钥服务器的访问问题。
  - 驱动器上的启用操作失败，请确定是否可能获取了错误的密钥。如果这两种情况都不是导致故障的原因，则可能需要更换驱动器。

  您可以尝试恢复未成功启用安全保护的驱动器，即使提供的身份验证密钥正确也是如此。要执行此操作，请将驱动器移至 "Available" （可用）以从系统中删除，对驱动器执行安全擦除并将其移回 "Active" （活动）。

- * 信号群已降级 *

  一个或多个集合节点已断开网络连接或电源。

要解决此故障，请还原网络连接或电源。

- * 异常 *

  报告的故障不是例行故障。这些故障不会自动从故障队列中清除。

  请联系 NetApp 支持部门以获得帮助。

- * 故障空间 TooFull*

  块服务未响应数据写入请求。这会导致分区服务用尽存储失败写入的空间。

  要解决此故障，请还原块服务功能，以允许继续正常写入并从分区服务刷新故障空间。

- * 风扇传感器 *

  风扇传感器出现故障或缺失。

  要解决此故障，请更换任何出现故障的硬件。

- * 光纤通道访问已降级 *

  光纤通道节点在一段时间内未通过其存储 IP 对存储集群中的其他节点做出响应。在此状态下，节点将被视为无响应并生成集群故障。

  检查网络连接。

- * 光纤通道访问不可用 *

  所有光纤通道节点均无响应。此时将显示节点 ID 。

  检查网络连接。

- * fibreChannelActiveIxL*

  IXL Nexus 计数即将达到支持的限制，即每个光纤通道节点具有 8000 个活动会话。

  - 最佳实践限制为 5500 。
  - 警告限制为 7500 。
  - 最大限制（未强制实施）为 8192 。

  要解决此故障，请将 IXL Nexus 计数降至最佳实践限制 5500 以下。

- * fibreChannelConfig*

  此集群故障指示以下情况之一：

  - PCI 插槽上存在意外的光纤通道端口。
  - 存在意外的光纤通道 HBA 型号。
  - 光纤通道 HBA 的固件存在问题。
  - 光纤通道端口未联机。

- 有一个永久性问题描述正在配置光纤通道直通。

请联系 NetApp 支持部门以获得帮助。

- * 光纤通道 IOPS*

  集群中光纤通道节点的总 IOPS 计数即将达到 IOPS 限制。限制包括：

  - FC0025 ： 每个光纤通道节点 4 k 块大小时的 IOPS 限制为 450 k 。
  - FCN001 ： 每个光纤通道节点 4 K 块大小时的 625K 操作数限制。

  要解决此故障，请在所有可用光纤通道节点之间平衡负载。

- * fibreChannelStaticIxL*

  IXL Nexus 计数即将达到支持的限制，即每个光纤通道节点有 16000 个静态会话。

  - 最佳实践限制为 11000 。
  - 警告限制为 15000 。
  - 最大限制（强制实施）为 16384 。

  要解决此故障，请将 IXL Nexus 计数降至最佳实践限制 11000 以下。

- * 文件系统容量低 *

  其中一个文件系统空间不足。

  要解决此故障，请向文件系统添加更多容量。

- *文件系统IsReadOnly *

  文件系统已移至只读模式。

  请联系 NetApp 支持部门以获得帮助。

- * fipsDrivesMismatch*

  已将非 FIPS 驱动器物理插入支持 FIPS 的存储节点，或者已将 FIPS 驱动器物理插入非 FIPS 存储节点。每个节点会生成一个故障，并列出所有受影响的驱动器。

  要解决此故障，请卸下或更换不匹配的相关驱动器。

- * fipsDrivesOutOfCompliance"

  在启用 FIPS 驱动器功能后，系统检测到已禁用空闲加密。如果启用了 FIPS 驱动器功能且存储集群中存在非 FIPS 驱动器或节点，则也会生成此故障。

  要解决此故障，请启用空闲加密或从存储集群中删除非 FIPS 硬件。

- * fipsSelfTestFailure*

  FIPS 子系统在自检期间检测到故障。

请联系 NetApp 支持部门以获得帮助。

- * 硬件配置不匹配 *

  此集群故障指示以下情况之一：

  - 此配置与节点定义不匹配。
  - 此类节点的驱动器大小不正确。
  - 检测到不受支持的驱动器。可能的原因是，安装的 Element 版本无法识别此驱动器。建议更新此节点上的 Element 软件。
  - 驱动器固件不匹配。
  - 驱动器加密功能状态与节点不匹配。

  请联系 NetApp 支持部门以获得帮助。

- * idPCertificateExpiration*

  用于第三方身份提供程序（ IdP ）的集群服务提供商 SSL 证书即将到期或已过期。此故障会根据紧急程度使用以下严重性：

severity	Description
警告	证书将在 30 天内过期。
error	证书将在 7 天内过期。
严重	证书将在 3 天内过期或已过期。

  要解决此故障，请在 SSL 证书过期之前对其进行更新。将 UpdateIdpConfiguration API 方法与 `refreshCertificate`呼 出时间 `=true` 结合使用，以提供更新后的 SSL 证书。

- * 不一致的绑定模式 *

  VLAN 设备上缺少绑定模式。此故障将显示预期的绑定模式和当前正在使用的绑定模式。

- * 不一致的 Mtus*

  此集群故障指示以下情况之一：

  - Bond1G mismatch ： 在绑定 1G 接口上检测到 MTU 不一致。
  - Bond10G mismatch ： 在绑定 10G 接口上检测到 MTU 不一致。

  此故障将显示相关节点以及关联的 MTU 值。

- * 不一致的路由规则 *

  此接口的路由规则不一致。

- * 不一致的子网询问 *

VLAN 设备上的网络掩码与内部记录的 VLAN 网络掩码不匹配。此故障将显示预期的网络掩码和当前正在使用的网络掩码。

- * 绑定端口数不正确 *

  绑定端口数不正确。

- * invuidConfiguredFibreChannelNodeCount*

  两个预期光纤通道节点连接中的一个已降级。如果仅连接了一个光纤通道节点，则会出现此故障。

  要解决此故障，请检查集群网络连接和网络布线，并检查服务是否出现故障。如果没有网络或服务问题，请联系 NetApp 支持部门更换光纤通道节点。

- * irqBalanceFailed

  尝试平衡中断时出现异常。

  请联系 NetApp 支持部门以获得帮助。

- * kmipCertificateFault ：
  - 根证书颁发机构（ CA ）证书即将到期。

    要解决此故障，请从根 CA 获取一个新证书，此证书的到期日期至少为 30 天后，并使用 ModifyKeyServerKmip 提供更新后的根 CA 证书。

  - 客户端证书即将到期。

    要解决此故障，请使用 GetClientCertificateSigningRequest 创建一个新的 CSR ，并对其进行签名以确保新的到期日期至少在 30 天后，然后使用 ModifyKeyServerKmip 将即将到期的 KMIP 客户端证书替换为新证书。

  - 根证书颁发机构（ CA ）证书已过期。

    要解决此故障，请从根 CA 获取一个新证书，此证书的到期日期至少为 30 天后，并使用 ModifyKeyServerKmip 提供更新后的根 CA 证书。

  - 客户端证书已过期。

    要解决此故障，请使用 GetClientCertificateSigningRequest 创建一个新的 CSR ，并对其进行签名以确保新的到期日期至少在 30 天后，然后使用 ModifyKeyServerKmip 将已过期的 KMIP 客户端证书替换为新证书。

  - 根证书颁发机构（ CA ）证书错误。

    要解决此故障，请检查提供的证书是否正确，如果需要，请从根 CA 重新获取此证书。使用 ModifyKeyServerKmip 安装正确的 KMIP 客户端证书。

  - 客户端证书错误。

    要解决此故障，请检查是否安装了正确的 KMIP 客户端证书。客户端证书的根 CA 应安装在 EKS 上。使用 ModifyKeyServerKmip 安装正确的 KMIP 客户端证书。

- * kmipServerFault *：
  - 连接失败

    要解决此故障，请检查外部密钥服务器是否处于活动状态并可通过网络访问。使用 TestKeyServerKimp 和 TestKeyProviderKmip 测试连接。

  - 身份验证失败

    要解决此故障，请检查使用的根 CA 和 KMIP 客户端证书是否正确，以及私钥和 KMIP 客户端证书是否匹配。

  - 服务器错误

    要解决此故障，请查看此错误的详细信息。根据返回的错误，可能需要在外部密钥服务器上进行故障排除。

- * 内存 EccThreshold *

  检测到大量可更正或不可更正的 ECC 错误。此故障会根据紧急程度使用以下严重性：

事件	severity	Description
一个 DIMM cErrorCount 达到 cDImmCorrectableErrWarnThreshold 。	警告	DIMM 上的可更正 ECC 内存错误超过阈值： <Processor> <DIMM Slot>
在 DIMM 的 cErrorFault计时 器过期之前，一个 DIMM cErrorCount 将保持在 cDIMMCorrectableErrWarnThreshold 以上。	error	DIMM <Processor> <DIMM> 上的可更正 ECC 内存错误超过阈值
内存控制器报告 cErrorCount 高于 cMemCtrl+Alt+CorrectErrWarnThreshold ，并指定 cMemcerrCorrectableErrWarnDuration 。	警告	内存控制器 <Processor> <Memory Controller> 上的可更正 ECC 内存错误超过阈值
在内存控制器的 cErrorFault计时器过期之前，内存控制器会报告 cErrorCount 高于 cMemCtrl+Alt+CorrectErrWarnThreshold 。	error	DIMM <Processor> <DIMM> 上的可更正 ECC 内存错误超过阈值
单个 DIMM 报告的 uErrorCount 超过零，但小于 cdimmUncorrecteErrFaultThreshold 。	警告	在 DIMM： <Processor> <DIMM Slot> 上检测到不可更正的 ECC 内存错误

单个 DIMM 报告的 uErrorCount 至少为 cDIMMUncorrectErrFaultThreshold 。	error	在 DIMM： <Processor> <DIMM Slot> 上检测到不可更正的 ECC 内存错误
内存控制器报告 uErrorCount 超过零，但小于 cMemcerrUncorrectErrFaultThreshold 。	警告	在内存控制器 < 处理器 > < 内存控制器 > 上检测到不可更正的 ECC 内存错误
内存控制器报告的 uErrorCount 至少为 cMemcerrcerr无法 更正 ErrFaultThreshold 。	error	在内存控制器 < 处理器 > < 内存控制器 > 上检测到不可更正的 ECC 内存错误

要解决此故障，请联系 NetApp 支持部门以获得帮助。

- * 内存使用阈值 *

  内存使用量超过正常值。此故障会根据紧急程度使用以下严重性：

  有关故障类型的更多详细信息，请参见错误故障中的 * 详细信息 * 标题。

severity	Description
警告	系统内存不足。
error	系统内存非常低。
严重	系统内存已完全耗尽。

要解决此故障，请联系 NetApp 支持部门以获得帮助。

- * 元数据 ClusterFull*

  没有足够的可用元数据存储空间来支持单节点丢失。有关集群填充度级别的详细信息，请参见 GetClusterFullThreshold API 方法。此集群故障指示以下情况之一：

  - stage3Low （ Warning ）：已超过用户定义的阈值。调整 "Cluster Full" 设置或添加更多节点。
  - stage4Critical （ Error ）：没有足够的空间从单节点故障中恢复。不允许创建卷，快照和克隆。
  - stage5CompletelyConsumed （严重） 1 ；不允许写入或新的 iSCSI 连接。将保持当前的 iSCSI 连接。写入将失败，直到向集群添加更多容量为止。清除或删除数据或添加更多节点。

  要解决此故障，请清除或删除卷，或者向存储集群添加另一个存储节点。

- * mtuCheckFailure *

  未为网络设备配置正确的 MTU 大小。

要解决此故障，请确保为所有网络接口和交换机端口配置巨型帧（ MTU 大小高达 9000 字节）。

- * 网络配置 *

  此集群故障指示以下情况之一：

  - 预期接口不存在。
  - 存在重复接口。
  - 已配置的接口已关闭。
  - 需要重新启动网络。

  请联系 NetApp 支持部门以获得帮助。

- * 节点可用虚拟网络 IP 插件 *

  IP 地址块中没有可用的虚拟网络地址。

  - virtualNetworkID 标 记 (##)没有可用的存储IP地址。无法向集群添加其他节点。

  要解决此故障，请向虚拟网络地址块添加更多 IP 地址。

- *nodeHardwareFault （网络接口 <name> 已关闭或缆线已拔出） *

  网络接口已关闭或已拔下缆线。

  要解决此故障，请检查一个或多个节点的网络连接。

- *nodeHardwareFault （驱动器加密功能状态与插槽 <node slot><drive slot> 中驱动器的节点加密功能状态不匹配） *

  驱动器的加密功能与安装该驱动器的存储节点不匹配。

- * 节点 HardwareFault （此节点类型的插槽 < 驱动器插槽 >< 驱动器插槽 > 中驱动器的驱动器 < 驱动器类型 > 驱动器大小 < 实际大小 > 不正确 - 应为 < 预期大小 > ） *

  存储节点中的驱动器大小不正确。

- * 节点硬件故障（在插槽 < 节点插槽 >< 驱动器插槽 > 中检测到不支持的驱动器；驱动器统计信息和运行状况信息将不可用） *

  存储节点包含其不支持的驱动器。

- * 节点硬件故障（插槽 < 节点插槽 >< 驱动器插槽 > 中的驱动器应使用固件版本 < 预期版本 > ，但使用的版本 < 实际版本 > 不受支持） *

  存储节点包含运行不受支持的固件版本的驱动器。

- * 节点维护模式 *

  节点已置于维护模式。此故障会根据紧急程度使用以下严重性：

severity	Description

警告	指示节点仍处于维护模式。
error	表示维护模式无法禁用，最可能的原因是备用磁盘出现故障或处于活动状态。

要解决此故障，请在维护完成后禁用维护模式。如果错误级别故障仍然存在，请联系 NetApp 支持部门以获得帮助。

- * 节点脱机 *

  Element 软件无法与指定节点进行通信。检查网络连接。

- * 不使用 LACPBondMode*

  未配置 LACP 绑定模式。

  要解决此故障，请在部署存储节点时使用 LACP 绑定；如果未启用并正确配置 LACP ，客户端可能会遇到性能问题。

- * 无法访问 ntpServer*

  存储集群无法与指定的一个或多个 NTP 服务器进行通信。

  要解决此故障，请检查 NTP 服务器，网络和防火墙的配置。

- * ntpTimeNotInSync*

  存储集群时间与指定 NTP 服务器时间之间的差异过大。存储集群无法自动更正此差异。

  要解决此故障，请使用网络内部的 NTP 服务器，而不是使用安装默认值。如果您使用的是内部 NTP 服务器，并且问题描述仍然存在，请联系 NetApp 支持部门以获得帮助。

- * nvramDeviceStatus*

  NVRAM 设备出现错误，正在发生故障或已发生故障。此故障具有以下严重性：

severity	Description
警告	硬件检测到警告。这种情况可能是暂时的，例如温度警告。 • nvmLifetimeError • nvmLifetimeStatus • 生成源 LifetimeStatus • energySourceTemperatureStatus • warningThresholdExceeded

error	硬件检测到错误或严重状态。集群主节点尝试从操作中删除分区驱动器（此操作会生成驱动器删除事件）。如果二级分区服务不可用，则不会删除驱动器。除了警告级别错误之外，还返回错误： • NVRAM 设备挂载点不存在。 • NVRAM 设备分区不存在。 • NVRAM 设备分区已存在，但未挂载。
严重	硬件检测到错误或严重状态。集群主节点尝试从操作中删除分区驱动器（此操作会生成驱动器删除事件）。如果二级分区服务不可用，则不会删除驱动器。 • 持久性 Lost • armStatusSaveNarm • csaveStatusError

更换节点中的所有故障硬件。如果无法解决问题描述问题，请联系 NetApp 支持部门以获得帮助。

- * 电源供应错误 *

  此集群故障指示以下情况之一：

  - 电源不存在。
  - 电源出现故障。
  - 电源输入缺失或超出范围。

  要解决此故障，请验证是否已为所有节点提供冗余电源。请联系 NetApp 支持部门以获得帮助。

- * 配置空间 TooFull*

  集群的整体已配置容量过满。

  要解决此故障，请添加更多已配置空间，或者删除并清除卷。

- * remoteRePAsyncDelayExceedd*

  已超过为复制配置的异步延迟。检查集群之间的网络连接。

- * 远程 remoteClusterFull*

  卷已暂停远程复制，因为目标存储集群太满。

  要解决此故障，请释放目标存储集群上的一些空间。

- * remoteSnapshotClusterFull*

  由于目标存储集群太满，卷已暂停快照远程复制。

要解决此故障，请释放目标存储集群上的一些空间。

- * remoteSnapshotsExceededLimit*

  由于目标存储集群卷已超过其快照限制，卷已暂停快照远程复制。

  要解决此故障，请增加目标存储集群上的快照限制。

- * 计划操作错误 *

  已运行一个或多个计划活动，但失败。

  如果计划活动再次运行并成功，计划活动已删除或活动已暂停并恢复，则此故障将清除。

- * 传感器读取已成功 *

  传感器无法与基板管理控制器(BMC)通信。

  请联系 NetApp 支持部门以获得帮助。

- * 服务未运行 *

  所需服务未运行。

  请联系 NetApp 支持部门以获得帮助。

- * sliceServiceTooFull*

  为分区服务分配的已配置容量太少。

  要解决此故障，请添加更多已配置容量。

- * sliceServiceUnhealth*

  系统已检测到分区服务运行状况不正常，并且正在自动停用该服务。

  - 严重性 = 警告：不执行任何操作。此警告期限将在 6 分钟后过期。
  - 严重性 = 错误：系统正在自动停用数据并将其数据重新复制到其他运行状况良好的驱动器。

  检查网络连接问题和硬件错误。如果特定硬件组件出现故障，则会出现其他故障。当分区服务可访问或服务已停用时，此故障将得以清除。

- * 已启用 ssh*

  已在存储集群中的一个或多个节点上启用 SSH 服务。

  要解决此故障，请在相应节点上禁用 SSH 服务，或者联系 NetApp 支持部门以获得帮助。

- * sslCertificateExpiration*

  与此节点关联的 SSL 证书即将到期或已过期。此故障会根据紧急程度使用以下严重性：

severity	Description

警告	证书将在 30 天内过期。
error	证书将在 7 天内过期。
严重	证书将在 3 天内过期或已过期。

要解决此故障，请续订 SSL 证书。如果需要，请联系 NetApp 支持部门以获得帮助。

- * strandedCapacity"

  单个节点占用的存储集群容量超过一半。

  为了保持数据冗余，系统会减少最大节点的容量，以使其部分块容量处于孤立状态（未使用）。

  要解决此故障，请向现有存储节点添加更多驱动器或向集群添加存储节点。

- * TempSensor *

  温度传感器报告的温度高于正常温度。此故障可能会与 powerSupplyError 或 FanSensor 故障一起触发。

  要解决此故障，请检查存储集群附近是否存在气流障碍。如果需要，请联系 NetApp 支持部门以获得帮助。

- * 升级 *

  升级已进行 24 小时以上。

  要解决此故障，请恢复升级或联系 NetApp 支持部门以获得帮助。

- * 无响应服务 *

  服务已变得无响应。

  请联系 NetApp 支持部门以获得帮助。

- * 虚拟网络配置 *

  此集群故障指示以下情况之一：

  - 接口不存在。
  - 接口上的命名空间不正确。
  - 网络掩码不正确。
  - IP 地址不正确。
  - 某个接口未启动且未运行。
  - 节点上存在多余的接口。

  请联系 NetApp 支持部门以获得帮助。

- * 卷已降级 *

二级卷尚未完成复制和同步。同步完成后，此消息将被清除。

- * 卷脱机 *

  存储集群中的一个或多个卷已脱机。此外，还将出现 * 卷已降级 * 故障。

  请联系 NetApp 支持部门以获得帮助。

查看节点性能活动

您可以以图形格式查看每个节点的性能活动。此信息可提供节点中每个驱动器的实时 CPU 和每秒读 / 写 I/O 操作数（ IOPS ）统计信息。利用率图形每五秒更新一次，驱动器统计信息图形每十秒更新一次。

1. 单击 * 集群 * > * 节点 * 。
2. 单击要查看的节点的 * 操作 * 。
3. 单击 * 查看详细信息 * 。

通过将光标置于折线或条形上方，您可以在折线图和条形图上查看特定时间点。

销量表现

查看卷性能

您可以查看集群中所有卷的详细性能信息。您可以按卷 ID 或任何性能列对信息进行排序。您也可以使用按特定条件筛选信息。

您可以通过单击 * 刷新间隔 * 列表并选择其他值来更改系统刷新页面上性能信息的频率。如果集群中的卷少于 1000 个，则默认刷新间隔为 10 秒；否则，默认刷新间隔为 60 秒。如果选择从不，则会禁用自动页面刷新。

您可以通过单击 * 打开自动刷新 * 来重新启用自动刷新。

1. 在 Element UI 中，选择 * 报告 * > * 卷性能 * 。
2. 在卷列表中，单击某个卷对应的 "Actions" 图标。
3. 单击 * 查看详细信息 * 。

   页面底部将显示一个托盘，其中包含有关卷的常规信息。

4. 要查看有关卷的更多详细信息，请单击 * 查看更多详细信息 * 。

   系统将显示卷的详细信息以及性能图形。

了解更多信息

卷性能详细信息

您可以从 Element UI 中的 Reporting 选项卡的 Volume Performance 页面查看卷的性能统计信息。

以下列表介绍了您可以使用的详细信息：

- * ID *

  系统为卷生成的 ID 。

- * 名称 *

  创建卷时为卷指定的名称。

- * 帐户 *

  分配给卷的帐户的名称。

- * 访问组 *

  卷所属的一个或多个卷访问组的名称。

- * 卷利用率 *

  一个百分比值，用于说明客户端使用卷的容量。

  可能值：

  - 0 = 客户端未使用此卷
  - 100 = 客户端正在使用最大值
  - >100 = 客户端正在使用突发

- * 总 IOPS*

  当前对卷执行的 IOPS （读取和写入）总数。

- * 读取 IOPS*

  当前对卷执行的读取 IOPS 总数。

- * 写入 IOPS*

  当前对卷执行的写入 IOPS 总数。

- * 总吞吐量 *

  当前对卷执行的总吞吐量（读取和写入）。

- * 读取吞吐量 *

  当前对卷执行的读取吞吐量总量。

- * 写入吞吐量 *

  当前对卷执行的写入吞吐量总量。

- * 总延迟 *

  完成卷读写操作的平均时间（以微秒为单位）。

- * 读取延迟 *

  在过去 500 毫秒内完成卷读取操作的平均时间（以微秒为单位）。

- * 写入延迟 *

  在过去 500 毫秒内完成卷写入操作的平均时间（以微秒为单位）。

- * 队列深度 *

  对卷执行的未完成读取和写入操作的数量。

- * 平均 IO 大小 *

  过去 500 毫秒内卷的最近 I/O 的平均大小（以字节为单位）。

iSCSI 会话

查看 iSCSI 会话

您可以查看连接到集群的 iSCSI 会话。您可以对信息进行筛选，使其仅包含所需的会话。

1. 在 Element UI 中，选择 * 报告 * > * iSCSI 会话 * 。
2. 要查看筛选条件字段，请单击 * 筛选器 * 。

了解更多信息

iSCSI 会话详细信息

iSCSI 会话详细信息

您可以查看有关连接到集群的 iSCSI 会话的信息。

以下列表介绍了有关 iSCSI 会话的信息：

- * 节点 *

  托管卷的主元数据分区的节点。

- * 帐户 *

  拥有卷的帐户的名称。如果值为空，则会显示一个短划线（ - ）。

- * 卷 *

  节点上标识的卷名称。

- * 卷 ID*

  与目标 IQN 关联的卷的 ID 。

- * 启动程序 ID*

  系统为启动程序生成的 ID 。

- * 启动程序别名 *

  启动程序的一个可选名称，在长列表中更容易找到启动程序。

- * 启动程序 IP*

  启动会话的端点的 IP 地址。

- * 启动程序 IQN*

  启动会话的端点的 IQN 。

- * 目标 IP*

  托管卷的节点的 IP 地址。

- * 目标 IQN*

  卷的 IQN 。

- **CHAP**

  iSCSI会话的CHAP算法。如果未使用CHAP算法，则会显示一个短划线(-)。从Element 12.8开始提供。

- * 创建于 *

  建立会话的日期。

光纤通道会议

查看光纤通道会话

您可以查看连接到集群的光纤通道（ FC ）会话。您可以对信息进行筛选，以便仅包括要在窗口中显示的连接。

1. 在 Element UI 中，选择 * 报告 * > * FC 会话 * 。
2. 要查看筛选条件字段，请单击 * 筛选器 * 。

了解更多信息

光纤通道会话详细信息

光纤通道会话详细信息

您可以找到有关连接到集群的活动光纤通道（ FC ）会话的信息。

以下列表介绍了有关连接到集群的 FC 会话的信息：

- * 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。

- * 启动程序 ID*

  系统为启动程序生成的 ID 。

- * 启动程序 WWPN *

  发起全球通用端口名称。

- * 启动程序别名 *

  启动程序的一个可选名称，在长列表中更容易找到启动程序。

- * 目标 WWPN *

  目标全球通用端口名称。

- * 卷访问组 *

  会话所属的卷访问组的名称。

- * 卷访问组 ID*

  系统为访问组生成的 ID 。

对驱动器进行故障排除

对驱动器进行故障排除

您可以将发生故障的固态驱动器（ SSD ）更换为替代驱动器。SolidFire 存储节点的 SSD 可热插拔。如果您怀疑 SSD 发生故障，请联系 NetApp 支持部门验证故障并指导您完成正确的解决方法操作步骤。NetApp 支持部门还会与您合作，根据您的服务级别协议获取一个替代驱动器。

在这种情况下，如何插拔意味着您可以从活动节点中删除故障驱动器，并将其更换为 NetApp 提供的新 SSD 驱动器。建议不要删除活动集群上的无故障驱动器。

您应维护 NetApp 支持部门建议的现场备件，以便在驱动器出现故障时可以立即更换。

出于测试目的，如果要通过从节点中拉出驱动器来模拟驱动器故障，则必须等待 30 秒，然后才能将驱动器重新插入驱动器插槽。

如果某个驱动器发生故障，双 Helix 会在集群中的其余节点之间重新分布该驱动器上的数据。同一节点上的多个驱动器故障不是问题描述，因为 Element 软件可防止同一节点上存在两个数据副本。发生故障的驱动器会导致以下事件：

- 数据将从驱动器中迁移。
- 整体集群容量会通过驱动器容量减少。
- 双 Helix 数据保护可确保有两个有效的数据副本。

如果删除驱动器会导致存储空间不足，无法迁移数据，则 SolidFire 存储系统不支持删除该驱动器。

有关详细信息 ...

- 从集群中删除故障驱动器
- 基本 MDSS 驱动器故障排除
- 删除 MDSS 驱动器
- "更换 SolidFire 存储节点的驱动器"
- "更换 H600S 系列存储节点的驱动器"
- "H410S 和 H610S 硬件信息"
- "SF 系列硬件信息"

从集群中删除故障驱动器

如果驱动器的自我诊断功能告诉节点驱动器发生故障，或者与驱动器的通信停止五分半或更长时间，则 SolidFire 系统会将驱动器置于故障状态。系统将显示故障驱动器的列表。您必须从 NetApp Element 软件的故障驱动器列表中删除故障驱动器。

当节点脱机时， * 警报 * 列表中的驱动器显示为 * 块服务运行状况不正常 * 。重新启动节点时，如果节点及其驱动器在五到半分钟内恢复联机，则这些驱动器会自动更新并继续作为集群中的活动驱动器运行。

1. 在 Element UI 中，选择 * 集群 * > * 驱动器 * 。
2. 单击 * 失败 * 以查看故障驱动器的列表。
3. 记下故障驱动器的插槽编号。

   要在机箱中找到故障驱动器，您需要此信息。

4. 使用以下方法之一删除故障驱动器：

选项	步骤
删除单个驱动器	a. 单击要删除的驱动器的 * 操作 * 。 b. 单击 * 删除 * 。
删除多个驱动器	a. 选择要删除的所有驱动器，然后单击 * 批量操作 * 。 b. 单击 * 删除 * 。

基本 **MDSS** 驱动器故障排除

如果一个或两个元数据驱动器发生故障，您可以通过将元数据（或分区）驱动器重新添加到集群来恢复这些驱动器。如果已在节点上启用 NetApp Element 功能，则可以在 MDSS UI 中执行恢复操作。

如果节点中的一个或两个元数据驱动器发生故障，分区服务将关闭，并且两个驱动器中的数据将备份到节点中的不同驱动器。

以下场景概述了可能的故障情形，并提供了更正问题描述的基本建议：

系统分区驱动器出现故障

- 在这种情况下，插槽 2 会经过验证并恢复为可用状态。
- 必须重新填充系统分区驱动器，才能使分区服务恢复联机。
- 您应更换系统分区驱动器，当系统分区驱动器可用时，请同时添加该驱动器和插槽 2 驱动器。

> 您不能将插槽 2 中的驱动器本身添加为元数据驱动器。您必须同时将这两个驱动器重新添加到节点。

插槽 **2** 发生故障

- 在这种情况下，系统分区驱动器会经过验证并返回到可用状态。
- 您应将插槽 2 更换为备用驱动器，当插槽 2 可用时，请同时添加系统分区驱动器和插槽 2 驱动器。

系统分区驱动器和插槽 **2** 发生故障

- 您应将系统分区驱动器和插槽 2 更换为备用驱动器。当这两个驱动器都可用时，请同时添加系统分区驱动器和插槽 2 驱动器。

操作顺序

- 将故障硬件驱动器更换为备用驱动器（如果两个驱动器都发生故障，请同时更换这两个驱动器）。
- 重新填充驱动器并使其处于可用状态后，请将其重新添加到集群中。

验证操作

- 验证插槽 0 （或内部）和插槽 2 中的驱动器是否已在 "Active Drives" 列表中标识为元数据驱动器。
- 验证所有分区平衡是否已完成（至少 30 分钟内，事件日志中不会再显示移动分区消息）。

有关详细信息 ...

添加 MDSS 驱动器

添加 **MDSS** 驱动器

通过将插槽 2 中的块驱动器转换为分区驱动器，您可以在 SolidFire 节点上添加第二个元数据驱动器。这是通过启用多驱动器分区服务（ MDSS ）功能来实现的。要启用此功能，您必须联系 NetApp 支持部门。

要使分区驱动器变为可用状态，可能需要将故障驱动器更换为新驱动器或备用驱动器。您必须在为插槽 2 添加驱动器的同时添加系统分区驱动器。如果您尝试单独添加插槽 2 分区驱动器或在添加系统分区驱动器之前添加该驱动器，则系统将生成错误。

1. 单击 * 集群 * > * 驱动器 * 。
2. 单击 * 可用 * 以查看可用驱动器列表。
3. 选择要添加的分区驱动器。
4. 单击 * 批量操作 * 。
5. 单击 * 添加 * 。
6. 从 * 活动驱动器 * 选项卡中确认已添加这些驱动器。

删除 **MDSS** 驱动器

您可以删除多驱动器分区服务（ MDSS ）驱动器。只有当节点具有多个分区驱动器时，此操作步骤才适用。

如果系统分区驱动器和插槽 2 驱动器发生故障，系统将关闭分区服务并删除这些驱动器。如果未发生故障，并且您删除了这些驱动器，则必须同时删除这两个驱动器。

1. 单击 * 集群 * > * 驱动器 * 。
2. 在 * 可用 * 驱动器选项卡中，单击要删除的分区驱动器对应的复选框。
3. 单击 * 批量操作 * 。
4. 单击 * 删除 * 。
5. 确认操作。

对节点进行故障排除

从集群中移除节点

您可以从集群中删除节点以进行维护或更换。您应先使用 NetApp Element UI 或 API 删除

节点，然后再使其脱机。

要删除存储节点的操作步骤概述如下：

- 确保集群中有足够的容量来为节点上的数据创建副本。
- 使用 UI 或 RemoveDrives API 方法从集群中删除驱动器。

  这会导致系统将数据从节点的驱动器迁移到集群中的其他驱动器。此过程所需时间取决于必须迁移的数据量。

- 从集群中删除节点。

在关闭或启动节点之前，请牢记以下注意事项：

- 如果未正确关闭节点和集群，则会面临风险。

  关闭节点应在 NetApp 支持部门的指导下完成。

- 如果某个节点在任何类型的关闭条件下关闭时间超过 5.5 分钟，则双 Helix 数据保护将开始将单个复制块写入另一个节点以复制数据的任务。在这种情况下，请联系 NetApp 支持部门以帮助分析故障节点。
- 要安全地重新启动或关闭节点，您可以使用 Shutdown API 命令。
- 如果节点处于关闭或关闭状态，则必须先联系 NetApp 支持部门，然后再将其恢复联机。
- 节点恢复联机后，您必须根据其停止服务的时间将驱动器重新添加到集群中。

有关详细信息 ...

"更换发生故障的 SolidFire 机箱"

"更换发生故障的 H600S 系列节点"

关闭集群

执行以下操作步骤 以关闭整个集群。

步骤

1. (可选)请联系NetApp支持部门以协助完成准备步骤。
2. 验证所有I/O是否均已停止。
3. 断开所有iSCSI会话的连接：
   a. 导航到集群上的管理虚拟 IP （ MVIP ）地址以打开 Element UI 。
   b. 记下节点列表中列出的节点。
   c. 使用集群中每个节点 ID 上指定的 halt 选项运行 Shutdown API 方法。

重新启动集群时、必须按照特定步骤验证所有节点是否均已联机：

1. 验证所有严重严重性和 `volumesOffline` 集群故障已解决。
2. 等待10到15分钟、以使集群建立连接。
3. 启动主机以访问数据。

如果要在打开节点电源并在维护后验证其运行状况是否良好时留出更多时间、请联系技术支持以帮助延迟数据同步以防止不必要的箱同步。

了解更多信息

"如何正常关闭和启动NetApp Solidfire/HCI存储集群"

使用存储节点的每节点实用程序

使用存储节点的每节点实用程序

如果 NetApp Element 软件 UI 中的标准监控工具无法为您提供足够的故障排除信息，您可以使用每节点实用程序对网络问题进行故障排除。每节点实用程序提供了特定的信息和工具，可帮助您解决节点之间或管理节点的网络问题。

了解更多信息

- 使用每节点 UI 访问每个节点的设置
- 每个节点 UI 中的网络设置详细信息
- 每个节点 UI 中的集群设置详细信息
- 使用每节点 UI 运行系统测试
- 使用每节点 UI 运行系统实用程序

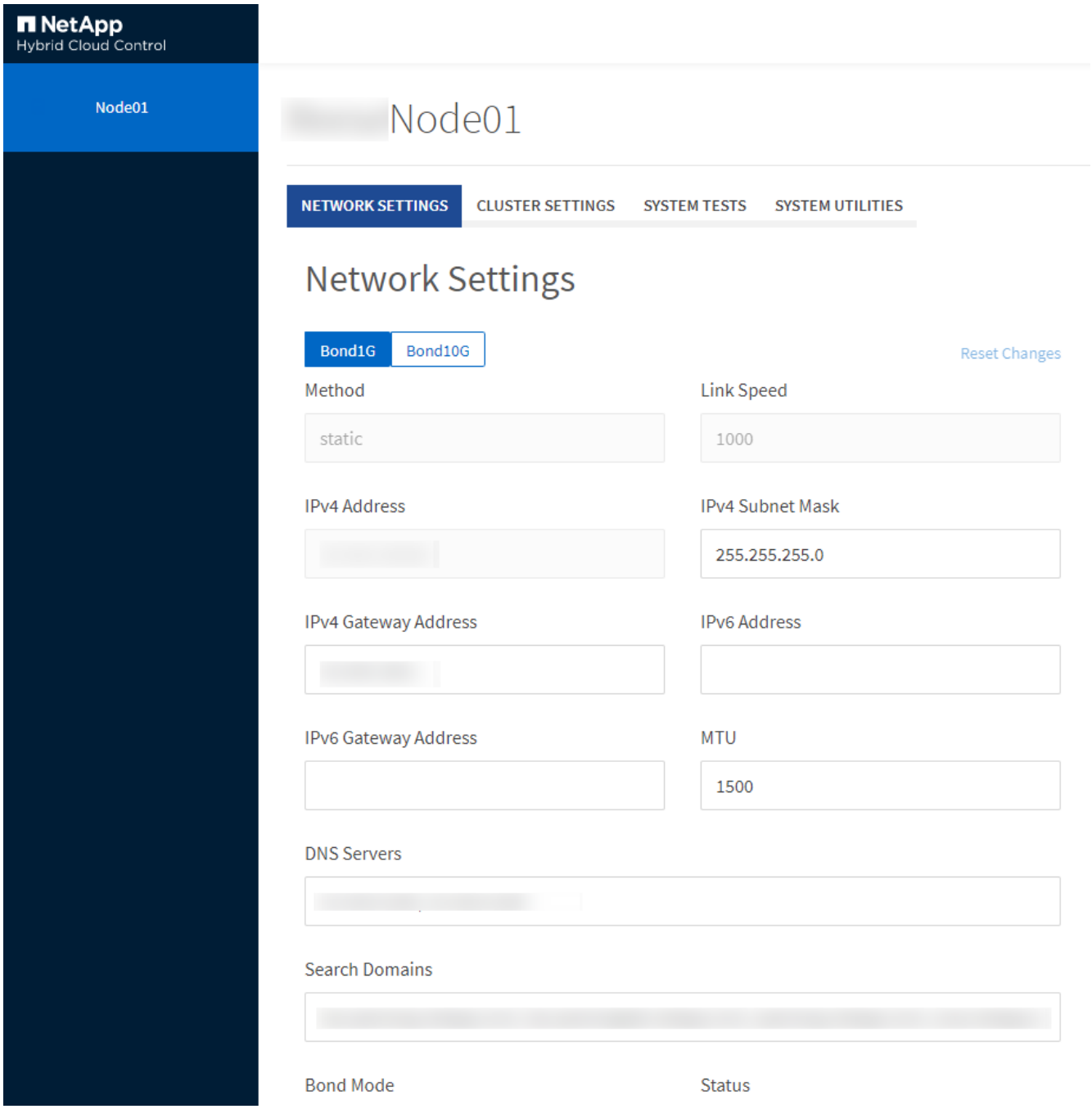
使用每节点 **UI** 访问每个节点的设置

输入管理节点 IP 并进行身份验证后，您可以在每节点用户界面中访问网络设置，集群设置以及系统测试和实用程序。

如果要修改集群中处于活动状态的节点的设置，必须以集群管理员用户身份登录。

您应一次配置或修改一个节点。在修改其他节点之前，应确保指定的网络设置具有预期效果，并且网络稳定且性能良好。

1. 使用以下方法之一打开每节点 UI：
   - 在浏览器窗口中输入管理 IP 地址并后跟： 442 ，然后使用管理员用户名和密码登录。
   - 在 Element UI 中，选择 * 集群 * > * 节点 * ，然后单击要配置或修改的节点的管理 IP 地址链接。在打开的浏览器窗口中，您可以编辑节点的设置。



每个节点 UI 中的网络设置详细信息

您可以更改存储节点网络设置，为节点提供一组新的网络属性。

登录到存储节点后，您可以在"网络设置"页面上查看该节点的网络设置。（`https://<node_IP>:442/hcc/node/network-settings`）。您可以选择 **Bond1G**（管理）或 **Bond10G**（存储）设置。以下列表描述了存储节点处于可用、待处理或活动状态时可以修改的设置：

- * 方法 *

  用于配置接口的方法。可能的方法：

  - loopback ： 用于定义 IPv4 环回接口。

- manual： 用于定义默认情况下不会对其进行配置的接口。
- dhcp： 用于通过 DHCP 获取 IP 地址。
- static： 用于使用静态分配的 IPv4 地址定义以太网接口。

- * 链路速度 *

  虚拟 NIC 协商的速度。

- * IPv4 地址 *

  eth0 网络的 IPv4 地址。

- * IPv4 子网掩码 *

  IPv4 网络的细分地址。

- * IPv4 网关地址 *

  用于从本地网络发送数据包的路由器网络地址。

- * IPv6 地址 *

  eth0 网络的 IPv6 地址。

- * IPv6 网关地址 *

  用于从本地网络发送数据包的路由器网络地址。

- * MTU *

  网络协议可以传输的最大数据包大小。必须大于或等于 1500 。如果添加第二个存储 NIC ，则此值应为 9000 。

- * DNS 服务器 *

  用于集群通信的网络接口。

- * 搜索域 *

  搜索系统可用的其他 MAC 地址。

- * 绑定模式 *

  可以是以下模式之一：

  - ActivePassive （默认）
  - ALB
  - LACP

- * 状态 *

  可能值：

- 正常运行
- 已关闭
- 已启动

- * 虚拟网络标记 *

  创建虚拟网络时分配的标记。

- * 路由 *

  通过路由所配置的关联接口连接到特定主机或网络的静态路由。

每个节点 **UI** 中的集群设置详细信息

您可以在配置集群后验证存储节点的集群设置，并修改节点主机名。

以下列表描述了从每个节点的 UI 的“集群设置”页面中指定的存储节点的集群设置。(`https://<node_IP>:442/hcc/node/cluster-settings`）。

- * 角色 *

  节点在集群中的角色。可能值：

  - 存储：存储或光纤通道节点。
  - Management： 节点是一个管理节点。

- * 主机名 *

  节点的名称。

- * 集群 *

  集群的名称。

- * 集群成员资格 *

  节点的状态。可能值：

  - Available： 节点没有关联的集群名称，并且尚未加入集群。
  - Pending： 节点已配置，可添加到指定集群。访问节点不需要身份验证。
  - PendingActive： 系统正在节点上安装兼容软件。完成后，节点将变为 "Active" 状态。
  - Active： 节点正在加入集群。要修改节点，需要进行身份验证。

- * 版本 *

  节点上运行的 Element 软件版本。

- * 整体 *

  属于数据库集合的节点。

- * 节点 ID*

  将节点添加到集群时分配的 ID 。

- * 集群接口 *

  用于集群通信的网络接口。

- * 管理接口 *

  管理网络接口。默认为绑定 1G ，但也可以使用绑定 10G 。

- * 存储接口 *

  使用绑定 10G 的存储网络接口。

- * 支持加密 *

  指示节点是否支持驱动器加密。

使用每节点 **UI** 运行系统测试

在将网络设置提交到网络配置后，您可以测试对这些设置所做的更改。您可以运行测试以确保存储节点稳定，并且可以使其联机而不出现任何问题。

您已登录到存储节点的每节点 UI 。

1. 单击 * 系统测试 * 。
2. 单击要运行的测试旁边的 * 运行测试 * ，或者选择 * 运行所有测试 * 。

   运行所有测试操作可能非常耗时，只能在 NetApp 支持部门的指示下执行。

   - * 测试连接的 Ensemble*

     测试并验证与数据库集合的连接。默认情况下，此测试将对与此节点关联的集群使用集合。或者，您也可以提供其他集合来测试连接。

   - * 测试连接 Mvip*

     对指定的管理虚拟 IP （ MVIP ）地址执行 Ping 操作，然后对 MVIP 执行简单的 API 调用以验证连接。默认情况下，此测试会对与此节点关联的集群使用 MVIP 。

   - * 测试连接 Svip*

     使用与网络适配器上设置的最大传输单元（ Maximum Transmission Unit ， MTU ）大小匹配的 Internet 控制消息协议（ Internet Control Message Protocol ， ICMP ）数据包对指定的存储虚拟 IP （ Storage Virtual IP ， SVIP ）地址执行 Ping 操作。然后，它会作为 iSCSI 启动程序连接到 SVIP 。默认情况下，此测试会对与此节点关联的集群使用 SVIP 。

   - * 测试硬件配置 *

测试所有硬件配置是否正确，验证固件版本是否正确，并确认所有驱动器均已安装并正常运行。这与出厂测试相同。

此测试需要大量资源，只有在 NetApp 支持部门要求时才应运行。

- * 测试本地连接 *

  通过对每个节点上的集群 IP （ CIP ）执行 Ping 操作，测试与集群中所有其他节点的连接。只有当节点属于活动集群时，此测试才会显示在节点上。

- * 测试定位集群 *

  验证节点是否可以找到在集群配置中指定的集群。

- * 测试网络配置 *

  验证已配置的网络设置是否与系统上正在使用的网络设置匹配。此测试不用于检测节点主动加入集群时的硬件故障。

- * 测试 Ping*

  对指定的主机列表执行 Ping 操作，或者如果未指定任何主机，则动态构建集群中所有已注册节点的列表，并对每个节点执行 Ping 操作以实现简单连接。

- * 测试远程连接 *

  通过对每个节点上的集群 IP （ CIP ）执行 Ping 操作，测试与远程配对集群中所有节点的连接。只有当节点属于活动集群时，此测试才会显示在节点上。

使用每节点 **UI** 运行系统实用程序

您可以使用存储节点的每节点 UI 创建或删除支持包，重置驱动器的配置设置以及重新启动网络或集群服务。

您已登录到存储节点的每节点 UI 。

1. 单击 * 系统实用程序 * 。
2. 单击要运行的系统实用程序对应的按钮。
   - * 控制电源 *

     重新启动，重新启动或关闭节点。

     此操作会导致网络连接暂时断开。

     指定以下参数：

     - 操作：选项包括重新启动和暂停（关闭）。
     - 唤醒延迟：节点恢复联机之前的任何其他时间。
   - * 收集节点日志 *

在节点的 /tmp/bundles 目录下创建支持包。

指定以下参数：

- Bundle Name ： 创建的每个支持包的唯一名称。如果未提供名称，则使用 "supportbundle" 和节点名称作为文件名。
- 额外的 args ： 此参数将馈送到 sf_make_support_bundle 脚本。只有在 NetApp 支持部门要求时，才应使用此参数。
- Timeout Sec ： 指定等待每个 ping 响应的秒数。

◦ * 删除节点日志 *

删除节点上使用 * 创建集群支持包 * 或 CreateSupportBundle API 方法创建的任何当前支持包。

◦ * 重置驱动器 *

初始化驱动器并删除当前驻留在驱动器上的所有数据。您可以在现有节点或升级后的节点中重复使用此驱动器。

指定以下参数：

- Drives ： 要重置的设备名称（非驱动器 ID ）的列表。

◦ * 重置网络配置 *

帮助解决单个节点的网络配置问题，并将单个节点的网络配置重置为出厂默认设置。

◦ * 重置节点 *

将节点重置为出厂设置。此操作会删除所有数据，但会保留节点的网络设置。只有当节点未分配到集群且处于可用状态时，才能重置节点。

使用此选项时，所有数据，软件包（软件升级），配置和日志文件都会从节点中删除。

◦ * 重新启动网络连接 *

重新启动节点上的所有网络服务。

此操作可能发生原因会导致网络连接暂时断开。

◦ * 重新启动服务 *

重新启动节点上的 Element 软件服务。

此操作可能发生原因会导致节点服务临时中断。您只能在 NetApp 支持部门的指示下执行此操作。

指定以下参数：

- service ： 要重新启动的服务名称。

- 操作：要对服务执行的操作。选项包括启动，停止和重新启动。

使用管理节点

您可以使用管理节点（ mNode ）升级系统服务，管理集群资产和设置，运行系统测试和实用程序，配置 Active IQ 以进行系统监控以及启用 NetApp 支持访问以进行故障排除。

最佳实践是，仅将一个管理节点与一个 VMware vCenter 实例相关联，并避免在多个管理节点中定义相同的存储和计算资源或 vCenter 实例。

请参见 "管理节点文档" 有关详细信息 …

了解集群填充度级别

运行 Element 软件的集群会生成集群故障，以便在集群容量即将用尽时向存储管理员发出警告。集群填充度分为三个级别，所有这些级别均显示在 NetApp Element UI 中：警告，错误和严重。

系统使用 BlockClusterFull 错误代码警告集群块存储填充度。您可以从 Element UI 的 Alerts 选项卡查看集群填充度严重性级别。

以下列表包含有关 BlockClusterFull 严重性级别的信息：

- * 警告 *

  此警告可由客户配置，在集群的块容量接近错误严重性级别时显示。默认情况下，此级别设置为比错误级别低 3% ，可通过 Element UI 和 API 进行调整。您必须尽快添加更多容量或释放容量。

- * 错误 *

  当集群处于此状态时，如果节点丢失，集群中的容量将不足以重建双 Helix 数据保护。当集群处于此状态时，所有新卷创建，克隆和快照都会被阻止。对于任何集群而言，此状态都不是安全状态，也不是建议的状态。您必须立即添加更多容量或释放容量。

- * 严重 *

  之所以出现此严重错误，是因为集群已被占用 100% 。它处于只读状态，无法与集群建立新的 iSCSI 连接。达到此阶段后，您必须立即释放或添加更多容量。

系统使用 MetadataClusterFull 错误代码发出有关集群元数据存储填充度的警告。您可以从 Element UI 中 "Reporting" 选项卡的 "Overview" 页面上的 "Cluster Capacity" 部分查看集群元数据存储填充度。

以下列表包含有关 MetadataClusterFull 严重性级别的信息：

- * 警告 *

  此警告可由客户配置，在集群的元数据容量接近错误严重性级别时显示。默认情况下，此级别设置为比错误级别低 3% ，可通过 Element API 进行调整。您必须尽快添加更多容量或释放容量。

- * 错误 *

当集群处于此状态时，如果节点丢失，集群中的容量将不足以重建双 Helix 数据保护。当集群处于此状态时，所有新卷创建，克隆和快照都会被阻止。对于任何集群而言，此状态都不是安全状态，也不是建议的状态。您必须立即添加更多容量或释放容量。

- * 严重 *

  之所以出现此严重错误，是因为集群已被占用 100% 。它处于只读状态，无法与集群建立新的 iSCSI 连接。达到此阶段后，您必须立即释放或添加更多容量。

以下适用场景双节点集群阈值：

- 元数据填充度错误比严重程度低 20% 。
- 块填充度错误为 1 个块驱动器（包括孤立容量）低于严重值；这意味着它是两个块驱动器，其容量低于严重值。